UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO CHUNCHI, DEL CANTÓN CHUNCHI, BAJO LA NORMA ISO 27001

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

AUTOR: CARLOS REINALDO DÍAZ USHO

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 DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA CHUNCHI, DEL CANTÓN CHUNCHI, BAJO LA NORMA ISO 27001

PPROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: CARLOS REINALDO DÍAZ USHO

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Carlos Reinaldo Díaz Usho portador de la cédula de ciudadanía Nº 0605716059 Declaro ser el autor de la obra: **"Propuesta de manual de políticas de seguridad de la información para la Cooperativa de Chunchi, del cantón Chunchi, bajo la norma ISO 27001"** sobre la cual me hago responsable sobre 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.

Carlos Diaz Reinaldo Díaz Usho

C.I. **030605716059**

CERTIFICACIÓN DEL TUTOR

El presente trabajo de titulación denominado **"Propuesta de manual de políticas de seguridad de la información para la Cooperativa de ahorro y crédito Chunchi, del cantón Chunchi, bajo la norma ISO 27001",** elaborado por **Carlos Reinaldo Diaz Usho**, previo a la obtención del título de Ingeniero de Sistemas 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,27 de noviembre de 2024

Ing. Cristian Flores Urgiles
Tutora del trabajo investigativo

DEDICATORIA

A Dios, por ser mi guía, mi fortaleza y mi mayor inspiración. Gracias por darme la sabiduría, el valor y la perseverancia para superar cada desafío en este camino. A Él le debe todo lo que soy y lo que he logrado.

A mi madre, María Usho, por su amor incondicional, sus sacrificios y su apoyo constante. Eres mi mayor ejemplo de esfuerzo, dedicación y valentía.

A mi hermano, Luis Díaz, por su compañerismo, palabras de aliento y por estar siempre presente en los momentos más importantes de mi vida.

A mis queridas hermanas**,** Isabel Díaz, Mabel Zuña y Tatiana Zuña**,**
por su cariño y apoyo incondicional, por ser una fuente de inspiración y motivación en mi vida.

Esta tesis es para ustedes, quienes han sido mi sustento espiritual, emocional y familiar.

AGRADECIMIENTO

En primer lugar, deseo expresar mi más sincero agradecimiento a los docentes de la Universidad Católica de Cuenca Extensión Cañar, quienes, con su dedicación y esfuerzo, han sido fundamentales en mi formación académica. Su compromiso con la enseñanza y su constante apoyo me han permitido crecer no solo como profesional, sino también como persona.

Quiero extender un reconocimiento especial al Ing. Cristhian Flores, director de esta tesis, por su inquebrantable guía, paciencia y consejos a lo largo de todo el proceso. Su experiencia y orientación fueron esenciales para la culminación exitosa de este trabajo. Agradezco profundamente el tiempo que dedicó a resolver mis inquietudes y por su disposición para compartir sus conocimientos, los cuales fueron clave para alcanzar los objetivos propuestos.

Finalmente, a todos aquellos que, de una manera u otra, contribuyeron a mi desarrollo durante esta etapa de mi vida académica, les extiendo mi más sincero agradecimiento.

RESUMEN

Esta tesis presenta el desarrollo de un Manual de Política de Seguridad de la Información para la Cooperativa de Ahorro y Crédito Chunchi, basado en la norma ISO/IEC 27001:2013. El proyecto tiene como objetivo abordar la falta de políticas de seguridad formalizadas, lo que plantea riesgos significativos para la información sensible de la cooperativa. Al evaluar el estado actual de la seguridad de la información de la cooperativa a través de encuestas y análisis de riesgos, este estudio identifica vulnerabilidades y brechas críticas. Utilizando la metodología MAGERIT, se analizaron activos, amenazas y vulnerabilidades para desarrollar políticas personalizadas que garanticen la confidencialidad, integridad y disponibilidad de la información. El manual propuesto se alinea con las normas ISO 27001, centrándose en fortalecer las prácticas de seguridad, mejorar el cumplimiento normativo y fomentar una cultura organizacional orientada a la seguridad. Este trabajo contribuye a salvaguardar los datos sensibles y mejorar la resiliencia operativa y la reputación de la cooperativa.

Palabras clave: seguridad de la información, ISO 27001, manual de política de seguridad,

ABSTRACT

This thesis presents the development of an Information Security Policy Manual for the Chunchi Savings and Credit Cooperative based on the ISO/IEC 27001:2013 standard. The project aims to address the lack of formalized security policies, which presents significant risks to the cooperative's sensitive information. This study identifies critical vulnerabilities and gaps by evaluating the current state of the cooperative's information security through surveys and risk analysis. Using the MAGERIT methodology, assets, threats, and vulnerabilities were analyzed to develop customized policies that ensure the information confidentiality, integrity, and availability. The proposed manual aligns with ISO 27001 standards, focusing on strengthening security practices, improving regulatory compliance, and fostering a security-oriented organizational culture. This work contributes to safeguarding sensitive data and improving the operational resilience and reputation of the cooperative.

Keywords: information security, ISO 27001, security policy manual.

.

ÍNDICE

Tabla de ilustraciones

Tabla de Gráficos

Tabla de Tablas

INTRODUCCIÓN

Hoy en día, la tecnología ha transformado radicalmente el mundo, convirtiéndose en una necesidad imperante para la sociedad. La información, los sistemas y las redes se han vuelto activos vitales para las entidades, lo que demanda una protección eficaz frente a las amenazas que puedan comprometer su disponibilidad, integridad y confidencialidad.

Las organizaciones enfrentan constantes amenazas que ponen en riesgo sus activos, lo que puede resultar en pérdidas significativas. Las vulnerabilidades en los sistemas de información representan un peligro latente, por lo que es crucial que tanto las empresas como los individuos comprendan conceptos que les permitan defenderse de posibles ataques a su información. Entre las amenazas potenciales a las que se enfrentan las redes corporativas se encuentran los virus, troyanos, vándalos, entre otros, lo que hace imprescindible que las empresas estén protegidas tanto interna como externamente.

En este contexto, esta investigación se centra en la formulación de políticas que contribuyan a prevenir tales ataques en los sistemas de información del GADIC Cañar, tomando como referencia el estándar ISO/IEC 27000. Esta norma abarca un conjunto de estándares relacionados con la seguridad de la información, siendo la ISO/IEC 27001 la seleccionada para este proyecto, debido a que, al ser un Sistema de Gestión de la Seguridad de la Información, permite a las organizaciones evaluar riesgos e implementar los controles necesarios para mitigar o eliminar dichos riesgos.

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

Capítulo 1: Marco referencial, donde se plantea y formula el problema, se presenta una investigación breve sobre los antecedentes, la justificación de la investigación, el objetivo general y los específicos, así como las limitaciones y delimitaciones.

Capítulo 2: Marco teórico, donde se recopila información sobre normas o estándares de seguridad, metodologías para análisis de riesgo, tipos de ataques a sistemas de información, entre otros aspectos relevantes.

Capítulo 3: Detalle del enfoque y tipo de investigación, la población objetivo, el levantamiento de información y la selección de una metodología para el análisis de riesgo.

Capítulo 4: Desarrollo de la propuesta de políticas de prevención de ataques a los sistemas de información, basadas en la norma ISO 27001 y la guía de buenas prácticas ISO 27002, así como un análisis de riesgo utilizando la metodología seleccionada.

CAPITULO I

MARCO REFERENCIAL

1.1 Planteamiento del Problema

El manejo adecuado de la información dentro de las organizaciones es un elemento crucial para garantizar la seguridad y la integridad de los datos sensibles. En el caso de la Cooperativa de Ahorro y Crédito Chunchi, ubicada en el Cantón Chunchi, la ausencia de un manual formalizado de políticas de seguridad de la información puede exponer a la entidad a riesgos significativos, como fugas de información, pérdida de datos y ataques cibernéticos. Esto no solo afecta la operatividad diaria, sino que también puede tener repercusiones legales y en la reputación de la cooperativa ante sus socios y clientes.

Considerando que la Cooperativa de Ahorro y Crédito Chunchi maneja información sensible, tanto financiera como personal de sus miembros, la implementación de un manual de políticas de seguridad que cumpla con la norma ISO 27001 se vuelve indispensable. Esta norma internacional proporciona un marco de referencia que ayuda a proteger la información de manera efectiva, asegurando la confidencialidad, integridad y disponibilidad de los datos. La carencia de dicho manual no solo limita la capacidad de respuesta ante incidentes de seguridad, sino que también impide la adopción de una cultura organizacional que priorice la seguridad de la información. A través de este estudio, se busca abordar esta carencia identificando los requerimientos específicos y creando un conjunto de políticas adecuadas que sean prácticas, aplicables y alineadas con las mejores prácticas internacionales.

1.2 Formulación del Problema

- ¿Cuáles son los fundamentos teóricos relacionados con las políticas de seguridad de la información y la norma ISO 27001 que servirán como base para el desarrollo del manual

de políticas de seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi?

- ¿Cuál es la situación actual de la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi, según los estándares de la norma ISO/IEC 27001:2013 y la guía de buenas prácticas ISO 27002?
- ¿Cuáles son los riesgos identificados en la Cooperativa de Ahorro y Crédito Chunchi, incluyendo activos, amenazas y vulnerabilidades, utilizando una metodología de análisis de riesgos adecuada?
- ¿Cómo se pueden desarrollar políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Chunchi que estén alineadas con los procesos internos, lineamientos y requerimientos específicos de la cooperativa, basándose en los estándares y directrices de la norma ISO 27001?

1.3 Antecedentes de la Investigación

Desde el surgimiento del internet, los ataques informáticos han representado un riesgo creciente para la seguridad de la información en las organizaciones; en respuesta a esta amenaza, diversos autores han llevado a cabo investigaciones con el objetivo de proporcionar soluciones efectivas. Estos estudios han generado una guía de las mejores prácticas en seguridad informática, destacando hallazgos relevantes que han contribuido a fortalecer la protección de la información en instituciones. A continuación, se menciona:

Un estudio similar realizado en la Universidad Internacional SEK de la facultad de Arquitectura e ingenierías por Julio Pilla que se titula “DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC 27002:2013”, en la cual proporciona una descripción

general completa del proceso de desarrollo de políticas de seguridad de la información. El autor ha identificado claramente los objetivos de la política, el ámbito de aplicación y los controles ISO/IEC 27002:2013 aplicables. El documento también incluye un plan de implementación detallado y una matriz de evaluación de riesgos. (Pilla Yanzapanta, 2019)

Esta investigación será de gran ayuda para la realización en profundizar las bases teóricas y obtener un conocimiento más claro acerca de los controles y dominios que presenta la norma ISO 27002.

Así mismo Cristian Puga llevo a cabo una investigación con título "DISEÑO DE UNA POLITICA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE IMAGENOLOGÍA DEL HOSPITAL GENERAL DOCENTE DE CALDERÓN UTILIZANDO LOS ESTANDARES ISO 27001 E ISO 27799", en donde utiliza las normas de la ISO antes mencionada proporcionando directrices específicas para la protección de la información médica y la salud en el área de imagenología, con el objetivo es generar un documento que establezca buenas prácticas en seguridad de la información, el cual deberá ser aprobado por la gerencia del hospital para convertirse en una herramienta de control en el manejo de la información dentro del área de imagenología. (Puga Jacome , 2019)

Este estudio servirá como una guía para implementar las políticas de seguridad de la información basada en normas como ISO y el cumplimiento de regulaciones este documento valida la eficacia y la pertinencia de tu enfoque metodológico.

Otro estudio realizado por Madheline Torres de la Universidad Tecnológica Empresarial de Guayaquil titulada "MODELO DE GESTIÓN DE RIESGOS DE PROCESOS DE TECNOLOGÍA DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27000 EN EMPRESAS AÉREAS DEL ECUADOR" , en esta investigación evidencia que ciertas empresas del Ecuador enfrentan deficiencias en la seguridad de la información, lo que provoca

pérdida de datos, con esto Se propone implementar un modelo de gestión de procesos de tecnología de la información basado en la Norma ISO/IEC 27000. Se ha identificado una correlación positiva moderada entre la Gestión de Riesgos de Información y la Seguridad en las Tecnologías. Esto respalda la estructuración de la propuesta utilizando las Normas ISO 27001 y 27002.

Es esencial establecer políticas de seguridad centradas en riesgos operacionales y de reputación. (Torres Hallo, 2020)

Basándose en este documento, se podrán identificar las vulnerabilidades y los riesgos que puedan afectar a la seguridad de los sistemas, así como determinar los procesos críticos que requieran la implementación de controles para asegurar su funcionamiento seguro dentro de la organización.

1.4 Justificación de la Investigación

La implementación de un manual de políticas de seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi es fundamental debido al creciente número de amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos críticos. La norma ISO 27001 ofrece un marco robusto para la gestión de seguridad de la información, ayudando a las organizaciones a establecer, implementar, operar, monitorear, revisar y mejorar su sistema de gestión de seguridad de la información[1]. Considerando que la Cooperativa de Ahorro y Crédito Chunchi maneja información sensible tanto de sus miembros como de sus operaciones, se hace imperativo contar con políticas claras y efectivas que no solo protejan esta información contra posibles ataques, sino que también promuevan una cultura de seguridad de la información entre los empleados y colaboradores.

[1] SGSI

La creación de este manual no solo ayudará a mitigar los riesgos asociados a la seguridad de la información, sino que también proporcionará a la cooperativa una ventaja competitiva, demostrando su compromiso con la seguridad y la protección de datos, un aspecto cada vez más valorado tanto por clientes como por reguladores. Además, la implementación de este manual permitirá a la Cooperativa de Ahorro y Crédito Chunchi cumplir con las normativas legales y reglamentarias pertinentes, evitando sanciones y otras consecuencias negativas asociadas a la gestión inadecuada de la seguridad de la información. Esta justificación resalta la relevancia de la propuesta, destacando su impacto potencial en la mejora continua y el cumplimiento normativo en la cooperativa.

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Chunchi, utilizando como marco de referencia los estándares establecidos por la norma ISO 27001.

1.5.2 Objetivos Específicos

- Revisar y sintetizar el marco teórico relacionado con las políticas de seguridad de la información y la norma ISO 27001, para establecer una base sólida de conocimientos que guíe el desarrollo del manual de políticas de seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi.
- Realizar el levantamiento de información para determinar el diagnóstico de la situación actual de la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi, utilizando el marco de trabajo de la norma ISO/IEC 27001:2013 y la guía de buenas prácticas ISO 27002:2013.

- Realizar un análisis de riesgo en la Cooperativa de Ahorro y Crédito Chunchi, incluyendo el levantamiento de activos, amenazas a las que están expuestos dichos activos y vulnerabilidades, utilizando una metodología de análisis de riesgos adecuada.
- Desarrollar una propuesta de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Chunchi, que esté alineada con los procesos internos, lineamientos y requerimientos específicos de la cooperativa, basándose en los estándares y directrices de la norma ISO 27001.

1.6 Limitaciones

- La investigación puede enfrentar limitaciones en términos de recursos financieros, humanos y tecnológicos, lo que podría influir en la profundidad y amplitud del análisis realizado.
- La disponibilidad y accesibilidad de datos relevantes sobre la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi pueden ser limitadas debido a restricciones de confidencialidad o a la falta de registros actualizados, lo que podría afectar la exhaustividad del diagnóstico realizado.
- La disponibilidad y accesibilidad de datos relevantes sobre la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi pueden ser limitadas debido a restricciones de confidencialidad o a la falta de registros actualizados, lo que podría afectar la exhaustividad del diagnóstico realizado.

1.7 Delimitaciones

- La investigación se enfocará específicamente en la Cooperativa de Ahorro y Crédito Chunchi del Cantón Chunchi, por lo que los hallazgos y recomendaciones podrían no ser directamente aplicables a otras organizaciones o contextos geográficos.

- La investigación se centrará en el enfoque propuesto y en la metodología seleccionada para el análisis de riesgos y el desarrollo de políticas de seguridad de la información, lo que podría limitar la consideración de otras metodologías o enfoques alternativos.

CAPITULO II

2. MARCO TEÓRICO

2.1 Seguridad de la información

La seguridad de la información se refiere al conjunto de medidas y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas de información dentro de una organización. Esto incluye la identificación de riesgos, la implementación de controles y políticas adecuadas, así como la capacitación del personal para prevenir y mitigar amenazas que puedan comprometer la seguridad de los activos de información. (Villegas Limaico, 2019)

2.1.1 Importancia de la Seguridad de la Información

Radica en su papel fundamental para garantizar la confianza, la integridad y la continuidad operativa de las organizaciones en un entorno digital. Al proteger los datos sensibles y los sistemas de información, se previenen riesgos como el robo de información, la pérdida de la confianza de los clientes, la interrupción de los servicios y el daño a la reputación. Además, la seguridad de la información es crucial para cumplir con las regulaciones legales y mantener la competitividad en un mercado cada vez más dependiente de la tecnología y los datos (Quispe Ayquipa, 2021)

2.1.1.1 Protegiendo la confidencialidad

La confidencialidad se refiere a la protección de la información contra el acceso no autorizado, asegurando que solo las personas autorizadas puedan visualizar o utilizar los datos, lo cual es fundamental para mantener la privacidad y la confianza en la información gestionada por la organización.

2.1.1.2 Asegurando la integridad

La integridad implica mantener la exactitud y la consistencia de los datos a lo largo de su ciclo de vida, evitando modificaciones no autorizadas o alteraciones accidentales, de manera que la información se mantenga confiable y precisa para la toma de decisiones.

2.1.1.3 Garantizando la disponibilidad

La disponibilidad se refiere a la capacidad de acceder y utilizar la información y los sistemas cuando se necesiten, asegurando que los recursos informáticos estén operativos y accesibles para los usuarios autorizados, minimizando tiempos de inactividad y asegurando la continuidad de las operaciones.

2.1.1.4 La autenticidad:

Asegura que se atribuya correctamente la propiedad o creación de los datos. Por ejemplo, si se modifica un correo electrónico para que parezca enviado desde otra dirección, se estaría comprometiendo la autenticidad del mensaje. El uso de firmas digitales es una manera de garantizar esta autenticidad. (Vega Briceño, 2021)

2.1.1.5 El no repudio

Evita que una persona niegue haber realizado una acción, como el envío de un correo electrónico, después de haberla llevado a cabo. Este concepto es crucial para el comercio electrónico y está regulado por leyes que gobiernan las transacciones (Vega Briceño, 2021, pág. 15).

2.2. Norma ISO 27001

Es un estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información [2]. Su objetivo principal es proporcionar un enfoque sistemático y estructurado para identificar, gestionar y reducir los riesgos de seguridad de la información en una organización. La ISO 27001 establece un marco de referencia para implementar controles de seguridad y establecer procesos de mejora continua, lo que ayuda a proteger los activos de información y a mantener la confianza de las partes interesadas. (Maliza Malisa, 2021).

2.2.1 Objetivos y Beneficios

2.2.1.1. Objetivos

- Cumplimiento de los requisitos y contractuales.
- Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.
- Revisiones de seguridad de la información.
- Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales (Ramos Mamam, Cahuaya Ancco, & Llanqui Argollo, 2023).

2.2.1.2. Beneficios de utilizar la norma 27001 en las organizaciones

La norma ISO/IEC 27001 es una norma internacional que proporciona un marco para la gestión de la seguridad de la información. Implementar esta norma en una organización ofrece varios beneficios, incluyendo:

[2] SGSI

1. **Protección de Información Sensible**: Ayuda a proteger información sensible y confidencial de la empresa, incluyendo datos de clientes, empleados, y operaciones internas, reduciendo el riesgo de filtraciones y accesos no autorizados.
2. **Cumplimiento Normativo**: Facilita el cumplimiento de requisitos legales y regulatorios, así como de otros estándares y políticas internas, evitando sanciones y multas.
3. **Mejora de la Confianza**: Incrementa la confianza de clientes, socios y partes interesadas al demostrar un compromiso con la seguridad de la información y la protección de datos.
4. **Reducción de Riesgos**: El proceso de implementación de ISO 27001 incluye la identificación y evaluación de riesgos, así como la implementación de controles para mitigarlos. Esto reduce la probabilidad de incidentes de seguridad y sus posibles impactos negativos.
5. **Eficiencia Operativa**: Promueve la implementación de procesos y controles eficientes que mejoran la gestión de la seguridad de la información y reducen costos relacionados con incidentes de seguridad.
6. **Reputación y Ventaja Competitiva**: Mejora la reputación de la organización y puede proporcionar una ventaja competitiva al diferenciarse de los competidores que no cuentan con la certificación.
7. **Preparación y Resiliencia**: Ayuda a la organización a prepararse mejor y responder eficazmente a incidentes de seguridad, garantizando la continuidad del negocio y minimizando el impacto de las interrupciones.
8. **Reducción de Costos a Largo Plazo**: Aunque la implementación de ISO 27001 puede requerir una inversión inicial significativa, a largo plazo puede resultar en una

reducción de costos. Esto se debe a la disminución de incidentes de seguridad, multas por incumplimiento normativo y pérdidas de reputación.

9. **Mejora Continua:** La norma ISO 27001 promueve la mejora continua en la gestión de la seguridad de la información. Esto se logra mediante la aplicación del ciclo PDCA (Planificar, Hacer, Verificar, Actuar), que permite a las organizaciones identificar áreas de mejora, implementar acciones correctivas y preventivas, y monitorear constantemente el desempeño del sistema de gestión de seguridad de la información (SGSI). (nqa., 2024)

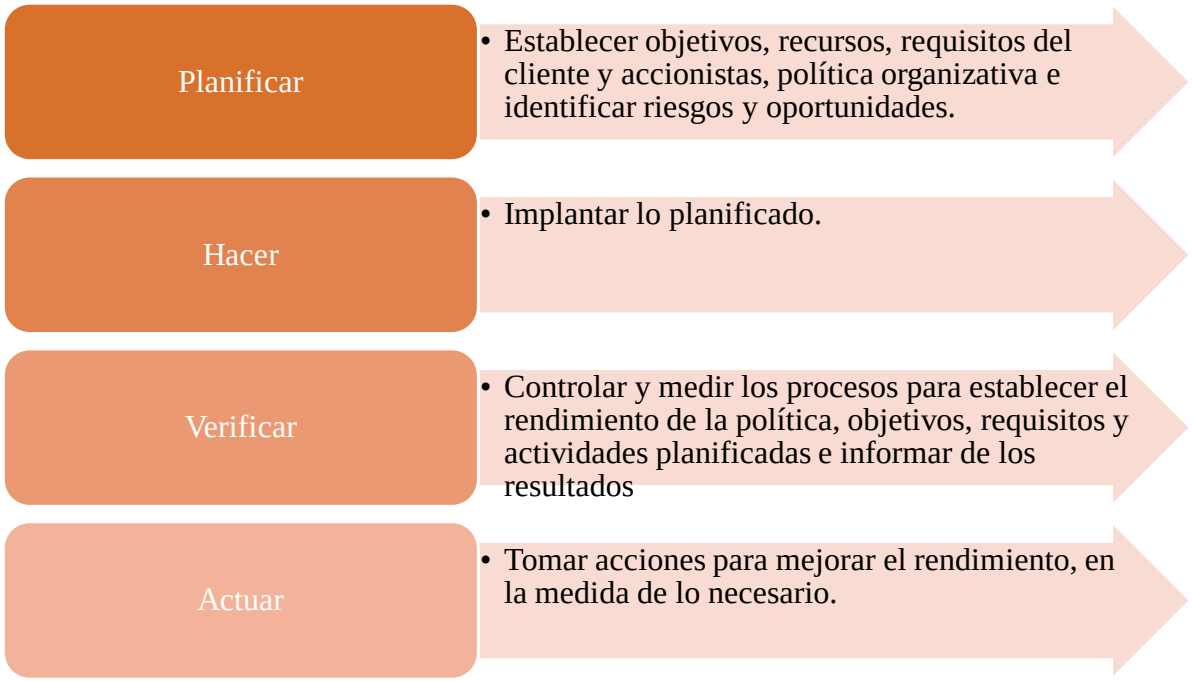

Ilustración 1. Ciclo PHVA. Fuente: (nqa., 2024).

El gráfico muestra el Ciclo PHVA (Planificar, Hacer, Verificar, Actuar), una metodología de mejora continua. Incluye: Planificar objetivos y recursos, Hacer implementando lo planificado, Verificar midiendo resultados y Actuar realizando mejoras según los hallazgos, fomentando así la optimización constante de procesos en las organizaciones.

10. **Alineación con las Mejores Prácticas Internacionales:** ISO 27001 asegura que las organizaciones adopten y mantengan prácticas de seguridad de la información alineadas con estándares reconocidos a nivel internacional. Esto no solo fortalece la seguridad interna de la organización, sino que también facilita la interoperabilidad y la confianza con socios comerciales y clientes que operan según las mismas normativas y principios de seguridad (nqa., 2024).

2.2.2. Principales Componentes de la Norma ISO 27001

Es un estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad

2.2.3. Políticas de Seguridad de la Información

Las Políticas de Seguridad de la Información son documentos que establecen las directrices, principios y procedimientos que una organización debe seguir para proteger sus activos de información contra amenazas y riesgos. Estas políticas definen las responsabilidades, roles y comportamientos esperados de los empleados en relación con la seguridad de la información. Además, proporcionan un marco para la toma de decisiones y la implementación de controles y medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos. (Méndez Gálvez, 2020)

2.2.3.1. Organización de la Seguridad de la Información

Establece una estructura clara con roles y responsabilidades definidos para gestionar la seguridad de la información dentro de la entidad. Esto incluye la creación de comités de seguridad, la designación de coordinadores y la asignación de tareas específicas para asegurar que todas las áreas de la organización estén alineadas y comprometidas con la protección de los datos y sistemas. (Aules Pineida, 2021)

2.2.3.2.Gestión de Activos

Implica identificar, clasificar y proteger todos los activos de información de la organización. Este proceso asegura que cada activo tenga un propietario responsable y que se apliquen controles adecuados para su protección, garantizando así la confidencialidad, integridad y disponibilidad de la información gestionada por la organización. (Maliza Malisa, 2021).

2.2.3.3.Seguridad de los recursos humanos

Abarca medidas antes, durante y después de la contratación para asegurar que los empleados y contratistas comprenden y cumplen con las responsabilidades de seguridad de la información. Incluye verificaciones de antecedentes, capacitación en seguridad, y la revocación de accesos y privilegios al finalizar la relación laboral, asegurando así que los individuos actúen de manera segura y responsable respecto a la información de la organización (Huaman Tena, 2021).

2.2.3.4.Seguridad física y del entorno

Se refiere a las medidas y controles implementados para proteger las instalaciones físicas y los recursos tecnológicos de la organización contra amenazas físicas y ambientales. Esto incluye sistemas de acceso controlado, protección contra incendios, sistemas de vigilancia, y medidas contra desastres naturales, asegurando que los activos de información estén protegidos de daños físicos y accesos no autorizados. (Rodríguez Guerra., 2019)

2.2.3.5.Gestión de Comunicaciones y Operaciones

Engloba los procedimientos y controles necesarios para asegurar el manejo seguro y eficiente de las operaciones y comunicaciones de TI. Esto incluye la administración de cambios, la realización de copias de seguridad, la gestión de la configuración, la protección contra malware y otras amenazas, y la supervisión de las actividades de TI, garantizando así la continuidad y seguridad de los servicios y sistemas de información de la organización. (Torres Hallo, 2020)

2.2.3.6.Control de Acceso

Indican las políticas y mecanismos implementados para regular quién puede acceder a la información y a los sistemas de la organización. Esto incluye la autenticación de usuarios, la autorización de accesos y la implementación de permisos y restricciones, asegurando que solo las personas autorizadas puedan acceder a la información y recursos necesarios para desempeñar sus funciones, protegiendo así la confidencialidad, integridad y disponibilidad de los datos. (Vasquez Zevallos & Delgado Saavedra, 2019)

2.3. Riesgos

En el contexto de la seguridad de la información, los riesgos pueden incluir amenazas internas o externas que podrían comprometer la confidencialidad, integridad o disponibilidad de los datos. Identificar, evaluar y gestionar estos riesgos es fundamental para proteger los activos de información y garantizar la continuidad operativa de la organización. (Lara Guijarro, 2019)

2.3.2. Gestión de Riesgos de Seguridad de la Información

Es un proceso sistemático para identificar, evaluar y mitigar los riesgos asociados con los activos de información de una organización. Este proceso implica la identificación de amenazas potenciales, la evaluación de la probabilidad de que ocurran y el impacto que tendrían en la organización. A través de la implementación de controles y medidas de seguridad adecuadas, la gestión de riesgos busca minimizar la probabilidad de ocurrencia de eventos no deseados y reducir su impacto en caso de que ocurran. (Guancanes Castro & Vilatuña Morales, 2022).

2.3.3. Gestión Metodología del análisis de riesgos

Es un proceso sistemático para identificar, evaluar y mitigar los riesgos asociados con los activos de información de una organización. Este proceso implica la identificación de amenazas potenciales, la evaluación de la probabilidad de que ocurran y el impacto que tendrían en la organización. A través de la implementación de controles y medidas de seguridad adecuadas, la gestión de riesgos busca minimizar la probabilidad de ocurrencia de eventos no deseados y

reducir su impacto en caso de que ocurran (Guancanes Castro & Vilatuña Morales, bibdigital.epn.edu.ec, 2022)

2.3.4. Metodología del análisis de riesgos

Es un enfoque estructurado y sistemático para identificar, evaluar y gestionar los riesgos asociados con los activos de información de una organización. Esta metodología implica la identificación de amenazas potenciales, la determinación de las vulnerabilidades y debilidades que podrían ser explotadas por estas amenazas, y la evaluación del impacto que los eventos adversos podrían tener en la organización. A través de este proceso, se pueden identificar y priorizar los riesgos más significativos y desarrollar estrategias de mitigación adecuadas para gestionarlos de manera efectiva. (Maliza Malisa, 2021)

2.3.4.1.Metodología MAGERIT

La Metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco estructurado desarrollado por el Gobierno de España para llevar a cabo el análisis y la gestión de riesgos de seguridad de la información en los sistemas de información de una organización. MAGERIT proporciona un conjunto de técnicas, métodos y herramientas que permiten identificar, evaluar y tratar los riesgos de seguridad de la información de manera sistemática y efectiva. (Linares Fernández & Balverdi Cruz, 2022).

2.3.4.2.Fases de Metodología MAGERIT

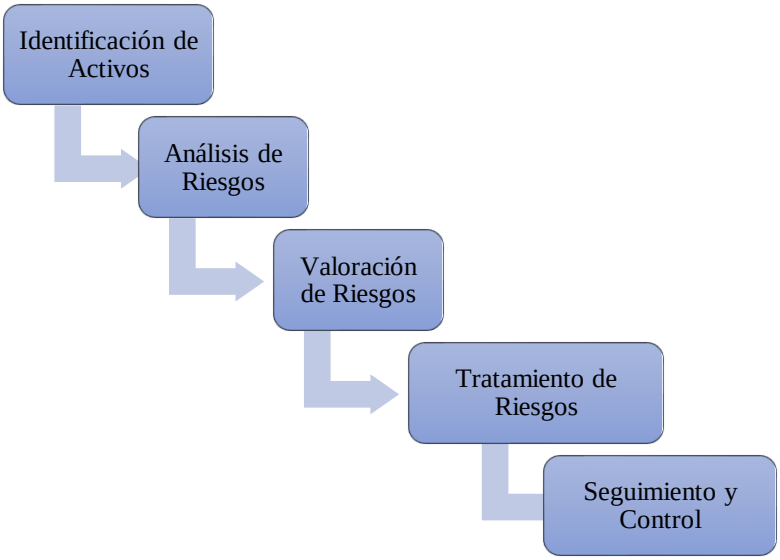

Ilustración 2. Fases de Metodología MAGERIT. Fuente: Autoría Propia.

La ilustración muestra el proceso de gestión de riesgos, comenzando por la identificación de activos relevantes. Luego, se realiza el análisis y valoración de riesgos para determinar su impacto y probabilidad. Con base en esto, se procede al tratamiento de riesgos, implementando medidas de mitigación o control. Finalmente, se lleva a cabo un seguimiento y control continuo para asegurar la efectividad del tratamiento aplicado.

2.3.4.3.Metodología NIST SP 800:30

Es un enfoque establecido por el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos para realizar la evaluación y gestión de riesgos de seguridad de la información en sistemas y organizaciones. Esta metodología proporciona un marco detallado que guía a las organizaciones a través del proceso de identificación, evaluación y tratamiento de los riesgos de seguridad de la información. (Lara Guijarro, 2019).

2.3.4.4.Fases de Metodología NIST SP 800:30

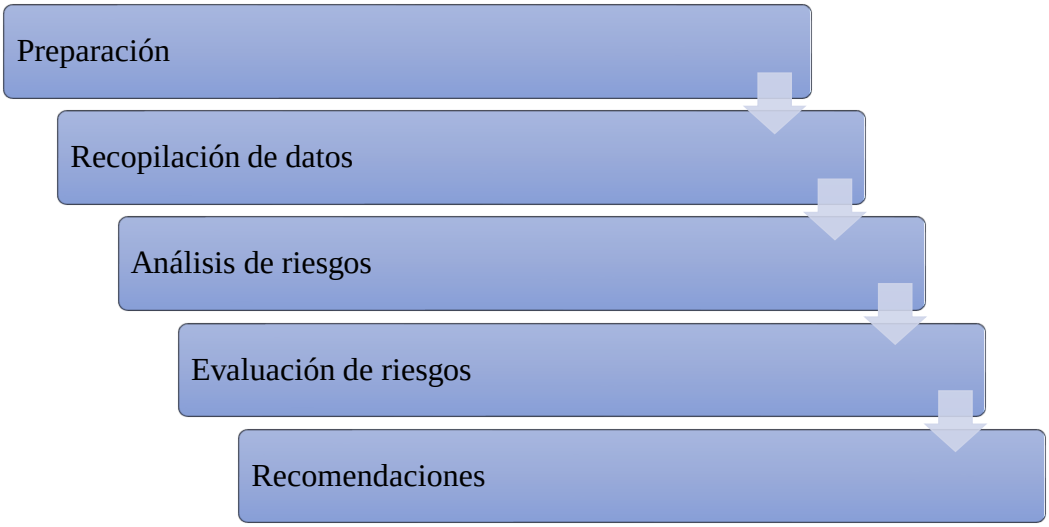

Ilustración 3. Fases de Metodología NIST SP 800:30. Fuente: Autoría propia.

La metodología NIST SP 800-30 incluye cinco fases: Preparación, donde se definen objetivos y recursos; Recopilación de datos, para obtener información sobre activos, amenazas y vulnerabilidades; Análisis de riesgos, identificando amenazas y su impacto; Evaluación de riesgos, priorizando según impacto y probabilidad; y Recomendaciones, proponiendo medidas para mitigar los riesgos identificados.

2.3.4.5.Metodología CRAMM

Es un enfoque estructurado desarrollado por el Gobierno del Reino Unido para llevar a cabo el análisis y la gestión de riesgos de seguridad de la información en sistemas y organizaciones. Esta metodología proporciona un marco detallado que guía a las organizaciones a través del proceso de identificación, evaluación y tratamiento de los riesgos de seguridad de la información. (Linares Fernández & Balverdi Cruz, 2022)

2.3.4.6.**Fases de la metodología CRAMM**

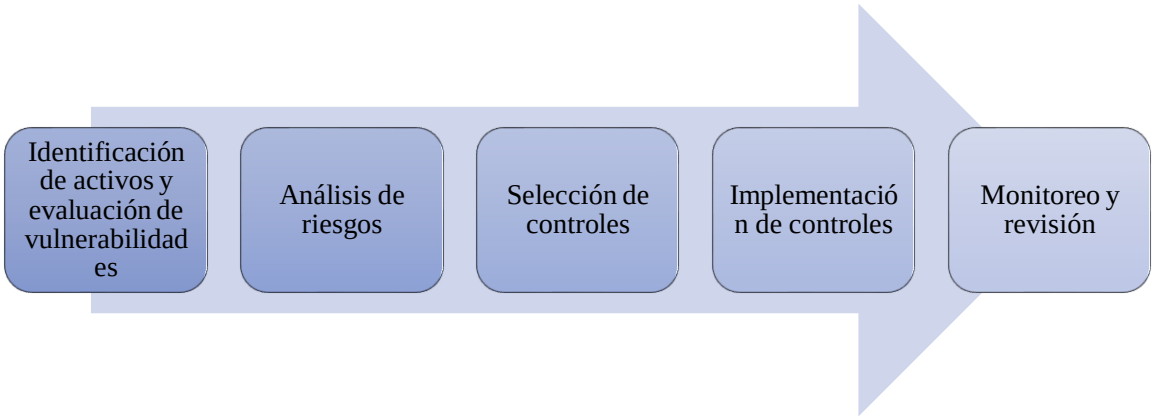

Ilustración 4. Fases de la metodología CRAMM. Fuente: Autoría propia

La metodología CRAMM se compone de cinco fases: Identificación de activos y evaluación de vulnerabilidades, para conocer riesgos potenciales; Análisis de riesgos, evaluando amenazas y su impacto; Selección de controles, eligiendo medidas de mitigación; Implementación de controles, aplicando las soluciones propuestas; y Monitoreo y revisión, verificando continuamente la efectividad de los controles para asegurar la gestión adecuada de los riesgos.

2.3.4.7.Metodología ISO/IEC 27005

La norma proporciona directrices para la gestión de riesgos de seguridad de la información. Apoya los principios generales especificados en la NTC-ISO/IEC 27001 y está diseñada para facilitar la implementación eficaz del análisis y gestión del riesgo, una fase crucial en el diseño de cualquier sistema de gestión de seguridad de la información (SGSI) sólido. Comprender los conceptos, modelos, procesos y terminología descritos en las normas NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002 es fundamental para alcanzar una comprensión completa de la NTC-ISO/IEC 27005.

2.3.4.8.Fases de la Metodología ISO/IEC 27005

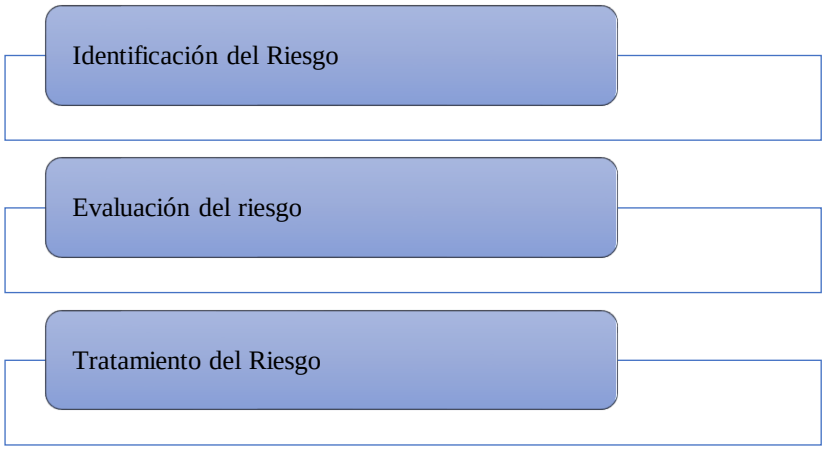

Ilustración 5. Fases de la Metodología ISO/IEC 27005.Fuente: Autoría propia

El gráfico muestra las fases de la metodología ISO/IEC 27005: Identificación del riesgo, donde se reconocen activos, amenazas y vulnerabilidades; Evaluación del riesgo, analizando su impacto y probabilidad para priorizar su tratamiento; y Tratamiento del riesgo, aplicando medidas de mitigación, transferencia o aceptación para gestionar los riesgos identificados, garantizando la seguridad de la información en la organización.

2.1.5.9 Matriz comparativa de metodologías de gestión de riesgos

En la matriz a continuación se comparan distintas metodologías empleando diversos criterios, lo cual nos permitirá identificar la opción más adecuada. Estos criterios posibilitan una evaluación minuciosa y precisa de cada metodología, facilitando la elección de la que mejor se ajuste a nuestras necesidades.

Tabla 1. Matriz Comparativa de las Metodologías de análisis de riesgo. Fuente: Autoría propia

Metodologías del análisis de riesgos	Enfoque	Enfoque de Riesgo	Etapas del Estudio	Método de Valoración	Aplicación de Casos	Marco de Referencia	Grado de Especificidad
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Se centra en la identificación y gestión de los riesgos asociados a los sistemas de información	Identificación, Valoración, Tratamiento	Evaluación cualitativa y cuantitativa	Uso de escenarios	Basado en estándares y regulaciones	Mayor nivel de detalle en el análisis y valoración
NIST SP 800:30	Metodología de Gestión de Riesgos de la NIST (National Institute of Standards and Technology)	Enfoque en la gestión integral de riesgos de sistemas de información	Preparación, Evaluación, Mitigación, Comunicación	Evaluación cuantitativa y cualitativa	Ejemplos específicos de amenazas y vulnerabilidades	Basado en estándares de seguridad de la información	Detallado en la evaluación y mitigación de riesgos

CRAMM	Método de Análisis de Gestión de Riesgos Computacionales	Enfoque en identificar y gestionar riesgos computacionales y de sistemas	Identificación, Evaluación, Gestión, Monitoreo	Evaluación cualitativa principalmente	Casos y ejemplos prácticos de riesgos específicos	Basado en buenas prácticas de seguridad de TI	Específico en riesgos computacionales y de sistemas
ISO/IEC 27005	Metodología para la gestión de riesgos de seguridad de la información según ISO/IEC 27005	Gestión de riesgos de seguridad de la información	Evaluación del riesgo, Tratamiento del riesgo, Aceptación del riesgo, Comunicación del riesgo	Evaluación cualitativa y cuantitativa	Casos de estudio y ejemplos	Basado en estándares internacionales ISO/IEC 27001 y 27002	Detallado en la gestión y tratamiento del riesgo

MAGERIT se posiciona como una elección sobresaliente debido a su enfoque exhaustivo en la identificación y gestión de riesgos inherentes a los sistemas de información. Esta metodología se distingue por su capacidad para realizar evaluaciones tanto cualitativas como cuantitativas, permitiendo así una comprensión detallada de la naturaleza y magnitud de los riesgos. Además, emplea escenarios prácticos y se fundamenta en estándares y regulaciones reconocidos, asegurando un marco sólido y fiable para el análisis de riesgos en entornos de sistemas de información. Su nivel de detalle elevado en el análisis y valoración facilita una gestión precisa y efectiva de los riesgos, convirtiéndola en una opción recomendada para organizaciones que buscan asegurar la integridad y seguridad de sus sistemas de información de manera sistemática y rigurosa.

2.4. Normativas y Buenas Prácticas Relacionadas

2.4.1. ISO/IEC 27002

ISO/IEC 27002, anteriormente conocida como ISO 17799, es una norma internacional que proporciona directrices y controles de seguridad de la información. Está diseñada para ayudar a las organizaciones a seleccionar controles de seguridad adecuados basados en buenas prácticas reconocidas a nivel mundial. Algunos ejemplos de áreas cubiertas por esta norma incluyen:

- **Políticas de seguridad de la información**: Definir las directrices y el enfoque de la organización hacia la seguridad de la información.
- **Gestión de activos:** Gestionar los activos de información para asegurar su protección adecuada.

    - **Inventario de activos**: Creación y mantenimiento de un inventario de activos que incluye información sobre su propiedad, uso y clasificación.
    - **Clasificación de la información**: Determinar el valor, la sensibilidad y las medidas de protección requeridas para cada tipo de información.
    - **Manejo de medios**: Controlar la gestión, el almacenamiento y la eliminación segura de los medios de almacenamiento de datos.
- **Seguridad en recursos humanos:** Asegurar que los empleados, contratistas y terceros comprenden sus responsabilidades de seguridad.
- **Control de acceso:** Restringir el acceso a la información y los sistemas únicamente a las personas autorizadas.
- **Cifrado:** Proteger la confidencialidad, integridad y, en algunos casos, la autenticidad de la información.
- **Seguridad física y ambiental:** Proteger los activos físicos y la infraestructura de la organización contra amenazas físicas y ambientales.
- **Gestión de comunicaciones y operaciones:** Asegurar la operación segura y confiable de las tecnologías de la información.
- **Gestión de incidentes de seguridad de la información:** Gestionar y responder efectivamente a los incidentes de seguridad.

La ISO/IEC 27002 es complementaria a la ISO 27001 y proporciona detalles específicos sobre los controles que las organizaciones pueden implementar para gestionar los riesgos de seguridad de la información de manera efectiva (ISO, 2024).

2.4.2. NIST Cybersecurity Framework

El Marco de Ciberseguridad del NIST es una estructura creada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, diseñada para asistir a las organizaciones en el fortalecimiento de su seguridad cibernética. Este marco ofrece

directrices sobre la gestión y mitigación de riesgos relacionados con las actividades cruciales de la infraestructura de tecnología de la información. Está estructurado en torno a cinco funciones principales

- Identificar: Desarrollar la comprensión de los sistemas, activos, datos y capacidades críticas de la organización para la ciberseguridad.
- Proteger: Implementar medidas de seguridad adecuadas para proteger los activos críticos y los datos.
- Detectar: Implementar actividades de monitoreo y detección continua para identificar incidentes de ciberseguridad.
- Responder: Desarrollar y ejecutar planes de respuesta eficaces para manejar incidentes de ciberseguridad cuando ocurran.
- Recuperar: Restaurar capacidades operativas normales y servicios afectados después de un incidente de ciberseguridad.

El marco NIST CSF es ampliamente utilizado en Estados Unidos y globalmente como un marco de referencia para mejorar la ciberresiliencia organizacional (National Institute of Standards and Technology, 2024)

2.4.3. Buenas Prácticas de Seguridad Informática

Gestión de Contraseñas: Incluye políticas y procedimientos para la creación, almacenamiento y gestión segura de contraseñas, como el uso de contraseñas fuertes, el cambio periódico de contraseñas y el uso de autenticación multifactor.

- Actualizaciones y Parches de Software: Consiste en mantener el software actualizado con las últimas versiones y parches de seguridad disponibles para mitigar vulnerabilidades conocidas y potenciales.

- Copias de Seguridad y Recuperación: Implica la implementación de procedimientos para realizar copias de seguridad regulares de datos críticos y sistemas, junto con planes de recuperación de desastres para restaurar datos y servicios en caso de pérdida o interrupción.

Estas buenas prácticas son fundamentales para fortalecer la seguridad de la información y proteger los activos críticos contra amenazas cibernéticas y otros riesgos. Implementarlas de manera efectiva ayuda a las organizaciones a reducir el riesgo de incidentes de seguridad y mantener la continuidad del negocio (incibe, 2024).

CAPITULO III

3. MARCO METODOLÓGICO

3.1 Enfoque de la Investigación

La presente investigación tiene un enfoque mixto. Se combinarán métodos cuantitativos y cualitativos para obtener una comprensión integral de la situación actual de la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi y desarrollar un manual de políticas de seguridad efectivo conforme a la norma ISO 27001. El enfoque cualitativo se llevará a cabo mediante una encuesta que permitirá explorar en profundidad las percepciones y experiencias del personal respecto a la seguridad de la información, mientras que el enfoque cuantitativo facilitará la medición de la eficacia de las políticas actuales y el grado de cumplimiento de las mismas.

3.2 Nivel de Investigación

La investigación es de carácter descriptiva ya que se pretende describir las políticas de seguridad de la información de la cooperativa de Chunchi.

3.3 Población y Muestra

La población de estudio está constituida por todos los empleados de la Cooperativa de Ahorro y Crédito Chunchi, incluyendo personal administrativo, operativo y directivo

La muestra será principalmente va dirigida al gerente y al encargado del departamento de TI.

3.4 Técnicas e Instrumentos de Recolección

Para recolectar la información necesaria, se utilizará encuestas y se realizará un análisis de documentos provenientes de diversas fuentes científicas. Este proceso tiene como objetivo obtener una visión integral de las prácticas actuales de seguridad de la

información en la Cooperativa de Ahorro y Crédito Chunchi, así como entender las percepciones y opiniones del personal sobre las políticas de seguridad vigentes. Con esta metodología, se podrá identificar áreas de mejora y fundamentar el desarrollo de un manual de políticas de seguridad de la información alineado con los requisitos de la norma ISO 27001.

3.5 Tratamiento de la Información

Los datos recopilados se organizarán sistemáticamente. Posteriormente, se procederá a analizar e interpretar los resultados obtenidos de las encuestas y el análisis de documentos, centrándose en las necesidades de seguridad de la información de la cooperativa.

3.6 Interpretación de Resultados

La evaluación se realizará mediante un análisis sistemático de las respuestas recopiladas en las encuestas por el responsable del departamento de TIC y el gerente. Los datos obtenidos fueron clasificados y analizados según los dominios definidos en la norma ISO/IEC 27001, la cual guía a las organizaciones en el establecimiento de políticas de seguridad de la información. Esta metodología proporciona una base sólida para llevar a cabo una evaluación exhaustiva y coherente de las políticas y prácticas actuales de seguridad de la información dentro de la organización.

3.6.1 Análisis detallado de la encuesta realizada en base a la norma ISO 27001 para determinar el nivel de cumplimiento en el departamento de TIC.

Para evaluar la seguridad de la información en la Cooperativa de Chunchi, se aplicó una encuesta al responsable del departamento de TIC y al gerente. La información obtenida permite conocer el estado actual de la seguridad de la información en la cooperativa.

Tabla 2. Respuestas obtenidas de la encuesta. Autoría: Propia.

CHUNCHI Ltda.
Cooperativa de Ahorro y Crédito

Secciones/ ISO27001:2013	Encuesta	Si	NO	Parcialmente
Contexto de la Organización	¿La Cooperativa de Chunchi ha identificado las partes interesadas relevantes y sus requisitos en relación con la seguridad de la información?	**X**		
	¿Se ha definido el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) dentro de la cooperativa?			**X**
	¿Se han identificado y documentado los factores internos y externos que pueden afectar la capacidad de la cooperativa para alcanzar los resultados previstos del SGSI?		**X**	
	¿Se han identificado y evaluado los procesos críticos de negocio que deben ser protegidos mediante el SGSI?	**X**		
Liderazgo	¿La alta dirección de la cooperativa demuestra liderazgo y compromiso con respecto al SGSI?	**X**		
	¿Se han establecido políticas de seguridad de la información que sean apropiadas para el propósito de la cooperativa?	**X**		

	¿Se asignan roles y responsabilidades claros en relación con la seguridad de la información?			**X**
Planificación	¿Se lleva a cabo una evaluación regular de riesgos de seguridad de la información?		**X**	
	¿Se han establecido planes de tratamiento de riesgos para abordar los riesgos de seguridad de la información identificados?			**X**
	¿Se han definido objetivos de seguridad de la información que sean medibles y estén alineados con las políticas de la cooperativa?	**X**		
Soporte	¿La cooperativa proporciona los recursos necesarios para establecer, implementar, mantener y mejorar el SGSI?	**X**		
	¿El personal relevante recibe la capacitación adecuada en seguridad de la información?			**X**
	¿Existen procesos de comunicación eficaces para la seguridad de la información dentro de la cooperativa?	**X**		
Operación	¿Se implementan y operan los controles necesarios para gestionar los riesgos de seguridad de la información?			**X**
	¿Se monitorean y revisan regularmente los procesos de seguridad de la información?		**X**	
	¿Existen procedimientos documentados para la gestión de incidentes de seguridad de la información?	**X**		
Evaluación del Desempeño	¿Se realizan auditorías internas regulares del SGSI?			**X**
	¿Se revisa periódicamente el desempeño del SGSI por parte de la alta dirección?	**X**		

	¿Se utilizan indicadores de desempeño para medir la eficacia de los controles de seguridad de la información?	**X**		
Mejora Continua	¿Se toman acciones correctivas para abordar no conformidades en el SGSI?	**X**		
	¿Se busca mejorar continuamente la idoneidad, adecuación y eficacia del SGSI?			**X**
	¿Se promueve una cultura de mejora continua en todos los niveles de la cooperativa?		**X**	

Tabla 3. Respuestas obtenidas de la encuesta. Autoría: Propia.

CHUNCHI Ltda.
Cooperativa de Ahorro y Crédito

Código:	
Fecha:	
Versión:	

Dominios - ISO27002:2013	**Preguntas**	**Si**	**No**	**En proceso**
Políticas de la Seguridad	¿Existe en su organización un documento que contenga las políticas de seguridad de la información?	**X**		
	¿Considera que este documento está adecuadamente difundido y comunicado a todos los miembros de la organización?			**X**
	¿El documento de seguridad se revisa periódicamente y en caso de ocurrencia de eventos significativos?	**X**		
	¿El personal de la cooperativa tiene conocimiento sobre las políticas de seguridad de la información?			**X**

	¿Existe un comité de gestión de seguridad que proponga o dé soporte a las iniciativas de seguridad?	**X**		
Aspectos organizativos de la Seguridad de la Información.	¿Se han definido claramente los roles y responsabilidades relacionadas con la seguridad de la información?	**X**		
	¿Existen procedimientos documentados para la gestión de la seguridad de la información?			
	¿Se realizan reuniones periódicas para revisar el estado de la seguridad de la información?			**X**
	¿Hay un comité de seguridad de la información establecido en la organización?	**X**		
	¿Se cuenta con un plan estratégico para la seguridad de la información?	**X**		
Seguridad Ligada a los Recursos Humanos.	¿Se verifica la integridad de los empleados antes de su contratación?	**X**		
	¿Se proporciona formación en seguridad de la información a los empleados de manera regular?			**X**
	¿Existen procedimientos para la gestión de incidentes de seguridad relacionados con el personal?	**X**		
	¿Se realizan evaluaciones de desempeño considerando la seguridad de la información?		**X**	

	¿Se incluyen cláusulas de confidencialidad y seguridad de la información en los contratos de los empleados?	**X**	
Gestión de Activos.	¿Se mantienen inventarios actualizados de todos los activos de información?	**X**	
	¿Cada activo de información tiene un responsable designado?	**X**	
	¿Se categorizan los activos según su importancia para la organización?		**X**
	¿Se realizan evaluaciones de riesgos para cada activo de información?	**X**	
	¿Se implementan medidas de protección adecuadas para los activos de información críticos?	**X**	
Control de Accesos.	¿Existe un proceso formal de gestión de acceso a la información?	**X**	
	¿Se revisan periódicamente los derechos de acceso de los usuarios?	**X**	
	¿Se implementan medidas para asegurar el acceso seguro a los sistemas de información?	**X**	
	¿Se utilizan mecanismos de autenticación robustos para el acceso a los sistemas?	**X**	
	¿Se controlan y monitorizan los accesos privilegiados?		**X**
Cifrado	¿Se utilizan algoritmos de cifrado fuertes para proteger la información sensible?	**X**	

	¿Se implementan procedimientos para la gestión de claves de cifrado?	**X**	
	¿Existe una política documentada sobre el uso de cifrado en la organización?	**X**	
	¿Se revisan periódicamente las políticas y procedimientos de cifrado?		**X**
	¿Se asegura el cifrado de datos en tránsito y en reposo?	**X**	
Seguridad Física y Ambiental.	¿Se implementan controles para proteger las instalaciones físicas que albergan sistemas de información?	**X**	
	¿Existen medidas para proteger el equipo y los datos en caso de desastres naturales o accidentes?	**X**	
	¿Se restringe el acceso físico a áreas críticas y sensibles?	**X**	
	¿Se cuenta con sistemas de monitoreo y alarmas en las instalaciones físicas?		**X**
	¿Se realizan simulacros periódicos de respuesta a emergencias	**X**	
Seguridad en la Operativa	¿Se monitorizan y revisan regularmente los registros de eventos de seguridad?	**X**	
	¿Se han implementado procedimientos de gestión de incidentes de seguridad?	**X**	
	¿Existe un plan de continuidad del negocio que incluya la seguridad de la información?	**X**	
	¿Se realizan pruebas regulares del plan de continuidad del negocio?		**X**
	¿Se gestionan adecuadamente las copias de seguridad de la información?	**X**	

Seguridad en las Telecomunicaciones	¿Se utilizan mecanismos seguros para la transmisión de información confidencial?	**X**	
	¿Se implementan controles para proteger las redes internas y externas?	**X**	
	¿Se supervisan las comunicaciones de red para detectar actividades sospechosas?	**X**	
	¿Se actualizan y gestionan adecuadamente los dispositivos de red?	**X**	
	¿Se segmentan las redes para limitar el acceso a recursos críticos?		**X**
adquisición, desarrollo y mantenimiento de los sistemas de información.	¿Se incluyen requisitos de seguridad en las especificaciones de los sistemas de información?	**X**	
	¿Se realizan pruebas de seguridad durante el desarrollo de sistemas de información?		**X**
	¿Se implementan controles de seguridad en todo el ciclo de vida del desarrollo de software?	**X**	
	¿Se revisan y prueban las actualizaciones y parches de seguridad antes de su implementación?	**X**	
	¿Se realizan auditorías de seguridad para los nuevos sistemas antes de su despliegue?	**X**	
relaciones con suministradores	¿Se incluyen requisitos de seguridad en las especificaciones de los sistemas de información?	**X**	
	¿Se realizan pruebas de seguridad durante el desarrollo de sistemas de información?	**X**	
	¿Se implementan controles de seguridad en todo el ciclo de vida del desarrollo de software?		**X**
	¿Se revisan y prueban las actualizaciones y parches de seguridad antes de su implementación?	**X**	

	¿Se realizan auditorías de seguridad para los nuevos sistemas antes de su despliegue?	**X**	
Gestión de incidentes en la Seguridad de la Información.	¿Existe un procedimiento documentado para la gestión de incidentes de seguridad?	**X**	
	¿Se registran y analizan todos los incidentes de seguridad?	**X**	
	¿Se toman medidas correctivas para evitar la recurrencia de incidentes de seguridad?	**X**	
	¿Se informa a la alta dirección sobre los incidentes de seguridad significativos?	**X**	
	¿Se realiza una revisión post-incidente para identificar mejoras en los procesos de seguridad?	**X**	
Cumplimiento	¿La organización cumple con todas las leyes y regulaciones aplicables en materia de seguridad de la información?	**X**	
	¿Se realizan revisiones periódicas para asegurar el cumplimiento de las políticas de seguridad de la información?		**X**
	¿Se llevan a cabo auditorías externas de seguridad de la información?	**X**	
	¿Se asegura el cumplimiento de los contratos y acuerdos con terceros en relación con la seguridad de la información?	**X**	

	¿Se actualizan las políticas de seguridad para reflejar cambios en las regulaciones y estándares?	**X**

Después de haber realizado la encuesta al gerente y al encargado del departamento de TIC, se ha procedido a realizar el respectivo análisis la norma ISO 27001:2013 y de la norma 27002: 2013, tal como se muestra en las tablas anteriores.

3.7 Análisis de la norma ISO 27001:2013

3.7.1 Sección Contexto de la Organización

Según los resultados de la encuesta realizada al responsable de Tecnología de la Información (TI) de la Cooperativa de Chunchi, se ha identificado que la organización se encuentra en una fase de desarrollo (50%) para definir el contexto organizacional en relación con la seguridad de la información. Sin embargo, un 25% de las respuestas indican que aún no se han abordado completamente los aspectos necesarios para asegurar un marco sólido en este contexto, y otro 25% muestra que algunos elementos han sido implementados solo parcialmente. Esto sugiere que, aunque se han dado pasos importantes hacia la formalización del Sistema de Gestión de Seguridad de la Información (SGSI), todavía existen áreas críticas que requieren atención para asegurar una cobertura completa y efectiva, como se observa en el gráfico No. 1.

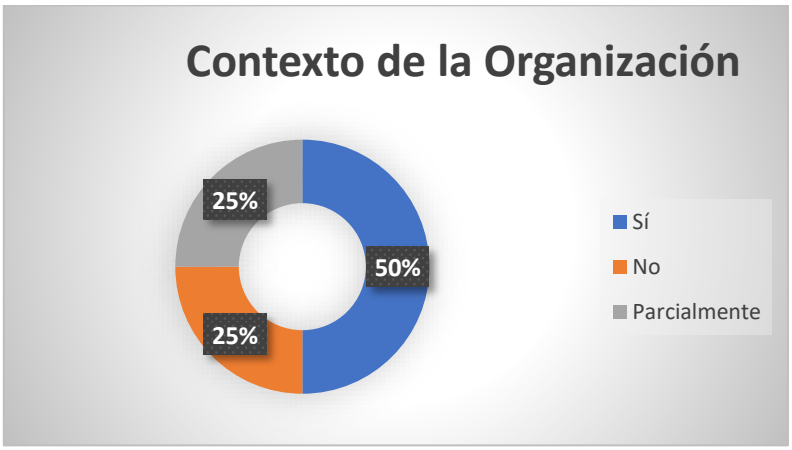

Gráfico 1.Contexto de la organización. Fuente; Autoría Propia.

3.7.2 Sección Liderazgo

Como se observa en el Gráfico N.º 2, se ha identificado que la alta dirección de la cooperativa demuestra un liderazgo y compromiso significativos con respecto al Sistema de Gestión de Seguridad de la Información (SGSI), con un 67% de respuestas afirmativas. Sin embargo, el 33% de las respuestas indican que todavía existen áreas donde este liderazgo y compromiso no se han manifestado de manera efectiva. Esto sugiere que, aunque la mayoría de los aspectos de liderazgo están bien implementados, es crucial trabajar en las áreas faltantes para asegurar un apoyo completo y coherente por parte de la alta dirección hacia la seguridad de la información.

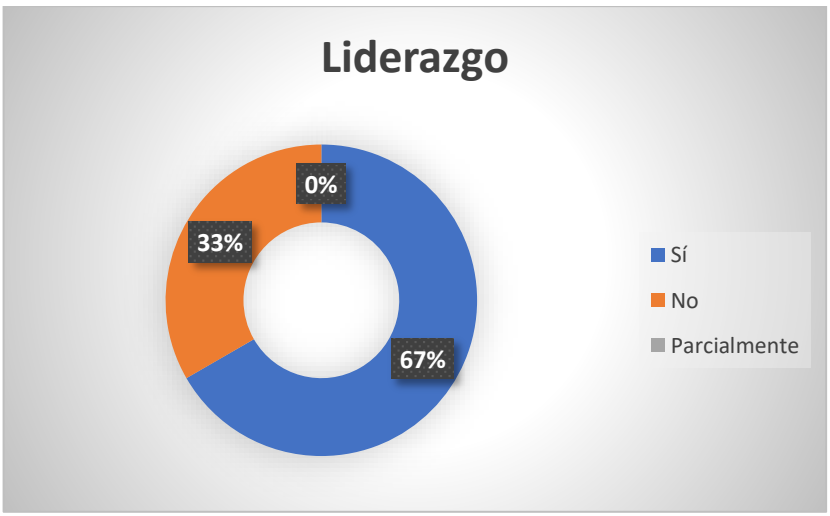

Gráfico 2.Sección Liderazgo. Fuente: Autoría Propia.

3.7.3 Sección Planificación

De acuerdo con el gráfico No. 3, los resultados obtenidos en la sección de planificación, se destaca que solo un 33% de las actividades planificadas para la gestión de seguridad de la información en la Cooperativa de Chunchi han sido implementadas de manera adecuada. Por otro lado, un 67% de las respuestas indican que estas actividades no se han llevado a cabo, lo que subraya una brecha significativa en la planificación efectiva de la seguridad de la información. Este resultado resalta la necesidad urgente de mejorar los procesos de planificación para asegurar que la gestión de riesgos y las acciones correctivas se realicen de manera oportuna y efectiva.

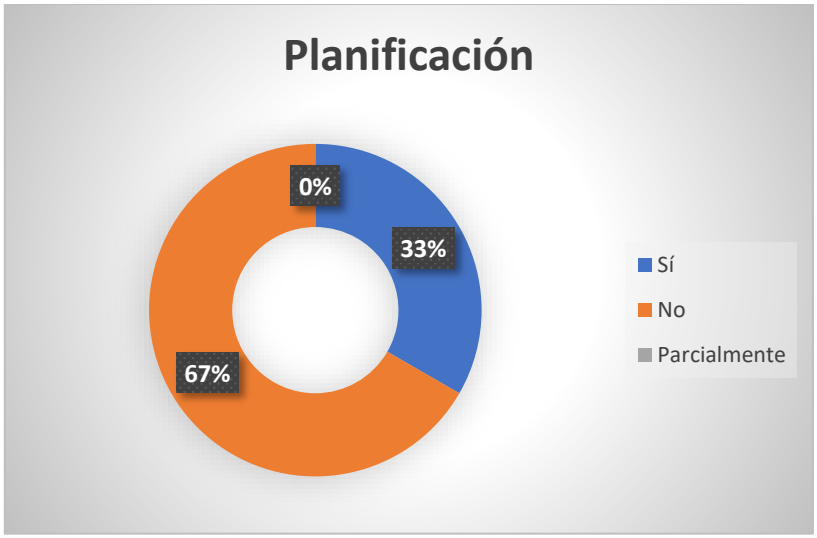

Gráfico 3.Sección Planificación; Autoría Propia.

3.7.4 Sección Soporte

Refiriéndose a los resultados de la encuesta en la sección de soporte, se observa que un 67% de los recursos y actividades de soporte relacionados con la seguridad de la información en la Cooperativa de Chunchi están adecuadamente implementados. No obstante, un 33% de las respuestas indican la falta de implementación en ciertas áreas clave. Este panorama evidencia la necesidad de reforzar los recursos de soporte para asegurar una implementación integral y efectiva del Sistema de Gestión de Seguridad de la Información[3], como se observa en el gráfico N.º 4.

[3] SGSI

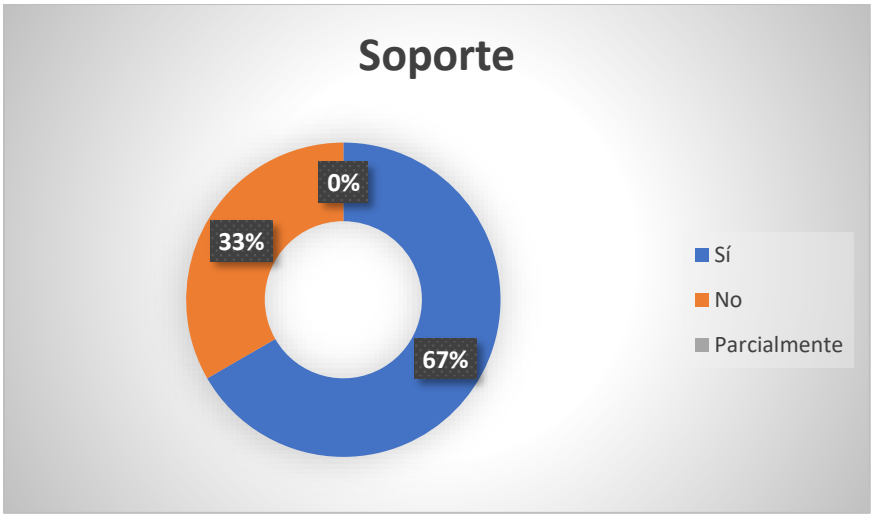

Gráfico 4. Sección Soporte; Autoría propia.

3.7.5 Sección Operación

Como se observa en el Gráfico N.º 5, los datos obtenidos para la sección de operación indican que solo el 34% de las operaciones necesarias para gestionar la seguridad de la información en la Cooperativa de Chunchi se han implementado de manera adecuada. Además, se identificó que un 33% de las operaciones no han sido implementadas y otro 33% se ha realizado de manera parcial. Estos resultados evidencian una implementación inconsistente y subrayan la necesidad de mejorar tanto la planificación como la ejecución de las operaciones para garantizar una protección efectiva y continua de la información.

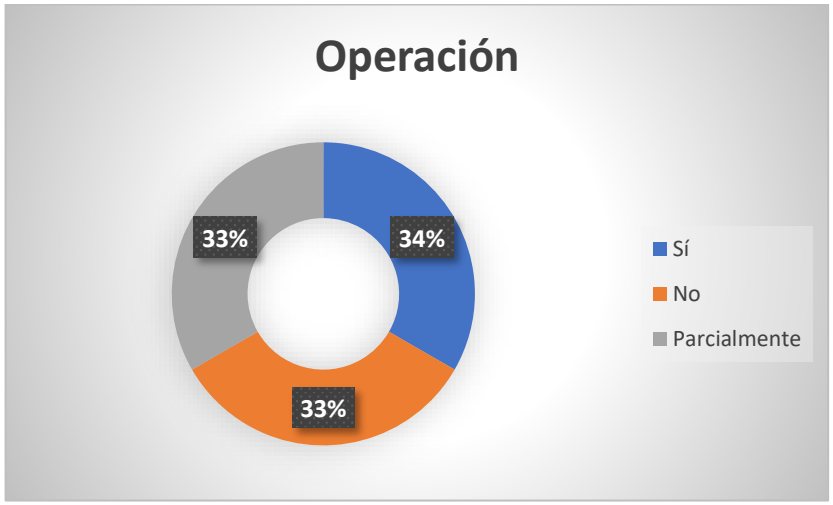

Gráfico 5.Sección Operación. Fuente: Autoría propia.

3.7.6 Sección Evaluación del Desempeño

Basado en los resultados reflejados en la sección de evaluación del desempeño, se puede afirmar que un 67% de las actividades relacionadas con la evaluación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Chunchi se han implementado de manera adecuada. Sin embargo, un 33% de las respuestas indican la ausencia de estas evaluaciones en ciertas áreas clave. Esto sugiere que, aunque la mayoría de las actividades de evaluación están bien cubiertas, es esencial cubrir las áreas faltantes para garantizar una evaluación integral y continua del desempeño del SGSI, como se muestra en el gráfico N.º 6.

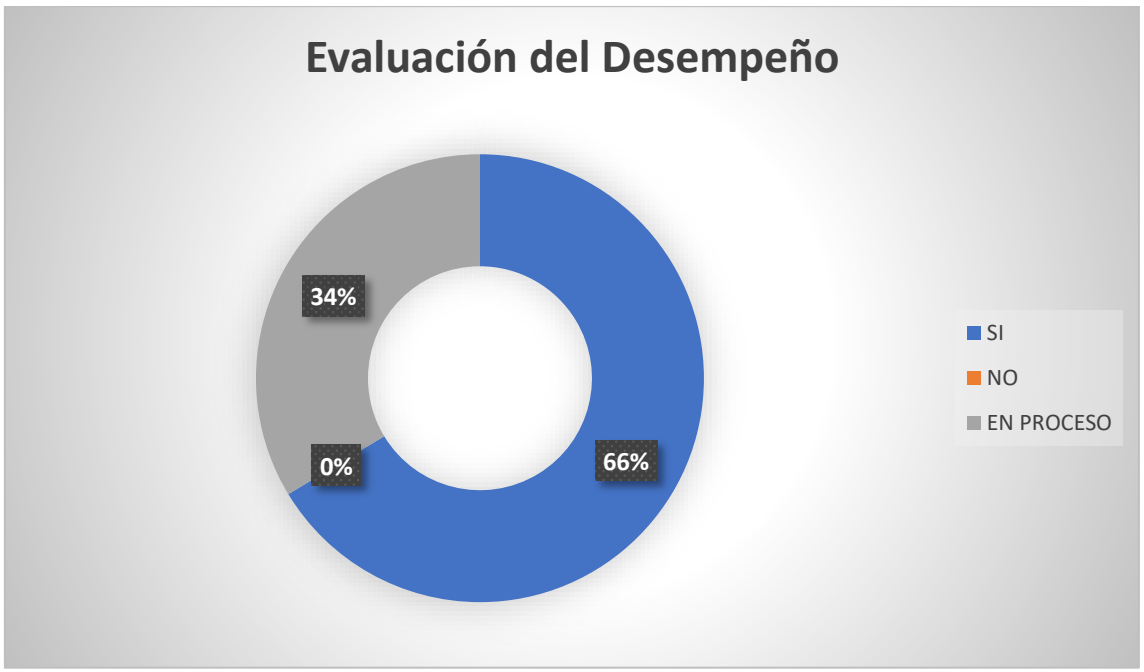

Gráfico 6.Sección Evaluación del Desempeño. Fuente: Autoría propia.

3.7.7 Sección Mejora Continua

Como se observa en el Gráfico N.º 7 que la Cooperativa de Chunchi presenta desafíos importantes en la implementación del SGSI. Según la encuesta, solo el 34% de las acciones correctivas necesarias para abordar no conformidades se están llevando a cabo, lo que indica un avance limitado en esta área. Además, otro 33% muestra que la cooperativa no busca mejorar continuamente la idoneidad, adecuación y eficacia del SGSI, lo que puede afectar su capacidad para mantener un sistema de gestión efectivo. Finalmente, el 33% de las respuestas

revela que la cultura de mejora continua no está completamente promovida dentro de la cooperativa, lo cual es esencial para garantizar la sostenibilidad del SGSI a largo plazo.

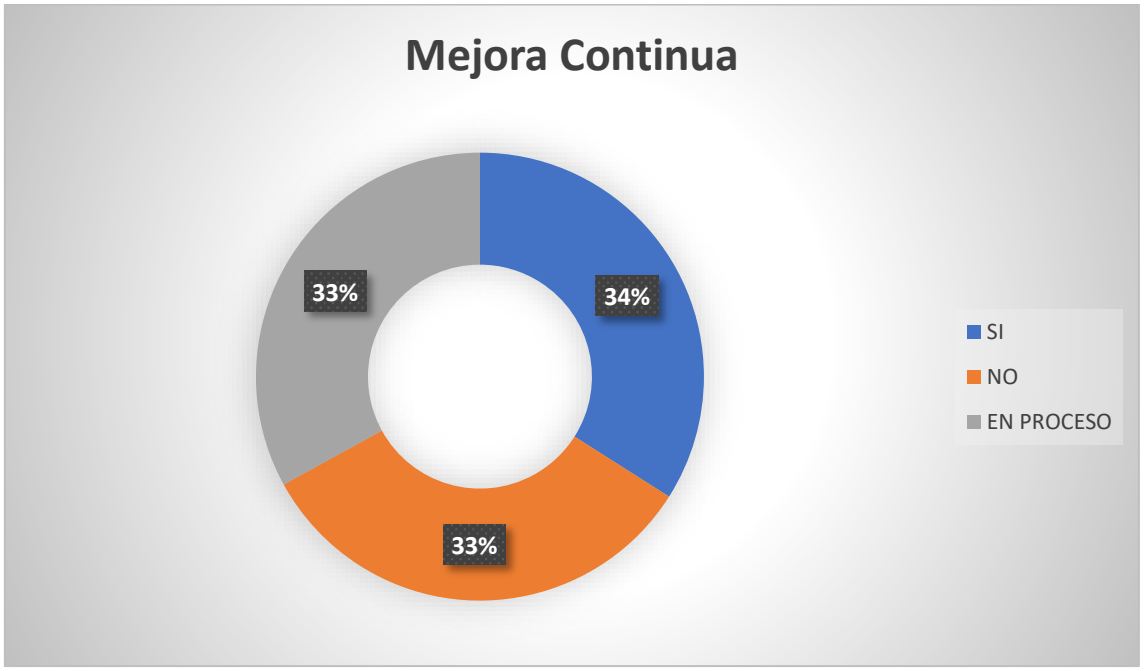

Gráfico 7. Sección Soporte. Fuente: Autoría propia.

3.8 Análisis de la guía de buenas prácticas ISO27002:2013

3.8.1 Dominio Políticas de la Seguridad

Basado en los resultados obtenidos en el dominio de Políticas de la Seguridad, como se muestra en el gráfico N.º 8 se evidencia que el 60% de las políticas de seguridad de la información en la Cooperativa de Chunchi están debidamente documentadas y han sido implementadas. Sin embargo, el 40% de las respuestas indican que estas políticas aún se encuentran en proceso de implementación. Este resultado subraya la importancia de completar y formalizar todas las políticas de seguridad para asegurar que toda la organización esté alineada con los estándares de seguridad establecidos.

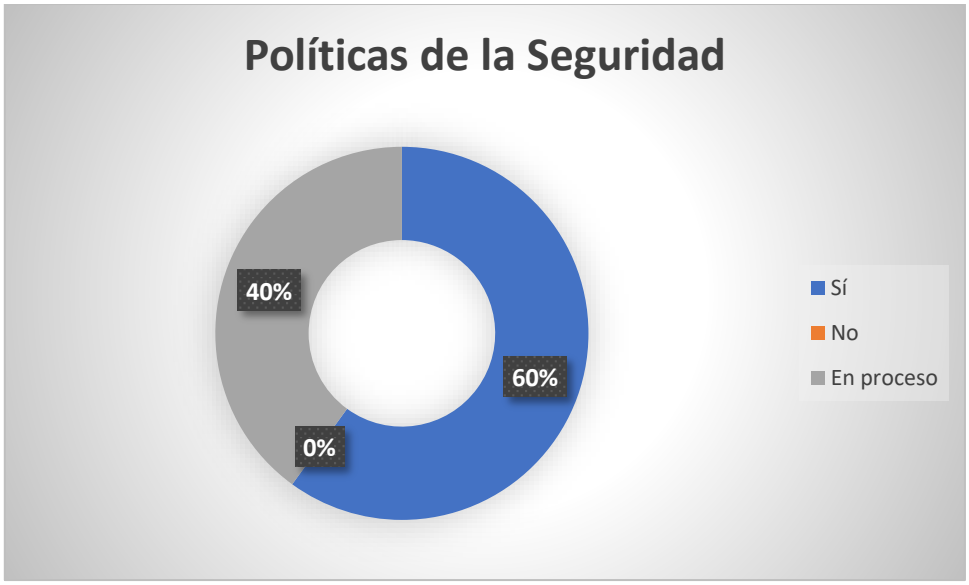

Gráfico 8. Políticas de seguridad. Fuente: Autoría Propia.

3.8.2 Dominio Aspectos organizativos de la Seguridad de la Información

En cuanto a los Aspectos Organizativos de la Seguridad de la Información, el 80% de los procedimientos están claramente definidos y se aplican de manera regular. Esto incluye la documentación de roles y responsabilidades, la existencia de un comité de seguridad de la información, y la implementación de un plan estratégico para la seguridad. Sin embargo, el 20% restante está en proceso, lo que refleja la necesidad de mejorar la frecuencia de las reuniones periódicas para revisar el estado de la seguridad. Este análisis muestra que la organización tiene una estructura sólida en cuanto a la gestión de la seguridad de la información, pero necesita fortalecer la consistencia y regularidad de sus revisiones para mantener una seguridad proactiva y bien gestionada.

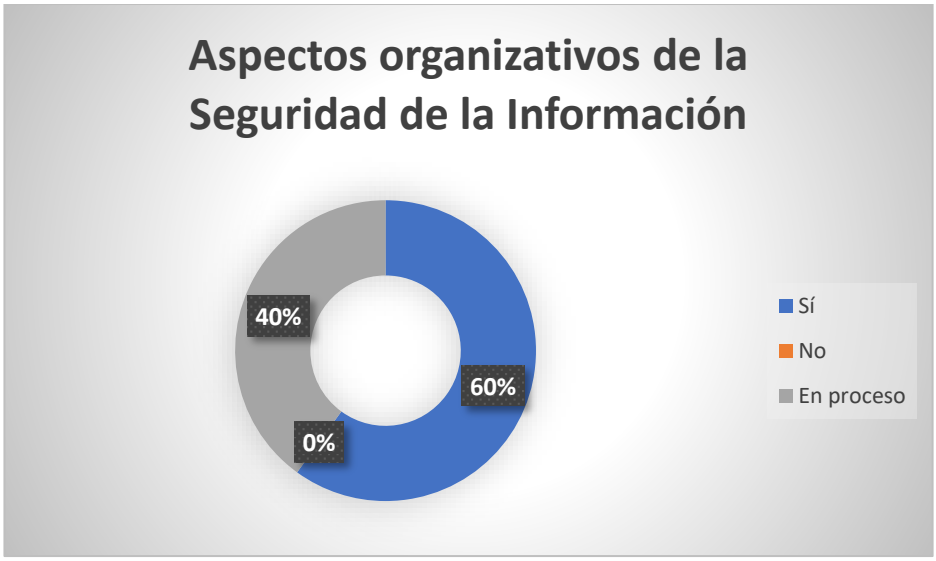

Gráfico 9. Aspectos organizativos de la Seguridad de la Información. Fuente: Autoría Propia.

3.8.3 Dominio Seguridad Ligada a los Recursos Humanos

Considerando los resultados del dominio Seguridad Ligada a los Recursos Humanos, se evidencia que el 80% de las prácticas y políticas relacionadas con la seguridad en los recursos humanos en la Cooperativa de Chunchi están implementadas adecuadamente. Sin embargo, un 20% de las respuestas indican que aún hay aspectos que están en proceso de implementación. Este hallazgo subraya la importancia de completar estas implementaciones para garantizar que todos los aspectos relacionados con la seguridad de los recursos humanos estén plenamente operativos y alineados con los objetivos de seguridad de la organización como se muestra en el Gráfico N.º 10.

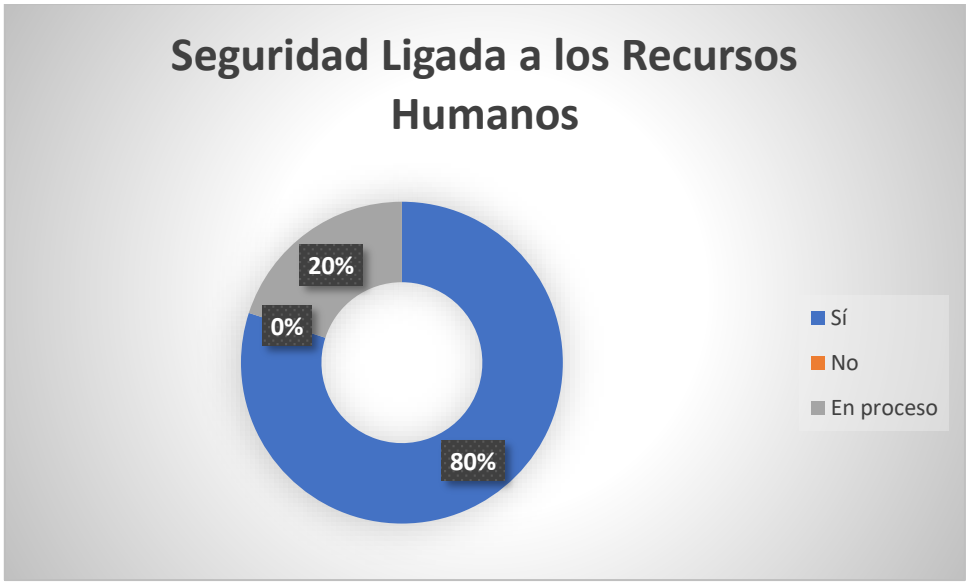

Gráfico 10. Sección Evaluación del Desempeño. Fuente: Autoría Propia.

3.8.4 Dominio Gestión de Activos

En cuanto a los resultados obtenidos en el dominio Gestión de Activos, se puede observar que el 80% de las actividades y controles relacionados con la gestión de activos en la Cooperativa de Chunchi están completamente implementados. Sin embargo, un 20% de las respuestas revelan que algunas de estas actividades aún se encuentran en proceso de implementación. Este resultado pone de manifiesto la necesidad de finalizar estos procesos para garantizar una gestión integral y efectiva de los activos de información dentro de la organización.

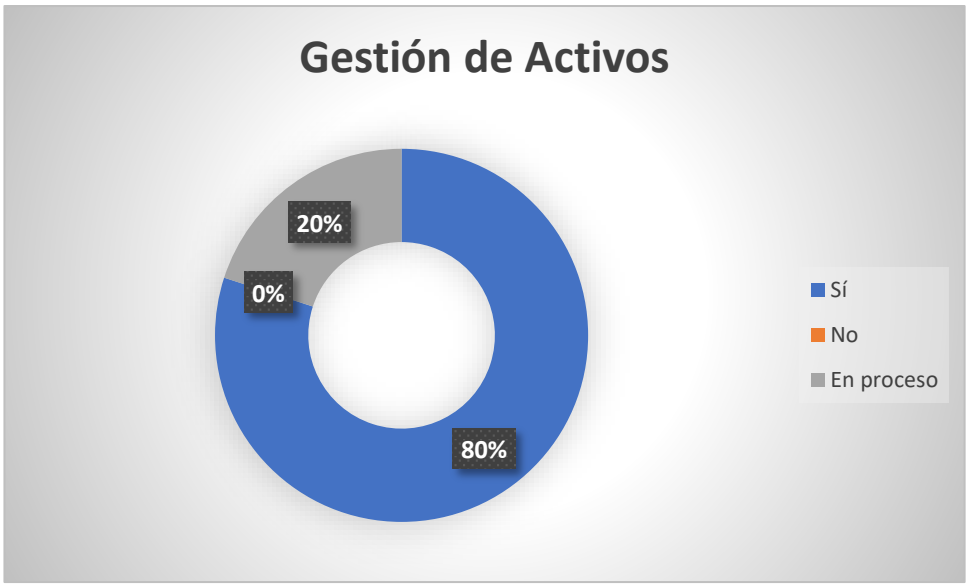

Gráfico 11. Gestión de Activos. Fuente: Autoría propia.

3.8.5 Dominio Control de Accesos

En el gráfico N.º 12 al analizar los resultados del dominio Control de Accesos, se puede concluir que el 80% de las medidas y procedimientos de control de acceso en la Cooperativa de Chunchi han sido implementados satisfactoriamente. Sin embargo, el 20% restante indica que algunas de estas medidas aún están en proceso de implementación. Este resultado enfatiza la importancia de completar la implementación de todos los controles de acceso para asegurar la protección adecuada de la información y los recursos críticos de la organización.

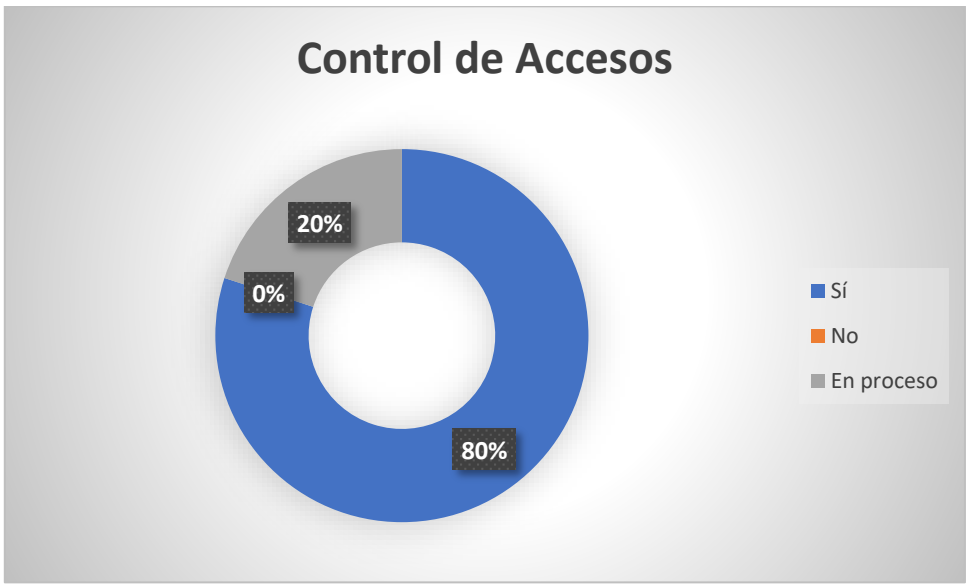

Gráfico 12. Sección Control de Accesos. Fuente: Autoría Propia.

3.8.6 Dominio Cifrado

En el Grafico N.º 13 muestra los resultados obtenidos en el dominio Cifrado, se observa que el 80% de las políticas y mecanismos de cifrado en la Cooperativa de Chunchi están adecuadamente implementados. Sin embargo, un 20% de las respuestas indican que ciertas implementaciones de cifrado aún están en proceso. Este resultado destaca la necesidad de finalizar la implementación de todas las medidas de cifrado para asegurar la protección completa de la información sensible tanto en tránsito como en reposo dentro de la organización.

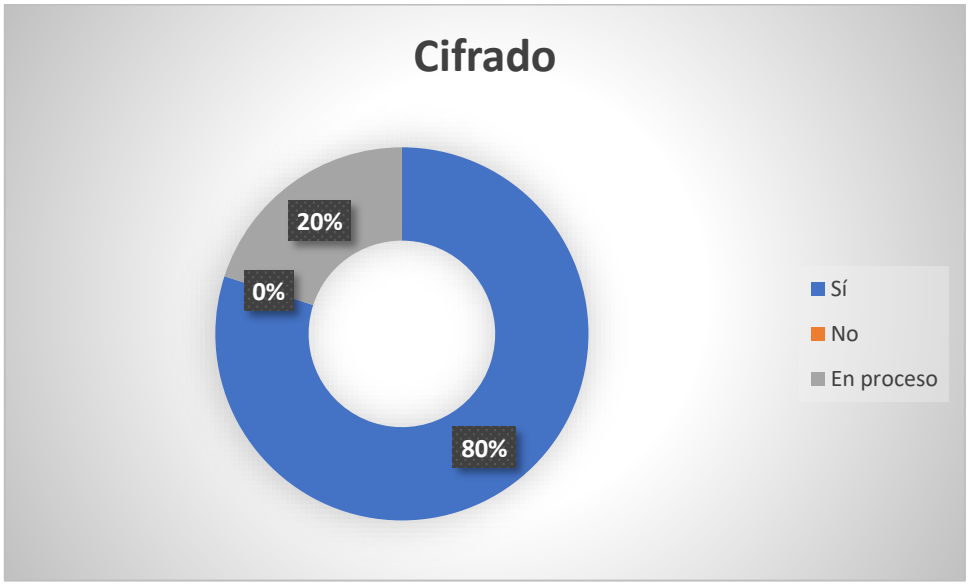

Gráfico 13. Dominio Cifrado. Fuente: Autoría Propia.

3.8.7 Dominio Seguridad Física y Ambiental

Analizando los resultados obtenidos en el dominio Seguridad Física y Ambiental, se puede concluir que el 60% de las medidas de seguridad física y ambiental en la Cooperativa de Chunchi están implementadas de manera adecuada. Sin embargo, un 40% de las respuestas indican que estas medidas aún se encuentran en proceso de implementación. Este resultado subraya la importancia de completar y consolidar todas las acciones relacionadas con la seguridad física y ambiental para garantizar la protección integral de los recursos físicos y tecnológicos de la organización como se visualiza en el grafico N.º 14.

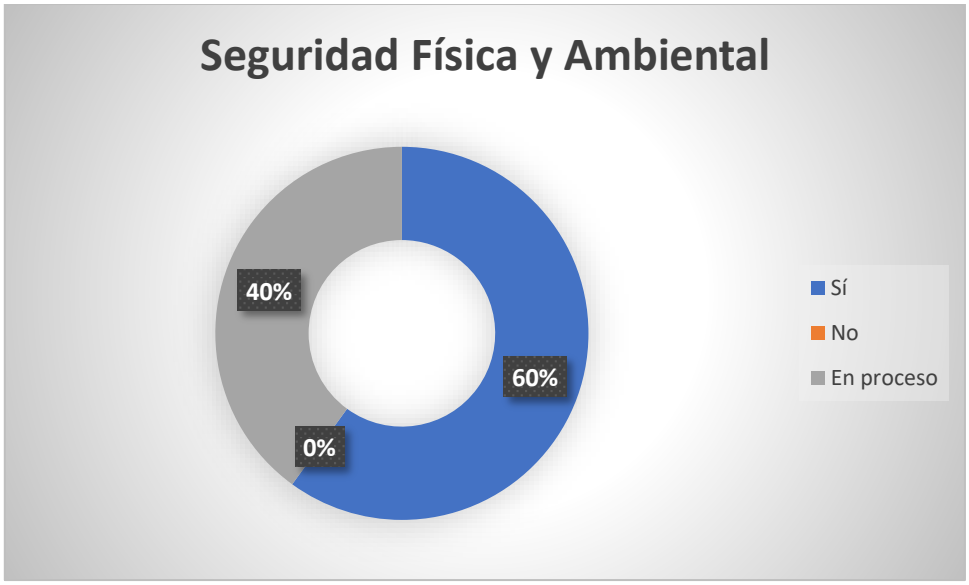

Gráfico 14. Dominio Seguridad Física y Ambiental. Fuente: Autoría Propia.

3.8.8 Dominio Seguridad en la Operativa

De acuerdo con los resultados obtenidos en el dominio Seguridad en la Operativa, se observa que el 80% de las medidas y procedimientos operativos de seguridad en la Cooperativa de Chunchi están implementados de manera adecuada. Sin embargo, un 20% de las respuestas indican que algunas de estas medidas aún están en proceso de implementación. Este resultado pone de manifiesto la necesidad de completar estos procesos para asegurar la eficacia y continuidad de la seguridad operativa en la organización, como se presenta en el Gráfico N.º 15.

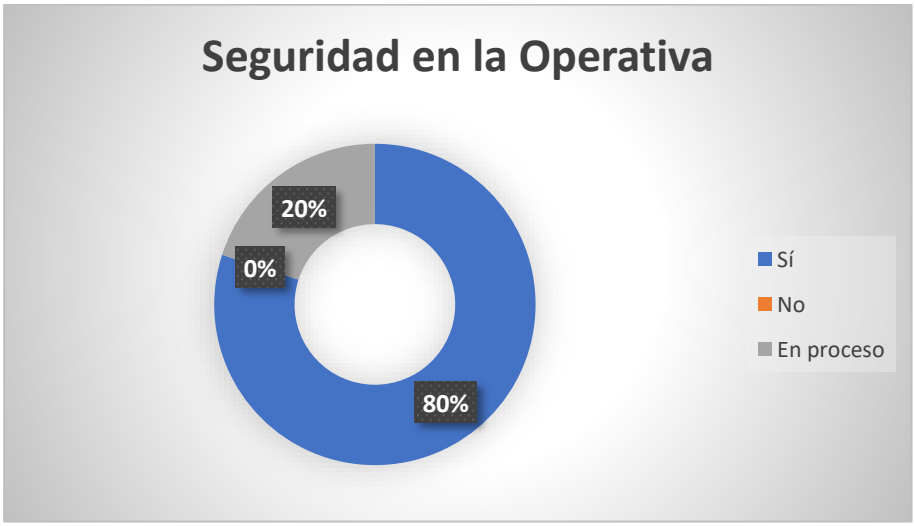

Gráfico 15. Dominio. Seguridad en la Operativa. Fuente: Autoría Propia.

3.8.9 Dominio Seguridad en las Telecomunicaciones

Según el Gráfico N.º 16, basado en los resultados obtenidos en el dominio en las Telecomunicaciones, se puede observar que el 80% de las medidas de seguridad en las telecomunicaciones en la Cooperativa de Chunchi han sido implementadas de manera satisfactoria. Sin embargo, un 20% de las respuestas indican que algunas de estas medidas aún están en proceso de implementación. Este resultado resalta la importancia de completar la implementación de todas las medidas de seguridad en las telecomunicaciones para garantizar la protección de la información que se transmite y recibe a través de las redes de la organización.

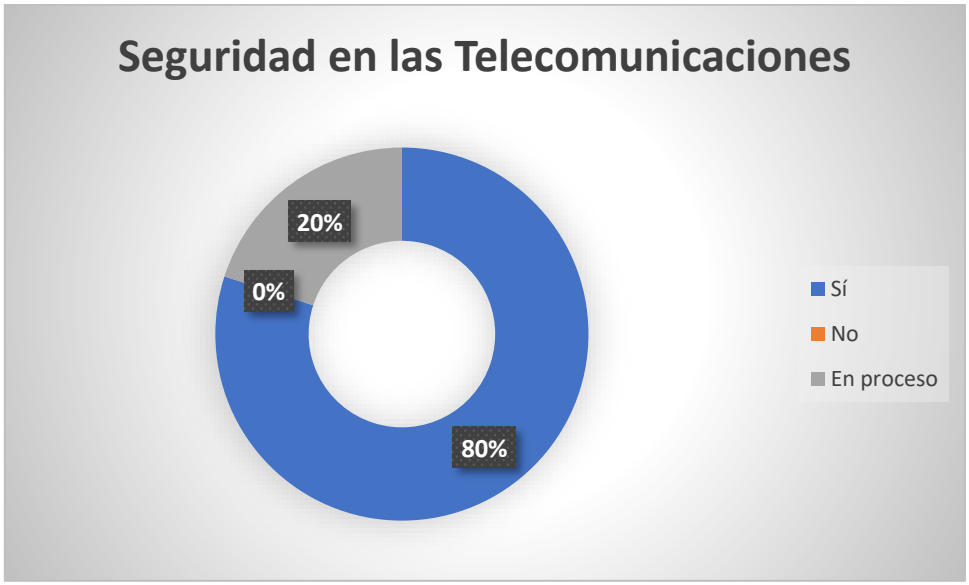

Gráfico 16. Dominio Seguridad en las Telecomunicaciones. Fuente: Autoría Propia.

3.8.10 Dominio Adquisición, desarrollo y mantenimiento de los sistemas de información

De acuerdo con los resultados obtenidos en el dominio Adquisición, desarrollo y mantenimiento de los sistemas de información, se puede concluir que el 80% de las prácticas relacionadas con la adquisición, desarrollo y mantenimiento de sistemas en la Cooperativa de Chunchi han sido implementadas de manera adecuada. No obstante, un 20% de las respuestas indican que algunas de estas prácticas aún están en proceso de implementación. Este resultado subraya la importancia de completar la implementación de todas las medidas necesarias para

garantizar que los sistemas de información sean seguros y estén alineados con los objetivos de seguridad de la organización como se muestra en el gráfico N.º 17.

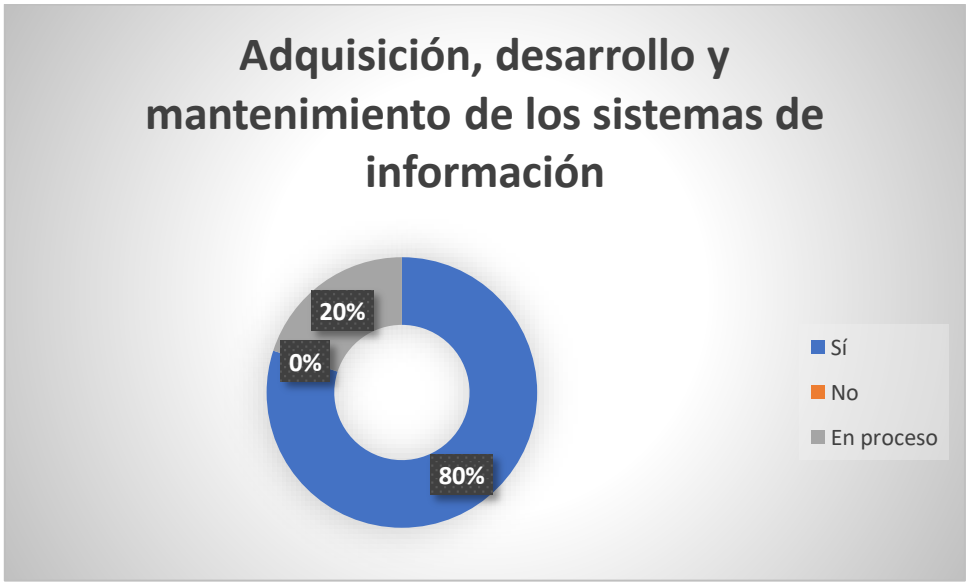

Gráfico 17. Adquisición, desarrollo y mantenimiento de los sistemas de información. Fuente: Autoría Propia.

3.8.10 Dominio Relaciones con suministradores

Refiriéndonos a los resultados obtenidos en el gráfico N.º 18, en el dominio Relaciones con Suministradores, se observa que el 80% de las prácticas relacionadas con la gestión de relaciones con los suministradores en la Cooperativa de Chunchi están adecuadamente implementadas. Sin embargo, un 20% de las respuestas indican que algunas de estas prácticas aún están en proceso de implementación. Este resultado pone de relieve la necesidad de completar estos procesos para asegurar que todas las relaciones con los suministradores estén alineadas con los estándares de seguridad de la información de la organización.

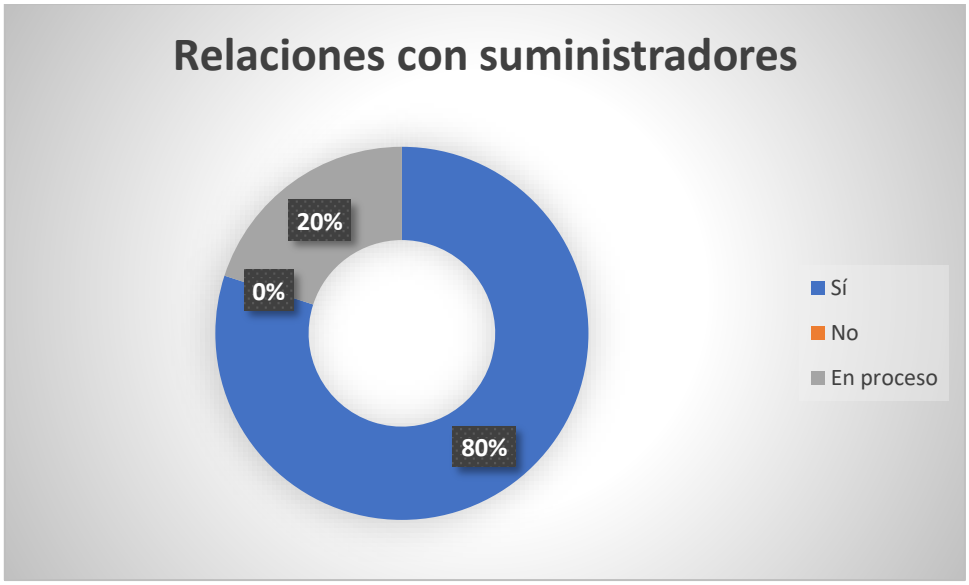

Gráfico 18. Dominio Relaciones con suministradores. Fuente: Autoría Propia.

3.8.11 Dominio Gestión de incidentes en la Seguridad de la Información

Como se muestra en el grafico N.º 19, que la Cooperativa de Chunchi presenta un cumplimiento parcial en varias áreas clave. El 33% de las preguntas fueron respondidas afirmativamente, lo que indica que existen procedimientos documentados para la gestión de incidentes de seguridad, un paso fundamental para responder adecuadamente a los incidentes. Sin embargo, un 33% de las respuestas indican que no se están implementando ni operando los controles necesarios para gestionar los riesgos de seguridad de la información, lo que expone a la organización a vulnerabilidades significativas. Además, el 33% de cumplimiento parcial refleja que no se está llevando a cabo un monitoreo y revisión regular de los procesos de seguridad, lo cual es crucial para la detección temprana la respuesta efectiva a los incidentes. Es esencial mejorar la implementación y el monitoreo para fortalecer la gestión de incidentes en la cooperativa.

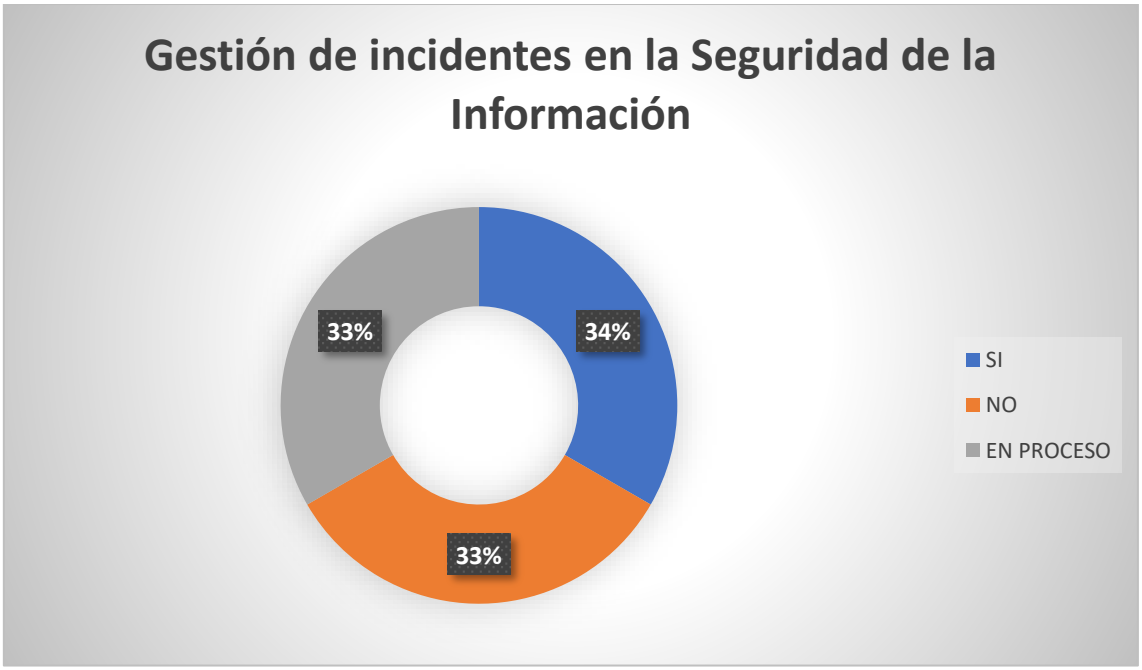

Gráfico 19. Dominio Gestión de incidentes en la Seguridad de la Información. Fuente: Autoría Propia.

3.8.12 Dominio Cumplimiento

En el gráfico N.º 20 se presenta los resultados obtenidos en el dominio Cumplimiento, se observa que el 60% de las prácticas y procedimientos relacionados con el cumplimiento en la Cooperativa de Chunchi están implementados de manera adecuada. Sin embargo, un 40% de las respuestas indican que algunas de estas prácticas aún se encuentran en proceso de implementación. Este resultado subraya la importancia de completar estos procesos para asegurar que la organización cumpla con todas las leyes, regulaciones y normativas aplicables en materia de seguridad de la información.

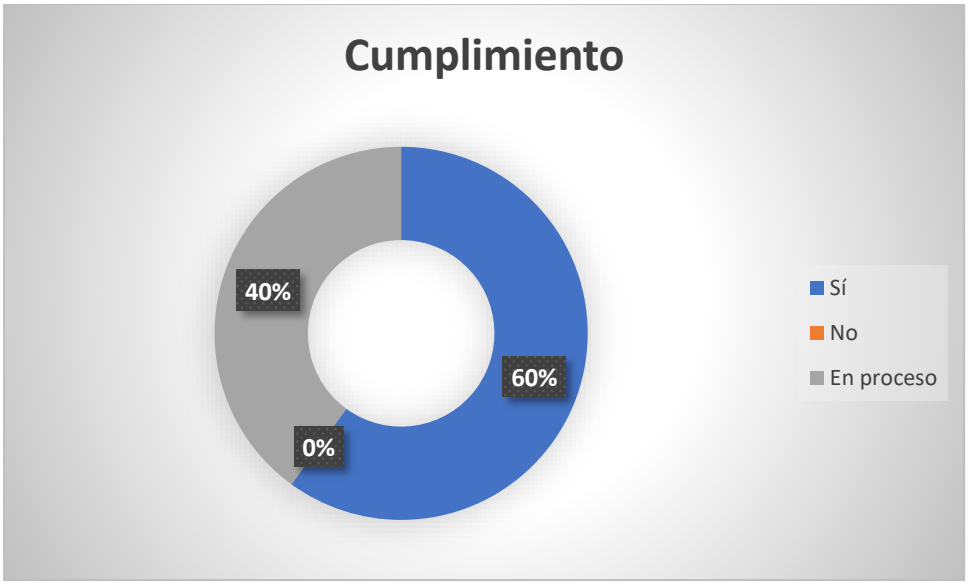

Gráfico 20. Dominio Cumplimiento. Fuente: Autoría Propia.

3.9 Análisis general de la encuesta norma ISO 27001:2013

La encuesta relacionada con la norma ISO 27001:2013 en la Cooperativa de Ahorro y Crédito Chunchi pone de manifiesto una mezcla de logros y desafíos en la gestión de la seguridad de la información. Por un lado, se ha observado un compromiso sólido por parte de la alta dirección, lo cual es fundamental para el éxito de cualquier Sistema de Gestión de Seguridad de la Información (SGSI). Este liderazgo ha permitido que se tomen medidas significativas en la implementación de políticas y procedimientos de seguridad, lo que demuestra una base bien establecida para la protección de la información. Sin embargo, a pesar de estos avances, es evidente que la organización enfrenta retos considerables que deben ser abordados con urgencia.

Uno de los aspectos más críticos es la planificación, donde se ha identificado una falta de rigor en la formulación y ejecución de planes que aborden los riesgos de seguridad de manera integral. Esta deficiencia en la planificación afecta la capacidad de la cooperativa para anticipar y mitigar posibles amenazas, lo que podría comprometer la integridad y disponibilidad de la información. De igual manera, la mejora continua, un pilar fundamental para la sostenibilidad y evolución del SGSI, no ha sido implementada de manera consistente. Esta falta de un enfoque

sistemático en la mejora continua sugiere que la organización podría estar perdiendo oportunidades para fortalecer sus controles de seguridad y adaptarse a las nuevas amenazas.

La ejecución operativa de las medidas de seguridad también presenta inconsistencias. La gestión eficaz de la seguridad de la información depende en gran medida de la correcta implementación de operaciones diarias que aseguren la protección de los activos informáticos y la confidencialidad de los datos. En la Cooperativa de Ahorro y Crédito Chunchi, estas operaciones no han sido implementadas de manera uniforme, lo que genera vulnerabilidades que podrían ser explotadas si no se corrigen a tiempo. No obstante, es importante reconocer que los recursos y actividades de soporte están relativamente bien dotados, lo que ofrece una base sólida sobre la cual se pueden construir mejoras adicionales.

3.10 Análisis general de la encuesta de la guía de buenas prácticas ISO27002:2013

La encuesta relacionada con la norma ISO/IEC 27002:2013 en la Cooperativa de Ahorro y Crédito Chunchi proporciona una visión detallada de cómo la organización está implementando y gestionando sus controles de seguridad de la información. A partir de los resultados, se observa que la cooperativa ha hecho avances importantes en la adopción de varias prácticas recomendadas por la norma, especialmente en áreas clave como el control de accesos, el cifrado, y la gestión de activos. Estas medidas son fundamentales para asegurar la protección de la información crítica y mantener la integridad, confidencialidad y disponibilidad de los datos.

Sin embargo, el análisis también revela que existen aspectos que requieren mayor atención. A pesar de que una buena parte de los controles están en proceso de implementación, todavía hay un número significativo de áreas en las que las prácticas no se han completado o necesitan ser fortalecidas. Por ejemplo, la seguridad física y ambiental, y la gestión de relaciones con suministradores, son dominios donde aún se perciben debilidades, lo que podría comprometer

la capacidad de la organización para proteger su infraestructura y gestionar adecuadamente sus relaciones con terceros. Estas brechas sugieren que, aunque la cooperativa está en el camino correcto, aún necesita consolidar y finalizar la implementación de varios controles de seguridad.

Además, el enfoque en la mejora continua y la adaptación a nuevas amenazas es otro aspecto crítico destacado por la encuesta. La norma ISO/IEC 27002:2013 enfatiza la necesidad de no solo implementar controles de seguridad, sino también de revisar y mejorar constantemente estos controles para enfrentar los cambios en el entorno de seguridad. En este sentido, la cooperativa muestra un progreso en ciertas áreas, pero la necesidad de un enfoque más proactivo y sistemático en la mejora continua es evidente. Esto implicaría no solo finalizar la implementación de los controles pendientes, sino también asegurar que estos controles sean regularmente evaluados y actualizados para mantenerse alineados con las mejores prácticas y responder eficazmente a las amenazas emergentes.

3.11 Selección de la metodología

Luego de analizar las metodologías de análisis de riesgo MAGERIT, NIST SP 800:30, CRAMM e ISO/IEC 27005 a través de una matriz comparativa, se ha seleccionado MAGERIT para su implementación. La elección de MAGERIT se justifica por su enfoque exhaustivo en la identificación y gestión de riesgos inherentes a los sistemas de información, su capacidad para realizar evaluaciones tanto cualitativas como cuantitativas, y su empleo de escenarios prácticos que permiten una comprensión detallada de la naturaleza y magnitud de los riesgos. Además, la metodología MAGERIT cuenta con un reconocimiento considerable del Consejo Superior de Administración Electrónica de España, y las numerosas herramientas y documentación que la acompañan refuerzan su aplicabilidad y robustez. Este conjunto de ventajas hace que MAGERIT sea la opción más adecuada para llevar a cabo un análisis de riesgo efectivo y alineado con los estándares internacionales en la presente investigación.

CAPITULO IV

4. PROPUESTA

4.1. Tema

"Propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Chunchi, del Cantón Chunchi, bajo la norma ISO 27001"

4.2. Justificación

La información manejada por la Cooperativa de Ahorro y Crédito Chunchi es crucial para garantizar la integridad, seguridad, confiabilidad y accesibilidad de los datos para sus usuarios. No obstante, esta información está expuesta a riesgos de alteración o acceso no autorizado, lo que subraya la necesidad de implementar sólidas medidas de seguridad informática.

Actualmente, en la Cooperativa de Ahorro y Crédito Chunchi no se han formalizado normas ni metodologías específicas para la seguridad de la información, dejando los sistemas de información y comunicación vulnerables. En respuesta a esta situación, se propone desarrollar un manual de políticas de seguridad de la información basado en la norma ISO 27001 y apoyado por las buenas prácticas de la ISO 27002, las cuales ofrecen una amplia gama de estrategias para la protección efectiva de la información.

Esta propuesta es factible, dado que se dispone de los recursos necesarios para recopilar la información pertinente. Además, se cuenta con el apoyo del departamento de TI y con las herramientas adecuadas para iniciar las actividades planificadas.

4.3. Antecedentes de la Empresa

La Cooperativa de Ahorro y Crédito Chunchi Ltda. surge el 20 de febrero del 2010 gracias a la visión de un grupo de 11 personas, entre ellos emigrantes retornados y habitantes de Chunchi, quienes, motivados por el deseo de generar oportunidades para los sectores más vulnerables y

marginados por las entidades financieras, decidieron fundar una institución que promoviera una sociedad más justa y solidaria en el cantón Chunchi. Con un capital inicial de $40,000 y el respaldo de once socios fundadores, la cooperativa obtuvo su permiso de funcionamiento, priorizando desde sus inicios al ser humano sobre el capital (Cooperativa de Ahorro y Crédito Chunchi Ltda., 2019).

4.4. Objetivos del "Manual de Políticas"

4.4.1. Objetivo General

"Desarrollar un Manual de Políticas de Seguridad De Información para la cooperativa de Ahorro y Crédito de la Cooperativa de Chunchi"

4.4.2. Objetivos Específicos

- Realizar un inventario detallado de los activos de información críticos de la Cooperativa de Ahorro y Crédito Chunchi.
- Evaluar y priorizar los riesgos asociados a estos activos, considerando amenazas y vulnerabilidades.
- Calcular los niveles de riesgo aplicando la metodología MAGERIT.
- Desarrollar e implementar un plan de control para mitigar los riesgos identificados en los activos de información.

Desarrollo de la Propuesta

4.5. Determinación del riesgo con MARGERIT

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un enfoque sistemático diseñado para identificar, analizar y gestionar los riesgos asociados a los sistemas de información. Este método es ampliamente reconocido por su capacidad de evaluar tanto riesgos cualitativos como cuantitativos, lo que facilita a las organizaciones tomar decisiones informadas para proteger sus activos (Romo Sañicela & Bojorque Chasi, 2023).

Las fases de la metodología MARGERIT son las siguientes:

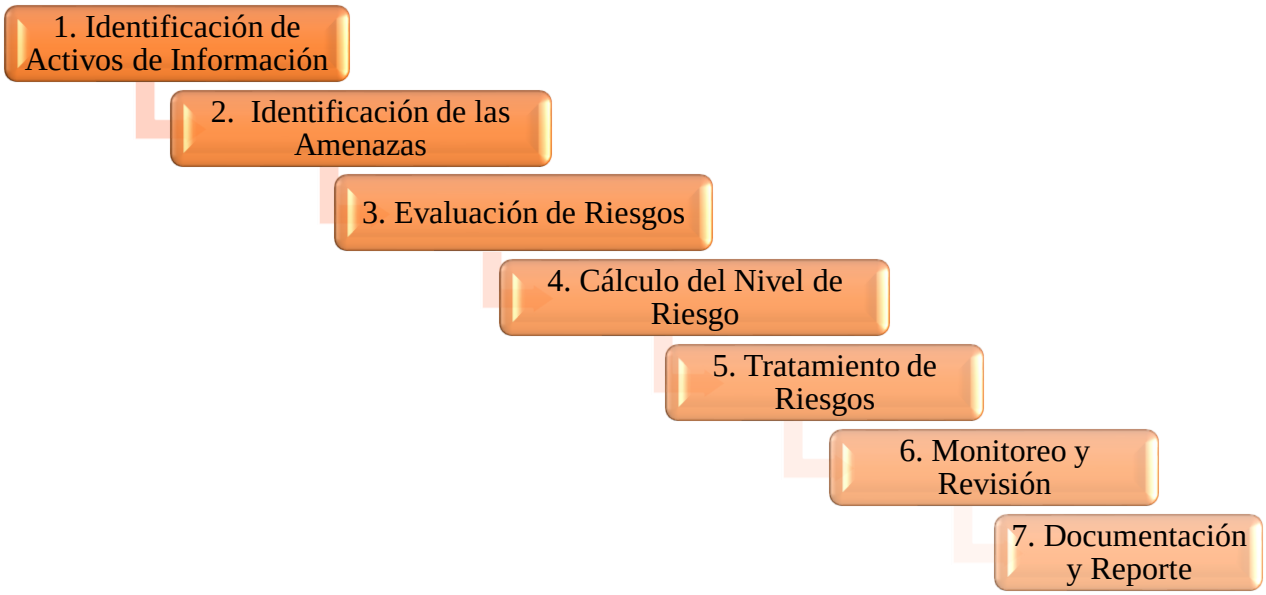

Ilustración 6. Fases de la metodología MARGERIT. Fuente: Autoría Propia.

La metodología MAGERIT se enfoca en la gestión de riesgos para proteger los activos de información. Sus fases incluyen: 1. Identificación de Activos de Información , donde se reconocen los recursos críticos; 2. Identificación de Amenazas , evaluando

posibles riesgos; 3. Evaluación de Riesgos , analizando impacto y probabilidad; 4. Cálculo del Nivel de Riesgo , priorizando los más críticos; 5. Tratamiento de Riesgos , aplicando medidas para mitigarlos; 6. Monitoreo y Revisión , verificando continuamente la efectividad de los controles; y 7. Documentación y Reporte , registrando todo el proceso para asegurar la trazabilidad y toma de decisiones informadas. Esto garantiza la protección de la información en la organización.

4.5.1. Identificación de Activos de Información

La identificación de activos de información es un proceso crítico en la gestión de la seguridad, que permite catalogar y valorar los recursos clave de la organización, tales como datos, sistemas e infraestructuras. En la Cooperativa de Ahorro y Crédito Chunchi, este proceso es fundamental para establecer un SGSI efectivo, facilitando el análisis de riesgos y la implementación de controles para garantizar la confidencialidad, integridad y disponibilidad de la información.

Los activos de información se detallan en la siguiente tabla:

Tabla 4. Activos de información. Fuente: Autoría Propia.

ID ACTIVO	Tipo de Activo	Activo
1	Software /Aplicaciones informáticas	- App Coac Chunchi - Conexus - Informix - Virtualcop - JPCSystem - Facilito - Financop - SPI BANCO CENTRAL

		- Credit report - SIALAFT - UFE
2	Hardware	- Servidor principal - Computadoras de escritorio - Switch - Router - Teléfono IP
3	Datos/Información	- BBDD de clientes - Documentación financiera y contable
4	Claves criptográficas	- Claves de encriptación de los servidores - Encriptación de Huella - Correos
5	Redes de comunicaciones	- Red interna de la cooperativa - WAN - LAN
6	Sistemas de Información	- SAGA
7	Personal	- Jefe de TI - Ayudantes de TI

8	Equipamiento auxiliar	- Equipos de respaldo de energía (UPS) - Impresoras y escáneres - Cámaras de vigilancia
9	Soportes de información	- Discos duros externos para copias de seguridad - Archivos físicos de contratos
10	Servicios	- Servicio de alojamiento en la nube - Créditos - Ahorros - Transferencias

4.5.2. Valoración de los activos

La valoración de los activos de información es crucial para establecer su relevancia dentro de una organización, considerando diferentes aspectos o dimensiones. La metodología MAGERIT define varias dimensiones, tales como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, que permiten evaluar el impacto de la pérdida o afectación de cada activo. Esta valoración puede realizarse tanto de forma cuantitativa, asignando valores numéricos, como cualitativa, utilizando escalas de niveles. Para la Cooperativa de Ahorro y Crédito Chunchi, el análisis de riesgos se enfocará en las dimensiones clave de disponibilidad, integridad y confidencialidad, dado que son esenciales para la protección efectiva de la información.

Tabla 5. Valoración de los activos. Fuente: Autoría Propia.

Confidencialidad	Integridad	Disponibilidad
Garantizar que la información sea accesible únicamente para aquellos usuarios autorizados.	Asegurar la exactitud y completitud de la información y de los procesos relacionados con su manejo.	Asegurar que la información esté disponible para los usuarios autorizados cuando sea necesario.

La evaluación de los activos se realizará tomando como base la escala especificada. Este proceso consistirá en analizar cada activo de manera individual y asignarles un valor conforme a los criterios definidos en dicha tabla. Tabla No 6.

Tabla 6. Escala de la valoración de los Activos de información. Fuente: (Amutio Gómez, Candau , & Mañas, 2012)

Valor			Impacto para la organización
0	Muy Bajo	MB	Daño extremadamente grave
1-4	Baja	B	Daño muy Grande a la Organización
5-8	Medio	M	Daño Grave a la Organización
9-12	Alto	A	Daño Importante a la Organización
13-15	Muy Alto	MA	Daño Menor a la Organización

En la tabla Nro. 7 se muestran las puntuaciones asignadas a cada activo, basadas en la evaluación de los criterios de confidencialidad, integridad y disponibilidad. Esta evaluación es crucial para orientar las decisiones en la gestión de riesgos y establecer prioridades en la implementación de medidas de seguridad, ajustadas a las características y requerimientos de cada activo.

Tabla 7. Puntuación de los activos. Fuente: Autoría Propia.

Tipo de activo	**Código**	**Activos**	**Valoración**			
			Disponibilidad	**Integridad**	**Confidencial**	**Total/ 15**
[SW] Software /Aplicaciones informáticas	1	App Coac Chunchi	5	5	5	**15**
	2	Conexus	5	5	5	**15**
	3	Informix	4	5	5	**14**
	4	VirtualCop	4	4	4	**12**
	5	JPCSystem	4	4	4	**12**
	6	Facilito	4	3	5	**12**
	7	Financop	4	4	5	**13**
	8	SPI BANCO CENTRAL	5	5	5	**15**
	9	Credit report	5	5	5	**15**
	10	SIALAFT - UFE	4	3	5	**12**
[HW] Hardware	11	Servidor principal	4	3	4	11

	12	Computadoras de escritorio	5	4	4	13
	13	Switch	3	3	3	9
	14	Router	4	3	3	10
	15	Teléfono IP	3	2	2	7
	16	Mouse	5	1	1	7
	17	Laptop HP	4	4	5	13
	18	Teclado	4	3	2	9
[D] Datos/Información	19	BBDD de clientes	5	5	5	15
	20	Documentación financiera y contable	5	5	4	15
[K] Claves criptográficas	21	Claves de encriptación de los servidores	5	5	4	14
	22	Encriptación de Huella	5	5	4	14
	23	Encriptación de Correos	4	4	4	12

	24	Respaldos	5	5	4	14
[COM] Redes de comunicaciones	25	Red interna de la cooperativa	5	5	4	14
	26	WAN	5	5	5	15
	27	LAN	5	5	5	15
[SI] Sistemas de Información	28	SAGA	5	5	5	15
[P] Personal	29	Jefe de TI	5	5	5	15
	30	Ayudantes de TI	5	5	5	15
[AUX] Equipamiento auxiliar	31	Equipos de respaldo de energía (UPS)	5	3	5	13
	33	Impresoras y escáneres	2	2	3	7
	34	Cámaras de vigilancia	4	4	4	12
	35	Servidor	5	5	5	15

[Media] Soportes de información	36	Discos duros externos para copias de seguridad	5	5	5	15
	37	Archivos físicos de contratos	4	4	4	12
[S] Servicios	38	Servicio de alojamiento en la nube	5	5	5	15
	39	Créditos	5	5	5	15
	40	Ahorros	5	5	5	15
	41	Transferencias	5	5	5	15
	42	Conexus	4	5	4	13

4.5.3. Identificación de las Amenazas

Las amenazas, ya sean naturales o provocadas por el ser humano, tienen la capacidad de afectar significativamente los activos de información de una organización. Estos activos son fundamentales para garantizar el correcto funcionamiento de la entidad, y cualquier daño que sufran podría resultar en interrupciones operativas, pérdidas financieras, y

deterioro de la confianza de los clientes. Además, las amenazas no solo impactan los activos tecnológicos, sino que también pueden comprometer la estabilidad y la reputación de la organización en su conjunto. Por lo tanto, es crucial identificar y gestionar estas amenazas de manera adecuada. En esta sección, se presentarán las amenazas identificadas mediante la metodología MAGERIT, aplicadas específicamente al análisis de riesgo del departamento de informática de la Cooperativa de Ahorro y Crédito Chunchi.

Tabla 8. Amenazas según el libro de MAGERIT. Fuente: (Amutio Gómez, Candau , & Mañas, 2012)

CATÁLOGO DE AMENAZAS	
Tipo de amenazas	**Amenazas**
[N] Desastres Naturales	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales
[I] DE ORIGEN INDUSTRIAL	[I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación mecánica [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales [I.10] Degradación de los soportes de almacenamiento de la información [I.11] Emanaciones electromagnéticas
[E] Errores y Fallos no Intencionados	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.8] Difusión de software dañino [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información

	[E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.28] Indisponibilidad del personal
[A] Ataques Intencionados	[A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información [A.22] Manipulación de programas [A.23] Manipulación de los equipos [A.24] Denegación de servicio [A.25] Robo [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.29] Extorsión [A.30] Ingeniería social (picaresca)

4.5.4. Evaluación de Impacto y Probabilidad

valuar el impacto y la probabilidad de las amenazas es un componente esencial en el análisis de riesgos. Este proceso comienza con la identificación del daño potencial que una amenaza podría causar a un activo en caso de que se concrete. Esta evaluación considera cómo la amenaza podría comprometer la confidencialidad, integridad y disponibilidad de los activos. Luego, se analiza la probabilidad de que cada amenaza ocurra, teniendo en cuenta factores como la presencia de vulnerabilidades, la eficacia de las medidas de seguridad existentes y el entorno en el que opera la organización. Al combinar estos dos elementos ¨impacto y probabilidad¨ se determina el nivel de riesgo asociado con cada amenaza. Este análisis es fundamental para priorizar los riesgos y tomar decisiones informadas sobre las medidas de mitigación necesarias.

La metodología MAGERIT propone una escala de evaluación del impacto, que se clasifica de 1 a 5, como se presenta en la siguiente Ilustración:

Tabla 9. Calificación del IMPACTO. Fuente: (Amutio Gómez, Candau , & Mañas, 2012)

IMPACTO		DESCRIPCION
Bajo	1	El impacto es manejable y no afecta significativamente a la organización.
Medio	2	El impacto podría tener un efecto significativo en la organización, pero es probable que no amenace la supervivencia de la misma.
Alto	3	El impacto es severo y podría amenazar la supervivencia de la organización.
Muy alto	4	El impacto es extremadamente grave, muy probablemente amenaza la supervivencia de la organización.
Catastrófico	5	El impacto es tan severo que amenaza directamente la supervivencia de la organización.

La utilización de esta escala permite a las organizaciones evaluar de manera precisa el impacto que las diferentes amenazas podrían tener sobre sus sistemas de información, lo que facilita la priorización en la gestión de riesgos. Para determinar la probabilidad de que una amenaza afecte a un activo específico, se realiza un análisis

exhaustivo. Esta probabilidad se clasifica en una escala del 1 al 5, donde un valor de 1 indica una probabilidad extremadamente baja, y un valor de 5 sugiere una probabilidad muy alta, tal como se ilustra a continuación:

Tabla 10. Escala de calificación de la probabilidad. Fuente: (Amutio Gómez, Candau , & Mañas, 2012)

PROBABILIDAD		DESCRIPCION
Baja	1	Es posible que el riesgo se materialice, pero las circunstancias que lo desencadenarían son improbables.
Media	2	Existen circunstancias que podrían desencadenar el riesgo y es relativamente posible que se produzcan.
Alta	3	Es probable que el riesgo se materialice si no se toman medidas para evitarlo.
Muy alto	4	Es casi seguro que el riesgo se materialice si no se toman medidas para evitarlo.

4.5.5. Cálculo del riesgo

El cálculo del riesgo se lleva a cabo mediante una operación matemática simple que implica multiplicar la probabilidad de que ocurra una amenaza por el impacto que tendría si se materializara. El resultado de esta multiplicación produce un valor que se sitúa en un rango de 1 a 25, lo que refleja la severidad del riesgo. A continuación, en la Tabla 10, se presenta una matriz que establece los intervalos correspondientes para determinar el nivel de riesgo, permitiendo a la organización clasificar y priorizar cada riesgo de acuerdo a su gravedad.

Tabla 11. Escala de calificación de la probabilidad. Fuente: (Amutio Gómez, Candau , & Mañas, 2012).

RIESGO		DESCRIPCION
Riesgo Mínimo	1-5	El riesgo es muy bajo y puede ser tolerable sin necesidad de aplicar medidas de mitigación inmediatas
Riesgo Bajo	6-10	El riesgo es bajo, pero deberían considerarse medidas de mitigación para reducir aún más el riesgo.
Riesgo Medio	11-15	El riesgo es moderado y se requieren medidas de mitigación para reducir el riesgo a un nivel aceptable.
Riesgo Alto	16-20	El riesgo es alto y se requieren medidas de mitigación urgentes para reducir el riesgo a un nivel aceptable.
Riesgo Maximo	21-25	El riesgo es muy alto y se requiere una acción inmediata y prioritaria para mitigar el riesgo.

Matriz de Riesgo Metodología MAGERIT

La Matriz de Riesgo en la metodología MAGERIT proporciona una herramienta fundamental para la evaluación de la seguridad de los activos. En primer lugar, la matriz clasifica cada activo según tres dimensiones clave: Disponibilidad, Integridad y Confidencialidad. Cada una de estas dimensiones recibe una calificación específica, y la suma de estas puntuaciones ofrece un total que puede alcanzar hasta 15 puntos. Este total refleja la relevancia y la importancia relativa de cada activo en el contexto de la seguridad de la información.

A continuación, se identifica un catálogo de amenazas potenciales para cada activo. Cada amenaza se evalúa en términos de impacto y probabilidad, y al combinar estas dos evaluaciones mediante su multiplicación, se obtiene un valor de riesgo. Este valor cuantitativo proporciona una medida precisa del nivel de amenaza que cada situación representa para el activo, facilitando así una gestión más efectiva y priorizada de los riesgos.

Tabla 12. Matriz de Riesgo. Fuente: Autoría Propia.

Tipo de activo	Código	Activos	Valoración				Catálogo de Amenazas	Cálculo del Riesgo		
			Disponibilidad	Integridad	Confidencial	Total/15	Amenazas	Impacto	Probabilidad	Riesgo
[SW] Software /Aplicaciones informáticas	1	App Coac Chunchi	5	5	5	**15**	[E.19] Fugas de información	3	5	**15**
							[E.8] Difusión de software dañino	4	4	**16**
							[A.11] Acceso no autorizado	4	5	**20**
							[A.15] Modificación deliberada de la información	3	5	**12**
							[A.24] Denegación de servicio	4	3	**12**
							[A.30] Ingeniería social (picaresca)	4	4	**16**
	2	Conexus	5	5	5	**15**	[I.6] Corte del suministro eléctrico	2	5	**10**
							[E.8] Difusión de software dañino	4	4	**16**
							[E.19] Fugas de información	3		**15**
							[A.11] Acceso no autorizado	4	4	**16**
							[A.15] Modificación deliberada de la información	3	4	**12**
							[A.24] Denegación de servicio	3	4	**12**

							[A.30] Ingeniería social (picaresca)	4	4	**16**
	3	Informix	4		5	5	**14**	[E.8] Difusión de software dañino	4	4	**16**
								[E.19] Fugas de información	5	2	**10**
								[A.5] Suplantación de la identidad del usuario	3	4	**12**
								[A.11] Acceso no autorizado	2	5	**10**
								[A.24] Denegación de servicio	4	3	**12**
	4	VirtualCop	4		4	4	**12**	[I.6] Corte del suministro eléctrico	2	5	**10**
								[E.8] Difusión de software dañino	4	4	**16**
								[E.19] Fugas de información	3	5	**15**
								[A.11] Acceso no autorizado	4	2	**8**
								[A.15] Modificación deliberada de la información	2	5	**10**
								[A.24] Denegación de servicio	3	4	**12**
	5	JPCSystem	4		4	4	**12**	[I.1] Fuego	2	4	**8**
								[I.6] Corte del suministro eléctrico	2	5	**10**
								[E.4] Errores de configuración	4	3	**12**
								[E.8] Difusión de software dañino	4	4	**16**

							[E.15] Alteración accidental de la información	4	3	**12**
							[E.19] Fugas de información	5	2	**10**
							[A.11] Acceso no autorizado	3	4	**12**
							[A.15] Modificación deliberada de la información	2	5	**10**
							[A.23] Manipulación de los equipos	3	3	**9**
	6	Facilito	4		3	5	**12**	[I.6] Corte del suministro eléctrico	2	5	**10**
								[E.1] Errores de los usuarios	2	5	**10**
								[E.8] Difusión de software dañino	4	4	**16**
								[E.21] Errores de mantenimiento/actualización de software	3	5	**15**
								[A.11] Acceso no autorizado	3	4	**12**
	7	Financop	4		4	5	**13**	[I.6] Corte del suministro eléctrico	2	4	**8**
								[I.8] Fallo de servicios de comunicaciones	4	3	**12**
								[E.8] Difusión de software dañino	4	4	**16**
								[E.19] Fugas de información	2	5	**10**
								[A.11] Acceso no autorizado	2	5	**10**
								[A.25] Robo	3	3	**9**
	8	SPI BANCO CENTRAL	5		5	5	**15**	[I.6] Corte del suministro eléctrico	2	4	**8**
								[E.4] Errores de configuración	4	3	**12**

							[E.14] Escapes de información	3	4	**12**
							[A.5] Suplantación de la identidad del usuario	3	4	**12**
							[A.15] Modificación deliberada de la información	3	3	**9**
							[A.30] Ingeniería social (picaresca)	5	2	**10**
	9	Credit report	5		5	5	**15**	[I.6] Corte del suministro eléctrico	2	5	**10**
								[I.7] Condiciones inadecuadas de temperatura o humedad	3	2	**6**
								[E.8] Difusión de software dañino	4	4	**16**
								[E.19] Fugas de información	2	5	**10**
								[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	**12**
								[E.20] Vulnerabilidades de los programas (software)	3	4	**12**
								[A.11] Acceso no autorizado	3	3	**9**
								[A.24] Denegación de servicio	2	5	**10**
								[A.15] Modificación deliberada de la información	2	5	**10**
	10	SIALAFT - UFE	4		3	5	**12**	[I.6] Corte del suministro eléctrico	2	5	**10**

								[I.8] Fallo de servicios de comunicaciones	3	4	**12**
								[E.8] Difusión de software dañino	4	2	**8**
								[E.19] Fugas de información	3	3	**9**
								[E.20] Vulnerabilidades de los programas (software)	3	4	**12**
[HW] Hardware	11	Servidor principal	4		3	4	11	[I.1] Fuego	2	4	**8**
								[I.6] Corte del suministro eléctrico	2	5	**10**
								[E.8] Difusión de software dañino	4	4	**16**
								[A.6] Abuso de privilegios de acceso	3	5	**15**
								[A.11] Acceso no autorizado	3	4	**12**
								[A.24] Denegación de servicio	3	3	**9**
								[A.15] Modificación deliberada de la información	3	3	**9**
	12	Computadoras de escritorio	5		4	4	13	[N.1] Fuego	3	3	**9**
								[N.2] Daños por agua	3	2	**6**
								[I.8] Fallo de servicios de comunicaciones	3	3	**9**
								[E.8] Difusión de software dañino	4	4	**16**
								[E.19] Fugas de información	3	4	**12**
								[E.23] Errores de mantenimiento /	3	3	**9**

							actualización de equipos (hardware)		
							[E.25] Pérdida de equipos	4	2	**8**
							[A.11] Acceso no autorizado	4	3	**12**
							[A.24] Denegación de servicio	2	5	**10**
							[A.15] Modificación deliberada de la información	4	2	**8**
	13	4 switch	3	3	3	9	[I.8] Fallo de servicios de comunicaciones	3	3	**9**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	**8**
							[E.24] Caída del sistema por agotamiento de recursos	3	4	**12**
							[A.24] Denegación de servicio	3	4	**12**
							[A.11] Acceso no autorizado	3	5	**15**
							[A.15] Modificación deliberada de la información	2	4	**8**
	14	Router	4	3	3	10	[N.1] Fuego	2	5	**10**
							[I.6] Corte del suministro eléctrico	3	4	**12**
							[E.24] Caída del sistema por agotamiento de recursos	3	4	**12**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	2	**8**

							[A.11] Acceso no autorizado	3	4	**12**
							[A.24] Denegación de servicio	3	3	**9**
							[A.15] Modificación deliberada de la información	4	2	**8**
15	Teléfono IP	3		2	2	7	[N.1] Fuego	2	5	**10**
							[E.8] Difusión de software dañino	3	3	**9**
							[E.24] Caída del sistema por agotamiento de recursos	2	5	**10**
							[A.11] Acceso no autorizado	3	3	**9**
							[A.14] Interceptación de información (escucha)	2	5	**10**
							[A.24] Denegación de servicio	3	2	**6**
16	Mouse	5		1	1	7	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	**6**
							[E.25] Pérdida de equipos	2	2	**4**
							[A.15] Modificación deliberada de la información	2	3	**6**
							[A.23] Manipulación de los equipos	2	2	**4**
17	Laptop HP	4		4	5	13	[N.1] Fuego	2	4	**8**
							[E.20] Vulnerabilidades de los programas (software)	4	3	**12**
							[E.23] Errores de mantenimiento /	4	2	**8**

							actualización de equipos (hardware)			
							[A.11] Acceso no autorizado	4	4	**16**
							[A.14] Interceptación de información (escucha)	3	5	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.25] Robo	5	2	**10**
	18	Teclado	4	3	2	9	[N.1] Fuego	2	4	**8**
							[E.25] Pérdida de equipos	2	2	**4**
							[A.15] Modificación deliberada de la información	3	3	**9**
							[A.23] Manipulación de los equipos	3	3	**9**
							[A.24] Denegación de servicio	2	3	**6**
[D] Datos/Información	19	BBDD de clientes	5	5	5	15	[E.20] Vulnerabilidades de los programas (software)	4	4	**16**
							[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	**12**
							[A.11] Acceso no autorizado	3	5	**15**
							[A.14] Interceptación de información (escucha)	3	3	**9**
							[A.15] Modificación deliberada de la información	3	5	**15**
							[A.24] Denegación de servicio	2	4	**8**
			5	5	4	15	[N.1] Fuego	2	4	**8**

	20	Documentación financiera y contable					[E.15] Alteración accidental de la información	3	4	**12**
							[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	**12**
							[A.11] Acceso no autorizado	3	5	**15**
							[A.15] Modificación deliberada de la información	3	5	**15**
[K] Claves criptográficas	21	Claves de encriptación de los servidores	5		5	4	14	[E.20] Vulnerabilidades de los programas (software)	3	5	**15**
								[A.11] Acceso no autorizado	3	5	**15**
								[A.15] Modificación deliberada de la información	5	2	**10**
								[A.24] Denegación de servicio	4	2	**8**
	22	Encriptación de Huella	5		5	4	14	[I.6] Corte del suministro eléctrico	4	2	**8**
								[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	**12**
								[E.20] Vulnerabilidades de los programas (software)	3	5	**15**
								[E.21] Errores de mantenimiento / actualización de programas (software)	3	5	**15**
								[A.11] Acceso no autorizado	3	5	**15**

							[A.15] Modificación deliberada de la información	2	5	**10**
	23	Encriptación de Correos	4		4	4	12	[E.20] Vulnerabilidades de los programas (software)	3	5	**15**
								[E.21] Errores de mantenimiento / actualización de programas (software)	3	5	**15**
								[A.11] Acceso no autorizado	3	5	**15**
								[A.15] Modificación deliberada de la información	2	5	**10**
	24	Respaldos	5		5	4	14	[I.6] Corte del suministro eléctrico	3	3	**9**
								[I.10] Degradación de los soportes de almacenamiento de la información	3	4	**12**
								[E.15] Alteración accidental de la información	4	3	**12**
								[E.24] Caída del sistema por agotamiento de recursos	3	5	**15**
								[E.25] Pérdida de equipos	2	5	**10**
[COM] Redes de comunicaciones	25	Red interna de la cooperativa	5		5	4	14	[I.6] Corte del suministro eléctrico	3	3	**9**
								[I.8] Fallo de servicios de comunicaciones	3	4	**12**
								[E.4] Errores de configuración	3	4	**12**
								[E.23] Errores de mantenimiento /	3	4	**12**

							actualización de equipos (hardware)		
							[A.24] Denegación de servicio	2	5	**10**
26	WAN	5		5	5	15	[I.6] Corte del suministro eléctrico	3	4	**12**
							[I.8] Fallo de servicios de comunicaciones	3	4	**12**
							[E.4] Errores de configuración	3	4	**12**
							[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	**9**
							[A.24] Denegación de servicio	2	5	**10**
27	LAN	5		5	5	15	[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	**8**
							[I.10] Degradación de los soportes de almacenamiento de la información	3	3	**9**
							[E.4] Errores de configuración	3	4	**12**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	**9**
							[A.11] Acceso no autorizado	3	5	**15**

[SI] Sistemas de Información	28	SAGA	5	5	5	15	[I.6] Corte del suministro eléctrico	2	4	**8**
							[I.8] Fallo de servicios de comunicaciones	4	4	**16**
							[E.4] Errores de configuración	3	4	**12**
							[E.20] Vulnerabilidades de los programas (software)	3	4	**12**
							[E.24] Caída del sistema por agotamiento de recursos	2	4	**8**
							[A.11] Acceso no autorizado	3	5	**15**
[P] Personal	29	Jefe de TI	5	5	5	15	[I.5] Avería de origen físico o lógico	3	3	**9**
							[I.6] Corte del suministro eléctrico	3	3	**9**
							[E.2] Errores del administrador	3	4	**12**
							[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	**9**
							[E.7] Deficiencias en la organización	3	4	**12**
	30	Ayudantes de TI	5	5	5	15	[I.5] Avería de origen físico o lógico	2	3	**6**
							[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	**8**
							[E.1] Errores de los usuarios	3	3	**9**

							[E.4] Errores de configuración	3	4	**12**
[AUX] Equipamiento auxiliar	31	Equipos de respaldo de energía (UPS)	5		3	5	13	[I.6] Corte del suministro eléctrico	3	4	**12**
								[I.7] Condiciones inadecuadas de temperatura o humedad	2	4	**8**
								[I.10] Degradación de los soportes de almacenamiento de la información	2	3	**6**
								[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	**9**
	32	Impresoras y escáneres	2		2	3	7	[I.5] Avería de origen físico o lógico	3	3	**9**
								[I.6] Corte del suministro eléctrico	2	3	**6**
								[E.8] Difusión de software dañino	2	4	**8**
								[E.4] Errores de configuración	3	3	**9**
								[E.14] Escapes de información	2	4	**8**
	33	Cámaras de vigilancia	4		4	4	12	[I.8] Fallo de servicios de comunicaciones	3	4	**12**
								[E.8] Difusión de software dañino	2	4	**8**
								[E.20] Vulnerabilidades de los programas (software)	3	3	**9**

							[A.11] Acceso no autorizado	3	4	**12**
[Media] Soportes de información	34	Discos duros externos para copias de seguridad	5	5	5	15	[E.18] Destrucción de información	2	4	**8**
							[E.25] Pérdida de equipos	3	3	**9**
							[A.25] Robo	3	4	**12**
							[A.15] Modificación deliberada de la información	2	4	**8**
	35	Archivos físicos de contratos	4	4	4	12	[N.1] Fuego	2	4	**8**
							[E.18] Destrucción de información	3	4	**12**
							[A.25] Robo	2	4	**8**
[S] Servicios	36	Servicio de alojamiento en la nube	5	5	5	15	[E.20] Vulnerabilidades de los programas (software)	3	4	**12**
							[E.24] Caída del sistema por agotamiento de recursos	2	3	**6**
							[A.11] Acceso no autorizado	3	4	**12**
							[A.24] Denegación de servicio	3	3	**9**
	37	Créditos	5	5	5	15	[E.14] Escapes de información	3	3	**9**
							[E.21] Errores de mantenimiento / actualización de programas (software)	3	3	**9**
							[A.5] Suplantación de la identidad del usuario	3	4	**12**
							[A.25] Robo	3	4	**12**

38	Ahorros	5	5	5	15	[E.14] Escapes de información	3	4	**12**
						[E.20] Vulnerabilidades de los programas (software)	3	3	**9**
						[A.11] Acceso no autorizado	3	4	**12**
						[A.25] Robo	2	4	**12**
39	Transferencias	5	5	5	15	[E.9] Errores de [re-]encaminamiento	3	3	**9**
						[E.4] Errores de configuración	4	3	**12**
						[A.11] Acceso no autorizado	3	4	**12**
						[A.8] Difusión de software dañino	2	4	**8**
40	Conexus	4	5	4	13	[E.20] Vulnerabilidades de los programas (software)	3	4	**12**
						[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	**9**
						[A.11] Acceso no autorizado	4	4	**16**
						[E.20] Vulnerabilidades de los programas (software)	4	3	**12**
						[A.24] Denegación de servicio	3	4	**12**
						[A.15] Modificación deliberada de la información	2	4	**8**

La tabla anterior ofrece una visión detallada de la evaluación de riesgos para cada activo, facilitando la identificación de áreas que requieren atención prioritaria. Esto permite implementar medidas de seguridad adecuadas para proteger los activos y minimizar el riesgo a niveles aceptables.

4.5.6. Controles de Seguridad

El análisis de riesgos ha proporcionado una comprensión integral de la situación actual de los activos en la Cooperativa de Ahorro y Crédito “Chunchi”. Se han detallado las deficiencias en la gestión de seguridad detectadas para estos activos, destacando la necesidad de mejorar la protección de los más vulnerables y las amenazas a las que se enfrentan. Las medidas de seguridad recomendadas se han establecido tras un análisis profundo de las amenazas y los niveles de riesgo asociados, siguiendo las pautas de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. La adecuada alineación de los activos con los controles establecidos en ambas normas facilita la formulación de un manual de políticas de seguridad que aborde de manera efectiva las áreas de mejora identificadas.

tabla 13. Controles para Amenazas con Riesgo Elevado según ISO/IEC 27001:2013, ISO/IEC 27002:2013. Fuente: Autoría Propia

Código	Activos	Valoración	Catálogo de Amenazas	Cálculo del Riesgo			Controles de la ISO/IEC 27001:2013	Controles de la ISO/IEC 27001:2013
		Total/15	Amenazas	Impacto	Probabilidad	Riesgo		
1	App Coac Chunchi	**15**	[E.19] Fugas de información	3	5	15	Implementación de controles de acceso	Gestión de fugas de información
			[E.8] Difusión de software dañino	4	4	16	Protección contra malware	Controles contra código malicioso
			[A.11] Acceso no autorizado	4	5	20	Autenticación segura	Control de acceso
			[A.15] Modificación deliberada de la información	3	5	12	Integridad de la información	Gestión de cambios
			[A.24] Denegación de servicio	4	3	12	Disponibilidad del servicio	Protección contra ataques de denegación de servicio
			[A.30] Ingeniería social (picaresca)	4	4	16	Sensibilización y formación en seguridad	Protección contra técnicas de ingeniería social
2	Conexus	**15**	[E.8] Difusión de software dañino	4	4	16	Protección contra malware	Protección contra malware
			[E.19] Fugas de información	3		15	Implementación de controles de acceso	Implementación de controles de acceso
			[A.11] Acceso no autorizado	4	4	16	Autenticación segura	Autenticación segura

			[A.15] Modificación deliberada de la información	3	4	12	Integridad de la información	Integridad de la información
			[A.24] Denegación de servicio	3	4	12	Disponibilidad del servicio	Disponibilidad del servicio
			[A.30] Ingeniería social (picaresca)	4	4	16	Sensibilización y formación en seguridad	Protección contra técnicas de ingeniería social
3	Informix	**14**	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
			[A.5] Suplantación de la identidad del usuario	3	4	12	Implementación de autenticación multifactor y mecanismos para detectar suplantación	Gestión de la identidad y autenticación
			[A.24] Denegación de servicio	4	3	12	Implementación de medidas de protección contra ataques de denegación de servicio (DoS)	Protección contra ataques de denegación de servicio
4	VirtualCop	**12**	[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
			[E.19] Fugas de información	3	5	15	Implementación de controles de acceso y encriptación de datos sensibles	Gestión de la fuga de información y protección de datos
			[A.24] Denegación de servicio	3	4	12	Implementación de medidas de alta disponibilidad y protección contra ataques	Protección contra ataques de denegación de servicio
5	JPCSystem	**12**	[E.4] Errores de configuración	4	3	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
			[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso

			[A.11] Acceso no autorizado	3	4	12	Implementación de autenticación segura y control de acceso	Control de acceso y autenticación estricta
			[E.15] Alteración accidental de la información	4	3	12	Implementación de controles de integridad y verificación de datos	Gestión de la integridad de la información
6	Facilito	**12**	[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
			[E.21] Errores de mantenimiento/actualización de software	3	5	15	Implementación de procedimientos rigurosos para la actualización y mantenimiento del software	Gestión de mantenimiento y actualización de software
			[A.11] Acceso no autorizado	3	4	12	Implementación de autenticación segura y control de acceso	Control de acceso y autenticación estricta
7	Financop	**13**	[I.8] Fallo de servicios de comunicaciones	4	3	12	Implementación de redundancia en comunicaciones y planes de contingencia	Gestión de la disponibilidad de los servicios de comunicación
			[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
8	SPI BANCO CENTRAL	**15**	[E.4] Errores de configuración	4	3	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
			[E.14] Escapes de información	3	4	12	Implementación de controles de acceso y encriptación de datos sensibles	Gestión de la fuga de información y protección de datos
			[A.5] Suplantación de la identidad del usuario	3	4	12	Implementación de autenticación multifactor y gestión de identidades	Verificación de identidad y control de acceso
9	Credit report	**15**	[E.8] Difusión de software dañino	4	4	16	Control de programas	Control de ejecución de software
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	12	Control de acceso a equipos	Instalación y mantenimiento de equipos
			[E.20] Vulnerabilidades de los programas (software)	3	4	12	Gestión de vulnerabilidades	Seguridad en el desarrollo y soporte de software

10	SIALAFT - UFE	**12**	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia y planes de contingencia para comunicaciones	Gestión de la disponibilidad de los servicios de comunicación
			[E.20] Vulnerabilidades de los programas (software)	3	4	12	Implementación de parches y actualización continua de software	Gestión de vulnerabilidades técnicas
11	Servidor principal	11	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
			[A.6] Abuso de privilegios de acceso	3	5	15	Implementación de controles de acceso y monitoreo de privilegios	Gestión de privilegios de acceso
			[A.11] Acceso no autorizado	3	4	12	Implementación de autenticación segura y controles de acceso físico y lógico	Control de acceso y autenticación estricta
12	Computadoras de escritorio	13	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
			[E.19] Fugas de información	3	4	12	Implementación de controles de acceso y cifrado de datos para prevenir fugas de información	Protección de la información
			[A.11] Acceso no autorizado	4	3	12	Implementación de autenticación segura y controles de acceso físico y lógico	Control de acceso y autenticación estricta
13	4 switch	9	[E.24] Caída del sistema por agotamiento de recursos	3	4	12	Implementación de mecanismos de gestión de recursos y monitoreo para prevenir el agotamiento	Gestión de capacidad y rendimiento
			[A.24] Denegación de servicio	3	4	12	Implementación de medidas de protección contra ataques de denegación de servicio (DoS)	Protección contra ataques de denegación de servicio

			[A.11] Acceso no autorizado	3	5	15	Implementación de controles de acceso físico y lógico para el switch	Control de acceso y autenticación estricta
14	Router	10	[I.6] Corte del suministro eléctrico	3	4	12	Implementación de sistemas de energía ininterrumpida (UPS)	Protección contra fallos en el suministro eléctrico
			[E.24] Caída del sistema por agotamiento de recursos	3	4	12	Monitoreo de la capacidad del sistema y planificación de recursos	Gestión de la capacidad y prevención de sobrecargas
			[A.11] Acceso no autorizado	3	4	12	Implementación de autenticación segura y control de acceso	Control de acceso y autenticación
17	Laptop HP	13	[E.20] Vulnerabilidades de los programas (software)	4	3	12	Aplicación de parches y actualizaciones de seguridad en el software del equipo	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	4	4	16	Implementación de autenticación segura y controles de acceso físico y lógico	Control de acceso y autenticación estricta
			[A.14] Interceptación de información (escucha)	3	5	15	Implementación de cifrado para la transmisión de datos y uso de redes seguras	Protección de la información en tránsito y en reposo
			[A.5] Suplantación de la identidad del usuario	4	3	12	implementación de autenticación multifactor y mecanismos para detectar suplantación	Gestión de la identidad y autenticación
19	BBDD de clientes	15	[E.20] Vulnerabilidades de los programas (software)	4	4	16	Aplicación de parches y actualizaciones de seguridad en el software de gestión de bases de datos	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	3	5	15	Implementación de controles de acceso y autenticación robustos para la base de datos de clientes	Control de acceso y autenticación estricta
			[A.14] Interceptación de información (escucha)	3	5	15	Implementación de cifrado para la transmisión y almacenamiento de datos sensibles	Protección de la información en tránsito y en reposo

			[A.15] Modificación deliberada de la información	3	5	15	Implementación de mecanismos para detectar y prevenir la modificación no autorizada de la información	Control de acceso y autenticación estricta
20	Documentación financiera y contable	15	[E.15] Alteración accidental de la información	3	4	12	Implementación de controles de integridad y mecanismos de auditoría para la documentación financiera	Gestión de la integridad de la información
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12	Procedimientos de actualización y mantenimiento de software aplicados a la gestión financiera	Gestión de mantenimiento y actualización de software
			[A.11] Acceso no autorizado	3	5	15	Implementación de controles de acceso y autenticación para proteger la documentación financiera	Control de acceso y autenticación estricta
			[A.15] Modificación deliberada de la información	3	5	15	Control de acceso y mecanismos para detectar y prevenir la modificación no autorizada de la información	Control de acceso y autenticación estricta
21	Claves de encriptación de los servidores	14	[E.20] Vulnerabilidades de los programas (software)	3	5	15	Aplicación de parches y actualización continua del software de encriptación	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso a las claves de encriptación	Control de acceso y autenticación estricta
22	Encriptación de Huella	14	[I.7] Condiciones inadecuadas de temperatura o humedad	3	4	12	Implementación de sistemas de control ambiental para regular la temperatura y humedad	Protección de los equipos y datos contra condiciones ambientales
			[E.20] Vulnerabilidades de los programas (software)	3	5	15	Aplicación de parches y actualización continua del software de encriptación	Gestión de vulnerabilidades técnicas

			[E.21] Errores de mantenimiento / actualización de programas (software)	3	5	15	Implementación de procedimientos rigurosos para la actualización y mantenimiento del software	Gestión de mantenimiento y actualización de software
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso a las claves de encriptación	Control de acceso y autenticación estricta
23	Encriptación de Correos	12	[E.20] Vulnerabilidades de los programas (software)	3	5	15	Aplicación de parches y actualización continua del software de encriptación	Gestión de vulnerabilidades técnicas
			[E.21] Errores de mantenimiento / actualización de programas (software)	3	5	15	Implementación de procedimientos rigurosos para la actualización y mantenimiento del software	Gestión de mantenimiento y actualización de software
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso a las claves de encriptación	Control de acceso y autenticación estricta
24	Respaldos	14	[I.10] Degradación de los soportes de almacenamiento de la información	3	4	12	Implementación de programas de monitoreo y rotación de soportes	Gestión del ciclo de vida de los medios de almacenamiento
			[E.15] Alteración accidental de la información	4	3	12	Implementación de controles de integridad y verificación de datos	Gestión de la integridad de la información
			[E.24] Caída del sistema por agotamiento de recursos	3	5	15	Monitoreo de la capacidad y planificación de recursos	Gestión de la capacidad y prevención de sobrecargas
25	Red interna de la cooperativa	14	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia en comunicaciones y planes de contingencia	Gestión de la disponibilidad de los servicios de comunicación
			[E.4] Errores de configuración	3	4	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	12	Implementación de programas de mantenimiento preventivo y correctivo	Gestión de mantenimiento y actualización de equipos

26	WAN	15	[I.6] Corte del suministro eléctrico	3	4	12	Implementación de sistemas de energía ininterrumpida (UPS)	Protección contra fallos en el suministro eléctrico
			[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia en comunicaciones y planes de contingencia	Gestión de la disponibilidad de los servicios de comunicación
			[E.4] Errores de configuración	3	4	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
27	LAN	15	[E.4] Errores de configuración	3	4	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso	Control de acceso y autenticación estricta
28	SAGA	15	[I.8] Fallo de servicios de comunicaciones	4	4	16	Implementación de redundancia y planes de contingencia para comunicaciones	Gestión de la disponibilidad de los servicios de comunicación
			[E.4] Errores de configuración	3	4	12	Procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios
			[E.20] Vulnerabilidades de los programas (software)	3	4	12	Aplicación de parches y actualización continua del software	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	3		15	Autenticación segura y control de acceso	Control de acceso y autenticación
29	Jefe de TI	15	[E.2] Errores del administrador	3	4	12	Implementación de controles y revisión de cambios	Procedimientos para la gestión de cambios y revisiones
			[E.7] Deficiencias en la organización	3	4	12	Mejora de la estructura organizativa y definición clara de roles	Gestión de la estructura organizativa y asignación de responsabilidades
30	Ayudante de TI	15	[E.4] Errores de configuración	3	4	12	Implementación de procedimientos de revisión y validación de configuraciones	Gestión de configuraciones y cambios

31	Equipos de respaldo de energía (UPS)	13	[I.6] Corte del suministro eléctrico	3	4	12	Implementación de redundancia en la energía	Protección contra fallos en el suministro eléctrico
33	Cámaras de vigilancia	12	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia en comunicaciones	Gestión de la disponibilidad de los servicios de comunicación
			[A.11] Acceso no autorizado	3	4	12	Autenticación segura y control de acceso	Control de acceso y monitoreo de sistemas
34	Discos duros externos para copias de seguridad	15	[A.25] Robo	3	4	12	Implementación de medidas de seguridad física y lógica	Protección física de activos y controles de acceso
35	Archivos físicos de contratos	12	[E.18] Destrucción de información	3	4	12	Gestión de la seguridad física y ambiental	Protección contra la destrucción de la información
36	Servicio de alojamiento en la nube	15	[E.20] Vulnerabilidades de los programas (software)	3	4	12	Gestión de la seguridad de aplicaciones y software	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	3	4	12	Autenticación segura y gestión de accesos	Control de acceso y autenticación
37	Créditos	15	[A.5] Suplantación de la identidad del usuario	3	4	12	Implementación de autenticación robusta	Verificación de identidad
			[A.25] Robo	3	4	12	Protección física y medidas contra el robo	Seguridad física y protección de activos
38	Ahorros	15	[E.14] Escapes de información	3	4	12	Protección contra fugas de datos	Gestión de la clasificación y etiquetado de la información
			[A.11] Acceso no autorizado	3	4	12	Autenticación segura y control de acceso	Control de acceso basado en roles
			[A.25] Robo	2	4	12	Protección física y lógica contra el robo	Seguridad física y protección de activos

39	Transferencias	15	[E.4] Errores de configuración	4	3	12	Implementación de procedimientos de configuración	Gestión de configuraciones y cambios
			[A.11] Acceso no autorizado	3	4	12	Autenticación segura y control de acceso	Control de acceso basado en roles
40	Conexus	13	[E.20] Vulnerabilidades de los programas (software)	3	4	12	Gestión de la seguridad de aplicaciones y software	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	4	4	16	Autenticación segura y control de acceso	Control de acceso y autenticación
			[A.24] Denegación de servicio	3	4	12	Implementación de medidas de alta disponibilidad	Protección contra ataques de denegación de servicio

En la tabla se detallan los mecanismos diseñados para mitigar las amenazas relacionadas con los activos que presentan un alto nivel de riesgo. Es fundamental reconocer que los controles implementados no siempre logran los resultados previstos; por lo tanto, se recomienda ajustar y optimizar las medidas de seguridad según sea necesario, seleccionando las más adecuadas. A continuación, se presenta una matriz sintetizada que enumera los activos más importantes para la cooperativa que poseen un nivel de riesgo elevado.

Tabla 14. Matriz de riesgo Crítica. Fuente: Autoría propia.

Código	Activos	Valoración	Catálogo de Amenazas	Cálculo del Riesgo				
			Amenazas			Riesgo	Controles de la ISO/IEC 27001:2013	Controles de la ISO/IEC 27001:2013
		Total/15		Impacto	Probabilidad			
1	App Coac Chunchi	**15**	[E.8] Difusión de software dañino	4	4	16	Protección contra malware	Controles contra código malicioso
			[A.11] Acceso no autorizado	4	5	20	Autenticación segura	Control de acceso
			[A.30] Ingeniería social (picaresca)	4	4	16	Sensibilización y formación en seguridad	Protección contra técnicas de ingeniería social
2	Conexus	**15**	[E.8] Difusión de software dañino	4	4	16	Protección contra malware	Protección contra malware
			[A.11] Acceso no autorizado	4	4	16	Autenticación segura	Autenticación segura
			[A.30] Ingeniería social (picaresca)	4	4	16	Sensibilización y formación en seguridad	Protección contra técnicas de ingeniería social

3	Informix	**14**	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
4	VirtualCop	**12**	[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
			[E.19] Fugas de información	3	5	15	Implementación de controles de acceso y encriptación de datos sensibles	Gestión de la fuga de información y protección de datos
5	JPCSystem	**12**	[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
6	Facilito	**12**	[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
			[E.21] Errores de mantenimiento/actualización de software	3	5	15	Implementación de procedimientos rigurosos para la actualización y mantenimiento del software	Gestión de mantenimiento y actualización de software
			[E.8] Difusión de software dañino	4	4	16	Implementación de soluciones antimalware y monitoreo continuo	Protección contra código malicioso
9	Credit report	**15**	[E.8] Difusión de software dañino	4	4	16	Control de programas	Control de ejecución de software
10	SIALAFT - UFE	14	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia y planes de contingencia para comunicaciones	Gestión de la disponibilidad de los servicios de comunicación

			[E.20] Vulnerabilidades de los programas (software)	3	4	12	Implementación de parches y actualización continua de software	Gestión de vulnerabilidades técnicas
11	Servidor principal	11	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
12	Computadoras de escritorio	13	[E.8] Difusión de software dañino	4	4	16	Implementación de software antivirus y soluciones de seguridad para detectar y prevenir malware	Protección contra software dañino
17	Laptop HP	13	[A.11] Acceso no autorizado	4	4	16	Implementación de autenticación segura y controles de acceso físico y lógico	Control de acceso y autenticación estricta
19	BBDD de clientes	15	[E.20] Vulnerabilidades de los programas (software)	4	4	16	Aplicación de parches y actualizaciones de seguridad en el software de gestión de bases de datos	Gestión de vulnerabilidades técnicas
21	Claves de encriptación de los servidores	14	[E.20] Vulnerabilidades de los programas (software)	3	5	15	Aplicación de parches y actualización continua del software de encriptación	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso a las claves de encriptación	Control de acceso y autenticación estricta
22	Encriptación de Huella	14	[E.20] Vulnerabilidades de los programas (software)	3	5	15	Aplicación de parches y actualización continua del software de encriptación	Gestión de vulnerabilidades técnicas
			[E.21] Errores de mantenimiento /	3	5	15	Implementación de procedimientos rigurosos para	Gestión de mantenimiento y actualización de software

			actualización de programas (software)				la actualización y mantenimiento del software	
			[A.11] Acceso no autorizado	3	5	15	Implementación de autenticación segura y control de acceso a las claves de encriptación	Control de acceso y autenticación estricta
24	Respaldos	14	[E.24] Caída del sistema por agotamiento de recursos	3	5	15	Monitoreo de la capacidad y planificación de recursos	Gestión de la capacidad y prevención de sobrecargas
25	Red interna de la cooperativa	14	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia en comunicaciones y planes de contingencia	Gestión de la disponibilidad de los servicios de comunicación
28	SAGA	15	[I.8] Fallo de servicios de comunicaciones	4	4	16	Implementación de redundancia y planes de contingencia para comunicaciones	Gestión de la disponibilidad de los servicios de comunicación
29	Jefe de TI	15	[E.7] Deficiencias en la organización	3	4	12	Mejora de la estructura organizativa y definición clara de roles	Gestión de la estructura organizativa y asignación de responsabilidades
31	Equipos de respaldo de energía (UPS)	13	[I.6] Corte del suministro eléctrico	3	4	12	Implementación de redundancia en la energía	Protección contra fallos en el suministro eléctrico
33	Cámaras de vigilancia	12	[I.8] Fallo de servicios de comunicaciones	3	4	12	Implementación de redundancia en comunicaciones	Gestión de la disponibilidad de los servicios de comunicación
			[A.11] Acceso no autorizado	3	4	12	Autenticación segura y control de acceso	Control de acceso y monitoreo de sistemas

34	Discos duros externos para copias de seguridad	15	[A.25] Robo	3	4	12	Implementación de medidas de seguridad física y lógica	Protección física de activos y controles de acceso
40	Conexus	13	[E.20] Vulnerabilidades de los programas (software)	3	4	12	Gestión de la seguridad de aplicaciones y software	Gestión de vulnerabilidades técnicas
			[A.11] Acceso no autorizado	4	4	16	Autenticación segura y control de acceso	Control de acceso y autenticación
			[A.24] Denegación de servicio	3	4	12	Implementación de medidas de alta disponibilidad	Protección contra ataques de denegación de servicio

4.5.7. Resumen de la matriz de riesgo

La Matriz de Riesgo Crítica fue desarrollada conforme a las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, con el objetivo de identificar y evaluar los riesgos que puedan comprometer la integridad, disponibilidad y confidencialidad de los activos críticos de la organización. Se detectaron amenazas significativas como la Difusión de software malicioso**,** el Acceso no autorizado **y** las Vulnerabilidades en el software**,** que presentan niveles de riesgo elevados. Para mitigar estos riesgos, se implementaron controles como soluciones antimalware avanzadas**,** mecanismos de autenticación segura y una gestión proactiva de vulnerabilidades técnicas, en línea con las recomendaciones de ambas normas. Además, la matriz también aborda riesgos relacionados con la Fuga de información **y** la Denegación de servicio**,** aplicando controles de acceso rigurosos**,** encriptación robusta de datos **y** estrategias de alta disponibilidad**.** Estos controles fueron seleccionados específicamente por su capacidad para reducir los riesgos a niveles aceptables, asegurando la continuidad operativa. En resumen, esta matriz no solo identifica y evalúa los riesgos, sino que también refleja una estrategia integral de gestión de riesgos basada en las mejores prácticas de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Cada control se eligió cuidadosamente para alinearse con las tolerancias de riesgo de la organización, garantizando así la protección continua de los activos de información.

4.6. Directrices o políticas para la seguridad de la Información

El desarrollo y la implementación de directrices o políticas para la seguridad de la información son fundamentales para establecer un marco de control robusto que proteja los activos de información de la organización. Estas políticas, alineadas con las normas ISO/IEC 27001:2013, sirven como guía para gestionar los riesgos asociados a la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad

de los datos. A través de estas directrices, se busca crear una cultura de seguridad dentro de la organización, donde cada miembro entienda y cumpla con las medidas necesarias para proteger la información de manera efectiva.

Los dominios clave para las directrices o políticas de seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi, basados en las normas:

4.6.1. Dominios Clave de la ISO/IEC 27001:2013

1. Políticas de Seguridad de la Información: Establece las directrices y el enfoque de la organización hacia la seguridad de la información, incluyendo la definición de roles y responsabilidades.

2. Organización de la Seguridad de la Información: Se enfoca en la estructura organizativa, asignación de responsabilidades y la creación de comités de seguridad que gestionen y mantengan la seguridad de la información.

3. Gestión de Activos: Involucra la identificación, clasificación y protección de los activos de información para garantizar su seguridad y la asignación de propietarios responsables.

4. Seguridad de los Recursos Humanos: Abarca las medidas antes, durante y después de la contratación de empleados para asegurar que comprendan y cumplan con las responsabilidades de seguridad de la información.

5. Gestión de Comunicaciones y Operaciones: Se asegura de que las operaciones y las comunicaciones se gestionen de forma segura y confiable, protegiendo la información en tránsito y en reposo.

6. Control de Acceso: Se enfoca en restringir el acceso a la información y a los sistemas únicamente a las personas autorizadas, asegurando que se implementen medidas de autenticación adecuadas.

4.6.2. Dominios Clave de la ISO/IEC 27002:2013

1. Políticas de la Seguridad de la Información: Incluye la documentación y difusión de las políticas de seguridad, asegurando que estén alineadas con los objetivos de la organización y que se revisen periódicamente.

2. Aspectos Organizativos de la Seguridad de la Información: Asegura que los roles y responsabilidades estén claramente definidos y documentados, con la existencia de un comité de seguridad de la información y reuniones periódicas para revisar la seguridad.

3. Seguridad Física y Ambiental: Proporciona directrices para proteger la infraestructura física y los activos contra amenazas físicas y ambientales.

4. Relaciones con Proveedores: Se centra en gestionar las relaciones con terceros, asegurando que los contratos y acuerdos cumplan con las políticas de seguridad de la información.

5. Gestión de Incidentes de Seguridad de la Información: Establece procedimientos para identificar, reportar y gestionar incidentes de seguridad de la información, minimizando su impacto.

6. Cumplimiento: Asegura que las políticas y procedimientos cumplan con las leyes y regulaciones aplicables, realizando auditorías internas y externas.

CONCLUSIÓN

Se logró desarrollar un marco teórico robusto que proporcionó una comprensión clara de los conceptos fundamentales de la seguridad de la información y la importancia de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Este marco conceptual fue esencial para guiar el proceso de implementación y asegurar que todos los aspectos clave de la seguridad de la información fueran considerados.

La evaluación realizada ha permitido una revisión detallada de la situación actual de la seguridad de la información en la Cooperativa de Ahorro y Crédito Chunchi. Esta evaluación identificó los activos críticos, así como las amenazas y vulnerabilidades asociadas. La metodología MAGERIT fue utilizada eficazmente para priorizar los riesgos y dirigir las acciones correctivas necesarias.

Se ha diseñado e implementado un manual de políticas de seguridad de la información que cumple con los requisitos de las normas ISO/IEC 27001:2013. Este manual proporciona directrices claras y estructuradas para la gestión de la seguridad de la información, abarcando desde la gestión de activos hasta el control de acceso y la gestión de incidentes de seguridad.

El desarrollo de un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Chunchi del Cantón Chunchi se presenta como una solución efectiva y práctica para abordar las carencias detectadas en la gestión de seguridad. Este manual proporcionará directrices detalladas para la administración de los activos informáticos, la implementación de medidas de seguridad específicas, y la formulación de un plan de acción ante incidentes. Su aplicación permitirá reforzar la seguridad de la cooperativa y asegurar una protección adecuada para la información confidencial de la organización.

RECOMENDACIONES

- Para la Cooperativa de Ahorro y Crédito Chunchi del Cantón Chunchi, se recomienda implementar programas de formación continua para todos los empleados, con un enfoque en las mejores prácticas de seguridad de la información y en la gestión de riesgos específicos identificados en el análisis. Esta formación ayudará a reducir el riesgo asociado a errores humanos y a la ingeniería social, asegurando que el personal esté capacitado para enfrentar las amenazas actuales.
- Además, es crucial revisar y mejorar los mecanismos de autenticación y autorización para garantizar que solo el personal autorizado pueda acceder a la información crítica. La implementación de autenticación multifactor debe ser considerada como una medida adicional de seguridad para reforzar el control de acceso.
- Es fundamental asegurar que todos los sistemas de software y hardware estén actualizados con los últimos parches y actualizaciones. Se deben establecer procedimientos rigurosos para el mantenimiento y la actualización de estos sistemas con el fin de evitar vulnerabilidades y errores que puedan comprometer la seguridad.

BIBLIOGRAFÍA

LEAL RODRIGUEZ, Y. P. (01 de 01 de 2021). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/42688/yplealr.pdf?sequence=3&isAllowed=y

Linares Fernández, E., & Balverdi Cruz, L. H. (03 de 2022). *repositorio.upeu.edu.pe.* Obtenido de repositorio.upeu.edu.pe: https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/5316/Eli_Tesis_Licenciatura_2022.pdf?sequence=5&isAllowed=y

Maliza Malisa, A. S. (2021). *dspace.uniandes.edu.ec.* Obtenido de dspace.uniandes.edu.ec: https://dspace.uniandes.edu.ec/bitstream/123456789/12752/1/PIUPSIS0001-2021.pdf

Amutio Gómez, M., Candau , J., & Mañas, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Aules Pineida, F. P. (2021). *dspace.udla.edu.ec.* Obtenido de dspace.udla.edu.ec: https://dspace.udla.edu.ec/bitstream/33000/13789/1/UDLA-EC-TMGSI-2021-08.pdf

Cooperativa de Ahorro y Crédito Chunchi Ltda. (2019). *www.coacchunchi.fin.ec*. Obtenido de www.coacchunchi.fin.ec: https://www.coacchunchi.fin.ec/quienes-somos/

Guancanes Castro, M. V., & Vilatuña Morales, J. A. (06 de 2022). *bibdigital.epn.edu.ec.* Obtenido de bibdigital.epn.edu.ec: https://bibdigital.epn.edu.ec/bitstream/15000/22812/1/CD%2012289.pdf

Huaman Tena, A. (2021). *repositorio.unjfsc.edu.pe.* Obtenido de repositorio.unjfsc.edu.pe: https://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/7216/TESIS_compressed.pdf?sequence=1&isAllowed=y

incibe. (14 de 06 de 2024). *www.incibe.es.* Obtenido de www.incibe.es: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_buenas_practicas_en_el_area_de_informatica.pdf

ISO. (03 de 06 de 2024). *www.iso.org.* Obtenido de www.iso.org: https://www.iso.org/es/contents/data/standard/07/56/75652.html

Lara Guijarro, E. G. (2019). *repositorio.uisek.edu.ec.* Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3260/1/TESIS%20ELVA%20LARA.pdf

Méndez Gálvez, C. (2020). *repositorio.uss.edu.pe.* Obtenido de repositorio.uss.edu.pe: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7827/M%C3%A9ndez%20G%C3%A1lvez,%20Cipriano.pdf?sequence=1

National Institute of Standards and Technology. (26 de 02 de 2024). *nvlpubs.nist.gov*. Obtenido de nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

nqa. (05 de 04 de 2024). *www.nqa.com*. Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pilla Yanzapanta, J. C. (2019). *repositorio.uisek.edu.ec*. Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%C3%91O%20DE%20UNA%20POL%C3%8DTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20PARA%20EL%20%C3%81REA%20DE%20TECNOLOG%C3%8DA%20DE%20LA%20INFORMACI%C3%93.pdf

Puga Jacome , C. E. (21 de 03 de 2019). *repositorio.uisek.edu.ec*. Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3343/1/TESIS%20MTI%20EDUARDO%20PUGA.pdf

Quispe Ayquipa, C. A. (2021). *repositorio.upci.edu.pe*. Obtenido de repositorio.upci.edu.pe: https://repositorio.upci.edu.pe/bitstream/handle/upci/309/TESIS%20CESAR_QUISPE_CORRECCION%20TURNITIN_FINAL_12_03_2021_FINAL%202.pdf?sequence=1&isAllowed=y

Ramos Mamam, R. G., Cahuaya Ancco, R., & Llanqui Argollo, R. R. (2023). Política informática y la gestión de la seguridad de la información en basea la norma ISO 27001. *Revista Innovación y Software*, 96-106.

Rodríguez Guerra., J. P. (02 de 2019). *repositorio.uisek.edu.ec*. Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3321/1/Tesis%20Final.pdf

Romo Sañicela, S., & Bojorque Chasi, R. (01 de 01 de 2023). *dspace.ups.edu.ec*. Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/26674/1/UPS-CT011073.pdf

Torres Hallo, M. (06 de 2020). *biblioteca.uteg.edu.ec*. Obtenido de biblioteca.uteg.edu.ec: http://biblioteca.uteg.edu.ec:8080/bitstream/handle/123456789/1173/Modelo%20de%20gestion%20de%20riesgos%20de%20procesos%20de%20tecnologias%20de%20informacion%20bajo%20la%20norma%20iso-iec%2027000%20en%20empresas%20a%C3%A9reas%20del%20Ecuador.pdf?sequence=

Vasquez Zevallos, J. L., & Delgado Saavedra, M. (2019). *core.ac.uk*. Obtenido de core.ac.uk: https://core.ac.uk/download/389312591.pdf

Vega Briceño, E. (2021). SEGURIDAD DE LA INFORMACIÓN. En E. V. Briceño, *SEGURIDAD DE LA INFORMACIÓN* (pág. 111). Alicantes: ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

Villegas Limaico, J. A. (2019). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: https://repositorio.espe.edu.ec/bitstream/21000/21529/1/T-ESPE-042059.pdf

Anexos

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Chunchi Ltda.

Cooperativa de ahorro y Crédito

2024

Diaz

El Departamento de Tecnologías de la Información (TIC) de la Cooperativa de Ahorro y Crédito "Chunchi" identifica y gestiona la información y los procesos que la soportan como activos críticos, cuya protección es vital para la continuidad operativa y el cumplimiento de los objetivos estratégicos de la cooperativa. La confidencialidad, integridad y disponibilidad de estos activos de información son componentes fundamentales que garantizan la resiliencia de los sistemas y la mitigación de riesgos inherentes al entorno tecnológico.

Este manual establece las políticas de seguridad de la información de la Cooperativa de Ahorro y Crédito Chunchi, alineadas con las mejores prácticas internacionales y en cumplimiento con los estándares ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Estas políticas están diseñadas para conformar un marco robusto de controles y procedimientos que protejan los sistemas de información frente a amenazas tanto internas como externas, garantizando así la continuidad operativa y la fiabilidad de las actividades de la cooperativa.

Objetivo

Establecer un conjunto de directrices y procedimientos que permitan a la Cooperativa de Ahorro y Crédito Chunchi proteger de manera efectiva la confidencialidad, integridad y disponibilidad de su información. Minimizar los riesgos asociados con la gestión de la información, asegurar el cumplimiento normativo, y fortalecer la confianza de los socios y partes interesadas en la capacidad de la cooperativa para manejar su información de manera segura y responsable mediante la implementación de estas políticas.

Alcance

Las políticas de seguridad de la información de la Cooperativa de Ahorro y Crédito Chunchi se implementan en todas las áreas de la organización y abarcan a todo el personal

involucrado, con el objetivo de asegurar la protección integral de la información manejada por la cooperativa. Estas políticas están diseñadas para proteger tanto los datos digitales como físicos, así como los sistemas y tecnologías que los soportan.

La aplicación rigurosa de estas políticas permitirá mantener un entorno de trabajo seguro y confiable, fortaleciendo la protección de la información de la Cooperativa de Ahorro y Crédito Chunchi y asegurando la confianza de sus socios y partes interesadas en la capacidad de la cooperativa para gestionar sus activos de información de manera segura y responsable.

1. RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

La correcta implementación y cumplimiento del presente Manual de Políticas de Seguridad de la Información en la Cooperativa de Ahorro y Crédito Chunchi es una responsabilidad compartida que involucra a diversos niveles de la organización. Para asegurar la eficacia de estas políticas, se asignan las siguientes responsabilidades:

- **Alta Gerencia:** Tiene la obligación de liderar y respaldar activamente la ejecución de las políticas de seguridad de la información, asegurando que se integren en la estrategia organizacional. Es su responsabilidad promover una cultura organizacional que valore la seguridad de la información como un aspecto clave del éxito operativo.
- **Departamento de Tecnologías de la Información (TIC):** Es el responsable de la ejecución directa de las políticas de seguridad. Esto incluye la supervisión constante de la implementación, el seguimiento de incidentes, y la gestión de riesgos asociados a la información. Además, debe asegurar que todos los empleados estén debidamente capacitados en las prácticas de seguridad, adaptando las medidas según sea necesario para responder a las amenazas emergentes.

- **Difusión de Políticas:** El Departamento de TIC, en colaboración con el área de Recursos Humanos, tiene la tarea de garantizar que todos los empleados y terceros asociados con la cooperativa comprendan y apliquen las políticas establecidas. La comunicación debe ser clara y continua para asegurar la correcta adherencia a las políticas.
- **Auditoría y Evaluación:** Es necesario que el Departamento de Auditoría Interna, en coordinación con TIC, realice evaluaciones periódicas para verificar el grado de cumplimiento de las políticas de seguridad. Estas auditorías deben identificar brechas y proponer mejoras para fortalecer la protección de los activos de información.
- **Revisión y Mejora Continua:** La revisión de este manual es un proceso dinámico. El Departamento de TIC es responsable de su actualización regular, incorporando nuevas mejores prácticas, avances tecnológicos, y cambios regulatorios para mantener la relevancia y efectividad del marco de seguridad de la información.

2. POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La información constituye un activo esencial para la Cooperativa de Ahorro y Crédito Chunchi, ya que su adecuada gestión es crucial tanto para la prestación eficiente de servicios a los socios como para la toma de decisiones estratégicas. Por esta razón, es imperativo que todo el personal involucrado en la gestión y procesamiento de la información comprenda la relevancia de estos activos y siga estrictamente las directrices establecidas en este Manual de Políticas de Seguridad de la Información. El propósito principal de este manual es asegurar una protección integral de la información mediante la implementación de políticas y controles que garanticen la confidencialidad, integridad y disponibilidad de los datos. Estas políticas han sido desarrolladas en conformidad con los estándares internacionales de las normas ISO/IEC

27001:2013 e ISO/IEC 27002:2013, reconocidas como marcos efectivos para la gestión y control de la seguridad de la información.

Adherirse a las políticas delineadas en este manual y alinearse con los requisitos de las normas ISO/IEC 27001 e ISO/IEC 27002 permitirá a la Cooperativa de Ahorro y Crédito Chunchi fortalecer su capacidad para mantener la confianza de sus socios, empleados y demás partes interesadas. La seguridad de la información se erige como un componente esencial para el logro de los objetivos estratégicos de la cooperativa y su sostenibilidad en un entorno competitivo. El Departamento de Tecnologías de la Información (TIC), o el personal designado para la gestión de la seguridad de la información, será responsable de implementar este manual y, cuando sea necesario, realizar revisiones y actualizaciones de las políticas, asegurando que se adapten continuamente a las necesidades de la cooperativa y al entorno de amenazas en constante evolución. Además, el cumplimiento de estas políticas no solo protegerá los activos de información de la cooperativa, sino que también contribuirá a la eficiencia operativa y a la toma de decisiones basada en datos seguros y confiables.

2.1. Política de Seguridad de la Información

2.1.1. Control A.5: Políticas de seguridad de la información

- Crear y aprobar una política de seguridad de la información que refleje las necesidades de la cooperativa y sus objetivos estratégicos.
- Comunicar la política a todo el personal y partes interesadas, y proporcionar capacitación para asegurar su comprensión y cumplimiento.
- Implementar la política en todas las operaciones de la cooperativa, definiendo roles y responsabilidades claras para garantizar el cumplimiento.

- Realizar un seguimiento continuo y revisiones periódicas para asegurar que la política siga siendo relevante y eficaz.
- Actualizar la política según sea necesario para adaptarse a cambios en la cooperativa o en el entorno de riesgo.

2.2. Organización de la Seguridad de la Información

2.2.1. Control A.6: Organización interna

- Establecer una estructura organizativa clara para la seguridad de la información, definiendo roles y responsabilidades específicas dentro de la cooperativa.
- Asignar responsabilidades y autoridad para la gestión de la seguridad de la información, asegurando que cada miembro del personal entienda su papel en el mantenimiento de la seguridad.
- Facilitar la coordinación entre diferentes áreas de la cooperativa para garantizar una gestión eficaz de la seguridad de la información.

2.2.2. Control A.7: Seguridad en las relaciones con terceros

- Evaluar los riesgos asociados con terceros que tienen acceso a la información de la cooperativa y asegurarse de que cumplan con los requisitos de seguridad.
- Establecer acuerdos contractuales claros que especifiquen las obligaciones de los terceros en relación con la seguridad de la información.
- Monitorear y revisar regularmente el cumplimiento de los terceros con los acuerdos de seguridad establecidos, tomando medidas correctivas si es necesario.

2.3. Seguridad de los Recursos Humanos

2.3.1. Control A.8: Seguridad en el proceso de empleo

- Implementar procedimientos para verificar la idoneidad de los candidatos antes de la contratación, incluyendo la comprobación de antecedentes y la evaluación de riesgos relacionados con la seguridad de la información.
- Asegurar que los nuevos empleados reciban formación en seguridad de la información como parte de su proceso de incorporación, para que comprendan sus responsabilidades y las políticas de seguridad de la cooperativa.
- Establecer condiciones claras en los contratos de trabajo que incluyan obligaciones relacionadas con la seguridad de la información y la protección de datos.

2.3.2 Control A.9: Seguridad en las relaciones laborales

- Establecer procedimientos para manejar incidentes de seguridad relacionados con el personal, incluyendo la aplicación de medidas disciplinarias cuando se violen las políticas de seguridad de la información.
- Asegurar que todos los empleados comprendan y mantengan la confidencialidad de la información. Controlar el acceso a datos sensibles según las responsabilidades y el rol de cada empleado.
- Implementar procesos para gestionar la salida de empleados, asegurando la revocación oportuna de accesos y la recuperación de activos de la cooperativa para proteger la información después de su salida.

2.4. Gestión de Activos

2.4.1. Control A.10: Identificación y clasificación de activos

- Crear y mantener un inventario completo de todos los activos de la cooperativa, incluyendo equipos, software, y documentos que contienen información sensible.
- Clasificar los activos según su importancia y el nivel de protección necesario, basándose en el valor de la información y los riesgos asociados.
- Etiquetar los activos de manera adecuada y mantener registros actualizados para facilitar su gestión y protección.

2.4.2. Control A.11: Manejo de activos

- Implementar medidas de seguridad para proteger los activos según su clasificación, asegurando que se mantengan en condiciones seguras y adecuadas durante su ciclo de vida.
- Establecer directrices claras sobre el uso aceptable de los activos, incluyendo restricciones y procedimientos para el uso seguro de equipos y datos.
- Definir procedimientos para la transferencia segura de activos entre diferentes áreas y para la eliminación adecuada de activos obsoletos o desechados, garantizando la protección de la información sensible.

2.5. Control de Acceso

2.5.1. Control A.12: Requisitos de control de acceso

- Establecer políticas claras que definan los requisitos para el control de acceso a la información y a los sistemas. Estas políticas deben especificar quién puede acceder a qué recursos y bajo qué condiciones.
- Implementar mecanismos de autenticación y autorización robustos para asegurar que solo las personas autorizadas puedan acceder a información sensible y recursos críticos.

- Revisar regularmente los derechos de acceso para asegurar que se mantengan actualizados y que reflejen correctamente las responsabilidades actuales de los usuarios. Ajustar los accesos según sea necesario para mantener la seguridad.

2.5.2. Control A.13: Gestión de acceso a la red

- Implementar medidas de seguridad para proteger el acceso a la red, incluyendo firewalls, sistemas de detección de intrusiones y otros controles técnicos para prevenir accesos no autorizados.
- Establecer políticas y procedimientos para gestionar el acceso remoto a la red, asegurando que se utilicen conexiones seguras y que se autentique adecuadamente a los usuarios remotos.
- Monitorear y registrar el acceso a la red para detectar y responder a actividades sospechosas. Realizar revisiones periódicas de los registros de acceso para identificar posibles brechas de seguridad.

2.6. Criptografía

2.6.1. Control A.14: Uso de criptografía

- Establecer y mantener políticas claras sobre el uso de criptografía para proteger la información sensible. Estas políticas deben definir cuándo y cómo se debe utilizar la criptografía para garantizar la confidencialidad, integridad y autenticidad de los datos.
- Utilizar técnicas criptográficas adecuadas para proteger la información, como el cifrado de datos en reposo y en tránsito, así como para la autenticación y firma digital. Asegurarse de que las técnicas utilizadas cumplan con estándares de seguridad reconocidos.

- Implementar procedimientos para la gestión segura de claves criptográficas, incluyendo la generación, almacenamiento, distribución y revocación de claves. Asegurar que las claves se protejan adecuadamente contra accesos no autorizados y se renueven periódicamente.
- Revisar y actualizar regularmente las políticas y prácticas criptográficas para adaptarse a nuevas amenazas y avances tecnológicos. Asegurarse de que los métodos criptográficos sigan siendo efectivos y se ajusten a los requisitos de seguridad actuales.

2.7. Seguridad Física y del Entorno

2.7.1. Control A.15: Seguridad física y del entorno

- Implementar medidas de seguridad física para proteger las instalaciones de la cooperativa, incluyendo el control de acceso a edificios y áreas sensibles. Utilizar sistemas de vigilancia, control de entradas y cerraduras seguras para prevenir accesos no autorizados.
- Asegurar que los equipos que almacenan o procesan información sensible estén protegidos contra daños físicos y accesos no autorizados. Esto incluye la protección contra incendios, inundaciones, y otras amenazas ambientales.
- Mantener un entorno seguro y controlado en las áreas donde se encuentran los equipos críticos y la información sensible. Realizar revisiones regulares para asegurar que las condiciones del entorno no afecten la seguridad de los activos.
- Establecer procedimientos para responder a incidentes de seguridad física, como brechas de seguridad o desastres, para minimizar el impacto en las operaciones y proteger los activos.

2.8. Seguridad en las Operaciones

2.8.1. Control A.16: Seguridad en las operaciones y comunicaciones

- Implementar medidas para proteger la seguridad de los sistemas y datos durante las operaciones y en las comunicaciones. Esto incluye el uso de firewalls, sistemas de detección de intrusiones y encriptación de datos en tránsito.
- Establecer procedimientos para la detección, respuesta y recuperación de incidentes de seguridad en las operaciones y comunicaciones. Asegurar una respuesta rápida y eficaz para minimizar el impacto de los incidentes.
- Implementar controles para gestionar y revisar los cambios en los sistemas y en la infraestructura de comunicaciones, asegurando que no introduzcan vulnerabilidades o brechas de seguridad.
- Realizar monitoreo continuo y mantener registros detallados de las actividades operativas y de comunicación para detectar anomalías y realizar análisis forense en caso de incidentes de seguridad.

2.8.2. Control A.17: Gestión de vulnerabilidades

- Implementar procesos para identificar vulnerabilidades en los sistemas y aplicaciones de la cooperativa. Utilizar herramientas de escaneo de vulnerabilidades y realizar evaluaciones periódicas de seguridad.
- Evaluar el riesgo asociado con las vulnerabilidades identificadas, considerando el impacto potencial en la seguridad de la información y en las operaciones de la cooperativa.
- Establecer procedimientos para aplicar parches y actualizaciones de seguridad de manera oportuna, asegurando que las vulnerabilidades se mitiguen de acuerdo con su prioridad y riesgo.
- Revisar y actualizar regularmente las prácticas de gestión de vulnerabilidades para adaptarse a nuevas amenazas y cambios en el entorno de TI. Monitorear continuamente para detectar y abordar nuevas vulnerabilidades emergentes.

2.9. Seguridad en las Comunicaciones y Operaciones

2.9.1. Control A.18: Seguridad en las redes

- Implementar medidas para proteger la red de la cooperativa, incluyendo el uso de firewalls, sistemas de detección y prevención de intrusiones, y segmentación de red para controlar el acceso y minimizar el riesgo de ataques.
- Asegurar que todas las comunicaciones de red estén protegidas mediante técnicas de cifrado y protocolos seguros para prevenir la interceptación y el acceso no autorizado a la información.
- Realizar monitoreo continuo de la red para detectar actividades sospechosas y responder a posibles amenazas. Mantener registros detallados para análisis y auditoría.

2.9.2 Control A.19: Seguridad en el desarrollo y mantenimiento de sistemas

- Incorporar prácticas de seguridad en el ciclo de vida del desarrollo de software, incluyendo la revisión de código, pruebas de seguridad y la implementación de controles de acceso durante el desarrollo.
- Establecer procedimientos para gestionar la seguridad en las actualizaciones y el mantenimiento de sistemas, asegurando que las nuevas versiones y parches no introduzcan vulnerabilidades.
- Implementar un proceso de control de cambios para revisar y aprobar modificaciones en los sistemas, garantizando que los cambios se realicen de manera segura y no afecten la integridad del sistema.

2.10 Gestión de Incidentes de Seguridad de la Información

2.10.1. Control A.20: Gestión de incidentes de seguridad de la información

- Establecer un proceso claro para la gestión de incidentes de seguridad, desde la detección y notificación hasta la resolución y recuperación. Incluir procedimientos para evaluar el impacto y aplicar medidas correctivas.
- Implementar procedimientos para una respuesta rápida y efectiva a los incidentes, y comunicar las acciones tomadas a las partes interesadas, según sea necesario.
- Revisar los incidentes después de su resolución para identificar lecciones aprendidas y mejorar los procedimientos de seguridad. Utilizar los incidentes como una oportunidad para fortalecer la postura de seguridad.

2.11. Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

2.11.1. Control A.21: Gestión de la continuidad del negocio

- Desarrollar y mantener planes de continuidad del negocio que aseguren la disponibilidad de las operaciones críticas en caso de incidentes graves o desastres. Incluir estrategias para la recuperación y restauración de servicios.
- Realizar pruebas periódicas de los planes de continuidad para verificar su efectividad y hacer ajustes según los resultados.
- Proporcionar formación y concienciación al personal sobre los procedimientos de continuidad del negocio para asegurar que estén preparados para actuar en caso de una interrupción.

2.12. Cumplimiento

2.12.1 Control A.22: Cumplimiento de requisitos legales y contractuales

- Identificar y comprender los requisitos legales y contractuales aplicables a la seguridad de la información que afectan a la cooperativa. Asegurar el cumplimiento de estas obligaciones.
- Implementar controles para cumplir con los requisitos legales y contractuales, y mantener registros para demostrar el cumplimiento.
- Revisar regularmente el cumplimiento de los requisitos y realizar auditorías para identificar cualquier brecha o incumplimiento. Tomar medidas correctivas según sea necesario para mantener el cumplimiento.

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Carlos Reinaldo Diaz Usho portador(a) de la cédula de ciudadanía N.º **0605716059**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación "**Propuesta de manual de políticas de seguridad de la información para la Cooperativa de ahorro y crédito Chunchi, del cantón Chunchi, bajo la norma ISO 27001",** 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, **27 de noviembre de 2024**

F: .....

Carlos Reinaldo Diaz Usho

C.I. **0605716059**