UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMATICA, CIENCIA DE LA COMPUTACION, E INNOVACION TECNOLOGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFOR MACIÓN

PROPUESTA DE MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR

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

AUTOR: SEGUNDO FRANCISCO BERMEJO PICHASACA

DIRECTOR: ING. CRISTHIAN FLORES URGILES. MGS

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMATICA, CIENCIAS DE LA COMPUTACION, E INNOVACION TECNOLOGÍCA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR

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

AUTOR: SEGUNDO FRANCISCO BERMEJO PICHASACA

DIRECTOR: ING. CRISTHIAN FLORES URGILES. MGS

CAÑAR - ECUADOR

Universidad Católica de Cuenca

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Yo Segundo Francisco Bermejo portador de la cédula de ciudadanía **Nº 0350152690**. Declaro ser el autor de la obra: **"Propuesta de Manual de Políticas de Seguridad de la Información para la Cooperativa de Ahorro y Crédito Achik Inti Ltda, del Cantón Cañar",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma hasido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar 14 de Agosto de 2023

Segundo Francisco Bermejo Pichasaca

C.I: 0350152690

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el estudiante Segundo Francisco Bermejo, bajo mi supervisión.

Ing. Cristhian Flores Urgilés, MSC.

DIRECTOR DELTRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

AGRADECIMIENTO

A MI TUTOR

"ING. CRISTHIAN FLORES URGILES. MGS docente de la formación. Sin usted y sus virtudes, su paciencia y constancia este trabajo no lo hubiese logrado tan fácil. Sus consejos fueron siempre útiles cuando no salían de mi pensamiento las ideas para escribir lo que hoy he logrado. Usted formó parte importante de esta historia con sus aportes profesionales que lo caracterizan. Muchas gracias por sus múltiples palabras de aliento, cuando más las necesite; por estar allí cuando mis horas de trabajo se hacían confusas. Gracias por sus orientaciones"

A LOS DOCENTES

"Sus palabras fueron sabias, sus conocimientos rigurosos y precisos, a ustedes mis profesores queridos, les debo mis conocimientos. Donde quiera que vaya, los llevaré conmigo en mí transitar profesional. Su semilla de conocimientos, germinó en el alma y el espíritu. Gracias por su paciencia, por compartir sus conocimientos de manera profesional e invaluable, por su dedicación perseverancia y tolerancia."

A MIS PADRES

"Ustedes han sido siempre el motor que impulsa mis sueños y esperanzas, quienes estuvieron siempre a mi lado en los días y noches más difíciles durante mis horas de estudio. Siempre han sido mis mejores guías de vida. Hoy cuando concluyo mis estudios, les dedico a ustedes este logro amado padres, como una meta más conquistada. Orgulloso de haberlos elegido como mis padres y que estén a mi lado en este momento tan importante.

Gracias por ser quienes son y por creer en mí"

A MIS COMPAÑEROS:

"Mis amigos y compañeros de viaje, hoy culminan esta maravillosa aventura y no puedo dejar de recordar cuantas tardes y horas de trabajo nos juntamos a lo largo de nuestra formación. Hoy nos toca cerrar un capítulo maravilloso en esta historia de vida y no puedo dejar de agradecerles por su apoyo y constancia, al estar en las horas más difíciles, por compartir horas de estudio. Gracias por estar siempre allí."

DEDICATORIA

Dedico esta tesis a Dios y a mis padres. Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar, a mis padres, quienes a lo largo de la vida han velado por mi bienestar y educación siendo mi apoyo en todo momento de la vida.

Resumen

La Cooperativa de Ahorro y Crédito Achik Inti ha desempeñado una función esencial proporcionando soluciones financieras en todo el cantón Cañar y se ha adaptado proactivamente a las competencias emergentes y a la ejecución de proyectos innovadores. Sin embargo, la carencia de protocolos de seguridad informática en la entidad plantea desafíos, haciéndola susceptible a intervenciones no autorizadas. Este proyecto se orienta a la elaboración de un "ESQUEMA DE NORMAS DE SEGURIDAD INFORMÁTICA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, EN EL CANTÓN CAÑAR". Para fortalecer la estructura de esta investigación, se recurrió a las directrices de ISO 27001:2013 y a las recomendaciones de ISO 27002. Estos marcos sirvieron para definir y aplicar medidas que garantizan la confidencialidad de la información. Se efectuó una evaluación de amenazas usando la metodología MAGERIT, lo que permitió detectar y valorar los activos en el departamento de Tecnologías de Información y Comunicación (TIC). Tras esta valoración, se identificaron los riesgos tecnológicos asociados a vulnerabilidades y se determinaron los controles necesarios para mitigarlos.

PALABRAS CLAVE: *MAGERIT, TIC, ISO 27001, riesgos tecnológicos*

Abstract

Achik Inti Savings and Credit Cooperative has played a key role in providing financial solutions throughout the Cañar canton and has proactively adapted to emerging competencies and the implementation of innovative projects. However, the lack of IT security protocols in the entity poses challenges, making it susceptible to unauthorized interventions. This project is oriented to the elaboration of an "IT SECURITY STANDARDS SCHEME FOR THE COOPERATIVE OF SAVINGS AND CREDIT ACHIK INTI LTDA, IN THE CANTON CAÑAR". To strengthen the structure of this research, the guidelines of ISO 27001:2013 and the recommendations of ISO 27002 were used. These frameworks were used to define and implement measures to ensure the confidentiality of information. A threat assessment was carried out using the MAGERIT methodology, which made it possible to detect and assess the assets in the Information and Communication Technologies (ICT) department. After this assessment, the technological risks associated with vulnerabilities were identified and the necessary controls to mitigate them were determined.

Keywords: technological risks, MAGERIT, ICT, ISO 27001

Índice de Tablas

Índice de ilustraciones

Introducción

A medida que surgen nuevas tecnologías de la información, las entidades financieras buscan adoptar servicios tecnológicos para mejorar sus procesos. Sin embargo, el uso inadecuado de estas tecnologías puede causar problemas a las organizaciones, ya que están expuestas a diversas amenazas que pueden convertirse en riesgos y afectar gravemente la integridad de la información. Por lo tanto, es importante que las instituciones financieras tomen medidas adecuadas para proteger la información que manejan y minimizar los riesgos asociados con el uso de las tecnologías de la información.

La seguridad de la información es un tema cada vez más relevante en el mundo empresarial. En la actualidad, las empresas y organizaciones manejan grandes cantidades de información sensible que requieren de medidas de protección adecuadas para evitar su pérdida, filtración o mal uso. Las cooperativas de ahorro y crédito no son la excepción, y es por ello que se hace necesario establecer políticas y procedimientos de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de los datos que manejan.

En este sentido, la Cooperativa de Ahorro y Crédito Achik Inti Ltda, ubicada en el cantón Cañar, requiere de un manual de políticas de seguridad de la información que le permita establecer un marco de referencia claro y coherente para la gestión de la seguridad de la información en la organización. Este manual permitirá a la cooperativa establecer medidas de protección adecuadas para garantizar la seguridad de la información y minimizar los riesgos asociados a su manejo.

CAPITULO I

MARCO REFERENCIAL

1.1. Planteamiento del Problema

En los últimos años, las empresas y organizaciones han adaptado a las tecnologías de la información, ya que estas generan valor en el negocio. Sin embargo, han sido víctimas de ataques informáticos que han afectado gravemente a activos importantes como la información.

Por ello, es importante instaurar una cultura de protección a través de un manual de políticas de seguridad de la información en las empresas, especialmente en las entidades financieras, con la finalidad de optimizar la seguridad, asegurando la continuidad del negocio, mitigando vulnerabilidades y estableciendo: criterios, directrices y estrategias que permitan la protección de los datos.

En base a lo expuesto, se pretende el diseño de un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, con el fin de proteger a los activos de la entidad financiera. Velando así por la confidencialidad, integridad y disponibilidad de la información de los diferentes departamentos.

1.2. Formulación del problema

¿Qué norma o estándar se utilizará como referencia para establecer las políticas de seguridad de la información?

¿Cuál será el enfoque metodológico aplicado para llevar a cabo el análisis y gestión de riesgos?

¿Cuáles son los procesos o activos que requieren mayor atención en cuanto a seguridad dentro de la organización?

1.3. Antecedentes de la Investigación

La aparición de Internet ha sido un factor determinante en el incremento de la exposición de las organizaciones a riesgos de seguridad informática, incluyendo ataques cibernéticos cada vez más sofisticados que afectan de manera perjudicial la integridad, disponibilidad y confidencialidad de la información almacenada en sus sistemas. Debido a esto, varios autores han realizado estudios de investigación sobre el tema, cuyos resultados han generado una serie de mejores prácticas que deben ser consideradas. A continuación, se presentan algunas de ellas:

La Corporación Autónoma Regional de Cundinamarca (2021), realiza un manual de políticas de seguridad de la información basado en la normativa ISO 27001:2013, definiendo pautas, directrices y reglas. Basándose también en un marco normativo de buenas prácticas, analizando la organización se seguridad de la información, sus funciones y las políticas de la Corporación.

De igual manera, Chimborazo (2021), desarrolla un manual de políticas de seguridad de la información tomando como referencia a la norma ISO 27001:2013 conjuntamente con la norma ISO 27002. El autor desarrolla una encuesta con la finalidad de determinar el estado de la infraestructura tecnológica y los procesos que realiza el área de TI del Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo. Concluyendo que el departamento de TI tiene como desventaja la falta de políticas de seguridad, y en caso de implementación del manual, este debe actualizarse según se requiera.

Arboleda (2021) en su documento, realiza una propuesta de seguridad de la información con la finalidad de proteger los activos de información en las organizaciones alineado a la ISO 27001:2013. Recalca que la falta de políticas de seguridad de la información es un problema que las empresas afrontan en base al uso y a la protección de los activos de información. Concluye que sería adecuado capacitar a los empleados de las organizaciones con el objetivo de que se cumplan las políticas de seguridad para la gestión de riesgos.

1.4. Justificación de la Investigación

En la actualidad, la información es uno de los activos más valiosos de cualquier organización, incluyendo las cooperativas de ahorro y crédito. La información financiera, personal y empresarial que manejan estas entidades es muy sensible y su seguridad es vital para garantizar la confianza y la satisfacción de los clientes.

Además, existen diversas amenazas cibernéticas que pueden poner en riesgo la seguridad de la información, como el robo de identidad, el fraude electrónico y el malware. Por lo tanto, es fundamental contar con políticas de seguridad de la información que permitan identificar, evaluar y gestionar los riesgos de seguridad y establecer medidas de protección adecuadas.

La propuesta de un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti Ltda, del cantón Cañar, contribuirá a mejorar la gestión de la seguridad de la información en esta entidad, promoviendo una cultura de seguridad y conciencia en el personal y los clientes. Además, permitirá a la cooperativa cumplir con las normativas y regulaciones en materia de seguridad de la información que sean aplicables.

1.5. Objetivos

1.5.1. Objetivo General

Diseñar una propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti Ltda del cantón Cañar.

1.5.2. Objetivos Específicos

- Realizar un estudio teórico sobre estándares de gestión de riesgos y guías de buenas prácticas de TI.
- Determinar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, a través del levantamiento y análisis de información de la seguridad de la información, vulnerabilidades, amenazas y riesgos del área de TI.
- Elaborar una propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar.

1.6. Limitaciones

- Acceso limitado a la información: Puede ser que no se tenga acceso completo a la información necesaria para diseñar el manual.
- La disponibilidad de tiempo y recursos limitara la capacidad de la tesis para cumplir con los objetivos establecidos de manera completa y efectiva.
- Limitaciones en el alcance de la tesis: Debido a la complejidad y extensión del tema, puede que sea necesario establecer un alcance limitado para la tesis, lo que podría limitar la profundidad del análisis y las recomendaciones.

1.7. Delimitaciones

- El presente proyecto será solamente una propuesta y no implicará su implementación.
- La propuesta del manual de políticas de seguridad de la información estará dirigida específicamente al departamento de Tecnologías de la Información y Comunicación (TIC) de la Cooperativa, con el objetivo de establecer lineamientos claros y efectivos en materia de seguridad de la información en este ámbito de la organización.

CAPITULO II

2. MARCO TEÓRICO

2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) cuenta con un conjunto de directrices fundamentales que permiten establecer, monitorear y mejorar de manera constante la gestión de la información en una organización. Esto se logra mediante la implementación de procesos adecuados en los sistemas de información, los cuales permiten la preservación de la confidencialidad, integridad y disponibilidad de la información. (Pilla Yanzapanta, 2019)

Asimismo, el SGSI contempla la identificación, seguimiento y mejora continua de los riesgos asociados a los eventos que puedan afectar la seguridad de la información de la organización.

El SGSI permite cumplir con los requisitos para la evaluación, seguimiento y tratamiento de los riesgos de seguridad de la información, de acuerdo a las necesidades de la organización. De esta manera, el SGSI puede ser implementado en una amplia variedad de organizaciones con el fin de proteger la seguridad de su información. (ISO2700.ES, s.f)

2.1.1. Uso de un SGSI

"Un Sistema de Gestión de la Seguridad de la información ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización" (Gestion de calidad , 2016, pág. 2). Esto se logra mediante la implementación de controles y medidas adecuadas que permiten reducir la exposición al riesgo por debajo del nivel de riesgo que la organización está dispuesta a asumir (Ilustración 1).

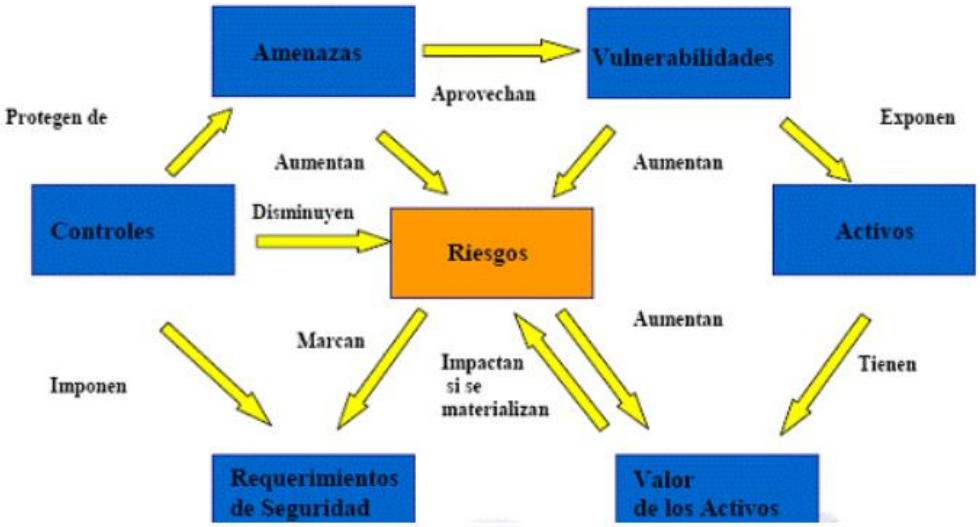


Ilustración 1: Uso del sistema de gestión de seguridad de la información

Fuente: recuperado de https://gestion-calidad.com/seguridad-informacion

2.1.2. Implementación de un sistema de gestión de seguridad de la información

El modelo PDCA se utiliza para gestionar un SGSI basado en la norma ISO 27001, y su enfoque continuo de mejora implica la constante revisión de las medidas de prevención, corrección y evaluación. Este enfoque es crucial para garantizar la eficacia y eficiencia del SGSI implementado.

El PDCA consta de 4 etapas principales tal como se visualiza en la Ilustración Nº 2, que se atraviesan en forma consecutiva. Una vez acabada la última etapa se vuelve a la primera repitiendo nuevamente el ciclo, de manera que se convierte en un ciclo iterativo de mejora continua.

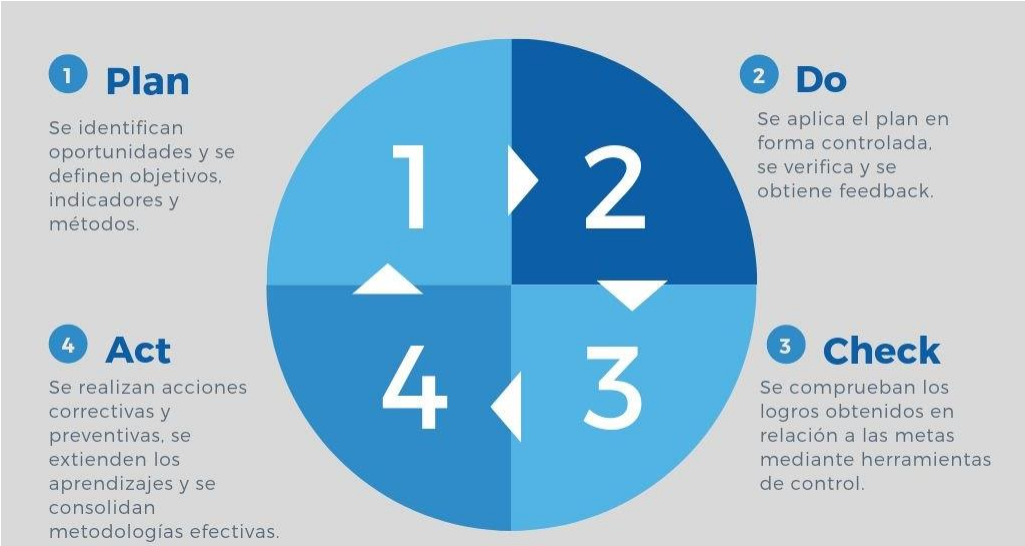


Ilustración 2: Ciclo PDCA
Fuente: Obtenido de https://twitter.com/MolteniCG/status/1154488524889976832?lang=zh-Hant

2.1.3. Seguridad informática y seguridad de la información

- **Seguridad informática:** La seguridad informática tiene como objetivo la protección de los recursos informáticos más importantes de una empresa, ayudando a cumplir los objetivos, a proteger los recursos financieros, los sistemas, la reputación de la entidad, entre otros. “En empresas privadas, la seguridad informática debe apoyar el capital socioeconómico. A esto los sistemas deben estar protegidos para evitar posibles pérdidas, que podrían causar la degradación de la funcionalidad del sistema o el acceso de personas no autorizadas” (Delgado, 2017, pág. 17)

- **Seguridad de la Información:** La seguridad de la información es un conjunto de métodos y técnicas que permiten el control y la salvaguarda de los datos de una determinada organización. Protegiendo los activos de los atacantes que invaden las redes, realizan robo o vandalismo informático. (Briceño, 2021)

2.2. Elementos de gestión de seguridad de la información

2.2.1. Identificación de activos

"Se denomina activos de información a todos los recursos que una organización posee y que tienen un valor significativo en relación a la generación, procesamiento, almacenamiento o transmisión de información" (Angeles, 2016, pág. 21).

La Ilustración Nº 3 presenta una clasificación de activos de información. En ella, se pueden identificar distintas categorías como recursos humanos, donde se reflejan aspectos relacionados con el personal y su gestión; recursos físicos, que engloban elementos tangibles esenciales para la organización, servicios, que abarcan las diferentes soluciones y atenciones proporcionadas, etc.

Ilustración 3: Activos de una organización
Fuente: obtenido de (Angeles, 2016)

2.2.2. Identificación de amenazas a los activos

La identificación de amenazas a los activos es el proceso de reconocer y determinar las posibles fuentes, eventos o circunstancias que podrían causar daño, pérdida o compromiso

de los activos de una organización. Implica catalogar las amenazas naturales, humanas y tecnológicas que podrían afectar la seguridad de los activos. Este proceso es esencial para la gestión de la seguridad de la información y ayuda a tomar decisiones informadas para proteger los activos de manera efectiva.

2.3. ISO/IEC 27001: 2013

2.3.1. Generalidades de la Norma

"Su función consiste en suministrar los criterios necesarios para instaurar un sistema de administración de seguridad informática en una empresa, sin importar su magnitud, ya que es adecuado para empresas de todos los tamaños" (Pilla Yanzapanta, 2019, pág. 11).

Paltán (2017) en su investigación sobre seguridad de la información, coincide con que el objetivo principal de estas estrategias es garantizar el uso correcto de los datos y tomar precauciones para evitar daños que puedan causar problemas tanto internos como externos.

En si "la norma ISO 27001 es un modelo de estándar desarrollado por ISO para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización" (Angeles, 2016, pág. 24).

2.4.ISO/EC 27002: 2013

"Se trata de una guía de buenas prácticas recomendadas que detalla los objetivos de control y los controles que se consideran apropiados en relación con la seguridad de la información" (ISO2700.ES, s.f, pág. 3).

Los contraponles de la ISO 27002 son los que ayudan a mantener las medidas de la seguridad de la información. Esta norma, que en un principio fue publicada como una actualización de la ISO 17799, ofrece directrices para la implementación de controles y

mecanismos que ayudan a garantizar la seguridad de la información, siguiendo las recomendaciones de la norma ISO 27001. (Pilla Yanzapanta, 2019)

2.4.1. Controles de la norma ISO/IEC 27002: 2013

En este texto se describe la especificación de los distintos elementos necesarios para llevar a cabo el análisis y desarrollo de la política de seguridad. Para esta nueva versión hay 93 controles los cuáles están organizados en 4 grupos, versus los 114 controles organizados en 14 categorías de la versión de 2013las cuales se pueden visualizar en la ilustración Nº 4

Ilustración 4

Dominios y controles de la norma ISPO 27001

LOS CONTROLES DE LA ISO 27002:2022					
5	**CONTROLES ORGANIZACIONALES**	**6**	**CONTROLES DE PERSONAS**	**8**	CONTROLES TECNOLOGICOS
5.1	Políticas de seguridad de la informacion	6.1	Selección	8.1	Dispositivos de punto final de usuario
5.2	Roles y responsabilidades en la Seguridad de la Información	6.2	Términos y condiciones de empleo	8.2	Derechos de acceso privilegiado
5.3	Segregación de deberes	6.3	Conciencia de seguridad de la información, educación y	8.3	Restricción de acceso a la información
5.4	Responsabilidades de la dirección	6.4	Proceso disciplinario	8.4	Acceso al código fuente
5.5	Contacto con las autoridades	6.5	Responsabilidades después de la terminación o cambio de	8.5	Autenticación segura
5.6	Contacto con grupos de interés especial	6.6	Acuerdos de confidencialidad o no divulgación	8.6	Gestión de la capacidad
5.7	Inteligencia de amenazas	6.7	Trabajo remoto	8.7	Protección contra malware
5.8	Seguridad de la Información en la gestión de proyectos	6.8	Informes de eventos de seguridad de la información	8.8	Gestión de vulnerabilidades técnicas
5.9	Inventario de información y otros activos asociados			8.9	Gestión de la configuración
5.10	Uso aceptable de la información y otros activos asociados	7	CONTROLES FISICOS	8.10	Eliminación de información
5.11	Devolución de activos	7.1	Perímetros de seguridad física	8.11	Enmascaramiento de datos
5.12	Clasificación de la información	7.2	Entrada física	8.12	Prevención de fugas de datos
5.13	Etiquetado de la información	7.3	Asegurar oficinas, habitaciones e instalaciones	8.13	Copia de seguridad de la información
5.14	Transferencia de información	7.4	Monitoreo de la seguridad física	8.14	Redundancia de las instalaciones de procesamiento de información
5.15	Control de acceso	7.5	Protección contra amenazas físicas y ambientales	8.15	Registro
5.16	Gestión de identidades	7.6	Trabajar en áreas seguras	8.16	Actividades de seguimiento
5.17	Información de autenticación	7.7	Escritorio y pantalla limpios	8.17	Sincronización de reloj
5.18	Derechos de acceso	7.8	Emplazamiento y protección de equipos	8.18	Uso de programas de utilidad privilegiados
5.19	Seguridad de la información en las relaciones con proveedores	7.9	Seguridad de los activos fuera de las instalaciones	8.19	Instalación de software en sistemas operativos
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	7.10	Medios de almacenamiento	8.20	Seguridad de redes
5.21	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	7.11	Servicios públicos de apoyo	8.21	Seguridad de los servicios de red
5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	7.12	Seguridad del cableado	8.22	Segregación de redes
5.23	Seguridad de la información para el uso de servicios en la nube	7.13	Mantenimiento de equipos	8.23	Filtrado web
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la	7.14	Disposición o reutilización segura de los equipos	8.24	Uso de la criptografía
5.25	Evaluación y decisión sobre eventos de seguridad de la información			8.25	Ciclo de vida de desarrollo seguro
5.26	Respuesta a incidentes de seguridad de la información			8.26	Requisitos de seguridad de las aplicaciones
5.27	Aprender de los incidentes de seguridad de la información			8.27	Arquitectura de sistemas seguros y principios de ingeniería
5.28	Recopilación de evidencias			8.28	Codificación segura
5.29	Seguridad de la información durante una interrupción			8.29	Pruebas de seguridad en el desarrollo y aceptación
5.30	Preparación de las TIC para la continuidad de negocio			8.30	Desarrollo externalizado
5.31	Requisitos legales, reglamentarios y contractuales			8.31	Separación de entornos de desarrollo, evidencia y producción
5.32	Derechos de propiedad intelectual			8.32	Gestión del cambio
5.33	Protección de registros			8.33	Información de las pruebas
5.34	Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)			8.34	Protección de los sistemas de información durante las pruebas de auditoría
5.35	Revisión independiente de la seguridad de la información				
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información				
5.37	Procedimientos operativos documentados				

2.5. Análisis y gestión de riesgo de la seguridad informática

Este proceso implica la identificación y evaluación de posibles amenazas y vulnerabilidades que puedan afectar la seguridad de los sistemas informáticos y los datos que se procesan y almacenan en ellos. También se explica que la gestión de riesgos de seguridad informática incluye la implementación de medidas y controles de seguridad apropiados para mitigar los riesgos identificados, así como la planificación y preparación para la respuesta a incidentes graves de seguridad

2.5.1. Metodología de gestión de riesgo informáticos

En la actualidad, hay diversas técnicas disponibles para examinar y manejar el riesgo, y la elección de la apropiada dependerá de las demandas de seguridad de la información de la empresa.

A continuación, se describe algunas metodologías para gestión de riesgo:

2.5.1.1. Metodología MAGERIT

El Consejo de Administración Electrónica en España diseñó una metodología para el análisis y gestión de riesgos en los sistemas de información. Esta técnica se emplea para examinar los riesgos que pueden afectar a los sistemas de información y para ofrecer soluciones de seguridad eficaces para su control.

MAGERIT es una metodología que presenta de manera clara y concisa los procedimientos y actividades fundamentales para llevar a cabo un proyecto de análisis y gestión de riesgo, y también incluye una serie de consejos y recomendaciones prácticas para su implementación efectiva. (Peña, 2019). Esta metodología plantea 4 etapas:

- **Planeación del análisis y la gestión de riesgos**: En esta etapa se consideran opiniones que puedan ser necesarias para dar inicio al análisis de riesgos y el proyecto de gestión, el cual ayuda a determinar si es conveniente llevarlo a cabo.

- **Análisis de Riesgos:** En esta etapa se identifica y evalúa cada uno de los elementos que intervengan en el riesgo, con el fin de lograr una evaluación del riesgo en las diferentes áreas del domino.

- **Gestión de Riesgos:** En esta etapa se identifica las salvaguardias necesarias que ayuden a reducir el riesgo que han sido detectados.

- **Selección de salvaguardas:** En esta etapa se selecciona las salvaguardas necesarias a implementarse, agrupa los documentos de trabajo para el análisis de riesgo y el proceso de gestión, presenta las documentaciones finales del proyecto y exhibe los resultados en diferentes niveles.

La metodología Magerit es una herramienta esencial desarrollada para la gestión y análisis de riesgos asociados con los sistemas de información. Esta metodología define un proceso compuesto por seis fases detalladas para realizar un análisis de riesgo adecuado, estas fases se presentan en la Ilustración Nº 5.

Ilustración 5: Procesos en metodología MAGERIT
Fuente: Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf

2.5.1.2. Metodología CRAMM

La metodología en cuestión se enfoca en la gestión y análisis de riesgos, lo que le permite identificar, medir y mitigar los ataques a los que se encuentran expuestas las organizaciones. Para ello, se realiza un análisis de riesgo que combina tanto técnicas cualitativas como cuantitativas, conformando una metodología mixta que proporciona una visión detallada de las amenazas. (Jimenez, 2021) Esta metodología trabaja con 3 fases para su desarrollo:

- **Identificación de activos y valoración:** En esta etapa se identifican los activos del sistema de información, incluyendo los físicos, el software y los datos.
- **Evaluación de amenazas y vulnerabilidades:** Determina la probabilidad de que ocurran inconvenientes en el sistema de información.
- **Selección de contramedidas y recomendaciones:** En esta fase, se compara la evaluación de los riesgos con el nivel de seguridad deseado para determinar la gravedad de los riesgos y justificar la implementación de contramedidas apropiadas.

La implementación adecuada de la metodología CRAMM garantiza una gestión de riesgos robusta y sistemática, protegiendo así los activos y la integridad del sistema o proyecto. En la ilustración Nº 6 se muestra el proceso a seguir para una correcta gestión de riesgo de acuerdo a esta metodología.

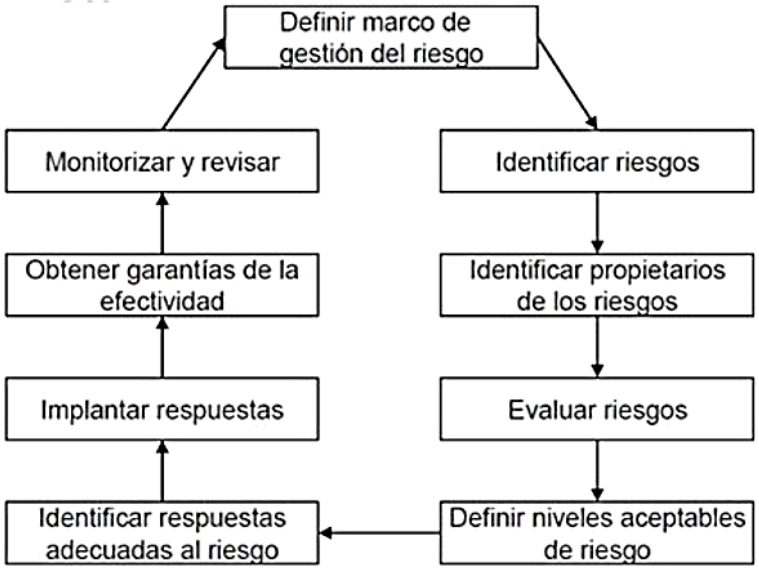


Ilustración 6: Proceso en la metodología CRAMM; **Fuente:** (Jimenez, 2021)

2.5.1.3.Metodología OCTAVE

"Permite tener en cuenta los riesgos operativos para los usuarios internos, identifica y evalúa los activos más críticos de la organización, realiza el monitoreo de riesgos y establece los componentes clave y las vulnerabilidades técnicas que causan los riesgos" (Jimenez, 2021, pág. 8). Esta metodología trabaja con 3 fases para su desarrollo:

- **Construir perfiles de amenazas basados en activos:** La primera fase identifica las amenazas que afectan los activos de la organización y las medidas de seguridad establecidas para protegerlos.

- **Identificar vulnerabilidades de la infraestructura:** Se identifica las vulnerabilidades de la infraestructura de TI que podrían conducir a acciones no autorizadas.
- **Desarrollar las estrategias y los planes de seguridad:** Se desarrolla un plan y estrategias de seguridad que toman en cuenta los riesgos identificados que podrían impactar a la organización.

En la ilustración Nº 7, se muestra un flujo secuencial desde la comprensión de la organización y sus activos críticos, pasando por la identificación y evaluación de amenazas hasta el desarrollo de estrategias adecuadas de mitigación.

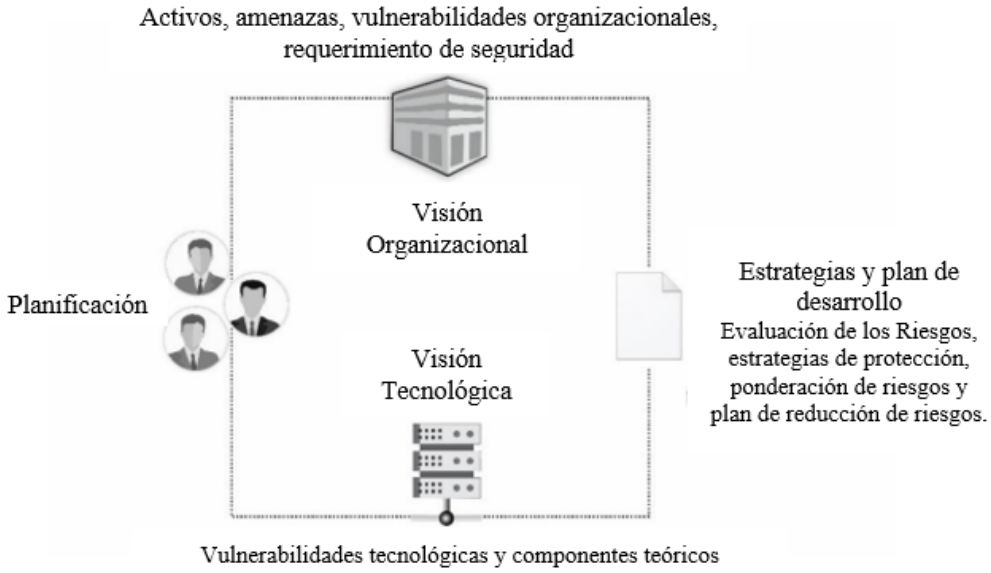


Ilustración 7: Fases del proceso de la metodología OCTAVE
Fuente: Obtenida de https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf

2.5.2. Norma internacional ISO/IEC 27005

La regulación establece pautas para la administración del riesgo de la seguridad de la información dentro de una empresa, enfocándose especialmente en los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la normativa NTE INEN-ISO/IEC 27001. (INEN, 2014)

2.5.2.1.Gestión de riesgo en tecnología de la información con ISO 27005

La ejecución de un Sistema de Gestión de Seguridad de Información (SGSI) y la ayuda de la norma ISO 27005 para la gestión de riesgos de seguridad informática, describe los procedimientos necesarios para llevar a cabo la evaluación, planificación, implementación y supervisión de las políticas de seguridad de información en cualquier organización. (Pilla Yanzapanta, 2019)

2.5.2.2. Identificación del Riesgo

La entidad realiza la identificación de riesgos mediante la identificación de las causas que pueden afectar los procesos. Estas causas pueden ser tanto internas como externas, y se determinan según el contexto estratégico de la entidad.

2.5.2.3. Evaluación del riesgo

El objetivo principal de la evaluación de riesgos es la identificación y valoración de cada uno de los riesgos detectados, lo que también ayuda a calcular el valor económico de cada activo de información y la relevancia de los mismos en la organización.

2.5.2.4.Tratamiento del Riesgo

Paltan (2017) determina que, “el tratamiento de riesgo es el proceso de selección e implementación de medidas de seguridad para corregir y mitigar los riesgos, con miras de

no afectar a la productividad, además de reducir estos riesgos con la menor inversión posible" (pág. 68).

2.5.3. Matriz comparativa de metodologías de gestión de riesgos Informáticos.

Esta matriz tiene como objetivo contrastar distintas metodologías en términos de su enfoque, gestión de riesgo, etapas de análisis, entre otros aspectos relevantes. Los indicadores seleccionados para la comparativa son: enfoque de la metodología, enfoque de riesgo, fases de análisis, enfoque de evaluación, uso de escenarios, marco de referencia y nivel de detalle. Cada uno de estos indicadores arroja luz sobre las características y diferencias clave entre las metodologías.

Tabla 1: Matriz de riesgo

Metodología	Enfoque	Enfoque de Riesgo	Fases de Análisis	Enfoque de Evaluación	Uso de Escenarios	Marco de Referencia	Nivel de Detalle
Magerit	Basada en riesgos	Enfoque cualitativo y cuantitativo	Identificación, Valoración, Tratamiento	Evaluación cualitativa y cuantitativa	Uso de escenarios	Basado en estándares y regulaciones	Mayor nivel de detalle en el análisis y valoración
OCTAVE	Basada en amenazas	Enfoque cualitativo y cuantitativo	Evaluación cualitativa y cuantitativa	Evaluación cuantitativa enfocada en amenazas	Uso de escenarios y evaluación de vulnerabilidades	Basado en mejores prácticas y experiencia	Enfoque más centrado en la gestión de riesgos internos y amenazas específicas
ISO 27005	Basada en riesgos	Enfoque cualitativo y cuantitativo	Identificación, Análisis, Evaluación y Tratamiento	Evaluación cualitativa y cuantitativa	Uso de escenarios y evaluación de vulnerabilidades	Basado en estándares internacionales	Nivel de detalle medio, se enfoca en el cumplimiento normativo y en la seguridad de la información

Tras llevar a cabo un minucioso análisis comparativo entre las metodologías presentadas en la tabla, es evidente que cada una tiene sus propias fortalezas y particularidades que la hacen única. Sin embargo, en función de los criterios considerados y las necesidades de nuestro contexto, **Magerit** ha emergido como la metodología más adecuada.

2.6. Políticas de seguridad de la información

"Las políticas de seguridad informática son un recurso empleado en las empresas para crear conciencia en los usuarios acerca de la relevancia y protección de la información confidencial y sensible vinculada con los procesos de la organización" (Pilla Yanzapanta, 2019, pág. 25).

El objetivo de las Políticas de Seguridad de la Información es establecer las normas y requisitos de seguridad necesarios para asegurar la confidencialidad, integridad y disponibilidad de los sistemas de información que forman parte de la empresa (Angeles, 2016).

- **Aspectos que debe asumir en las políticas de seguridad**

Los aspectos descritos en la ilustración Nº 8 garantizan que las políticas de seguridad aborden integralmente las necesidades de protección de la organización y sus activos.

ACCIÓN	PROPÓSITO
Garantizar en los sistemas de información	Confidencialidad Integridad Disponibilidad
Designar un responsable de seguridad	Delegado la gestión de la seguridad Debe estar dentro de las estructuras organizacionales de la empresa
Efectuar requisitos legales	Deben ser aplicable dentro de la empresa.
Gestionar incidencias	Todas las incidencias posibles de forma adecuada
Disponer de un plan de contingencia	El plan permite a la empresa recuperarse en caso de desastre.
Informar a lo empleados	Difundir entre los empleados sus obligaciones con respecto a la seguridad de los sistemas.

Ilustración 8: *Aspectos trascendentales;* ***Fuente:*** *(Angeles, 2016)*

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Enfoque de la Investigación

Para el desarrollo del presente proyecto se adoptará un enfoque metodológico mixtos, que combina técnicas cualitativa y cuantitativa.

Se llevaría a cabo investigación cualitativa, a través de entrevistas y encuestas, para entender las prácticas actuales y las necesidades de seguridad de la información. A su vez, se aplicaría investigación cuantitativa mediante auditorías de seguridad y análisis de riesgos para evaluar el estado actual de la seguridad. Los hallazgos de ambos enfoques orientarían el desarrollo de un manual de políticas personalizado, basado en las mejores prácticas de seguridad de la información y adaptado a las necesidades y capacidades específicas de la cooperativa.

3.2. Tipo de investigación

Para el proyecto se utiliza el tipo de investigación descriptiva y aplicada. Esta investigación descriptiva identificara y detallara las políticas y prácticas actuales de seguridad de la información de la cooperativa. Utilizando el tipo de investigación aplicada, se tomarán los resultados obtenidos de la investigación y se emplearán para crear una solución concreta y específica siendo esta: un manual de políticas de seguridad de la información destinado a mejorar la seguridad y reducir los riesgos en la cooperativa.

3.3. Población y Muestra

La población estará conformada por todos los miembros, empleados y partes interesadas de la Cooperativa de Ahorro y Crédito “Achik Inti”.

La muestra corresponde al personal encargado del departamento de TI y al gerente General de la Cooperativa.

3.4. Técnicas e Instrumentos de Recolección

Para la recolección de la información se aplicarán encuestas, entrevistas, análisis de documentos de diferentes bases científicas, con el fin de obtener una comprensión detallada de las prácticas de seguridad de la información y las percepciones sobre las políticas de seguridad.

3.5. Tratamiento de la Información

Una vez recopilado los datos a través de la entrevista, encuestas y análisis de documentos, los datos serán organizados de manera sistemática. Luego de la organización, se llevará a cabo el análisis de datos, basado en ello se procederá con la interpretación en el contexto de las necesidades de seguridad de la Información de la Cooperativa y finalmente se presentarán los hallazgos y conclusiones.

3.6. Interpretación de Resultados

La evaluación del grado de madurez se llevará a cabo mediante un análisis sistemático de las respuestas proporcionadas por el responsable del departamento de TIC y el gerente representando así el 100% de la población objetivo de este estudio. Los datos recogidos se categorizarán y analizarán de acuerdo a los dominios establecidos en la norma ISO/IEC 27002, una norma internacional para la gestión de la seguridad de la información. Este marco de referencia proporcionará las bases para 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 27002 para determinar el nivel de cumplimiento en el departamento de TIC.

Para evaluar el estado actual y el nivel de cumplimiento de la seguridad de la información en la Cooperativa de Ahorro y Crédito Achik Inti, se aplicó la encuesta al personal de TI y al gerente. Los datos obtenidos proporcionarán una perspectiva general del estado actual de la seguridad de la información en la cooperativa, permitiendo una evaluación del nivel de cumplimiento con los estándares de seguridad establecidos (ISO2700.ES, s.f).

Tabla 2: Resultados obtenidos por cada pregunta; ***Autor:*** *Propio*

Cooperativa de Ahorro y Crédito "ACHIK INTI" Ltda.

Código: A001
Fecha: 29/05/2023
Versión: 01

PREGUNTAS CLASIFICADAS POR DOMINIOS.

Dominios - ISO 27002	ENCUESTA	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 Usted que este documento es suficiente y apropiadamente difundido y comunicado a todos los miembros de la organización?		X	
	¿El documento de seguridad es revisado 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 de soporte a las iniciativas de seguridad?		X	
	¿En la entidad financiera se ha contratado personal con conocimientos en materia de seguridad de la información?	X		

Aspectos organizativos de la Seguridad de la Información.	¿Están claramente definidas los responsables, roles, y responsabilidades de la protección y aplicación de procesos de seguridad de todos los activos claves de la organización?	X	
	¿Están establecidos contactos y acuerdos de cooperación con organizaciones para el manejo de asuntos de seguridad?		X
	¿Se realizan auditorias de seguridad independientes a la implantación de las políticas de seguridad de la información de la organización?		X
	¿Se establecen contratos formales de seguridad cuando recursos de tecnologías de información de su organización serán accedidos y/o manejados por terceros?	X	
Seguridad Ligada a los Recursos Humanos.	¿Se cuenta con alguna política en la que se establezca que, en caso de abandono del puesto de trabajo de algún empleado se devuelva el equipamiento, así como también se elimine completamente los derechos de acceso (Acceso a información confidencial, Acceso a sistema)?	X	
	¿Se firman acuerdos de confidencialidad entre la organización y cada empleado como parte de los términos y condiciones de su trabajo?	X	
	¿Se educa y entrena a los empleados adecuadamente en las políticas y procedimientos de seguridad de la organización?		X
	¿Conocen los empleados los procedimientos para reportar amenazas, riesgos, sospechas u ocurrencias de: incidentes de seguridad, debilidades en sistemas o servicios e incorrecto funcionamiento de aplicaciones/software?	X	

	¿Están definidos los procesos disciplinarios para sancionar a aquellos empleados que incurran en violaciones a las políticas y procedimientos de seguridad de la información de la organización?	**X**	
Gestión de Activos.	¿Se dispone de inventario de activos asociados a los recursos del tratamiento de la información tales como: recursos de información (bases de datos, documentación de sistemas, manuales de usuario), recursos de software (software de aplicaciones, sistemas operativos, herramientas de desarrollo, etc.), activos físicos (equipamiento informático, dispositivos móviles, pen drives, mobiliario, etc.) y servicios (servicios informáticos y de comunicaciones, calefacción, iluminación, energía eléctrica, etc.)?	**X**	
	¿Existen esquemas o directrices para la clasificación de la información de la organización de acuerdo al grado de protección que deban recibir		**X**
	¿Están definidos los controles de protección asociados al grado de protección que deba recibir cada activo de información?		**X**
	¿Están definidos los procedimientos para el etiquetado y manejo de activos de información de acuerdo con el esquema de clasificación concebido por la organización?	**X**	
	¿Se protege los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización?	**X**	
	¿Para las aplicaciones que maneja la cooperativa se tienen políticas de control de acceso?	**X**	
	¿Existen diferentes niveles de acceso o privilegios para acceder a la información?	**X**	
	¿Existen procedimientos de auditoria para revisar y corregir los derechos de acceso de los usuarios de los sistemas de la organización?	**X**	

Control de Accesos.	¿Los usuarios son educados sobre sus responsabilidades o rutinas en el manejo de sus mecanismos de acceso a los sistemas?	X	
	¿Existe una política de uso de los servicios de la red?	X	
	¿Se restringe o controla el acceso a los servidores de la red?	X	
	¿Existen mecanismos de control de tráfico para evitar que flujos de datos y conexiones de otros nodos violenten la política de control de acceso?	X	
	¿Se utilizan mecanismos y herramientas de monitoreo para detectar usos irregulares de la red?	X	
	¿Se controla el acceso a la red y sistemas de la organización desde facilidades de computación móvil y tele-trabajo?	X	
	¿La organización cuenta con alguna política de uso de controles criptográficos?		X
	¿Se dispone de algún sistema de seguridad física contra desastres naturales, ataques maliciosos o accidentes en las oficinas, salas e instalaciones de la organización?	X	
	¿Se realiza el control de puntos de acceso a la organización como las áreas de entrada y salida, parqueaderos, (entre otras) para evitar el ingreso de personas no autorizadas a las dependencias de las instalaciones de procesamiento de información?	X	
	¿Se controla que los equipos, la información o el software se retiren del sitio después de la debida autorización?	X	
	¿Está el equipamiento en tecnologías de la información adecuadamente protegido para reducir riesgos o la exposición a amenazas ambientales o de acceso no autorizado?	X	

Seguridad Física y Ambiental.	¿Los equipos que conforman los servicios basados en tecnologías de la información son sometidos a las labores de mantenimiento indicadas por los fabricantes, así como en el período de tiempo especificado?	X		
	¿Se realiza algún tratamiento a la información almacenada en un equipo previo a su desincorporación o reúso?		X	
	¿En caso de alguna falla en el cableado de datos se está preparado para su pronta corrección?	X		
	¿Se dispone de áreas o sitios seguros para el desarrollo de proyectos o actividades propias de la entidad?			X
	¿Se documenta los procedimientos operativos y los mismos se deja a disposición de todos los usuarios que los necesiten?			X
	¿Están establecidos los procedimientos y roles para el manejo de incidentes de seguridad?			X
	¿Se dispone controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios?		X	
	¿Se definen criterios y planes de prueba para aceptar el uso de nuevos sistemas de información (o nuevas versiones/actualizaciones)?	X		
	¿Existen políticas y procedimientos para la ejecución de respaldos y su verificación?	X		
	¿Están implantados mecanismos para proteger la plataforma de red de la organización y la información que pasa a través de ella?	X		
	¿Se protege la documentación de los sistemas de información de la organización?	X		

Seguridad en la Operativa	¿Se ha implementado procedimientos para controlar la instalación de software en sistemas operacionales?	X		
	¿Existen reglas y procedimientos que gobiernen y controlen el intercambio de información y programas entre cooperativas?	X		
Seguridad en las Telecomunicaciones	¿Se cuenta con acciones en las redes para proteger la información en sistemas, aplicaciones y servicios?	X		
	¿Se tiene establecido procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito?	X		
	¿Se protege la mensajería electrónica?		X	
Gestión de incidentes en la Seguridad de la Información.	¿Se ha documentado algunos de los puntos débiles de la seguridad de la información?		X	
	¿Se realiza la valoración de eventos de seguridad de la información para poder tomar decisiones futuras?		X	
	¿Se definen los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?	X		
Cumplimiento	¿Se cuenta con políticas de protección de datos y privacidad de la información personal?			X
	¿Existe información con derechos de propiedad intelectual en la entidad?	X		

Conforme a la encuesta administrada al departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Achik Inti, donde se sometieron a evaluación los 14 dominios establecidos en la norma ISO 27002:2013, se procede a realizar un análisis cuantitativo para determinar el grado de adhesión a dichos dominios.

3.6.2. Dominio: Políticas de Seguridad

Según los resultados de la encuesta realizada al responsable de Tecnología de la Información (TI) de la Cooperativa Achik Inti, se ha identificado que la organización se encuentra en una fase de desarrollo (50%) para establecer las políticas de seguridad. Sin embargo, a pesar de que los empleados tienen un conocimiento general sobre las políticas de seguridad (25%), es importante destacar que la falta de una formalización oficial de dichas políticas de seguridad y su divulgación entre los miembros de la entidad constituyen un obstáculo significativo para la organización (25%). Ilustración Nª 9.

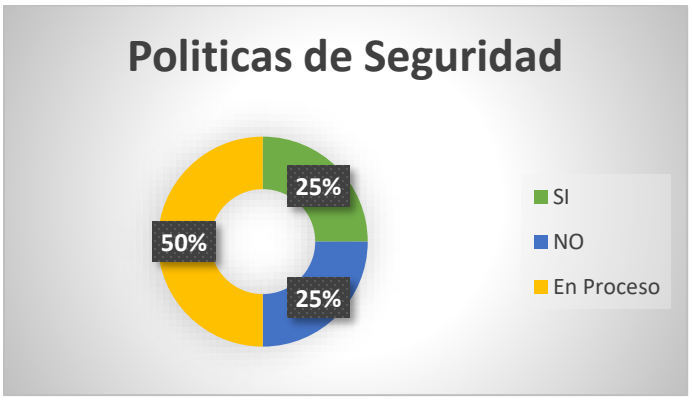


Ilustración 9: *Dominio Políticas de Seguridad; Autoría Propia*

3.6.3. Dominio: Aspectos organizativos de la seguridad de la información

De acuerdo a los resultados de la encuesta y la información recopilada en relación al dominio de *Aspectos Organizativos de la seguridad*, se puede constatar que la Cooperativa Achik Inti no tiene definidas las responsabilidades de seguridad. Además, solo cuenta con un empleado capacitado en seguridad de la información, lo que implica que esa persona asume toda la

responsabilidad en la entidad financiera. Razón por la cual se obtiene un promedio del 50% en cuanto al cumplimiento y un 50% de no cumplimento en los controles evaluados para este dominio, ver ilustración Nª 9.

Esta situación representa un riesgo tanto para la empresa como para el departamento de TI, debido a la falta de personal capacitado y la sobrecarga de trabajo para un único individuo. Esto dificulta el control adecuado de todos los activos informáticos.

Ilustración 10: *Dominio Aspectos Organizativos de la SI*

3.6.4. Dominio: Seguridad ligada a los recursos humanos

Según los resultados obtenidos del análisis de la encuesta en el dominio *de Seguridad relacionado con los recursos humanos*, se evidencia un cumplimiento adecuado en lo que respecta al proceso de contratación. Se ha implementado la firma de acuerdos de confidencialidad como medida preventiva para evitar la divulgación de información sensible. Además, se llevan a cabo capacitaciones orientadas a concientizar y mejorar el conocimiento sobre seguridad de la información, obteniendo un promedio del 80% en el total de su cumplimiento tal como se visualiza en la ilustración Nº 11.

Ilustración 11: *Dominio Seguridad Ligada a los RH*

3.6.5. Dominio: Gestión de Activos

En el ámbito de la *gestión de activos*, se realizó un análisis exhaustivo del dominio que reveló la presencia de inventarios de activos, diseñados para identificar el equipamiento disponible de la Cooperativa de Ahorro y Crédito ACHIK INTI. No cuentan con controles de protección, que varían dependiendo de la relevancia y el valor de cada activo de información, lo que puede ser un riego para los activos. Para garantizar un seguimiento y una supervisión eficientes de estos activos, se ha asignado un individuo responsable, en este caso, el coordinador de sistemas de la entidad. Este profesional tiene la tarea de gestionar y supervisar el estado, la utilización y la seguridad de todos los activos de información, garantizando así la integridad y la funcionalidad de estos valiosos recursos.

De acuerdo a los expuesto y el análisis técnico presentado, la Ilustración Nº 12 visualiza los resultados derivados. De estos datos, se evidencia que el 60% corresponde al grado de cumplimiento efectivo de los parámetros establecidos, mientras que el 40% representa deficiencias o la no implementación de controles específicos.

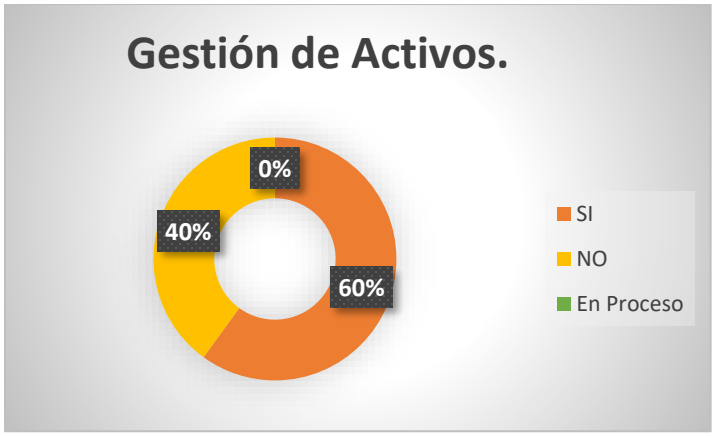


Ilustración 12: *Dominio Gestión de Activos*

3.6.6. Control de Acceso

Según los resultados de la evaluación realizada en el ámbito del dominio de *Control de Acceso*, se ha determinado que el departamento de Tecnologías de la Información (TI) cumple satisfactoriamente con la mayoría de los controles establecidos en este dominio. Específicamente, se ha observado que existen políticas claras y bien definidas en lo que respecta a la administración de redes, servicios, usuarios y autenticación basada en contraseñas.

No obstante, se ha identificado un vacío en las políticas de seguridad de la organización, puesto que no se han implementado procedimientos y controles Criptográficos de manera sistemática y estructurada. Dicho análisis se ve reflejado en la Ilustración Nº 13, con un porcentaje del 90% en el cumplimiento y 10% que representa el no cumplimiento de controles.

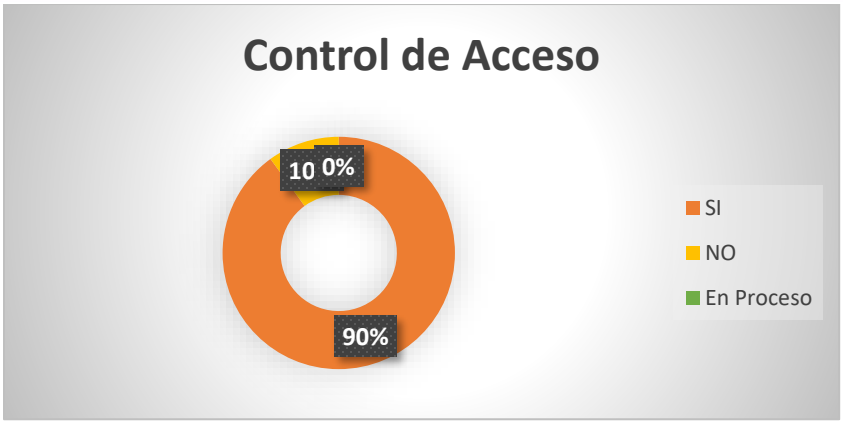


Ilustración 13: *Dominio Control de Acceso*

3.6.7. Dominio: Seguridad Física y Ambiental

De acuerdo a los resultados obtenidos en la encuesta referente al dominio *Seguridad Física y Ambiental*, se obtiene un porcentaje de 75% de los controles están en cumplimiento, el 13% están en procesos y el 12 no se están cumpliendo (Ilustración Nº 14), es decir, se determina dos áreas críticas en las que la Cooperativa ACHIK INTI carece de políticas adecuadas. Primero, la organización no está llevando a cabo un tratamiento de información efectivo, dejando un vacío en la gestión de la clasificación, almacenamiento y eliminación segura de la información. En segundo lugar, la organización no dispone de un área segura designada para el desarrollo de proyectos, lo que potencialmente puede comprometer la seguridad de la información y la integridad de los proyectos en curso.

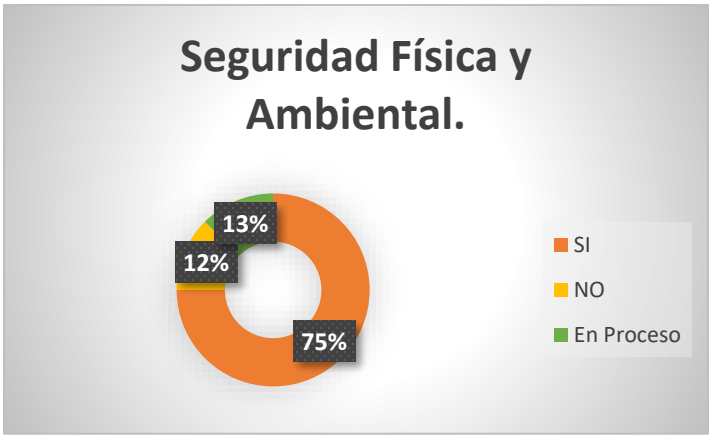


Ilustración 14*: Dominio Seguridad Fisca y Ambiental*

3.6.8. Dominio: Seguridad en la Operativa

Respecto a la *seguridad operativa*, se obtiene un 67% en el cumplimiento de controles, 22 % que se encuentran en procesos y el 11% no se está cumpliendo (Ilustración Nº 15), el análisis revela que la Cooperativa de Ahorro y Crédito Achik Inti tiene una sólida implementación de políticas y procedimientos de seguridad de la información. Esto incluye procedimientos documentados para la gestión de incidentes de seguridad, criterios y planes de prueba para nuevos sistemas de información, políticas para respaldos y su verificación, y medidas de protección para la plataforma de red y la instalación de software.

Sin embargo, la Cooperativa muestra una brecha significativa en su seguridad, al carecer de controles para la detección, prevención y recuperación de malware, junto con la educación adecuada de los usuarios sobre esta amenaza. Esta área debe ser abordada para fortalecer aún más la seguridad de la organización.

Ilustración 15: *Dominio Seguridad en la Operativa*

3.6.9. Dominio: Seguridad en las Telecomunicaciones

El análisis con respecto a la *seguridad de las telecomunicaciones* se obtiene un 67% en el cumplimiento de controles y 33% que no cumplen (Ilustración Nº 16), de acuerdo a estos resultados indica que la organización ha establecido medidas robustas para

salvaguardar la información en sistemas, aplicaciones y servicios, así como la información en tránsito. Sin embargo, se identifica un vacío de seguridad significativo en la protección de la mensajería electrónica. Este aspecto debe ser abordado para mejorar la seguridad general de la información de la organización.

Ilustración 16: *Dominio Seguridad en las telecomunicaciones*

3.6.10. Domino: Gestión de incidentes en la seguridad de las telecomunicaciones

Con respecto a la *Gestión de incidentes en la seguridad de la información* el análisis revela que el 75% de los controles no se cumplen o no se encuentran implementados y solo el 25% se encuentran en cumplimiento (Ilustración Nº 17), es decir que, aunque la Cooperativa ha definido procedimientos para la recolección y preservación de información como evidencia, existen brechas importantes en sus prácticas de seguridad de la información. Específicamente, la organización no documenta sus vulnerabilidades de seguridad ni evalúa los eventos de seguridad para guiar decisiones futuras.

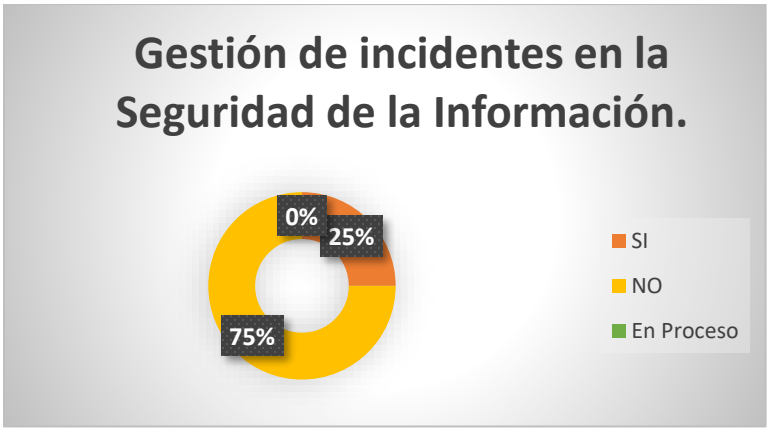


Ilustración 17: Dominio GISI

3.6.11. Dominio: Cumplimiento

En la evaluación del *Cumplimiento* se obtiene un porcentaje de 50% -50% (Ilustración Nº 18), el análisis señala que la Cooperativa está en proceso de implementar políticas de protección de datos y privacidad de la información personal, lo que indica una conciencia de la importancia de estas cuestiones. Además, se reconoce la presencia de información con derechos de propiedad intelectual en la organización, subrayando la necesidad de proteger adecuadamente estos activos valiosos. Sin embargo, para garantizar una seguridad completa, es crucial que se finalice la implementación de las políticas de protección de datos y privacidad.

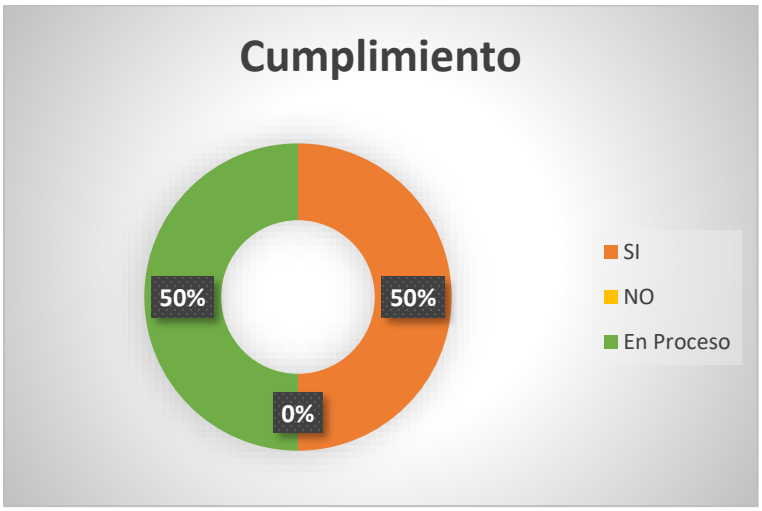


Ilustración 18: *Dominio Cumplimiento*

3.7. Análisis General de la Encuesta

La seguridad de la información en la Cooperativa Achik Inti revela una combinación de fortalezas y debilidades. Si bien se han tomado medidas efectivas en ciertos aspectos, como la implementación de políticas y procedimientos de seguridad, la gestión de activos y el control de acceso, también se han identificado importantes brechas. Estas incluyen la falta de formalización y divulgación de políticas de seguridad, la falta de asignación clara de responsabilidades de seguridad, la necesidad de controles de protección más sólidos, la falta de seguridad en la mensajería electrónica, la ausencia de documentación y evaluación de eventos de seguridad, y la finalización de políticas de protección de datos y privacidad. Es fundamental que la cooperativa aborde estas deficiencias para fortalecer su postura de seguridad y garantizar una protección adecuada de la información.

La Cooperativa Achik Inti Ltda., ha tomado algunas medidas para asegurar su información, pero se requiere una atención significativa para cerrar las brechas identificadas. Esto implica desarrollar e implementar políticas y procedimientos adecuados, fortalecer los controles de seguridad, mejorar la concienciación y formación del personal, y establecer una gestión integral y continua de la seguridad de la información. Al abordar estas áreas de mejora, la cooperativa podrá fortalecer su seguridad y proteger de manera más efectiva la información confidencial y los activos de la entidad financiera.

3.8. Selección de la metodología

Luego de estudiar las metodologías de análisis de riesgo MAGERIT, OCTAVE e ISO 27005 a través de una matriz comparativa, se ha seleccionado MAGERIT para su implementación. La elección de MAGERIT se justifica por su enfoque sistemático para el análisis y gestión de riesgos, su énfasis en los activos de la organización y su integración de

aspectos técnicos y organizativos. Además, su respaldo por parte del Consejo Superior de Administración Electrónica de España, sus guías y herramientas disponibles añaden valor y credibilidad a esta metodología. De esta manera, MAGERIT destaca como la principal elección para el análisis de riesgo 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 Achik Inti Ltda, del Cantón Cañar"

4.2. Justificación

Los datos dentro de las instituciones financieras como lo es la Cooperativa de Ahorro y Crédito "ACHIK INTI" Ltda., necesitan ser íntegros, seguros, fiables y accesibles a sus usuarios. Esta información, sin embargo, está expuesta a posibles alteraciones o violaciones, por lo que es imprescindible contar con medidas de seguridad informática.

En el departamento de sistemas de la entidad, no se han establecido normas ni metodologías de seguridad de la información, ya que los sistemas de información y comunicación no gozan de protección total. Por este motivo, se ha pensado en proponer un manual de apolíticas de SI basado en la norma de seguridad ISO 27001 y la guía de buenas prácticas ISO 27002, que incluyen numerosas estrategias de protección de la información en estos estándares.

Esta propuesta puede llevarse a cabo dado que existen los medios necesarios para recopilar información. Contamos con el respaldo del departamento de sistemas y con las herramientas requeridas para iniciar con las actividades planeadas.

4.3. Antecedentes de la Empresa

La Cooperativa de ahorro y crédito ACHIK INTI nace por las ideas de grupo jóvenes indígenas visionaros emprendedores, fue entonces que esta sociedad comenzó con reuniones

semanales, como no contaban con recursos suficientes para emprender grandes proyectos, se empezó con aportes económicos mensuales con lo cual se reunió un capital iniciándose con otorgamiento de préstamo a corto plazo especialmente a los personas de caso de recursos económicos de las parroquias y comunidades de la Provincia de Cañar ; entonces nació la mencionada cooperativa que pertenece a la nacionalidad kichwa del pueblo Cañari. (Chumaina, 2018)

La cooperativa actualmente viene trabajando en vinculación con las comunidades dando mayores beneficios en la agricultura, ganadería, artesanía, asociación de grupos de mujeres y jóvenes emprendedores buscando un mejor ingreso económico sustentable.

4.4. Objetivos del "Manual del manual de Políticas"

4.4.1.1. Objetivo General

"Diseñar un Manual de Políticas de Seguridad de la Información como propuesta para la Cooperativa de Ahorro Y Crédito Achik Inti Ltda, del cantón Cañar"

4.4.1.2. Objetivos Específicos

- Identificar los activos informáticos de la cooperativa de ahorro y crédito Achik Inti.
- Identificar los riesgos sobre los activos definidos.
- Analizar las probabilidades e impactos de los riesgos sobre los activos identificados bajo el alcance y calcular los niveles de riesgo, aplicando la metodología MAGERIT.
- Implementar controles sobre los activos, basado en un plan de tratamiento de riesgo.

Desarrollo de la Propuesta

4.5. Determinación del riesgo con MAGERIT

Es un procedimiento que permite identificar, evaluar y priorizar los riesgos a los que puede estar expuesto un sistema de información o un conjunto de activos de TI.

La metodología MAGERIT determina una serie de pasos o fase para la gestión de análisis de riesgo, ver Ilustración Nº 19:

- Identificar los Activos esenciales para la institución, su interrelación y su valor.
- Especificar las amenazas que enfrentan los activos
- Determinar las medidas de protección existentes (Controles, Salvaguardas)
- Estimar el impacto y la probabilidad, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el Riesgo

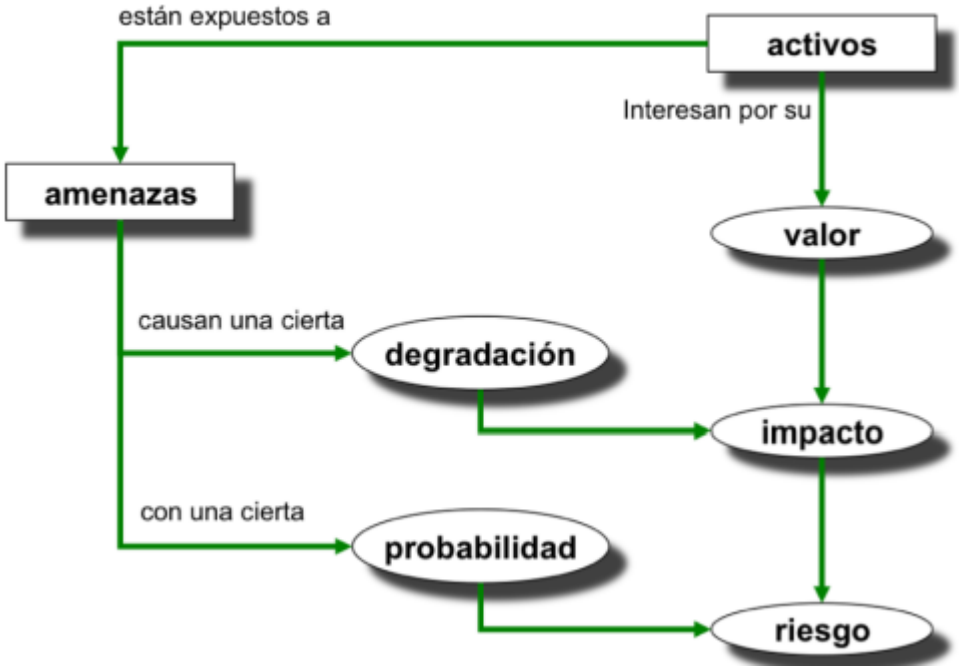


Ilustración 19: Elementos de Análisis de Riesgo; Fuente: (Amutio Gómez y otros, 2012)

4.5.1. Identificación de Activos de Información

El acto de identificar los activos de información es crucial, ya que facilita la determinación de los activos que están integrados a los procesos de la entidad.

Cada proceso demanda de activos de información específicos en múltiples formatos y tipos, que se enlistan en la tabla Nº 4 denominada Inventario de Activos, que se expondrá a continuación:

Tabla 3: Activos de Información; **Fuente:** Cooperativa de Ahorro y Crédito Achik Ini.

ID	Tipo de Activo	Activo
1	[SW] Software - Aplicaciones informáticas	- Achik Emprende - Achik Movil
2	[D] Datos / Información	- BBDD Financiero - BBDD Recaudador de Leche - Encriptación de la Huella de (Entrada y Salida) - Correos
3	[K] Claves criptográficas	- Reloj Biométrico - Servidores - Respaldos
4	[S] Servicios	- Créditos - Ahorros - Pago de Remesas (Rian y Western Union) - Pagos de Obligaciones Tributarios
5	[SI] Sistemas de Información	- Dima Cof
6	[HW] Equipamiento informático (hardware)	- Regulador CDP 8 compartimentos USB - Maquina lenovol, Rayzen 5 y 8 de Ram - Teléfono Ip Grandstream - Switch tplink 8 puertos - Mikrotik Router - Servidor Hp Dl380 Gen 10

7	[COM] Redes de comunicaciones	- Servidor Proilant Ml110 Gen 9 - Router A-Msr 900 - WAN - LAN - PPTP Juncal
8	[Media] Soportes de información	- Vima
9	[AUX] Equipamiento auxiliar	- Disco duro de 8T - Cámaras Vigilancia - Sensores de Movimiento
10	[P] Personal	- Iglesias Saiteros José Eduardo

4.5.2. Valoración de los Activos

Un activo puede tener valor en diversas perspectivas. Estas distintas perspectivas se denominan dimensiones. La metodología MAGERIT establece cinco dimensiones distintas que permiten medir el valor de un activo considerando el perjuicio que implicaría su desvalorización (Confidencialidad, Integridad, Disponibilidad, Autenticidad y trazabilidad).

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles).

En el Análisis de Riesgo que se llevará a cabo, se evaluarán las dimensiones [D] disponibilidad, [I] integridad de datos y [C] confidencialidad, puesto que estas son las dimensiones habitualmente tomadas en consideración en las organizaciones.

Tabla 4: Dimensiones; Autoría Propia

Confidencialidad	Integridad	Disponibilidad
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información

La valoración de los activos se llevará a cabo utilizando como referencia la escala detallada en la tabla Nº 6. Este proceso implicará examinar cada activo individualmente y asignarle un valor de acuerdo con los criterios establecidos en dicha tabla.

Tabla 5: Escala de Valoración de los Activos; Fuente: (Amutio Gómez y otros, 2012)

VALOR	NIVEL	CRITERIO
0	Muy Baja	Daño extremadamente grave
1-4	Baja	Daño muy Grande a la Organización
5-8	Medio	Daño Grave a la Organización
9-12	Alto	Daño Importante a la Organización
13-15	Muy Alto	Daño Menor a la Organización

A continuación, en la Ilustración Nº 20 se presenta las calificaciones específicas otorgadas a cada activo, basadas en la evaluación de la confidencialidad, disponibilidad e integridad. Esta evaluación es esencial para guiar las decisiones de gestión de riesgos y priorizar las medidas de seguridad a implementar en función de las necesidades de cada activo.

Tipo de activo	Codigo	Activos	Dimenciones de Valoracion			
			Disponibilidad	Integridad	Confidencialidad	TOTAL /15
[SW] Software - Aplicaciones informáticas	1	Achik Emprende	5	5	5	15
	2	Achik Movil	5	5	5	15
[D] Datos / Información	3	BBDD Financiero	5	5	5	15
	4	BBDD Recaudador de Leche	5	5	5	15
[K] Claves criptográficas	5	Incriptacion de la Huella de (Entrada y Salida)	5	5	4	14
	6	BBDD	5	5	5	15
	7	Reloj Biometrico	5	5	5	15
	8	Correos	4	5	4	13
	9	Servidores	5	5	4	14
	10	Respaldos	4	5	5	14
[S] Servicios	11	Creditos	5	5	5	15
	12	Ahorros	5	3	5	13
	13	Pago de Servicios Basicos	5	4	4	13
	14	Pago de Remesas (Rian y Western Union)	5	5	5	15
	15	Pagos de Obligaciones Tributarios	5	4	5	14
[SI] Sistemas de Información	16	Dima Cof	5	4	5	14
[HW] Equipamiento informático (hardware)	17	EQUIPO DE COMPUTO	5	5	5	15
	3	Teclado Xtech color negro	5	2	2	9
	19	Maquina lenovol, Rayzen 5 y 8 de Ram	5	2	5	12
	20	Regulador PCG 1200 6 compartimentos	5	4	5	14
	4	Mouse Genius alambrico	5	2	1	8
	21	Switch tplink 8 puertos	5	5	4	14
	22	Regulador de Voltaje CDP	3	5	5	13
	23	ROUTER A-MSR 900	4	5	3	12
	24	ROUTER A-MSR 901	5	4	4	13
	5	Altavoces duo Xtratech color negro	5	2	2	9
	25	GRANDSTREAM HT813	5	3	5	13
	26	MIKROTIK ROUTER	5	4	5	14
	6	Regulador CDP 8 compartimentos USB	5	1	1	7
	27	SERVIDOR HP DL380 GEN 10	3	5	5	13
	28	SERVIDOR PROILANT ML110 GEN 9	3	3	3	9
[COM] Redes de comunicaciones	29	Wan	5	5	5	15
	30	Lan	5	5	5	15
	31	PPTP Juncal	5	5	5	15
[Media] Soportes de información	32	vima	5	5	4	14
[AUX] Equipamiento auxiliar	33	Servidor	5	5	5	15
	34	Un disco duro de 8T	5	4	4	13
	35	Camaras Vijilancia	5	5	3	13
	36	Sensores de Movimiento	5	4	5	
[L] Instalaciones	37	Doumentacion de Redes	5	5	3	13
	38	Documentacion de licencias de los programas	5	5	4	14
[P] Personal	39	IGLESIAS SAITEROS JOSE EDUARDO	5	5	5	15
	40	JOSE MAURA	5	5	5	15

***Ilustración 20**: Calificación de Activos; **Autor**: Propio*

4.5.3. Identificación de las Amenazas

Las amenazas, que pueden ser de origen natural o humano, poseen el potencial de impactar negativamente o provocar perjuicios a los activos de información. Estos activos son esenciales para el funcionamiento eficaz de la organización, y cualquier daño a ellos podría llevar a la interrupción de las operaciones comerciales y pérdida de confianza de los clientes, entre otros problemas. Además de los activos de información, las amenazas pueden también poner en peligro la integridad de la organización en su conjunto, pudiendo causar daños que van desde perjuicios financieros hasta la pérdida de su reputación. Como tal, es de vital importancia identificar y manejar adecuadamente estas amenazas. Las amenazas que se detallarán a continuación (Tabla 7) provienen de Magerit y, por lo tanto, se aplicarán en el análisis de riesgo del departamento de informática de la Cooperativa de Ahorro y crédito "Achik Inti".

***Tabla 6**: Amenazas según el libro de MAGERIT; **Fuente**: (Amutio Gómez y otros, 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.1] Errores de los usuarios

[E] Errores y Fallos no Intencionados	[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

La evaluación del impacto de las amenazas y su probabilidad es fundamental en el análisis de riesgos. En primer lugar, se analiza el potencial daño que una amenaza específica podría ocasionar a un activo si llega a materializarse. Este impacto se valora en términos de los posibles efectos sobre la confidencialidad, integridad y disponibilidad del activo. En segundo lugar, se evalúa la probabilidad de que cada amenaza se materialice, considerando factores como la existencia de vulnerabilidades, la eficacia de los controles de seguridad y el entorno externo. Ambos factores, impacto y probabilidad, se combinan para determinar el nivel de riesgo de cada amenaza para cada activo, permitiendo priorizar los riesgos para su posterior mitigación.

Para la evaluación respectiva Magerit propone una escala de calificación de impacto basado en valores de 1 a 5, tal como se visualiza en la Tabla 8.

Tabla 7: Escala de calificación del IMPACTO; **Fuente:** (Amutio Gómez y otros, 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.

Esta escala permite a las organizaciones cuantificar el impacto potencial de las amenazas en sus sistemas de información y ayuda a determinar las prioridades para la gestión de riesgos.

Para calcular la probabilidad, se evalúa la posibilidad de que una amenaza se materialice en un activo específico. En la tabla 9 se muestra el valor de la probabilidad determinado en una escala de 1 a 5, donde 1 representa una probabilidad muy baja y 5 representa una probabilidad muy alta.

Tabla 8: Escala de calificación de la probabilidad; Fuente: (Amutio Gómez y otros, 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. Calculo del riesgo

Para el cálculo del riesgo se realiza una operación matemática, el cual consta de la multiplicación de la probabilidad por el impacto. El intervalo de calificación para el riesgo es entre 1 al 25 que representan la gravedad del riesgo. A continuación, la tabla 10 presenta una matriz de intervalos para determinar el nivel de riesgo.

Tabla 9: Intervalo de calificaciones del riesgo; Fuente: (Amutio Gómez y otros, 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

A continuación, la tabla 11 detalla la descripción específica de los activos activo con la calificación respectiva en las dimensiones de Disponibilidad, Integridad y Confidencialidad, las cuales son sumadas para ofrecer un total sobre 15 puntos que refleja la importancia relativa de cada activo en términos de seguridad.

Posteriormente, para cada activo, se presenta un catálogo de amenazas potenciales, cada una con una calificación de impacto y probabilidad. El producto de estas dos calificaciones genera una cifra de riesgo, que proporciona una medida cuantitativa del nivel de amenaza que representa cada situación para el activo en cuestión.

Tabla 10: Matriz de Riesgo

Tipo de activo	Código	Activos	Dimensiones de Valoración				Catálogo de Amenazas	Calculo del Riesgo		
			Disponibilidad	Integridad	Confidencialidad	TOTAL /15	Amenazas	Impacto	Probabilidad	RIESGO
[SW] Software - Aplicaciones informáticas	1	Achik Emprende	5	5	5	15	[N] Desastres naturales	5	3	**15**
							[I.5] Avería de origen físico o lógico	5	3	**15**
							[E.20] Vulnerabilidades de los programas (software)	5	3	**15**
							[A.10] Alteración de secuencia	5	3	**15**
	2	Achik Movil	5	5	5	15	[N.*] Desastres naturales	5	3	**15**
							[E.2] Errores del administrador	5	4	**20**
							[E.8] Difusión de software dañino	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	5	3	**15**
							[A.15] Modificación deliberada de la información	4	3	**12**
							[A.18] Destrucción de información	5	3	**15**
							[A.22] Manipulación de programas	4	3	**12**
							[E.19] Fugas de información	5	3	**15**
							[A.4] Manipulación de la configuración	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	5	3	**15**
							[A.6] Abuso de privilegios de acceso	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.19] Divulgación de información	5	3	**15**
						15	[E.19] Fugas de información	5	3	**15**
							[A.4] Manipulación de la configuración	5	4	**20**

	4	BBDD Recaudador de Leche	5	5	5		[A.5] Suplantación de la identidad del usuario	5	3	**15**
							[A.6] Abuso de privilegios de acceso	5	3	**15**
							[A.11] Acceso no autorizado	4	4	**16**
							[A.15] Modificación deliberada de la información	5	4	**20**
							[A.19] Divulgación de información	5	3	**15**
[K] Claves criptográficas	5	Incriptacion de la Huella de (Entrada y Salida)	5	5	4	14	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**
	6	BBDD	5	5	5	15	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	4	**20**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**
	7	Reloj Biometrico	5	5	5	15	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**

	8	Correos	4	5	4	13	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**
	9	Servidores	5	5	4	14	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**
	10	Respaldos	4	5	5	14	[E.1] Errores de los usuarios	4	3	**12**
							[E.18] Destrucción de información	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.15] Modificación deliberada de la información	5	3	**15**
							[A.18] Destrucción de información	4	3	**12**
							[A.19] Divulgación de información	5	3	**15**
[S] Servicios	11	Creditos	5	5	5	15	[E.1] Errores de los usuarios	4	3	**12**
							[E.10] Errores de secuencia	4	3	**12**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**

							[A.10] Alteración de secuencia	4	3	**12**
							[A.18] Destrucción de información	4	3	**12**
							[A.24] Denegación de servicio	5	3	**15**
	12	Ahorros	5	3	5	13	[E.1] Errores de los usuarios	4	3	**12**
							[E.10] Errores de secuencia	4	3	**12**
							[E.19] Fugas de información	5	5	**25**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.10] Alteración de secuencia	4	3	**12**
							[A.18] Destrucción de información	4	3	**12**
							[A.24] Denegación de servicio	5	3	**15**
	13	Pago de Servicios Basicos	5	4	4	13	[E.1] Errores de los usuarios	4	3	**12**
							[E.10] Errores de secuencia	4	3	**12**
							[E.19] Fugas de información	5	5	**25**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.10] Alteración de secuencia	4	3	**12**
							[A.18] Destrucción de información	4	3	**12**
							[A.24] Denegación de servicio	5	3	**15**
	14	Pago de Remesas (Rian y Western Union)	5	5	5	15	[E.1] Errores de los usuarios	4	3	**12**
							[E.10] Errores de secuencia	4	3	**12**
							[E.19] Fugas de información	5	5	**25**

							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.10] Alteración de secuencia	4	3	**12**
							[A.18] Destrucción de información	4	3	**12**
							[A.24] Denegación de servicio	5	3	**15**
	15	Pagos de Obligaciones Tributarios	5	4	5	14	[E.1] Errores de los usuarios	4	3	**12**
							[E.10] Errores de secuencia	4	3	**12**
							[E.19] Fugas de información	5	5	**25**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.5] Suplantación de la identidad del usuario	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.10] Alteración de secuencia	4	3	**12**
							[A.18] Destrucción de información	4	3	**12**
							[A.24] Denegación de servicio	5	3	**15**
[HW] Equipamiento informático (hardware)	17	EQUIPO DE COMPUTO	5	5	5	15	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	3	Teclado Xtech color negro	5	2	2	9	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**

							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	19	Maquina lenovol, Rayzen 5 y 8 de Ram	5	2	5	12	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	20	Regulador PCG 1200 6 compartimentos	5	4	5	14	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	4	Mouse Genius alambrico	5	2	1	8	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	21	Switch tplink 8 puertos	5	5	4	14	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**

							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	22	Regulador de Voltaje CDP	3	5	5	13	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	23	ROUTER A-MSR 900	4	5	3	12	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	24	ROUTER A-MSR 901	5	4	4	13	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	5	Altavoces duo Xtratech color negro	5	2	2	9	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**

	25	GRANDSTREAM HT813	5	3	5	13	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	26	MIKROTIK ROUTER	5	4	5	14	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	6	Regulador CDP 8 compartimentos USB	5	1	1	7	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	27	SERVIDOR HP DL380 GEN 10	3	5	5	13	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
	28	SERVIDOR PROILANT ML110 GEN 9	3	3	3	9	[N.1] Fuego	5	3	**15**
							[I.*] Desastres industriales	4	3	**12**
							[I.4] Contaminación electromagnética	4	3	**12**

							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.23] Manipulación de los equipos	4	3	**12**
[COM] Redes de comunicaciones	29	Wan	5	5	5	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**
							[E.2] Errores del administrador	5	3	**15**
							[E.18] Destrucción de información	4	3	**12**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.14] Interceptación de información (escucha)	4	3	**12**
	30	Lan	5	5	5	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**
							[E.2] Errores del administrador	5	3	**15**
							[E.18] Destrucción de información	4	3	**12**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.14] Interceptación de información (escucha)	4	3	**12**
	31	PPTP Juncal	5	5	5	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**
							[E.2] Errores del administrador	5	3	**15**
							[E.18] Destrucción de información	4	3	**12**
							[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.14] Interceptación de información (escucha)	4	3	**12**

[Media] Soportes de información	32	vima	5	5	4	14	[N.1] Fuego	5	3	**15**
							[N.*] Desastres naturales	4	3	**12**
							[I.5] Avería de origen físico o lógico	4	3	**12**
							[I.7] Condiciones inadecuadas de temperatura o humedad	4	3	**12**
							[E.19] Fugas de información	5	3	**15**
							[E.25] Pérdida de equipos	5	3	**15**
							[A.19] Divulgación de información	5	3	**15**
							[A.23] Manipulación de los equipos	5	3	**15**
							[A.25] Robo	5	3	**15**
							[A.26] Ataque destructivo	5	3	**15**
[AUX] Equipamiento auxiliar	33	Servidor	5	5	5	15	[N.1] Fuego	4	2	**8**
							[I.6] Corte del suministro eléctrico	5	3	**15**
							[I.7] Condiciones inadecuadas de temperatura o humedad	5	4	**20**
							[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**

							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**
							[E.25] Pérdida de equipos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	4	**20**
							[A.25] Robo	5	3	**15**
							[A.26] Ataque destructivo	5	4	**20**
	34	Un disco duro de 8T	5	4	4	13	[N.1] Fuego	4	2	**8**
							[I.6] Corte del suministro eléctrico	5	3	**15**
							[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**
							[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**
							[E.25] Pérdida de equipos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.25] Robo	5	3	**15**
							[A.26] Ataque destructivo	5	3	**15**
	35	Camaras Vijilancia	5	5	3	13	[N.1] Fuego	4	2	**8**
							[I.6] Corte del suministro eléctrico	5	3	**15**
							[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**
							[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**

							[E.25] Pérdida de equipos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.11] Acceso no autorizado	5	3	**15**
							[A.25] Robo	5	3	**15**
							[A.26] Ataque destructivo	5	3	**15**
	36	Sensores de Movimiento	5	4	5	14	[N.1] Fuego	4	2	**8**
							[I.6] Corte del suministro eléctrico	5	3	**15**
							[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**
							[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**
							[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**
							[E.25] Pérdida de equipos	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
[L] Instalaciones	37	Doumentacion de Redes	5	5	3	13	[N.1] Fuego	5	3	**15**
							[N.*] Desastres naturales	5	3	**15**
							[I.*] Desastres industriales	5	3	**15**
							[E.18] Destrucción de información	5	3	**15**
							[A.7] Uso no previsto	5	3	**15**
							[A.26] Ataque destructivo	4	3	**12**
							[A.27] Ocupación enemiga	4	3	**12**
[P] Personal	39	IGLESIAS SAITEROS JOSE EDUARDO	5	5	5	15	[E.7] Deficiencias en la organización	5	3	**15**
	40	JOSE MAURA	5	5	5	15	[E.7] Deficiencias en la organización	5	3	**15**

La matriz proporciona una visión completa de la valoración de riesgos para cada activo y permite identificar áreas de atención prioritaria para la implementación de medidas de seguridad que protejan los activos y reduzcan el riesgo a niveles aceptables.

4.5.6. Salvaguardas o Controles de Seguridad

El análisis de riesgos permitió entender la situación actual de los activos de la Cooperativa de Ahorro y Crédito “Achik Inti”. Las falencias detectadas en la gestión de seguridad de varios activos se exponen con detalle en la Tabla 10, en la cual enumera los activos de información que necesitan aumentar su protección, las amenazas potenciales, las medidas de seguridad que ayudarán a mitigar estas amenazas.

Las medidas de seguridad fueron seleccionadas basándose en un análisis de las amenazas y el nivel de riesgo a la que se exponen cada activo y las medidas de seguridad expuestas por la norma ISO 27002. La Tabla 12 representa claramente la alineación de los activos con los controles de la ISO/IEC 27002:2022. Estos constituyen los criterios de los dominios que deberían tenerse en cuenta al redactar el manual de políticas de seguridad.

Tabla 11: Controles determinados a cada amenaza con nivel de riesgo elevado (ISO 27002: 2022); Autoría Propia

Código	Activos	TOTAL /15	Catálogo de Amenazas	Calculo del Riesgo			
			Amenazas	Impacto	Probabilidad	RIESGO	Controles ISO 27002: 2022
1	Achik Emprende	15	[N] Desastres naturales	5	3	**15**	Protección contra amenazas físicas y ambientales
			[I.5] Avería de origen físico o lógico	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[E.20] Vulnerabilidades de los programas (software)	5	4	**20**	Gestión de la configuración
			[A.10] Alteración de secuencia	5	3	**15**	Codificación segura
2	Achik Móvil	15	[N.*] Desastres naturales	5	3	**15**	Protección contra amenazas físicas y ambientales
			[E.2] Errores del administrador	5	4	**20**	Ciclo de vida de desarrollo seguro
			[E.8] Difusión de software dañino	5	3	**15**	Protección contra malware
			[A.5] Suplantación de la identidad del usuario	5	3	**15**	Gestión de identidades
			[A.18] Destrucción de información	5	3	**15**	Transferencia de información
			[A.4] Manipulación de la configuración	5	3	**15**	Gestión de la configuración
			[A.6] Abuso de privilegios de acceso	5	3	**15**	Derechos de acceso
			[A.15] Modificación deliberada de la información	5	3	**15**	Políticas de seguridad de la información
4	BBDD Recaudador de Leche	15	[E.19] Fugas de información	5	3	**15**	Prevención de fugas de datos
			[A.4] Manipulación de la configuración	5	4	**20**	Gestión de la configuración
			[A.11] Acceso no autorizado	4	4	**16**	Autenticación segura
			[A.15] Modificación deliberada de la información	5	4	**20**	Políticas de seguridad de la información
		14	[E.1] Errores de los usuarios	4	3	**12**	Conciencia de seguridad de la información, educación y formación

5	Encriptación de la Huella de (Entrada y Salida)		[E.18] Destrucción de información	5	3	**15**	Transferencia de información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
			[A.15] Modificación deliberada de la información	5	3	**15**	Políticas de seguridad de la información
6	BBDD	15	[E.1] Errores de los usuarios	4	3	**12**	Conciencia de seguridad de la información, educación y formación
			[E.18] Destrucción de información	5	3	**15**	Transferencia de información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
			[A.15] Modificación deliberada de la información	5	4	**20**	Políticas de seguridad de la información
			[A.19] Divulgación de información	5	3	**15**	Acuerdos de confidencialidad o no divulgación
	Correos	13	[E.18] Destrucción de información	5	3	**15**	Transferencia de información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
			[A.15] Modificación deliberada de la información	5	3	**15**	Políticas de seguridad de la información
			[A.19] Divulgación de información	5	3	**15**	Acuerdos de confidencialidad o no divulgación
10	Respaldos	14	[E.1] Errores de los usuarios	4	3	**12**	Conciencia de seguridad de la información, educación y formación
			[E.18] Destrucción de información	5	3	**15**	Transferencia de información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
			[A.15] Modificación deliberada de la información	5	3	**15**	Políticas de seguridad de la información
			[A.19] Divulgación de información	5	3	**15**	Acuerdos de confidencialidad o no divulgación
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Redundancia de las instalaciones de procesamiento de información
			[A.7] Uso no previsto	5	3	**15**	Roles y responsabilidades en la Seguridad de la Información
			[A.24] Denegación de servicio	5	3	**15**	Seguridad de los servicios de red

	Ahorros	13	[E.19] Fugas de información	5	5	**25**	Prevención de fugas de datos
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Redundancia de las instalaciones de procesamiento de información
			[A.24] Denegación de servicio	5	3	**15**	Seguridad de los servicios de red
	Pago de Remesas (Rian y Western Union)	13	[E.19] Fugas de información	5	5	**25**	Prevención de fugas de datos
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Redundancia de las instalaciones de procesamiento de información
			[A.24] Denegación de servicio	5	3	**15**	Seguridad de los servicios de red
	Pagos de Obligaciones Tributarios	14	[E.19] Fugas de información	5	5	**25**	Prevención de fugas de datos
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Redundancia de las instalaciones de procesamiento de información
			[A.24] Denegación de servicio	5	3	**15**	Seguridad de los servicios de red
17	EQUIPO DE COMPUTO	15	[N.1] Fuego	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.7] Uso no previsto	5	3	**15**	Roles y responsabilidades en la Seguridad de la Información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
19	Maquina lenovol, Rayzen 5 y 8 de Ram	12	[N.1] Fuego	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.7] Uso no previsto	5	3	**15**	Roles y responsabilidades en la Seguridad de la Información
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
20	Regulador PCG 1200 6 compartimentos	14	[N.1] Fuego	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.7] Uso no previsto	5	3	**15**	Roles y responsabilidades en la Seguridad de la Información
21	Switch tplink 8 puertos	14	[N.1] Fuego	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.7] Uso no previsto	5	3	**15**	Roles y responsabilidades en la Seguridad de la Información

23	ROUTER A-MSR 900	12	[N.1] Fuego	5	3	**15**	
			[A.7] Uso no previsto	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
29	Wan	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**	Seguridad de los servicios de red
			[E.2] Errores del administrador	5	3	**15**	Ciclo de vida de desarrollo seguro
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Medios de almacenamiento
			[A.7] Uso no previsto	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
30	Lan	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**	Seguridad de los servicios de red
			[E.2] Errores del administrador	5	3	**15**	Ciclo de vida de desarrollo seguro
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Medios de almacenamiento
			[A.7] Uso no previsto	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
31	PPTP Juncal	15	[I.8] Fallo de servicios de comunicaciones	4	3	**12**	Seguridad de los servicios de red
			[E.2] Errores del administrador	5	3	**15**	Ciclo de vida de desarrollo seguro
			[E.24] Caída del sistema por agotamiento de recursos	5	3	**15**	Medios de almacenamiento
			[A.7] Uso no previsto	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[A.11] Acceso no autorizado	5	3	**15**	Autenticación segura
32	vima	14	[N.1] Fuego	5	3	**15**	Asegurar oficinas, habitaciones e instalaciones
			[E.19] Fugas de información	5	3	**15**	Prevención de fugas de datos
			[E.25] Pérdida de equipos	5	3	**15**	Inventario de información y otros activos asociados

			[A.19] Divulgación de información	5	3	**15**	Acuerdos de confidencialidad o no divulgación
			[A.23] Manipulación de los equipos	5	3	**15**	Disposición o reutilización segura de los equipos
			[A.25] Robo	5	3	**15**	Emplazamiento y protección de equipos
			[A.26] Ataque destructivo	5	3	**15**	Protección contra malware
	Servidor	15	[I.6] Corte del suministro eléctrico	5	3	**15**	Copia de seguridad de la información
			[I.7] Condiciones inadecuadas de temperatura o humedad	5	4	**20**	Trabajar en áreas seguras
			[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**	Gestión de vulnerabilidades técnicas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**	Mantenimiento de equipos
			[A.7] Uso no previsto	5	3	**15**	Emplazamiento y protección de equipos
			[A.11] Acceso no autorizado	5	4	**20**	Derechos de acceso
			[A.25] Robo	5	3	**15**	Emplazamiento y protección de equipos
			[A.26] Ataque destructivo	5	4	**20**	Protección contra malware
	Un disco duro de 8T	13	[I.6] Corte del suministro eléctrico	5	3	**15**	Seguridad de la información durante una interrupción
			[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**	Trabajar en áreas seguras
			[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**	Gestión de vulnerabilidades técnicas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**	Mantenimiento de equipos
			[E.25] Pérdida de equipos	5	3	**15**	Emplazamiento y protección de equipos

	Cámaras Vigilancia	13	[I.6] Corte del suministro eléctrico	5	3	**15**	Seguridad de la información durante una interrupción
			[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**	Trabajar en áreas seguras
			[I.9] Interrupción de otros servicios y suministros esenciales	5	3	**15**	Gestión de vulnerabilidades técnicas
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**	Mantenimiento de equipos
			[E.25] Pérdida de equipos	5	3	**15**	Emplazamiento y protección de equipos
			[A.11] Acceso no autorizado	5	3	**15**	Derechos de acceso
			[A.25] Robo	5	3	**15**	Entrada física
36	Sensores de Movimiento	14	[I.6] Corte del suministro eléctrico	5	3	**15**	Seguridad de la información durante una interrupción
			[I.7] Condiciones inadecuadas de temperatura o humedad	5	3	**15**	Trabajar en áreas seguras
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	3	**15**	Mantenimiento de equipos
			[E.25] Pérdida de equipos	5	3	**15**	Emplazamiento y protección de equipos
			[A.7] Uso no previsto	5	3	**15**	Términos y condiciones de empleo
37	Documentación de Redes	13	[N.1] Fuego	5	3	**15**	Protección contra amenazas físicas y ambientales
			[E.18] Destrucción de información	5	3	**15**	Conciencia de seguridad de la información, educación y formación
39	Iglesias Saeteros José Eduardo	15	[E.7] Deficiencias en la organización	5	3	**15**	Términos y condiciones de empleo
40	José Maura	15	[E.7] Deficiencias en la organización	5	3	**15**	Conciencia de seguridad de la información, educación y formación

En la tabla 13, se establecieron los mecanismos de control para cada activo de información susceptible a amenazas. Es importante destacar que los controles no siempre producen los resultados esperados, por lo tanto, se sugiere que se hagan modificaciones o actualizaciones, evaluarlas y así seleccionar las más adecuadas. A continuación, se presenta una matriz sintetizada que incluye todos los activos con un nivel de riesgo significativo.

Tabla 12: Clasificación de los riesgo más elevados; Autor: propio.

Código	Activos	TOTAL /15	Catálogo de Amenazas	Calculo del Riesgo			
			Amenazas	Impacto	Probabilidad	RIESGO	Controles ISO 27002: 2022
1	Achik Emprende	15	[E.20] Vulnerabilidades de los programas (software)	5	4	20	Gestión de la configuración
2	Achik Movil	15	[E.2] Errores del administrador	5	4	20	Ciclo de vida de desarrollo seguro
3	BBDD Recaudador de Leche		[A.4] Manipulación de la configuración	5	4	20	Gestión de la configuración
			[A.11] Acceso no autorizado	4	4	16	Autenticación segura
			[A.15] Modificación deliberada de la información	5	4	20	Políticas de seguridad de la información
6	BBDD	15	[A.15] Modificación deliberada de la información	5	4	20	Políticas de seguridad de la información
12	Ahorros	13	[E.19] Fugas de información	5	5	25	Prevención de fugas de datos
14	Pago de Remesas (Rian y Western Union)	13	[E.19] Fugas de información	5	5	25	Prevención de fugas de datos
15	Pagos de Obligaciones Tributarios	14	[E.19] Fugas de información	5	5	25	Prevención de fugas de datos
			[E.24] Caída del sistema por agotamiento de recursos	5	3	15	Redundancia de las instalaciones de procesamiento de información
			[A.24] Denegación de servicio	5	3	15	Seguridad de los servicios de red
17	EQUIPO DE COMPUTO	15	[N.1] Fuego	5	3	15	Asegurar oficinas, habitaciones e instalaciones
			[A.7] Uso no previsto	5	3	15	Roles y responsabilidades en la Seguridad de la Información
			[A.11] Acceso no autorizado	5	3	15	Autenticación segura
	Servidor	15	[I.6] Corte del suministro eléctrico	5	3	15	Copia de seguridad de la información

			[I.7] Condiciones inadecuadas de temperatura o humedad	5	4	**20**	Trabajar en áreas seguras
			[A.11] Acceso no autorizado	5	4	**20**	Derechos de acceso
			[A.26] Ataque destructivo	5	4	**20**	Protección contra malware
39	Iglesias Saiteros José Eduardo	15	[E.7] Deficiencias en la organización	5	3	**15**	Términos y condiciones de empleo

4.5.7. Resumen de la Matriz de Riesgo

Los objetivos de control y los controles establecidos por la norma ISO 27001 son ampliamente reconocidos y utilizados como referencia para la instauración de estrategias de seguridad en los sistemas de información. Este estándar proporciona un marco de trabajo robusto y detallado para asegurar la integridad, disponibilidad y confidencialidad de los activos de información.

En el proyecto actual, se hizo uso de estos controles, pero de una manera altamente específica y orientada al contexto de la organización. Para hacer esto, se realizó una evaluación exhaustiva del riesgo (como se muestra en la Tabla 10). Este proceso implicó la identificación de los activos de información relevantes, la determinación de las amenazas que podrían afectar a estos activos, y la evaluación de los impactos potenciales si estas amenazas se materializasen.

Una vez obtenida la matriz de cálculo de riesgo, se pudo seleccionar de manera informada los controles de seguridad más pertinentes para cada activo de información. El objetivo con esta selección no fue simplemente aplicar todos los controles posibles, sino escoger aquellos que contribuirían de manera efectiva a la reducción de los riesgos que fueron considerados inaceptables para nuestra organización. En otras palabras, se centró en aquellos riesgos que, tras el análisis, resultaron ser demasiado altos para tolerarlos.

Estos controles seleccionados se detallan en la Tabla 11. Esta tabla no solo refleja nuestra elección de controles de seguridad, sino también nuestra estrategia de gestión de riesgos. Al emplear los controles indicados, se busca reducir los riesgos a un nivel que esté en consonancia las tolerancias de riesgo, garantizando al mismo tiempo la continuidad de las operaciones y la protección de nuestros los activos de información.

4.6. Directrices o políticas para la seguridad de la Información

El objetivo principal del Sistema de Gestión de Seguridad de la Información (SGSI) es establecer un mecanismo eficiente para potenciar la protección de los datos e información manejada. Se desarrolló un Manual de Políticas de Seguridad de la Información para la Cooperativa de Ahorro y Crédito "ACHIK INTI" para mejorar la seguridad de la información y concienciar a los empleados sobre su importancia. Se establecieron políticas de seguridad basadas en la norma ISO 27001, que definen las conductas aceptables del personal y ayudan a preservar la confidencialidad, integridad y disponibilidad de la información.

Los puntos clave de los dominios de seguridad de la información son los siguientes:

- **Políticas de seguridad**: Establecer lineamientos para desarrollar políticas de seguridad que salvaguarden la integridad, confidencialidad y disponibilidad de la información.
- **Aspectos organizativos de la seguridad de la información:** Administra la seguridad mediante la asignación de procedimientos y responsabilidades.
- **Seguridad ligada a los recursos humanos:** Informa y concientiza a los empleados sobre la importancia de preservar la confidencialidad de la información y las consecuencias del incumplimiento de las políticas.
- **Gestión de activos:** Asegura que los funcionarios conozcan todos los activos de la entidad.
- **Control de acceso:** Controla el acceso a sistemas, servicios y bases de datos para proteger la información contra accesos no autorizados y manipulaciones.

- **Cifrado:** Utilizar sistemas criptográficos para proteger la información mediante un análisis de riesgos.
- **Seguridad física y ambiental:** Minimizar los riesgos causados por eventos naturales o falta de control en la seguridad física.
- **Seguridad en la operativa:** Controla y protege la documentación, bases de datos, copias de seguridad y recursos informáticos y de telecomunicaciones.
- **Seguridad en las telecomunicaciones:** Asegura la protección de la información comunicada y garantizar la confiabilidad de las comunicaciones entre instituciones y redes públicas.
- **Adquisición, desarrollo y mantenimiento de sistemas de información:** Establece controles y procedimientos para la adquisición, desarrollo y mantenimiento de sistemas de información.
- **Relaciones con proveedores:** Mantiene la seguridad de la información a través de convenios con proveedores de servicios de terceros.
- **Gestión de incidentes en la seguridad de la información:** Gestiona los incidentes de seguridad que puedan afectar los activos de información.
- **Cumplimiento:** Las políticas de seguridad deben ser cumplidas por todo el personal que procese información, especialmente aquellos relacionados con los sistemas de información.

Estos dominios son parte de un sistema de gestión de seguridad de la información (SGSI) diseñado para mejorar la seguridad de la información y concientizar al personal sobre su importancia.

Conclusiones y Recomendaciones

Conclusiones

El estudio teórico sobre estándares de gestión de riesgos y buenas prácticas de TI ha proporcionado un conocimiento sólido en seguridad de la información, lo cual es fundamental para el desarrollo de políticas y procedimientos de seguridad adecuados en la cooperativa.

Para determinar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, se llevó a cabo una entrevista con el gerente y el personal del área de TI. Durante la entrevista, se recopiló información sobre los activos existentes en el departamento de Tecnologías de la Información y Comunicación (TIC). A través del análisis de riesgo realizado, se pudo identificar los activos más críticos y las principales amenazas a las que la cooperativa se enfrenta.

El análisis de riesgo reveló deficiencias y áreas de mejora significativas en la gestión de activos, la protección de la información y la respuesta a incidentes de seguridad. Estas deficiencias ponen de manifiesto la necesidad urgente de implementar medidas de seguridad más efectivas.

La elaboración de una propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti es una acción concreta y práctica para abordar las deficiencias identificadas. Este manual proporcionará una guía clara de cómo gestionar los activos de información, implementar controles de seguridad apropiados y establecer un plan de respuesta a incidentes. Su implementación contribuirá a fortalecer la postura de seguridad de la cooperativa y proteger adecuadamente la información sensible de la organización.

Recomendaciones

- Realizar revisiones periódicas de la efectividad de los controles seleccionados: Aunque se ha llevado a cabo una evaluación exhaustiva del riesgo y se han seleccionado controles de seguridad pertinentes, es importante realizar revisiones periódicas para evaluar la efectividad de estos controles en la reducción de los riesgos identificados. Esto permitirá identificar posibles deficiencias o necesidades de actualización y realizar ajustes o mejoras según sea necesario.
- Establecer un proceso de seguimiento y actualización de la matriz de riesgo: Dado que la matriz de riesgo es un componente fundamental en la selección de controles de seguridad, se recomienda establecer un proceso estructurado para el seguimiento y actualización de dicha matriz. Esto implica revisar periódicamente los activos de información, las amenazas potenciales y los impactos, y ajustar la matriz de riesgo en función de los cambios en el entorno operativo y las nuevas amenazas identificadas. Mantener la matriz de riesgo actualizada garantizará la pertinencia y efectividad continua de los controles de seguridad implementados.

Referencias

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

Angeles, T. C. (11 de 05 de 2016). *repositorio.puce.edu.ec.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/11437/ELABORACI%C3%93N%20DE%20POLITICAS%20Y%20NORMAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf?sequence=1

ARBOLEDA, A. O. (01 de 01 de 2021). *repository.unad.edu.co.* Recuperado el 18 de 01 de 2023, de https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1&isAllowed=y

Briceño, E. V. (01 de 03 de 2021). *www.3ciencias.com.* Recuperado el 13 de 01 de 2023, de https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Casa, A. C., Gavilanez, M. L., Caiza, C. C., & Moreano, J. A. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Revista Ciencias de la Ingeniería y Aplicadas, 5*(2), 82-98.

Chumaina, M. M. (01 de 01 de 2018). *http://dspace.espoch.edu.ec/.* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/9842/1/82T00897.pdf

Corporación Autónoma Regional de Cundinamarca. (29 de 10 de 2021). *www.car.gov.co.* Recuperado el 18 de 01 de 2023, de https://www.car.gov.co/uploads/files/61840aaf4c32e.pdf

Delgado, C. A. (2017). *Fundamentos de seguridad informática.* Bogotá: Fondo editorial Areandino. Obtenido de https://core.ac.uk/download/pdf/326424171.pdf

Gestion de calidad . (07 de 11 de 2016). *gestion-calidad.com.* Obtenido de https://gestion-calidad.com/seguridad-informacion

INEN. (08 de 08 de 2014). *normalizacion.gob.ec.* Obtenido de https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27005.pdf

ISO2700.ES. (s.f). *www.iso27000.es.* Obtenido de https://www.iso27000.es/sgsi.html

Jimenez, J. N. (01 de 06 de 2021). *dspace.ups.edu.ec.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf

NQA.ISO. (4 de 10 de 2018). *www.nqa.com.* Recuperado el 13 de 01 de 2023, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Orellana, A. E. (10 de 09 de 2017). *epositorio.upse.edu.ec.* Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf

Orellana, A. E. (10 de 09 de 2017). *repositorio.upse.edu.ec.* Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf

Peña, H. M. (09 de 09 de 2019). *repository.unad.edu.co.* Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/27758/1/1075211684.pdf

Pilla Yanzapanta, J. C. (01 de 01 de 2019). *repositorio.uisek.edu.ec.* Obtenido de 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

QUIZHPI, C. F. (01 de 01 de 2021). *dspace.ucacue.edu.ec.* Recuperado el 18 de 01 de 2023, de https://dspace.ucacue.edu.ec/bitstream/ucacue/12762/1/Tesis%20Carlos%20Chimborazo%20Final.pdf

ROJAS, D. S., & ROMERO, E. L. (01 de 01 de 2018). *repository.udistrital.edu.co.* Recuperado el 13 de 01 de 2023, de https://repository.udistrital.edu.co/bitstream/handle/11349/13418/BuitragoRojasDanielaStefany2018.pdf;jsessionid=17B1BA11034E84877BBF012F88170964?sequence=1

Anexos

Trabajo de Titulación

Tema:

PROPUESTA DE MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR

Unidad Académica

Informática, Ciencias de la Computación e Innovación Tecnológica

Carrera

Ingeniera en Sistemas de la Información

Alumno

SEGUNDO FRANCISCO BERMEJO PICHASACA

Tutor:

Ing. Cristhian Humberto Flores Urgiles.

Octubre-Febrero
2023

Cañar, 14 de Enero del 2023

Ingeniero
Leopoldo Pauta Ayabaca, Msc.
DECANO DE LA UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA
Ciudad.

Yo, **SEGUNDO FRANCISCO BERMEJO PICHASACA**, con número de identificación **0350152690**, alumno de la carrera de Ingeniería de Sistemas de la Información, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"PROPUESTA DE MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR",** proponiendo como tutor de la misma al Ing. Cristhian Humberto Flores Urgilés., el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculada en la Unidad de Titulación.

Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;

_____

Sr. Segundo Francisco Bermejo Pichasaca
Estudiante de Ingeniería de Sistemas de la Información, extensión Cañar
CI: 0350152690

Anexo: Formato del Anteproyecto.

A. TÍTULO
PROPUESTA DE MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática y Seguridad Informática	x
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En los últimos años, las empresas y organizaciones han adoptado a las tecnologías de la información, ya que estas generan valor en el negocio. Sin embargo, han sido víctimas de ataques informáticos que han afectado gravemente a activos importantes como la información. Por ello, es importante instaurar una cultura de protección a través de un manual de políticas de información en empresas, especialmente en entidades financieras, con la finalidad de optimizar la seguridad, asegurando la continuidad del negocio, mitigando vulnerabilidades. Estableciendo criterios, directrices y estrategias que permitan la protección de los datos.

En base a lo expuesto, se pretende el diseño de un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, con el fin de proteger a los activos de la entidad financiera. Velando así por la confidencialidad, integridad y disponibilidad de la información de los diferentes departamentos.

D. OBJETIVO GENERAL

Diseñar un propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti Ltda del cantón Cañar.

E. OBJETIVOS ESPECÍFICOS

1. Realizar un estudio teórico sobre estándares de gestión de riesgos y guías de buenas prácticas de TI.

2. Determinar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, a través del levantamiento y análisis de información de la seguridad de la información, vulnerabilidades, amenazas y riesgos del área de TI.

3. Elaborar una propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar.

F. JUSTIFICACIÓN

Una medida preventiva y reactiva que deben utilizar las diferentes entidades financieras y organizaciones para el respaldo de su información, es la aplicación de la seguridad de la información. Con el fin de garantizar la privacidad, integridad, disponibilidad de la información.

Es importante considerar que un nivel de protección total, no es posible, por ello un sistema de gestión de la seguridad de la información debe endosar que los riesgos de la seguridad de la información sean conocidos, gestionados y sobre todo minimizados por la entidad. En función de lo descrito anteriormente, se propone realizar una propuesta de manual de políticas de información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, con la finalidad de especificar el manejo y uso adecuado de las tecnologías para la obtención de un mayor grado de ventajas que brindan estas herramientas y sobre todo, la integridad de la información.

G. ALCANCE

El alcance de la presente investigación va a permitir generar un manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, que proporcione controles de seguridad para reducir los riesgos y vulnerabilidades.

H. CONCEPTOS RELACIONADOS

Seguridad de la Información

La seguridad de la información es un conjunto de métodos y técnicas que permiten el control y la salvaguarda de los datos de una determinada organización. Protegiendo los activos de los atacantes que invaden las redes, realizan robo o vandalismo informático. (Briceño, 2021)

Seguridad Informática

La seguridad informática tiene como objetivo la protección de los recursos informáticos más importantes de una empresa, ayudando a cumplir los objetivos, a proteger los recursos financieros, los sistemas, la reputación de la entidad, entre otros. “En empresas privadas, la seguridad informática debe apoyar el capital socioeconómico. A esto los sistemas deben estar protegidos para evitar posibles pérdidas, que podrían causar

la degradación de la funcionalidad del sistema o el acceso de personas no autorizadas" (Delgado, 2017, pág. 17)

ISO 27001:2013

La norma ISO 27001:2013, permite el aseguramiento, confidencialidad e integridad de la información y de sus sistemas, proporcionando un marco robusto para la protección de los datos en organizaciones de tipo y tamaño. "El enfoque de la ISO 27001 fomenta el desarrollo de una cultura interna que esté alerta a los riesgos de seguridad de la información y tenga un enfoque coherente para enfrentarlos. Esta coherencia de enfoque conduce a controles que son más robustos en el manejo de amenazas. El costo de implementarlos y mantenerlos también se minimiza, y en caso de que fallen, las consecuencias se minimizarán y se mitigarán de manera más efectiva" (NQA.ISO, 2018, pág. 5)

Sistema de Gestión de Seguridad de la Información (SGSI)

Buitrago y Alvarado (2018) manifiesta que el sistema de Gestión de Seguridad de la Información, tiene como fin la protección de la información y sobre todo de los sistemas de información. Preservando la confidencialidad, integridad y disponibilidad de la información, para garantizar que este se gestione correctamente, es necesario identificar el ciclo de vida, el cual es el ciclo de Deming.

Políticas de Seguridad Informática

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados Llano et al. (Casa y otros, 2021).

I. ANTECEDENTES DE LA INVESTIGACIÓN

Existen varios autores que han desarrollado diversos estudios de investigación sobre el tema, cuyos resultados han generado una guía a tomarse en consideración. A continuación, se mencionan algunos de ellos:

La Corporación Autónoma Regional de Cundinamarca (2021), realiza un manual de políticas de seguridad de la información basado en la normativa ISO 27001:2013, definiendo pautas, directrices y reglas. Basándose

también en un marco normativo de buenas prácticas, analizando la organización se seguridad de la información, sus funciones y las políticas de la Corporación.

De igual manera, Chimborazo (2021), desarrolla un manual de políticas de seguridad de la información tomando como referencia a la norma ISO 27001:2013 conjuntamente con la norma ISO 27002. El autor desarrolla una encuesta con la finalidad de determinar el estado de la infraestructura tecnológica y los procesos que realiza el área de TI del Gobierno Autónomo Descentralizado Municipal Intercultural El Tambo. Concluyendo que el departamento de TI tiene como desventaja la falta de políticas de seguridad, y en caso de implementación del manual, este debe actualizarse según se requiera.

Arboleda (2021) en su documento, realiza una propuesta de seguridad de la información con la finalidad de proteger los activos de información en las organizaciones alineado a la ISO 27001:2013. Recalca que la falta de políticas de seguridad de la información es un problema que las empresas afrontan en base al uso y a la protección de los activos de información. Concluye que sería adecuado capacitar a los empleados de las organizaciones con el objetivo de que se cumplan las políticas de seguridad para la gestión de riesgos.

J. METODOLOGÍA

El método a utilizar en el presente trabajo de investigación, será deductivo puesto que parte de lo general a lo específico, es decir, se realizará un análisis de las situaciones actuales del área de TI en la cooperativa Achik Inti del cantón Cañar, evaluando la seguridad de la información basado en una normativa como la ISO/IEC 27001:2013.

Recolectando información a través de entrevistas o encuestas a las personas encargadas del área de TI en cuanto a los procesos que realizan en esta área.

K. CRONOGRAMA DE ACTIVIDADES																								
N°	ACTIVIDAD	MES I				MES II				MES III				MES IV				MES V				
		S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S4	MEDIOS DE VERIFICACIÓN
1.	Realizar un estudio teórico sobre estándares de gestión de riesgos y guías de buenas prácticas de TI																					
1.1	Bases teóricas sobre la gestión de riesgos y guías de buenas prácticas de TI	X	X	X	X	X	X															Lista de documentos almacenados en la herramienta Mendeley
2.	Determinar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, a través del levantamiento y análisis de información de la seguridad de la información, vulnerabilidades, amenazas y riesgos del área de TI.																					
2.1	. Aplicar las encuestas y entrevistas al personal de TI. -								X	X	X	X										Documento con los resultados de las encuestas
2.2	Aplicar un análisis en base a los dominios de la ISO27001											X	X	X	X							Documento con el análisis en base a la norma ISO 27001:2013
3.	Elaborar una propuesta de manual de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar																					
3.1	Desarrollo de la propuesta de manual de políticas de seguridad de la información													X								Elaboración del Documento de Políticas de información

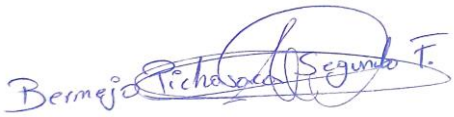
L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Ing. Cristhian Flores Urgilés
ESTUDIANTE 1	Segundo Francisco Bermejo Pichasaca

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	

Firmas:



Nombre: Ing. Cristhian Flores Urgilés	Nombre: Segundo Francisco Bermejo Pichasaca
CC: 0301638375	C.C.: 0350152690
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

Referencias

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

Angeles, T. C. (11 de 05 de 2016). *repositorio.puce.edu.ec.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/11437/ELABORACI%C3%93N%20DE%20POLITICAS%20Y%20NORMAS%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf?sequence=1

ARBOLEDA, A. O. (01 de 01 de 2021). *repository.unad.edu.co.* Recuperado el 18 de 01 de 2023, de https://repository.unad.edu.co/bitstream/handle/10596/41984/aonatear_3ago2021.pdf?sequence=1&isAllowed=y

Briceño, E. V. (01 de 03 de 2021). *www.3ciencias.com.* Recuperado el 13 de 01 de 2023, de https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Casa, A. C., Gavilanez, M. L., Caiza, C. C., & Moreano, J. A. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Revista Ciencias de la Ingeniería y Aplicadas*, *5*(2), 82-98.

Chumaina, M. M. (01 de 01 de 2018). *http://dspace.espoch.edu.ec/.* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/9842/1/82T00897.pdf

Corporación Autónoma Regional de Cundinamarca. (29 de 10 de 2021). *www.car.gov.co.* Recuperado el 18 de 01 de 2023, de https://www.car.gov.co/uploads/files/61840aaf4c32e.pdf

Delgado, C. A. (2017). *Fundamentos de seguridad informática.* Bogotá: Fondo editorial Areandino. Obtenido de https://core.ac.uk/download/pdf/326424171.pdf

Gestion de calidad . (07 de 11 de 2016). *gestion-calidad.com.* Obtenido de https://gestion-calidad.com/seguridad-informacion

INEN. (08 de 08 de 2014). *normalizacion.gob.ec.* Obtenido de https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27005.pdf

ISO2700.ES. (s.f). *www.iso27000.es.* Obtenido de https://www.iso27000.es/sgsi.html

Jimenez, J. N. (01 de 06 de 2021). *dspace.ups.edu.ec.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf

NQA.ISO. (4 de 10 de 2018). *www.nqa.com.* Recuperado el 13 de 01 de 2023, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Orellana, A. E. (10 de 09 de 2017). *epositorio.upse.edu.ec.* Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf

Orellana, A. E. (10 de 09 de 2017). *repositorio.upse.edu.ec.* Obtenido de https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf

Peña, H. M. (09 de 09 de 2019). *repository.unad.edu.co.* Obtenido de https://repository.unad.edu.co/jspui/bitstream/10596/27758/1/1075211684.pdf

Pilla Yanzapanta, J. C. (01 de 01 de 2019). *repositorio.uisek.edu.ec.* Obtenido de 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

QUIZHPI, C. F. (01 de 01 de 2021). *dspace.ucacue.edu.ec.* Recuperado el 18 de 01 de 2023, de https://dspace.ucacue.edu.ec/bitstream/ucacue/12762/1/Tesis%20Carlos%20Chimborazo%20Final.pdf

ROJAS, D. S., & ROMERO, E. L. (01 de 01 de 2018). *repository.udistrital.edu.co.* Recuperado el 13 de 01 de 2023, de https://repository.udistrital.edu.co/bitstream/handle/11349/13418/BuitragoRojasDanielaStefany2018.pdf;jsessionid=17B1BA11034E84877BBF012F88170964?sequence=1

Universidad Católica de Cuenca

ACHIK INTI Ltda.
Cooperativa de Ahorro y Crédito

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

El departamento de TIC de la Cooperativa de Ahorro y Crédito “ACHIK INTI”, determina a la información junto con los procesos que la administran además de cada una de las personas que hacen parte de los mismos como activo de gran importancia, siendo estos el pilar fundamental para la compañía. La confidencialidad, integridad y disponibilidad de la información, son elementos esenciales para mantener la seguridad y lograr los objetivos de la organización.

El presente documento refleja las políticas propuestas para la Cooperativa ACHIK INTI, estas se encuentran establecidas de acuerdo a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001 e ISO 27002: 2022.

He aquí una lista de los controles de seguridad que cubre el presente manual.

- Controles Organizacionales
- Controles de Persona
- Controles Físicos
- Controles Tecnológicos

OBJETIVO

Implementar un conjunto de políticas de seguridad de la información para la Cooperativa de Ahorro y Crédito con el fin de garantizar la disponibilidad continua, integridad sin alteraciones y confidencialidad adecuada de los datos y recursos almacenados y gestionados por la entidad financiera.

ALCANCE

Las políticas de seguridad de la cooperativa ACHIK INTI se implementan en el departamento de Tecnologías de la Información y abarcan a todo el personal involucrado, con el propósito de garantizar una adecuada protección de la información.

La aplicación rigurosa de estas políticas contribuirá a mantener un entorno de trabajo seguro y confiable, fortaleciendo la protección de la información de la cooperativa ACHIK INTI y asegurando la confianza de sus clientes y socios comerciales.

1. RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

Teniendo en cuenta que el presente manual es solo una propuesta para la Cooperativa Achik Inti, se definen algunas responsabilidades en caso de existir aplicabilidad de la misma.

- La alta gerencia de la cooperativa es el encargado de apoyar el proceso de implementación de las políticas de seguridad de la información.
- El encargado del departamento de TIC es responsable de realizar un seguimiento de la implementación de las políticas, supervisar al personal a su cargo para garantizar que les dé debido cumplimiento y brindar apoyo cuando sea necesario.
- El departamento de TIC demostrara compromiso en la divulgación de este manual de políticas a todos los funcionarios de la institución.
- El departamento de TIC tiene la obligación de verificar periódicamente el cumplimiento de las políticas de seguridad de la información.
- También se le designa la responsabilidad al departamento de TIC, para su debida revisión del presente manual, ya sea por actualización o mejoras.

2. POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La información representa un recurso de vital importancia para el correcto funcionamiento de la Cooperativa de Ahorro y Crédito, ya que permite la prestación efectiva de servicios a los ciudadanos y facilita la toma de decisiones estratégicas. Por consiguiente, es de suma importancia que todo el personal con responsabilidades en el manejo y procesamiento de la información esté debidamente informado y cumpla con los lineamientos establecidos en este manual de seguridad de la información.

El objetivo principal de este manual es garantizar la confidencialidad, integridad y disponibilidad de la información que maneja la Cooperativa. Para ello, se han propuesto políticas de seguridad que se basan en los controles definidos por la norma internacional ISO 27002:2022, una referencia ampliamente reconocida y aceptada en el ámbito de la seguridad de la información.

Al adherirse a las políticas definidas en este manual y alinearse con los estándares de la norma ISO 27002:2022, la Cooperativa de Ahorro y Crédito ACHIK INTI fortalece su posición para mantener la confianza y satisfacción de sus clientes, socios y otras partes interesadas. La seguridad de la información se convierte en un pilar fundamental para el cumplimiento de sus objetivos estratégicos y su correcto funcionamiento en el competitivo entorno financiero. El departamento de TIC o el personal encargado de la seguridad tendrá la potestad de aplicar en presente manual o en su defecto modificar las políticas según las necesidades de revisión en un tiempo determinado.

2.1. CONTROLES ORGANIZACIONALES

2.1.1. Políticas de Seguridad de la Información

Las políticas se establecerán teniendo en cuenta las necesidades identificadas durante el análisis de riesgo. Estas políticas deben ser aprobadas y comunicadas de manera efectiva a todo el personal que esté involucrado con la institución, ya sea interna o externamente. Realizar el proceso de seguimiento para mantener un entorno proactivo y sólido de seguridad de la información, asegurando que las políticas implementadas sean seguidas de manera consistente y respaldando el compromiso de la organización de proteger la información sensible y mantener la confidencialidad, integridad y disponibilidad de los datos.

2.1.2. Roles y responsabilidades en la Seguridad de la Información

- Se definirán claramente los roles y responsabilidades relacionados con la seguridad de la información para garantizar una distribución adecuada de las tareas y la responsabilidad.
- Se asignarán roles específicos, como el responsable de seguridad de la información, los administradores de sistemas, el equipo de respuesta a incidentes de seguridad, entre otros, y se les encomendarán tareas y funciones específicas.
- El responsable de seguridad de la información coordinará y supervisará todas las actividades relacionadas con la seguridad de la información, incluyendo la elaboración de políticas y

procedimientos, la implementación de controles de seguridad, la capacitación del personal y la gestión de incidentes de seguridad

2.1.3. Transferencia de información

- En la Cooperativa de Ahorro y Crédito Achik Inti, se implementarán medidas de seguridad de alto nivel para asegurar la confidencialidad e integridad de la información durante su transferencia, tanto dentro de la red interna como en comunicaciones externas.
- La Cooperativa debe hacer uso de Protocolos Seguros de Comunicación, como HTTPS (HTTP seguro) y SFTP (FTP seguro), que utilizan cifrado para proteger la información durante su transferencia. Así como también una VPN (Red Privada Virtual), para crear conexión segura y encriptada entre las diferentes ubicaciones y sucursales de la cooperativa.

2.1.4. Inventario de información y otros activos asociados

- Se llevará a cabo un inventario de los activos de información para tener un control adecuado sobre ellos y asegurar su protección. Este inventario incluirá todos los sistemas, dispositivos y datos críticos de la organización, identificando su ubicación, características técnicas, propietarios y niveles de clasificación de seguridad

2.1.5. Control de Acceso

Gestión de Identidades y Credenciales: Se establecerá un sistema de gestión de identidades que permita asignar de forma precisa y oportuna los permisos y roles de acceso adecuados a cada usuario, de acuerdo con sus responsabilidades y funciones dentro de la organización.

Todos los usuarios deberán contar con credenciales de autenticación únicas y seguras, como contraseñas fuertes o autenticación multifactor, para asegurar la verificación adecuada de su identidad al acceder a los sistemas y recursos de la cooperativa.

Se realizarán revisiones periódicas de los privilegios y accesos asignados a los usuarios para garantizar que sean adecuados y estén actualizados en función de las necesidades cambiantes de la organización.

Control de Acceso Físico: Se establecerán áreas restringidas y controladas mediante sistemas de vigilancia y control de acceso, garantizando que solo el personal autorizado tenga acceso a las instalaciones y áreas sensibles.

2.1.6. Derechos de Acceso

- En la Cooperativa de Ahorro y Crédito Achik Inti, se establecerán políticas claras de derechos de acceso a la información, basadas en la asignación de roles y permisos específicos para cada usuario. Se implementarán controles de autenticación y autorización para garantizar que solo los usuarios autorizados tengan acceso a la información relevante para sus funciones y responsabilidades dentro de la organización. Estas políticas se aplicarán a todos los sistemas y aplicaciones utilizados en la cooperativa, asegurando que se cumpla con los principios de seguridad y privacidad de la información, y mitigando el riesgo de acceso no autorizado o divulgar información confidencial a personas no autorizadas.

2.1.7. Seguridad de la información durante una interrupción

Se implementarán medidas técnicas de seguridad para garantizar la disponibilidad y protección de la información durante interrupciones o fallos en los servicios. Se establecerán sistemas de copias de seguridad y redundancia de los datos y sistemas críticos, asegurando su replicación en ubicaciones seguras y separadas, lo que permitirá una rápida recuperación en caso de fallas. Además, se implementarán soluciones de respaldo de energía, como generadores y sistemas de alimentación ininterrumpida (UPS), para asegurar el funcionamiento ininterrumpido de los equipos y servicios esenciales en situaciones de cortes de energía

2.1.8. Gestión de Identidades

- En la Cooperativa de Ahorro y Crédito Achik Inti, se implementará un sistema de gestión de identidades (Identity and Access Management, IAM) que facilite la asignación de permisos y roles de acceso adecuados a los usuarios de la red y los sistemas de información.

2.2. Controles de Persona

2.2.1. Términos y condiciones de Empleo

Se incluirán cláusulas de seguridad de la información en los contratos y términos de empleo para garantizar que los empleados comprendan y cumplan con las políticas de seguridad.

2.2.2. Conciencia de seguridad de la información, educación y formación

- se implementarán programas de concienciación y formación en seguridad de la información para garantizar que todos los empleados estén debidamente informados y capacitados en las prácticas de seguridad. Se realizarán sesiones periódicas de capacitación que abordarán temas como el manejo seguro de contraseñas, el reconocimiento de ataques de phishing y otras amenazas cibernéticas, el uso adecuado de dispositivos y sistemas, así como la importancia de proteger información confidencial y respetar las políticas de seguridad establecidas. Además, se brindará entrenamiento específico a aquellos empleados con acceso a información sensible o sistemas críticos, para que estén al tanto de las medidas de seguridad adicionales que deben seguir.

2.2.3. Acuerdos de confidencialidad o no divulgación

- En la Cooperativa de Ahorro y Crédito Achik Inti, se establecerá un requisito obligatorio para que todos los empleados y terceros involucrados firmen acuerdos de confidencialidad o no divulgación. Estos acuerdos tendrán como objetivo proteger la información sensible y confidencial a la que puedan tener acceso

en el desempeño de sus funciones o en virtud de su relación con la cooperativa. Los acuerdos de confidencialidad establecerán claramente las obligaciones y responsabilidades de las partes para mantener la confidencialidad de la información y evitar su divulgación no autorizada. Además, se incluirán cláusulas que impongan restricciones sobre el uso y acceso a la información confidencial, así como medidas de protección adicionales, como la prohibición de compartir información con terceros sin la autorización previa de la cooperativa

2.3. Contraponles Físicos

2.3.1. Entrada Física

Se establecerán controles para asegurar que solo personal autorizado pueda acceder físicamente a los activos de información.

2.3.2. Asegurar oficinas, habitaciones e instalaciones

- Las oficinas, habitaciones e instalaciones deben contar con medidas de seguridad física adecuadas para prevenir accesos no autorizados.
- Se implementarán sistemas de vigilancia y control de acceso para garantizar la seguridad de las instalaciones.

2.3.3. Protección contra amenazas físicas y ambientales

- Medidas de seguridad física en todas las instalaciones: Se implementarán rigurosas medidas de seguridad física en todas las instalaciones de la Cooperativa con el objetivo de salvaguardar los activos contra una variedad de amenazas, incluyendo desastres naturales, como terremotos o inundaciones, y otros eventos externos que puedan afectar la integridad de los activos.
- Evaluaciones periódicas de vulnerabilidad: Se realizarán evaluaciones periódicas de vulnerabilidad tanto de los sistemas físicos como de los sistemas lógicos para identificar posibles puntos débiles que puedan ser explotados por amenazas externas o

internas. Estas evaluaciones se llevarán a cabo de manera sistemática y se revisarán y actualizarán regularmente para adaptarse a nuevos riesgos y escenarios.

- Se asegurará el acceso controlado y seguro a oficinas, habitaciones e instalaciones mediante sistemas de vigilancia y control de acceso

2.3.4. Trabajar en áreas seguras

- Se asegurará que las áreas de trabajo cumplan con condiciones adecuadas de seguridad, como la prevención de incendios y la protección contra riesgos ambientales.

2.3.5. Emplazamiento y protección de equipos

Se implementarán medidas técnicas de seguridad física para proteger los equipos y dispositivos utilizados en la organización. Esto incluirá el establecimiento de controles de acceso a las instalaciones, como sistemas de vigilancia y control de acceso con identificación biométrica o tarjetas de proximidad, para asegurar que solo el personal autorizado tenga acceso a los equipos y áreas sensibles.

2.3.6. Medios de almacenamiento

Se establecerán políticas técnicas para el manejo seguro y la protección de los medios de almacenamiento que contengan información sensible. Estas políticas incluirán directrices para el uso adecuado de unidades de almacenamiento, como discos duros, unidades flash USB y discos ópticos, asegurando su cifrado y protección mediante contraseñas sólidas. Se implementarán procedimientos para el respaldo y la restauración segura de datos en medios de almacenamiento autorizados y se establecerá un control riguroso sobre la distribución, transferencia y eliminación de estos medios para evitar la pérdida o divulgación no autorizada de información sensible

2.3.7. Mantenimiento de equipos

Se realizarán tareas de mantenimiento periódico en los equipos para asegurar su correcto funcionamiento y seguridad.

2.3.8. Disposición o reutilización segura de los equipos

Se establecerán procedimientos técnicos para la disposición o reutilización segura de equipos que ya no sean utilizados, garantizando la eliminación segura de los datos almacenados en ellos. Estos procedimientos seguirán estándares de borrado seguro y técnicas de destrucción de datos que cumplan con los requisitos de protección de la información sensible. Antes de reutilizar o desechar los equipos, se llevará a cabo un proceso de limpieza y eliminación de datos confidenciales utilizando métodos criptográficos u otras técnicas aprobadas que aseguren que los datos no puedan ser recuperados o accedidos de manera no autorizada.

2.4. Controles Tecnológicos

2.4.1. Autenticación segura

Se implementarán mecanismos de autenticación segura para garantizar que solo los usuarios autorizados puedan acceder a los sistemas y recursos de información.

2.4.2. Protección contra malware

- En el contexto de la Cooperativa de Ahorro y Crédito Achik Inti, se implementarán soluciones de seguridad avanzadas para mitigar los riesgos asociados con el malware. Se emplearán herramientas especializadas, tales como software antivirus y antimalware, para prevenir y detectar posibles amenazas de malware en los sistemas de información.
- Implementación de Software Antivirus: Se desplegará una solución de software antivirus en todos los dispositivos y servidores de la red de la cooperativa. El software antivirus se configurará para realizar análisis exhaustivos y continuos de los archivos y programas, con el objetivo de identificar y neutralizar cualquier software malicioso o código dañino que pueda estar presente.

- Utilización de Soluciones Antimalware: Además del software antivirus, se emplearán soluciones antimalware avanzadas para identificar y bloquear activamente amenazas de malware conocidas y desconocidas. Estas herramientas de seguridad estarán configuradas para detectar patrones de comportamiento malicioso y prevenir la ejecución de software sospechoso.

2.4.3. Gestión de la configuración

- Se establecerá un proceso estructurado y bien definido para la gestión de la configuración de todos los sistemas y activos de información en la organización. Este proceso abarcará desde la adquisición y desarrollo inicial de los sistemas hasta su eventual eliminación o reemplazo. Cada vez que se realice una modificación en la configuración, se documentarán los cambios realizados, incluyendo la razón, el autor y la fecha de la modificación.
- Se implementarán herramientas especializadas para el control y monitoreo continuo de los sistemas y sus configuraciones. Estas herramientas permitirán detectar cambios no autorizados o inesperados en la configuración de los sistemas, alertando inmediatamente al personal de seguridad o a los administradores responsables.

2.4.4. Prevención de fugas de datos

En la Cooperativa de Ahorro y Crédito Achik Inti, se implementarán controles de seguridad para prevenir la fuga de información confidencial o sensible fuera de la organización. Se emplearán soluciones avanzadas de prevención de pérdida de datos (Data Loss Prevention, DLP) que analizarán y monitorizarán tanto el tráfico de red como los datos almacenados en los sistemas, identificando patrones de información confidencial y aplicando reglas y políticas para evitar su filtración. Además, se establecerán mecanismos de

encriptación y restricciones de acceso para garantizar que solo los usuarios autorizados puedan acceder y manejar información sensible

2.4.5. Copia de seguridad de la información

La cooperativa debe implementar un proceso de copias de seguridad periódicas de la información crítica para garantizar la disponibilidad y recuperación en caso de fallos o incidentes.

- Deberá utilizar soluciones de respaldo que permitan realizar copias completas y/o incrementales de los datos y sistemas importantes, almacenándolos en ubicaciones seguras y separadas de los sistemas en producción. Las copias de seguridad se realizarán con una frecuencia adecuada según la criticidad de la información, asegurando que los datos estén protegidos y actualizados.
- Se llevarán a cabo pruebas de restauración periódicas para verificar la integridad de las copias y la capacidad de recuperar la información en caso de necesidad.

2.4.6. Redundancia de las instalaciones de procesamiento de información

Se implementarán medidas de redundancia para garantizar la continuidad del negocio en caso de fallos en los sistemas o instalaciones. Se establecerán sistemas de respaldo y replicación de datos en servidores y dispositivos de almacenamiento, de manera que la información crítica esté disponible en múltiples ubicaciones y pueda ser recuperada rápidamente en caso de una interrupción. Asimismo, se configurarán sistemas de alta disponibilidad que permitan la conmutación automática a servidores secundarios en caso de fallas en los servidores principales, asegurando la continuidad de los servicios y operaciones.

2.4.7. Seguridad de los servicios de red

En la Cooperativa de Ahorro y Crédito Achik Inti, se deberá implementar controles de seguridad en los servicios de red para proteger la información de accesos no autorizados. Estos controles

incluirán medidas como la configuración adecuada de firewalls y routers para filtrar y controlar el tráfico de red, el establecimiento de políticas de autenticación y autorización para limitar el acceso a recursos sensibles, la implementación de VPN (Red Privada Virtual) para asegurar la transmisión segura de datos a través de redes públicas, y el monitoreo constante de la actividad de red para detectar posibles intrusiones o comportamientos sospechosos. Además, se aplicarán parches y actualizaciones de seguridad de manera regular para mitigar vulnerabilidades conocidas en los servicios de red y se realizarán auditorías periódicas para evaluar la efectividad de los controles implementados.

2.4.8. Ciclo de vida de desarrollo seguro

- Se implementarán controles sólidos y rigurosos para garantizar que el desarrollo de aplicaciones y sistemas se lleve a cabo siguiendo prácticas de seguridad en cada etapa del ciclo de vida.

2.4.9. Codificación segura

- Se promoverá el uso de buenas prácticas de codificación segura para evitar vulnerabilidades y riesgos en las aplicaciones desarrolladas internamente o adquiridas de terceros.

Declaratoria de Autoría y Responsabilidad

SEGUNDO FRANCISCO BERMEJO PICHASACA portador(a) de la cédula de ciudadanía Nº **0350152690** Declaro ser el autor de la obra: **"PROPUESTA DE MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA, DEL CANTÓN CAÑAR",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, **12 de Octubre de 2023**

F: …….

SEGUNDO FRANCISCO BERMEJO PICHASACA

C.I. **0350152690**