UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

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

GESTIÓN DE RIESGOS DE LOS CANALES ELECTRÓNICOS DE LA COOPERATIVA YUYAY LTDA BASADO EN NORMAS Y ESTÁNDARES INTERNACIONALES.

AUTORA: GLORIA MERCEDES GUARTACHO TENESACA

DIRECTORA: ING. CRISTINA FLORES URGILES

CAÑAR - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

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

GESTIÓN DE RIESGOS DE LOS CANALES ELECTRÓNICOS DE LA COOPERATIVA YUYAY LTDA BASADO EN NORMAS Y ESTÁNDARES INTERNACIONALES.

AUTORA: GLORIA MERCEDES GUARTACHO TENESACA

DIRECTORA: ING. CRISTINA FLORES URGILES

CAÑAR – ECUADOR

2025

PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUDITORÍA Y RESPONSABILIDAD

Gloria Mercedes Guartacho Tenesaca, portadora de la cedula de ciudadanía N° 0302487624. Declaro ser el autor de la obra: "Gestión de riesgos de los canales electrónicos de la Cooperativa Yuyay Ltda basado en normas y estándares internacionales" sobre la cual me hago responsable sobre sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 6 de noviembre de 2025

F: ……..

Gloria Mercedes Guartacho Tenesaca
C.I.0302487624

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado "Gestión de riesgos de los canales electrónicos de la Cooperativa Yuyay Ltda basado en normas y estándares internacionales" realizado por Gloria Mercedes Guartacho Tenesaca, con documento de identidad No. 0302487624, previo a la obtención del título profesional de Ingeniería en Sistemas de Información, ha sido asesorado, supervisado y desarrollado bajo mi tutoría en todo su proceso, cumpliendo con la reglamentación pertinente que exige la Universidad Católica de Cuenca y los requisitos que determina la investigación científica.

Cañar, 6 de noviembre de 2025

Ing. Cristina Flores Urgiles
DIRECTO/TUTOR

DEDICATORIA

Dedico este trabajo a mis queridos padres, hermanos y a mi compañero de vida quienes, con su paciencia, apoyo constante y sabios consejos han sido pilar fundamenta en mi vida. Gracias por sus enseñanzas recibidas, he logrado llegar hasta aquí.

Extendiendo mi gratitud a las personas que de alguna manera estuvieron conmigo durante este tiempo, creyendo en mí y mi sueño ya que con sus sabios consejos me han impulsado a dar lo mejor de mí.

AGRADECIMIENTO

Al concluir esta etapa tan relevante en mi vida, agradezco de corazón a todas las personas que han tendido un rol significante para yo poder alcanzar este importante logro.

También agradezco a mi tutora de tesis, cuya enseñanza y sabiduría me han guiado, extendió su mano durante este trabajo tan significativo. De la misma manera, agradezco a mis docentes de carrera, quienes con su sabiduría me han ayudado a crecer como profesional también, como persona, gracias a sus conocimientos y vivencias, mi formación se ha enriquecido, inspirándome a seguir avanzando y aprendiendo día a día.

RESUMEN

Esta investigación propone la implementación de un modelo de gestión de riesgos de TI enfocado en los canales electrónicos de la Cooperativa de Ahorro y Crédito Yuyay Ltda., con el objetivo de proteger la información y garantizar la continuidad de las operaciones en un entorno cada vez más digital. Para ello, se estudiaron los conceptos clave de la gestión de riesgos de TI y se analizó el estado actual de los sistemas de información y la infraestructura tecnológica. La metodología adoptó un enfoque mixto, combinando análisis cualitativos y cuantitativos; la información se recopiló a través del jefe de TI y mediante la aplicación de matrices de riesgos basadas en MAGERIT, con el fin de identificar vulnerabilidades y amenazas sobre activos críticos. A partir de este diagnóstico, se plantearon estrategias de mitigación alineadas con la norma ISO/IEC 27002:2022, que reorganiza los controles en cuatro dimensiones (Organizacional, Personas, Físico y Tecnológico), incluyendo medidas de seguridad, planes de respuesta ante incidentes y recomendaciones para un monitoreo continuo.

***Palabras clave**: gestión de riesgos, canales electrónicos, MAGERIT, ISO/IEC 27002:2022*

ABSTRACT

This research proposes the implementation of an IT risk management model focused on the electronic channels of the 'Yuyay' Savings and Credit Cooperative Ltd., aiming to protect information and ensure operational continuity in an increasingly digital environment. To this end, the key concepts of IT risk management were examined, and the current state of information systems and technological infrastructure was analyzed. The methodology adopted a mixed approach, combining qualitative and quantitative analyses. Data were collected through interviews with the head of IT and the application of risk matrices based on MAGERIT to identify vulnerabilities and threats to critical assets. Based on this diagnosis, mitigation strategies aligned with the ISO/IEC 2700:2022 standard were proposed, reorganizing controls into four dimensions (Organizational, People, Physical, and Technological), and including security measures, incident response plans, and recommendations for continuous monitoring.

Keywords: risk management, electronic channels, MAGERIT, ISO/IEC 27002:2022

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

CAPÍTULO I

1.1. Planteamiento del problema

Hoy en día, la sociedad se encuentra en la cima de la era digital, donde las personas realizan cosas de la vida cotidiana con acceso a internet y un dispositivo electrónico. Por ello, varias de las organizaciones han implementado servicios tecnológicos, trayendo con ello innovaciones para la sociedad, no obstante, cabe recalcar que esto también dar lugar a problemas, entre ellas la ciberdelincuencia donde existe fraudes, robo de información que afectan significativamente a la personas u organizaciones.

Ahora bien, en el caso de la Cooperativa Yuyay Ltda, una empresa dedicada a prestar servicios financieros, que tiene un rol muy significativo en el cantón Cañar donde fomenta la cultura del ahorro, han implementado los canales electrónicos como parte de la estrategia de modernización y mejora de atención a los clientes. Estos canales electrónicos contienen servicios como aplicaciones móviles y otras funciones digitales. Por lo tanto, es evidente que contienen información importante de sus socios como las claves, saldos y transacciones.

Sin embargo, dichos servicios actualmente funcionan sin una gestión de riesgos de seguridad basada en normas internacionales, lo que implica que se encuentra expuestos a ataques cibernéticos como lo es robo de información, fraudes, accesos no autorizados lo que podría comprometer a la Cooperativa Yuyay Ltda a no ofrecer seguridad y confidencialidad a sus socios.

Por lo cual, es necesario indagar y aplicar metodologías relacionadas a la gestión de riesgos que ayude a reconocer los amenazas las vulnerabilidades asociadas con los canales electrónicos y en base a ellos proponer controles de seguridad de la información.

1.1.1 Formulación del problema

Actualmente la Cooperativa Yuyay Ltda no cuenta con un sistema de gestión de riesgos para sus canales electrónicos, lo que podría ser un problema para esta entidad dado que se encuentra expuesta a riesgos inherentes. Esta condición resulta especialmente crítica considerando, que en las entidades financieras la seguridad de la información es muy importante debido al manejo fondos económicos.

¿Cómo puede manejar la Cooperativa Yuyay Ltda los riesgos asociados a sus canales electrónicos, considerando la ausencia de un sistema estructurado para su gestión?

1.2. Antecedentes de la Investigación

Padilla (2023) en su estudio titulado "Diseño de la etapa de planificación de un sistema de gestión de seguridad de la información para el área de TI la empresa FESNEPONAL" propone la metodología MAGERIT para un sistema de gestión de riesgos, considerando que su objetivo es identificar dentro de los activos de la empresa amenazas, vulnerabilidades y riesgos existentes. Además, hace referencia a la normativa ISO/ IEC 27002: 2013 como un marco para los controles de seguridad de información. La adaptación y aplicación de estos enfoques en los canales electrónicos de Cooperativa Yuyay Ltda, puede mejorar la seguridad y la eficiencia basándose en los resultados obtenido en la empresa FESNEPONAL.

Guerrero & Leonardo (2021) busca implementar un modelo de gestión de riesgos para la seguridad de la información en la empresa "Juegos de Azar", Lima. En este estudio se dice que la seguridad de la información es un elemento fundamental dentro de la empresa ayudando a consolidar la disponibilidad, integridad y confidencialidad. La investigación adopta en enfoque de carácter cualitativo donde se trabaja con activos, de la empresa, los cuales son valorados para determinar amenazas y vulnerabilidades. Este estudio evidencia

aspectos cable como la necesidad de la identificación y valoración de activos en la Cooperativa Yuyay Ltda.

Almeida (2023) de igual manera en su estudio realizado en Quito, trata sobre la gestión de riesgos de datos sensibles en la Dirección General de Aviación Civil, alineándose al cumplimiento de la Ley Orgánica de Protección de Datos Personales. Esta investigación presenta conceptos clave como la definición de riesgos, el propósito de la gestión de riesgos y la importancia de la seguridad de la información. De igual manera, propone la metodología OCTAVE como marco de trabajo para la seguridad de información, lo cual puede ser considerado como un enfoque útil y complementario para la gestión de riesgos de los canales en la Cooperativa de ahorro y crédito Yuyay Ltda.

El artículo de investigación realizado por Marín & Molina (2021), titulado "Análisis de riesgos del Departamento de Tecnologías de la Información y Comunicación del Registro de la Propiedad de la ciudad de Cuenca, Ecuador", propone la valoración de activos y las salvaguardas como factor clave para la seguridad de información. Este documento sirve como base para identificar los fundamentos teóricos de un sistema de gestión de riesgos.

1.3. Justificación de la investigación

Un sistema de gestión de riesgos eficaz para los canales electrónicos de la Cooperativa Yuyay Ltda. Constituye un aspecto importante en la organización, debido que la empresa ha implementado estas funcionabilidades con el afán de fortalecer los servicios al cliente, donde desempeñan un papel fundamental en las actividades de la empresa. No obstante, esto implica que estas funciones se encuentren expuestos a ataques como robo de información, fraudes o accesos no autorizados.

Implementar un sistema de gestión de riesgos sólida para los canales electrónicos en la cooperativa permitirá identificar amenazas, vulnerabilidades y riesgos a los que se

encuentra expuestos. Además, contribuye a mitigar los riesgos detectados, y a su vez fortalece la confiabilidad en la organización. Esta acción resulta esencial para garantizar la continuidad operativa dentro del sector financiero.

Al implementar un entorno seguro, la organización generará mayor confianza para sus socios, además de permitir a la cooperativa seguir innovando y optar por implementar nuevas tecnologías.

1.3.1 Objetivo General

Gestionar riesgos asociados a los canales electrónicos de la Cooperativa Yuyay Ltda mediante identificación de vulnerabilidades y la evaluación de controles en base a normas y estándares internacionales.

1.3.2 Objetivos Específicos

- Realizar un estudio teórico y del estado del arte relacionado con la gestión de riesgos, identificando marcos de referencia y metodologías que faciliten una gestión eficaz en cooperativas de ahorro y crédito.

- Establecer el estado actual de la seguridad de la información y la gestión de riesgos en los canales electrónicos de la Cooperativa Yuyay Ltda, conforme a los lineamientos de las normas internacionales.

- Realizar la gestión de riesgos en los canales electrónicos de la Cooperativa Yuyay Ltda, mediante la identificación, análisis, evaluación y tratamiento de las amenazas, con el fin de reducir vulnerabilidades, proteger la seguridad de la información y garantizar la continuidad de los servicios digitales.

- Proponer controles y políticas de seguridad para mitigar los riesgos en los canales electrónicos de la Cooperativa Yuyay ltda, fortaleciendo la protección de los activos digitales y la continuidad del servicio.

1.3.3 Limitaciones

- Tiempo disponibilidad del tiempo, dado que está investigación se realizará en un tiempo aproximado de tres meses.

- Recursos económicos, humanos podría ser un factor limitante para el desarrollo integral y la evaluación efectiva de sistema de gestión de riesgos.

1.3.4 Delimitaciones

- Este estudio se centrará en todo lo que conlleva lo canales electrónicos de la Cooperativa.

- El presente trabajo se limita solo a la elaboración de una propuesta, cuya implementación quedara sujeta a la evaluación de la Cooperativa.

- La investigación se centrará en lo responsables de área de Sistemas de la Cooperativa, mas no en otras áreas interesadas.

CAPITULO II

2. MARCO TEÓRICO

2.1. Transformación digital en el sector financiero

La transformación digital ha revolucionado el funcionamiento del sector financiero, redefiniendo la forma en que las instituciones interactúan con sus clientes y gestionan sus procesos internos, así mismo este proceso implica mucho más que la simple adopción de tecnologías digitales; se trata de una reestructuración integral que abarca la cultura organizacional, los modelos de negocio y la experiencia del usuario, con el objetivo de responder a las nuevas demandas de un entorno altamente competitivo y dinámico. (Rivadeneira Aguirre, 2021)

En este contexto, las instituciones financieras han tenido que adaptar sus estrategias para incorporar herramientas digitales que les permitan ofrecer productos y servicios más ágiles, personalizados y accesibles. La implementación de plataformas móviles, portales web, cajeros automáticos inteligentes y otros canales electrónicos ha generado un entorno más eficiente, pero también más complejo desde el punto de vista de la gestión de riesgos. (Quinde Uyaguari, 2023)

El auge de la banca digital y el crecimiento acelerado del uso de tecnologías como la computación en la nube, la inteligencia artificial y el análisis de datos han permitido mejorar la toma de decisiones y optimizar procesos, sin embargo, también han incrementado la exposición a amenazas cibernéticas y han planteado desafíos en materia de seguridad, privacidad y cumplimiento normativo. (Sánchez Paredes, 2021)

2.2. Canales electrónicos en las instituciones financieras

En la actualidad, los canales electrónicos representan herramientas fundamentales para la entrega de servicios en el ámbito financiero. A través de medios digitales como la banca por internet, las aplicaciones móviles y los cajeros automáticos, las instituciones logran atender las demandas de sus usuarios, ofreciendo mayor rapidez, disponibilidad y comodidad. (Rivadeneira Aguirre, 2021) Esta transformación ha redefinido la interacción entre los clientes y las entidades, permitiendo operaciones más ágiles y fortaleciendo la eficiencia operativa. La correcta implementación de estos canales se ha convertido en un elemento clave para mantener la competitividad en un entorno digital en constante evolución**.** (Ortiz Alulema , 2020)

2.1.1 Beneficios de los canales electrónicos en Cooperativas

La incorporación de canales electrónicos en las cooperativas de ahorro y crédito ha generado múltiples beneficios tanto para las instituciones como para sus socios. Uno de los principales aportes radica en la mejora del acceso a los servicios financieros, ya que permite a los usuarios realizar transacciones desde cualquier lugar y en cualquier momento, reduciendo la necesidad de acudir físicamente a las agencias (Arellano Veloz, 2023)

2.1.2 Banca móvil (mobile banking).

La banca en línea es un canal digital que permite a los usuarios acceder a servicios financieros a través de internet, facilitando operaciones como consultas de saldo, transferencias, pagos y gestión de productos desde cualquier lugar y en cualquier momento., así mismo este servicio ha mejorado notablemente la eficiencia operativa de las instituciones financieras y ha ampliado la cobertura de atención, especialmente en zonas donde no existen oficinas físicas. (Álvarez Veintimilla , 2022)

2.1.3 Cajeros automáticos (ATM).

Son uno de los canales electrónicos más tradicionales y ampliamente utilizados en el sector financiero de los cuales ayudan a los usuarios realizar operaciones básicas como retiros de efectivo, consultas de saldo, transferencias entre cuentas, pagos de servicios y depósitos, sin la necesidad de atención directa por parte del personal de la entidad. (Quinde Uyaguari, 2023)

2.1.4 Otros canales emergentes (ej. chatbots, APIs bancarias).

Entre estos canales emergentes destacan los chatbots y las APIs bancarias, tecnologías que han ganado protagonismo por su capacidad de mejorar la experiencia del usuario y optimizar procesos internos. (Avila Ruiz & Jara Guarnizo , 2022)

Los chatbots, por ejemplo, permiten la atención automatizada de consultas frecuentes mediante inteligencia artificial, ofreciendo respuestas inmediatas y disponibles las 24 horas, lo que reduce la carga operativa del personal y mejora la interacción con los socios. (Calderón Morán, 2024)

2.3 Seguridad de la información en entornos digitales

La seguridad de la información en entornos digitales se ha convertido en un pilar fundamental para las organizaciones que operan en un ecosistema cada vez más interconectado. Esta disciplina se encarga de proteger los activos de información frente a accesos no autorizados, alteraciones, pérdida o destrucción, garantizando los principios de confidencialidad, integridad y disponibilidad. (Garzon Quito, 2021)

2.3.1 Principios de la seguridad

Confidencialidad

Es el principio de seguridad que busca restringir el acceso a la información únicamente a personas, sistemas o procesos autorizados; su propósito es evitar

que datos sensibles, como credenciales, información financiera o datos personales, sean expuestos, divulgados o utilizados de manera indebida. Este principio garantiza la privacidad de la información tanto en tránsito como en reposo, mediante mecanismos como el cifrado, el control de accesos y la autenticación. (Alvarado Véliz, 2024)

Integridad

Consiste en asegurar que la información permanezca exacta, completa y sin alteraciones no autorizadas durante todo su ciclo de vida. Implica que los datos no sean modificados, eliminados o falsificados por error o de forma maliciosa; el mantenimiento de la integridad es esencial para garantizar que la información refleje fielmente la realidad operativa, especialmente en entornos financieros donde cualquier alteración puede generar consecuencias críticas. (Alvarado Véliz, 2024)

Disponibilidad

Es el principio que garantiza que la información y los servicios relacionados estén accesibles y operativos cuando se requieran, sin interrupciones que afecten el desarrollo de las actividades, también implica la implementación de infraestructuras robustas, planes de contingencia, copias de seguridad y medidas de continuidad del negocio. (Rivadeneira Aguirre, 2021)

2.4 Gestión de riesgos en tecnologías de la información

La gestión de riesgos en tecnologías de la información consiste en un conjunto de actividades sistemáticas orientadas a identificar, analizar, evaluar y tratar las amenazas que pueden afectar la seguridad y continuidad de los sistemas informáticos. Este proceso permite anticiparse a eventos que podrían comprometer la confidencialidad, integridad y disponibilidad de los

activos digitales, reduciendo así el impacto negativo en la organización. (Molina & Chacon , 2022)

2.4.1 Componentes del riesgo

Activos

Es cualquier recurso de valor para una organización que debe ser protegido. Puede incluir elementos físicos, lógicos, humanos o de reputación, que son esenciales para el funcionamiento de los sistemas de información, entre los ejemplos tenemos base de datos con información de clientes, servidor de correo electrónico y aplicación web corporativa. (Larrauri , 2021)

Amenazas

Es un evento potencial o circunstancia que puede explotar una vulnerabilidad y causar daño o pérdida a un activo, asi mismo las amenazas pueden ser de origen interno o externo, intencionales o accidentales. Ejemplo de ellas ataques de malware, phishing o suplantación de identidad, fallo eléctrico o corte de energía y acceso no autorizado por parte de un empleado (Álvaro, 2023)

Vulnerabilidades

Es una debilidad en un activo, sistema o control que puede ser aprovechada por una amenaza para causar un incidente de seguridad. Las vulnerabilidades pueden ser técnicas, físicas, humanas o procedimentales, entre las cuales se puede mencionar: contraseñas débiles, falta de actualizaciones en el software, ausencia de copias de seguridad y personal no capacitado en ciberseguridad. (Braga Calderon, 2021)

2.4.2 Ciclo de vida de la gestión de riesgos (identificación, análisis, evaluación, tratamiento, monitoreo)

La implementación de canales electrónicos en las instituciones financieras ha transformado significativamente la forma en que los usuarios acceden y gestionan sus servicios. Sin embargo, esta evolución tecnológica también ha traído consigo una serie de riesgos que deben ser gestionados de manera adecuada para garantizar la seguridad y confianza en el entorno digital.

2.4.3 Riesgos de Ciberseguridad

- **Ataques de e, g., phishing y pharming**

  Es una técnica de suplantación de identidad que busca engañar al usuario mediante correos electrónicos, mensajes o sitios web falsos con el objetivo de obtener información confidencial, como credenciales de acceso o datos bancarios. (Braga Calderon, 2021). Por su parte, el pharming redirige al usuario, sin que este lo note, hacia sitios fraudulentos mediante la manipulación del sistema DNS o del equipo local. Ambos ataques afectan directamente a los canales electrónicos, ya que explotan la confianza del usuario y pueden comprometer cuentas, transacciones y servicios financieros si no se cuenta con mecanismos adecuados de autenticación y validación de sitios seguros. (Avila Ruiz & Jara Guarnizo , 2022)

- **Malware y ransomware**

  El malware es un software malicioso diseñado para infiltrarse en sistemas sin el consentimiento del usuario. Dentro de este grupo, el ransomware representa una amenaza especialmente grave, ya que bloquea el acceso a los datos del sistema mediante cifrado, exigiendo un rescate para su liberación. Estos programas pueden ser distribuidos a través de descargas, enlaces comprometidos o correos infectados, y su

presencia en canales electrónicos puede causar pérdidas operativas, daños reputacionales y exposición de información crítica. Su detección temprana y la implementación de medidas de seguridad como antivirus actualizados, análisis de comportamiento y segmentación de redes son esenciales para mitigar su impacto. (Braga Calderon, 2021)

- **Ataques de denegación de servicio (DDoS)**

  Consisten en saturar un sistema, servidor o red mediante un volumen masivo de solicitudes provenientes de múltiples dispositivos comprometidos, conocidos como botnets, sin embargo, el objetivo principal de estos ataques es interrumpir el funcionamiento normal de los servicios digitales, haciendo que sean inaccesibles para los usuarios legítimos. (Calderón Morán, 2024)

  En el caso de los canales electrónicos, un ataque DDoS puede paralizar completamente la banca en línea, aplicaciones móviles o sistemas de atención al cliente, afectando la disponibilidad del servicio y generando pérdidas operativas. (Avila Ruiz & Jara Guarnizo , 2022)

- **Fugas y robo de datos**

  Se producen cuando información sensible o confidencial es expuesta de manera no intencional, mientras que el robo de datos implica la extracción deliberada y maliciosa de dicha información. Ambos eventos representan amenazas severas para la seguridad de los canales electrónicos, ya que comprometen la confidencialidad de los datos personales, financieros o corporativos. (Avila Ruiz & Jara Guarnizo , 2022)

  Las causas pueden incluir fallos de seguridad en las aplicaciones, malas configuraciones, errores humanos o ataques externos. Las consecuencias abarcan desde

daños reputacionales hasta sanciones legales y pérdida de confianza por parte de los usuarios. (Calderón Morán, 2024)

- **Ingeniería social**

  La ingeniería social es una técnica de manipulación que explota el factor humano para obtener información confidencial o comprometer sistemas, diferenciándose de los ataques puramente técnicos, entre sus métodos más comunes están las llamadas falsas, correos fraudulentos, suplantación de identidad y accesos físicos no autorizados. Su prevención exige cultura organizacional en seguridad, capacitación constante y protocolos de verificación. (Campo Cucunuba , 2024)

2.4.4 Riesgos Operacionales

Los riesgos operacionales se refieren a posibles pérdidas causadas por fallos en procesos internos, errores humanos, deficiencias tecnológicas o eventos externos, en los canales electrónicos, estos riesgos son especialmente relevantes, ya que pueden afectar la continuidad del servicio, comprometer la calidad operativa y debilitar la confianza de los usuarios. (Calderón Morán, 2024)

- **Fallas en sistemas y plataformas tecnológicas.**

  El factor humano representa una fuente crítica de riesgo en entornos tecnológicos, donde errores como configuraciones incorrectas o divulgación involuntaria de credenciales pueden facilitar incidentes de seguridad y afectar la operatividad, especialmente en canales electrónicos, donde pequeños descuidos pueden ser explotados por atacantes. (Avila Ruiz & Jara Guarnizo , 2022)

- **Interrupciones del servicio**

  Implican la pérdida de acceso a los canales electrónicos, ya sea de forma temporal o definitiva, como resultado de fallas técnicas, mantenimientos deficientes, saturación

de los sistemas o acciones maliciosas; esta situación compromete la continuidad operativa de la cooperativa, dificultando que los socios realicen trámites como transferencias, pagos o consultas, lo cual en el contexto financiero genera desconfianza, daña la imagen institucional y ocasiona impactos económicos tanto para la entidad como para sus usuarios**.** (González, 2023)

2.5 Normas y estándares internacionales aplicables

La incorporación de normas y estándares internacionales en la gestión de riesgos tecnológicos se ha vuelto una práctica indispensable para garantizar la seguridad, la continuidad operativa y la disponibilidad de los canales electrónicos dentro del sector financiero, ya que estos marcos normativos, elaborados por organismos especializados, ofrecen directrices organizadas que orientan el proceso de identificación, análisis, tratamiento y seguimiento de riesgos; al aplicarlos se refuerza la protección de los sistemas, se optimiza la capacidad de reacción ante eventos adversos y se preserva la confianza de los usuarios en un entorno digital que enfrenta constantes desafíos en materia de ciberseguridad (Arellano Veloz, 2023).

2.5.1 ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI)

Establece los requisitos necesarios para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita proteger de manera integral los datos dentro de una organización, ya que su enfoque se basa en la identificación y tratamiento de riesgos para preservar la confidencialidad, integridad y disponibilidad de la información, promoviendo una gestión organizada que se adapta a las necesidades y contexto de cada entidad en un entorno digital cada vez más expuesto a amenazas. (Huaman Tena, 2021)

2.5.1.1 Ciclo PHVA

Ilustración 1 Ciclo PHVA Fuente: (Garzon Quito, 2021)

- **Planificar (Plan):** En esta fase se define el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), se identifican los activos de información relacionados con los canales electrónicos, se realiza un análisis de riesgos para evaluar amenazas y vulnerabilidades, y se establecen los controles necesarios para reducir dichos riesgos a niveles aceptables, lo cual requiere una comprensión profunda del contexto organizacional y de las necesidades de seguridad para diseñar una política sólida que respalde la protección de los sistemas tecnológicos involucrados. (Álvaro, 2023)

- **Hacer (Do):** Durante esta etapa se implementan las políticas, procedimientos y controles definidos en la planificación, integrándolos en los procesos operativos de la organización para gestionar adecuadamente los riesgos identificados, lo que implica la asignación de responsabilidades, la capacitación del personal, el despliegue de tecnologías de protección y la

puesta en marcha de mecanismos de control que garanticen la seguridad de los canales electrónicos de forma efectiva y continua en el entorno operativo. (Huaman Tena, 2021)

- **Verificar (Check):** Esta fase se lleva a cabo la revisión y evaluación del desempeño del sistema de gestión mediante auditorías internas, análisis de incidentes, revisión de registros y seguimiento de indicadores clave de seguridad, con el fin de determinar si los controles establecidos son eficaces para mitigar los riesgos, detectar desviaciones frente a lo planificado y generar evidencia documentada que permita a la alta dirección tomar decisiones informadas sobre la mejora del SGSI. (Álvaro, 2023)

- **Actuar (Act):** Se aplican acciones correctivas y preventivas para abordar las no conformidades encontradas durante la verificación y se realizan ajustes necesarios en el SGSI para optimizar su funcionamiento, promoviendo una cultura de mejora continua que refuerce la protección de la información y la capacidad de adaptación ante nuevos riesgos o cambios en los canales electrónicos, de modo que el sistema evolucione de forma dinámica y coherente con los desafíos tecnológicos actuales. (Rivadeneira Aguirre, 2021)

2.5.2 ISO/IEC 27005 Sistema de Gestión de Seguridad de la Información

Proporciona una guía detallada para la gestión de riesgos relacionados con la seguridad de la información, ya que establece un marco estructurado que facilita la identificación, evaluación y tratamiento de riesgos en función del contexto de la organización y de sus activos más críticos, lo cual resulta especialmente útil en entornos donde los canales electrónicos desempeñan un papel fundamental en las operaciones

institucionales, pues permite analizar amenazas específicas como ataques cibernéticos, errores de configuración o accesos no autorizados (Amparo Ortiz, 2021)

2.5.2.1 Principios de la gestión de riesgos según ISO/IEC 27005

Se rige por principios fundamentales como la integración con el sistema organizacional, la adaptación al contexto específico de cada entidad, la participación activa de las partes interesadas, la consideración del ciclo de vida de los activos, y la continuidad del proceso en el tiempo, lo cual implica que el tratamiento de riesgos no debe ser una actividad puntual sino un componente esencial de la cultura de seguridad que evoluciona junto con la tecnología y los cambios operativos (Álvaro, 2023)

2.5.2.2 Identificación de activos, amenazas y vulnerabilidades

Dentro del enfoque de ISO/IEC 27005 se establece como primer paso la identificación de activos de información que pueden verse comprometidos, incluyendo software, bases de datos, infraestructura tecnológica, usuarios, procesos y servicios críticos como los canales electrónicos, luego se procede a determinar las amenazas que podrían explotarlos, como accesos no autorizados, malware o errores humanos, y posteriormente se analizan las vulnerabilidades que permiten que dichas amenazas se materialicen, lo que permite construir una visión completa del entorno de riesgo para establecer medidas adecuadas de protección (Braga Calderon, 2021)

2.5.3 ISO 31000 Gestión del riesgo en organizaciones

Constituye un marco internacional diseñado para proporcionar principios y directrices sobre la gestión del riesgo en todo tipo de organizaciones, ya que promueve un enfoque integral y estructurado que permite identificar, evaluar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, operativos o tecnológicos, su aplicación no se limita a un área específica sino que abarca

desde la gobernanza institucional hasta la continuidad del negocio, incluyendo aspectos como riesgos financieros, reputacionales, legales y tecnológicos, en el caso de los canales electrónicos. (Álvaro, 2023)

2.5.3.1 Principios de la gestión del riesgo según ISO 31000

Se basa en una serie de principios que garantizan su eficacia dentro de la organización, entre ellos se destaca que debe integrarse en todos los procesos institucionales, formar parte de la toma de decisiones, abordar explícitamente la incertidumbre, considerar factores humanos y culturales, estar personalizada al entorno de la organización y mantenerse como un proceso dinámico que evoluciona con el contexto, lo cual asegura que la gestión de riesgos no sea una tarea aislada sino un componente esencial de la estrategia organizacional y tecnológica. (Álvarez Veintimilla , 2022)

2.5.3.2 Estructura del marco de trabajo de ISO 31000

Establece las bases necesarias para integrar la gestión de riesgos dentro de la cultura organizacional, comenzando con el liderazgo y el compromiso de la alta dirección, seguido por la planificación y diseño de políticas de gestión del riesgo, la asignación de responsabilidades, la disponibilidad de recursos adecuados y la promoción de una cultura basada en la toma de decisiones informadas, todo esto con el objetivo de asegurar que el proceso de gestión de riesgos sea sostenible, adaptable y coherente con la misión y visión institucional. (Ortiz Alulema , 2020)

2.5.4 MAGERIT

Desarrollada por el Consejo Superior de Administración Electrónica de España, constituye un marco técnico especializado en el análisis y gestión de riesgos en sistemas de información, su propósito principal es facilitar la toma de decisiones en materia de seguridad mediante un enfoque estructurado que identifica activos, valora amenazas y

evalúa vulnerabilidades con el fin de determinar el nivel de riesgo que enfrentan los servicios tecnológicos de una organización, esta metodología se apoya en la creación de escenarios de riesgo que combinan elementos como la probabilidad de ocurrencia, el impacto en los activos. (Amparo Ortiz, 2021)

2.5.4.1 Fases del análisis de riesgos en MAGERIT

- **Identificación de activos :** Esta fase inicial consiste en reconocer y documentar todos los elementos que conforman el sistema de información, tales como equipos, redes, aplicaciones, datos, usuarios, procesos y servicios relacionados con la operación tecnológica, cada activo debe ser clasificado en función de su importancia para la organización y su papel dentro de la arquitectura del sistema, lo cual permite construir un inventario detallado que servirá como base para el análisis posterior del riesgo. (Borbor Tumbaco, 2024)

- **Valoración de los activos:** Una vez identificados los activos, se procede a valorarlos en función de los tres criterios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, para cada uno de estos atributos se determina el nivel de impacto que generaría su alteración o pérdida, utilizando escalas cualitativas que expresan el grado de daño posible a la organización, este proceso permite establecer qué activos son más sensibles o críticos y, por tanto, cuáles deben recibir mayor atención en las fases siguientes del análisis de riesgos, ya que representan puntos clave en la continuidad y confiabilidad del sistema. (Amparo Ortiz, 2021)

- **Identificación de amenazas:** Reconocen todos los eventos o acciones que podrían poner en peligro los activos identificados, las amenazas pueden ser de origen humano, natural o tecnológico, intencionadas o accidentales, y su

identificación se realiza utilizando el catálogo de amenazas definido por MAGERIT, el cual clasifica los riesgos según su naturaleza y tipo de afectación, entre las amenazas más relevantes para los canales electrónicos se encuentran los accesos no autorizados, los errores de programación, el malware, las fallas en el suministro eléctrico y los desastres físicos, esta etapa permite establecer el vínculo entre cada amenaza y los activos potencialmente afectados. (Calderón Morán, 2024)

- **Evaluación de la probabilidad y el impacto:** Permite calcular el nivel de riesgo asociado a cada amenaza considerando dos factores principales: la probabilidad de que ocurra y el impacto que causaría en los activos, la probabilidad se evalúa en función del grado de exposición del sistema, la presencia de vulnerabilidades y el historial de incidentes similares, mientras que el impacto se basa en la valoración previa de los activos en términos de confidencialidad, integridad y disponibilidad, la combinación de estos factores permite clasificar los riesgos como bajos, medios o altos, y proporciona una base para priorizar la asignación de salvaguardas. (Borbor Tumbaco, 2024)

- **Determinación del nivel de riesgo:** Una vez obtenidos los valores de impacto y probabilidad, se utiliza una matriz de riesgos para determinar el nivel final de riesgo para cada activo-amenaza, esta matriz permite representar gráficamente el grado de exposición en diferentes niveles, lo cual facilita la priorización de los riesgos más críticos, el objetivo de esta fase es proporcionar una visión clara del panorama de amenazas que enfrenta la organización y establecer una jerarquía de atención que guíe la toma de decisiones sobre los recursos a proteger con mayor urgencia y profundidad. (González, 2023)

2.5.5 Tabla comparativa de las metodologías de análisis y gestión de riesgos

Con el fin de seleccionar la metodología más adecuada para la gestión de riesgos en los canales electrónicos de la Cooperativa Yuyay Ltda, se establecen una serie de criterios técnicos y prácticos que permiten evaluar y comparar las metodologías más utilizadas en el ámbito de la seguridad de la información.

Los criterios seleccionados en la tabla comparativa responden a la necesidad de evaluar la eficaz técnica y operativa de las metodologías de gestión de riesgos en el contexto específico de una cooperativa financiera con canales electrónicos.

- **Enfoque**: Este criterio permite identificar el propósito principal de cada metodología, diferenciando si está orientada a la seguridad de la información, a la gestión general de riesgos organizacionales o a sistemas tecnológicos específicos, lo cual es fundamental para un entorno altamente digitalizado como el de la Cooperativa Yuyay Ltda.

- **Fases principales:** Se evalúan las etapas estructurales de cada metodología para entender su lógica de aplicación y determinar cuál ofrece una secuencia más completa y técnica para el análisis y tratamiento de riesgos.

- **Nivel de detalle:** Es clave en entornos TI, donde se requiere un alto grado de especificidad para identificar amenazas y salvaguardas a nivel de activo. Este criterio permite discriminar entre metodologías más generales y aquellas con profundidad técnica.

- ***Catálogo de amenazas y activos***: Considera si la metodología proporciona herramientas o referencias concretas para identificar amenazas específicas y activos de información, elemento esencial para asegurar la trazabilidad y exhaustividad del análisis.

- ***Soporte con herramientas:*** Evalúa la disponibilidad de soluciones tecnológicas (como PILAR en el caso de MAGERIT), que permitan automatizar y estructurar el análisis, lo que mejora la eficiencia y la precisión del tratamiento de riesgos.

- ***Adaptación a entornos TI:*** Valora el grado en que la metodología se ajusta a escenarios tecnológicos, lo cual es determinante para garantizar su aplicabilidad en sistemas digitales como los canales electrónicos.

- ***Aplicabilidad en cooperativas pequeñas o medianas:*** Este criterio considera la viabilidad operativa y económica de adoptar la metodología en organizaciones con recursos limitados, como suele ser el caso de las cooperativas de ahorro y crédito.

- ***Ventajas y limitaciones:*** Finalmente, se consideran fortalezas y debilidades prácticas de cada enfoque para evaluar su conveniencia y sostenibilidad en función del contexto organizacional.

Tabla 1 Tabla comparativa de las metodologías de análisis y gestión de riesgos Fuente: Autor Propio

Criterio	**ISO/IEC 27005**	**ISO 31000**	**MAGERIT**
Enfoque	Seguridad de la información	Riesgos en general en cualquier organización	Riesgos en sistemas de información con detalle técnico
Fases principales	1. Establecer contexto 2. Identificar 3. Analizar 4. Evaluar 5. Tratar	1. Establecer contexto 2. Identificar 3. Analizar	1. Identificar activos 2. Valorar activos 3. Identificar amenazas

	6. Comunicar y monitorear	4. Evaluar 5. Tratar 6. Comunicar y revisar	4. Analizar impactos 5. Estimar riesgos 6. Aplicar salvaguardas
Nivel de detalle	Medio	Bajo	Alto
Catálogo de amenazas y activos	No	No	Sí, muy detallado (basado en catálogo de MAGERIT)
Soporte con herramientas	Limitado	No	Sí, con PILAR y otras herramientas de automatización
Adaptación a entornos TI	Alta	Media	Muy alta
Aplicabilidad en cooperativas pequeñas o medianas	Alta	Media	Alta (si se adapta correctamente)
Ventajas	Específica para seguridad TI, alinea con ISO 27001	General, adaptable a cualquier sector	Proporciona una visión profunda del entorno técnico, amenazas, y vulnerabilidades

Limitaciones	No incluye catálogos técnicos específicos	Muy general, no se enfoca en TI	Puede requerir capacitación inicial, mayor dedicación técnica

En base al análisis presentado en la tabla 1, se determina que MAGERIT es la metodología más idónea para aplicar a la Cooperativa Yuyay Ltda, ya que ofrece un mayor nivel de detalle técnico en la identificación y valoración de activos, amenazas y salvaguardas. A diferencia de MAGERIT cuenta con catálogos específicos y soporte de herramientas como PILAR, que permiten una evaluación más precisa y automatizada.

Esta capacidad resulta especialmente útil en entornos financieros donde los canales electrónicos manejan información sensible y están altamente expuestos a riesgos digitales, también su alta adaptabilidad a contextos tecnológicos y su aplicabilidad en organizaciones medianas refuerzan su pertinencia en este estudio.

3. CAPITULO III

MARCO METODOLOGICO

3.1 Enfoque de la Investigación

La investigación se desarrolla bajo un enfoque metodológico mixto, combinando elementos cualitativos y cuantitativos para abordar de forma estructurada y precisa la problemática asociada a la gestión de riesgos en los canales electrónicos de la Cooperativa.

Desde la perspectiva cualitativa, se lleva a cabo la identificación de activos, amenazas y vulnerabilidades mediante el análisis de documentos institucionales, entrevista focalizada y la evaluación del entorno organizacional.

El enfoque cuantitativo se implementa durante la etapa de evaluación de riesgos, utilizando la metodología MAGERIT como marco estructurado, esto posibilita la asignación de valores numéricos a los niveles de impacto y probabilidad de las amenazas detectadas, permitiendo así una medición objetiva del riesgo.

3.2 Nivel de la Investigación

El presente estudio se enmarca en un nivel descriptivo, lo cual permite realizar una caracterización técnica del estado actual de los canales electrónicos de la Cooperativa Yuyay Ltda, identificando activos de información, amenazas, vulnerabilidades y controles existentes.

3.3 Población y Muestra

La población de esta investigación corresponde al área de Tecnologías de la Información de la Cooperativa Yuyay Ltda, dado el enfoque técnico del estudio, se trabajará directamente con el jefe del Departamento de TI, quien actúa como informante clave por su conocimiento especializado sobre los canales electrónicos, activos digitales y riesgos asociados.

3.4 Tratamiento de la Información

La información será procesada mediante la matriz de análisis de riesgos MAGERIT, los activos serán evaluados según su criticidad, identificando amenazas y estimando niveles de impacto y probabilidad.

3.5 Fases para la aplicación de MAGERIT

MAGERIT estructura el análisis de riesgos en fases secuenciales que permiten identificar, valorar y tratar amenazas que comprometan la confidencialidad, integridad y disponibilidad de los servicios digitales. En esta investigación se aplicarán las siguientes etapas:

Identificación y valoración de activos

- Inventario de activos de información, tecnológicos y humanos vinculados a los canales electrónicos.
- Asignación de valores basados en criterios de criticidad, confidencialidad, integridad y disponibilidad.

Identificación de amenazas y vulnerabilidades

- Utilización del catálogo oficial de amenazas de MAGERIT para relacionar cada activo con riesgos potenciales.
- Detección de vulnerabilidades técnicas, procedimentales y humanas susceptibles de explotación.

Análisis de impactos

Estudio de las posibles consecuencias técnicas, operativas y económicas ante la materialización de una amenaza.

- Estimación y evaluación del riesgo

- Cálculo del riesgo inherente combinando impacto y probabilidad de ocurrencia.
- Determinación del riesgo residual después de aplicar los controles vigentes.

Selección y aplicación de salvaguardas

- Propuesta de medidas técnicas, administrativas y físicas para mitigar los riesgos identificados.
- Priorización de salvaguardas considerando su viabilidad y el nivel de criticidad.

CAPÍTULO IV

4. PROPUESTA

4.1 Introducción

La presente propuesta tiene como objetivo implementar un esquema metodológicamente estructurado para la gestión de riesgos en la seguridad de la información de los canales electrónicos de la Cooperativa Yuyay Ltda., basado en la metodología MAGERIT y complementado con los lineamientos de la norma ISO/IEC 27001.

El acelerado proceso de transformación digital en el sector financiero ha incrementado de forma considerable la superficie de exposición a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información crítica. En este contexto, los canales electrónicos incluyendo aplicaciones móviles, plataformas de banca en línea y sistemas de transacciones constituyen activos estratégicos que requieren un tratamiento sistemático de riesgos para asegurar la continuidad de las operaciones y mantener la confianza de los socios.

Esta propuesta se sustenta en los resultados del diagnóstico realizado, el cual permitió identificar activos críticos, amenazas, vulnerabilidades y controles actualmente implementados.

A partir de estos hallazgos, se desarrolla un plan de tratamiento de riesgos que integra medidas preventivas y correctivas, priorizadas según criterios de viabilidad técnica, impacto potencial y nivel de criticidad.

4.2 Descripción de la Organización

La Cooperativa de Ahorro y Crédito Yuyay Ltda. (COAC Yuyay Ltda.), constituida el 9 de mayo de 2013, opera como una entidad financiera del sector popular y solidario con sede en la comunidad San Rafael, cantón Cañar, provincia del mismo nombre en Ecuador

Durante el año 2021, la cooperativa reportó un notable crecimiento financiero: los ingresos netos aumentaron en un 13,82 %, mientras que el total de sus activos creció en un 57,75 %, reflejando una expansión institucional sostenida

Este desempeño financiero destaca la capacidad de la entidad para consolidarse como un actor solvente y dinámico dentro del sistema financiero local, con una orientación clara hacia la inclusión y desarrollo de su entorno comunitario. (Santos Camas, 2020)

4.2.1 **Misión**

Fortalecer y promover la economía local con los emprendimientos alternativos con servicios financieros y no financieros eficientes bajo los principios y valores culturales kañaris orientados al nuevo sistema de la economía y de buen vivir

4.2.2 **Visión**

Fortalecer y promover la economía local ser una cooperativa solida alternativa al servicio de la sociedad vulnerable y posesionada en el área de influencia, que trabaja mediante enlace con cooperativas, bancos rurales, financiando actividades productivas en base a la economía andina agro-céntrica.

4.3 Levantamiento de activos

El presente levantamiento de activos identifica y describe los recursos tecnológicos esenciales para el funcionamiento de la entidad, estos activos constituyen la base operativa de los procesos financieros, transaccionales y administrativos, y su adecuada gestión es fundamental para

garantizar la continuidad del negocio, la eficiencia operativa y la seguridad de la información. La tabla 2 detalla cada activo con su respectivo identificador, descripción y ubicación, permitiendo una visión clara de su función dentro de la infraestructura tecnológica institucional.

Tabla 2 Levantamiento de activos Fuente: Autor Propio

ID	Activo	Descripción	Ubicación
A-001	Core Financiero	Sistema central que gestiona todas las operaciones financieras de la entidad.	Data Center Principal
A-002	Orquestador de Servicios	Contenedor de varios servicios de uso interno para la institución.	Centro de Datos
A-003	Gestor de incidentes	Gestión de problemas	Centro de Datos
A-004	Plataforma para Registro de actividades	Todas las actividades	Centro de Datos
A-005	Aula Virtual	Registro de actividades capacitación	Centro de Datos
A-006	Simuladores	Herramientas de simulación de Crédito y Pólizas	Centro de Datos
A-007	GrandStrem	Dispositivos de comunicaciones	Centro de Datos
A-008	Switch	Dispositivos de red	Centro de Datos
A-009	Convertidor de Fibra	Dispositivo de conversión de señal óptica	Centro de Datos
A-010	Firewall	Protección perimetral	Centro de Datos
A-011	UPS	Sistema de respaldo eléctrico	Centro de Datos

A-012	Servidores en la Nube	Infraestructura virtualizada para servicios y aplicaciones	Nube
A-013	ATM1	Cajeros automáticos para retiro y consulta de saldos.	Oficinas y puntos estratégicos
A-014	ATM2	Cajeros automáticos para retiro y consulta de saldos.	Oficinas y puntos estratégicos
A-015	Web Transaccional	Plataforma en línea para realizar operaciones y consultas por internet.	Servidor Web / Hosting seguro
A-016	App Recaudaciones	Cobros de depósitos y interno	Centro de datos
A-017	Yuyay móvil	Software	Servidores de Aplicaciones
A-018	Aplicaciones	Software interno para gestión de procesos administrativos y operativos.	Servidores de Aplicaciones

4.4 Evaluación de los riesgos en base a la metodología MARGERIT

La evaluación de riesgos se desarrolla aplicando la metodología MAGERIT, que permite calcular el nivel de exposición de los activos en función de su confidencialidad, integridad y disponibilidad (CIA). Cada activo se relaciona con amenazas y vulnerabilidades, evaluando su impacto y probabilidad, lo que facilita determinar el riesgo inherente y residual.

Para la fase de identificación de riesgos, se emplearon distintos instrumentos de recolección de información que garantizan la consistencia de los datos obtenidos:

- **Entrevistas semiestructuradas** con personal clave de las áreas tecnológicas y de gestión, con el fin de identificar los activos críticos y las principales amenazas percibidas.
- **Listas de chequeo (checklists)** adaptadas de buenas prácticas internacionales, tomando como referencia las normas ISO/IEC 27001, ISO/IEC 27005 y el NIST

Cybersecurity Framework, lo que permitió asegurar una cobertura amplia de escenarios de riesgo.

- **Análisis documental** de políticas internas, manuales de procesos, inventarios de hardware y software, que complementó la información primaria para una visión más objetiva de los activos y sus vulnerabilidades.
- **Plantillas de identificación** de activos y riesgos de MAGERIT, que sirvieron para estandarizar la recolección y clasificación de los datos, facilitando su posterior valoración en términos de impacto y probabilidad.

4.4.1 Valoración de los activos

A continuación, se presenta la escala para la calificación de los activos en base a lo siguiente:

Alto (3): Impacto crítico si se ve afectado.

Medio (2): Impacto considerable pero no crítico.

Bajo (1): Impacto menor, fácilmente mitigable

Tabla 3 Escala de valoración

Escala de valoración de Activos	
Intervalo	**Cualificación**
De 1 al 3	Medio
De 4 al 6	Alto
De 7 al 9	Critico

La valoración de activos constituye una fase fundamental dentro del análisis de riesgos de la Cooperativa de Ahorro y Crédito Yuyay Ltda.

En la tabla 4 los activos críticos de la organización evaluados en función de los parámetros de confidencialidad, integridad y disponibilidad. A partir de esta valoración se obtiene un puntaje global que permite jerarquizar los activos según su nivel de riesgo, ya que permite identificar los recursos tecnológicos más relevantes y determinar su importancia en función de tres parámetros esenciales: confidencialidad, integridad y disponibilidad (CIA). Esta clasificación asegura que los activos con mayor criticidad reciban un tratamiento de seguridad adecuado y proporcional al nivel de riesgo que representan.

Tabla 4 Calificación de los activos: Autor Propio

ID	Activo	Confidencialidad	Integridad	Disponibilidad	Valoración
A-001	Core Financiero	3	3	3	9
A-002	Orquestador de Servicios	2	3	3	8
A-003	Gestor de incidentes	2	2	2	6
A-004	Plataforma para Registro de actividades	2	2	2	6
A-005	Aula Virtual	1	2	2	5
A-006	Simuladores	2	2	2	6
A-007	GrandStrem	2	2	2	6
A-008	Switch	1	2	3	6
A-009	Convertidor de Fibra	1	2	3	5

A-010	Firewall	3	3	3	9
A-011	UPS	1	2	3	6
A-012	Servidores en la Nube	3	3	3	9
A-013	ATM1	3	3	3	9
A-014	ATM2	3	3	3	9
A-015	Web Transaccional	3	3	3	9
A-016	App Recaudaciones	2	3	3	8
A-017	Yuyay móvil	3	3	3	9
A-018	Aplicaciones	2	3	2	7

4.4.2 Identificación de Amenazas

En este apartado se presentan las principales amenazas identificadas estas pueden originarse tanto en factores humanos como en factores naturales o técnicos.

En este proceso, cada amenaza fue evaluada en función de dos parámetros fundamentales: la probabilidad de ocurrencia y el impacto potencial que podría tener sobre la confidencialidad, integridad y disponibilidad de la información. Con base en estos factores, se aplicó la fórmula:

Riesgo = Probabilidad × Impacto

- **Impacto**

Se refiere al nivel de consecuencias que tendría la materialización de una amenaza sobre los activos de información o la infraestructura tecnológica de la organización.

En la siguiente tabla 5 se muestra la escala de valores de impacto utilizada para clasificar los efectos potenciales sobre los activos críticos**.** En la escala definida, los valores van de 1 a 5, donde:

Tabla 5 Escala de valores Impacto

Impacto		
Nivel de Impacto	**Descripción**	**Valor**
Insignificante	El efecto es mínimo y no compromete de forma apreciable la operación.	**1**
Menor	El daño es limitado, puede afectar un servicio parcial o por un corto período de tiempo.	**2**
Moderado	El incidente genera interrupciones o pérdidas que requieren acciones de recuperación significativas.	**3**
Mayor	Se producen daños severos que afectan procesos críticos y comprometen la confianza en los servicios.	**4**
Catastrófico	Implica la pérdida total o indisponibilidad prolongada de activos críticos, afectando gravemente la continuidad operativa	**5**

- **Probabilidad de ocurrencia**

  Corresponde a la frecuencia o posibilidad de que una amenaza llegue a materializarse.

  A continuación, en la tabla 6 se muestra la escala de valores asignados a la probabilidad de ocurrencia, la cual permite clasificar los eventos de acuerdo con su nivel de posibilidad de materialización. Se expresa en una escala de 1 a 3, donde:

Tabla 6 Escala de valores de probabilidad de ocurrencia

Probabilidad de ocurrencia		
Nivel de Probabilidad	**Descripción**	**Valor**
Improbable	Es poco factible que ocurra, puede considerarse excepcional.	**1**
Probable	Existe una posibilidad real de ocurrencia en un periodo determinado.	**2**
Casi Seguro	Alta probabilidad de que suceda, considerando antecedentes y vulnerabilidades detectadas.	**3**

Cálculo de riesgo

Tabla 7 Escala de valores de riesgos

Riesgo		
Nivel de riesgo	**Descripción**	**Valor**
Bajo	Riesgos tolerables con necesidad de controles básicos.	**1-4**
Medio	Riesgos que requieren medidas preventivas específicas.	**5-8**
Alto	Riesgos significativos que demandan controles avanzados y atención prioritaria.	**9-11**
Critico	Riesgos inaceptables que deben ser mitigados de manera inmediata, ya que comprometen la continuidad de los servicios y la seguridad de la información.	**12-15**

La tabla 8 expone la escala de valores de riesgos, la cual permite clasificar los eventos identificados en cuatro niveles: bajo, medio, alto y crítico. Esta calificación se basa en la información proporcionada por el jefe del departamento de TI.

Tabla 8 Matriz para el cálculo de riesgo: Autor Propio

Activo	Código Amenaza	Amenaza	Probabilidad de ocurrencia	Impacto	Impacto X probabilidad	Riesgo
Core Financiero	[A.11]	Acceso no autorizado	3	4	12	Critico
	[A.25]	Robo	1	4	4	Bajo
	[E.4]	Errores de configuración	2	4	8	Medio
	[I.6]	Corte del suministro eléctrico	2	5	10	Alto
	[A.24]	Denegación de servicio	3	5	15	Critico
	[E.19]	Fugas de Información	2	3	6	Medio
Orquestador de Servicios	[E.4]	Errores de configuración	3	4	12	Critico
	[I.8]	Fallo de servicios de comunicaciones	3	4	12	Critico
	[E.8]	Difusión de software dañino	3	5	15	Critico
	[E.18]	Destrucción de información	2	5	10	Alto
	[E.19]	Fugas de Información	3	3	9	Alto
	[A.4]	Manipulación de la configuración	3	4	12	Critico
	[A.11]	Acceso no autorizado	2	4	8	Medio
	[E.20]	Vulnerabilidades de los programas (software)	2	4	8	Medio
Firewall	[E.4]	Errores de configuración	2	4	8	Medio
	[E.20]	Vulnerabilidades de los programas (software)	2	3	6	Medio
	[E.21]	Errores de mantenimiento / actualización de programas (software)	2	4	8	Medio
	[A.11]	Acceso no autorizado	1	5	5	Medio
	[A.24]	Denegación de servicio	2	4	8	Medio
	[A.11]	Acceso no autorizado	2	4	8	Medio

Servidores en la Nube	[I.8]	Fallo de servicios de comunicaciones	2	3	6	Medio
	[E.4]	Errores de configuración	3	3	6	Medio
	[E.19]	Fugas de Información	2	4	8	Medio
	[E.18]	Destrucción de información	2	5	10	Alto
	[E.21]	Errores de mantenimiento / actualización de programas (software)	3	3	9	Alto
	[I.8]	Fallo de servicios de comunicaciones	2	3	6	Medio
ATM1	[I.5]	Avería de origen físico o lógico	3	5	15	Critico
	[I.6]	Corte del suministro eléctrico	2	3	6	Medio
	[A.25]	Robo	2	2	4	Bajo
	[A.23]	Manipulación de los equipos	2	5	10	Alto
	[E.25]	pérdida de equipos	3	3	9	Alto
	[A.24]	Denegación de servicio	2	3	6	Medio
	[A.5]	Suplantación de la identidad del usuario	3	5	15	Critico
	[A.11]	Acceso no autorizado	5	3	15	Critico
	[A.23]	Manipulación de los equipos	3	4	12	Critico
	[A.26]	Ataque destructivo	3	4	12	Critico
ATM2	[A.5]	Suplantación de la identidad del usuario	3	4	12	Critico
	[I.5]	Avería de origen físico o lógico	3	4	6	Medio
	[I.6]	Corte del suministro eléctrico	2	4	8	Medio
	[I.8]	Fallo de servicios de comunicaciones	2	2	4	Bajo
	[A.30]	Ingeniería social	3	4	12	Critico
	[A.11]	Acceso no autorizado	3	4	12	Critico
	[A.23]	Manipulación de los equipos	2	3	6	Medio

	[A.25]	Robo	2	3	6	Medio
	[A.26]	Ataque destructivo	2	3	6	Medio
Web Transaccional	[A.8]	Difusión de software dañino	2	5	10	Alto
	[A.22]	Manipulación de programas	2	4	8	Medio
	[A.5]	Suplantación de la identidad del usuario	2	3	6	Medio
	[A.25]	Robo	2	4	8	Medio
	[I.8]	Fallo de servicios de comunicaciones	2	2	4	Bajo
	[E.23]	Errores de mantenimiento / actualización de equipos	3	2	6	Medio
App Recaudaciones	[E.1]	Errores de usuario en la operación	2	4	8	Medio
	[A.11]	Acceso no autorizado	1	4	4	Bajo
	[E.19]	Fugas de información	2	3	6	Medio
	[E.14]	Escapes de información	2	3	6	Medio
Yuyay Móvil	[E.18]	Destrucción de información	1	5	5	Medio
	[A.5]	Suplantación de la identidad del usuario	2	4	8	Medio
	[A.26]	Interceptación de comunicaciones	2	3	6	Medio
	[A.13]	Publicación de versiones falsas de la aplicación	2	4	8	Medio
Aplicaciones	[E.4]	Errores de configuración	2	4	8	Medio
	[E.14]	Escapes de información	2	3	6	Medio
	[E.28]	Indisponibilidad del sistema	3	5	15	Critico
	[A.25]	Fuga de datos internos por permisos indebidos	2	4	8	Medio

	[A.24]	Denegación de servicio	2	4	8	Medio

La tabla 8 proporciona una visión clara de los escenarios más relevantes, destacando aquellos con calificación de crítico, entre los intervalos de 15 a 20 se encuentran el Core Financiero, el Orquestador de Servicios, ATM1, ATM2, la Web Transaccional y las Aplicaciones internas.

Mientras que las amenazas técnicas más relevantes identificadas corresponden a los: accesos no autorizados (A.11), robos y fugas de información (A.25, E.19, E.14), errores de configuración (E.4), denegaciones de servicio (A.24, A.26), así como averías físicas o lógicas (I.5) y cortes de suministro eléctrico (I.6). Estos eventos, al combinarse con sus valores de probabilidad e impacto, ubican a varios riesgos en categorías Crítico, destacando por ejemplo los ataques de manipulación de equipos en cajeros automáticos, la difusión de software dañino en la Web Transaccional y las vulnerabilidades de programas en el Orquestador de Servicio

i. **Controles/Salvagurdas para los activos**

La matriz de salvaguardas desarrollada para los activos críticos de la Cooperativa de Ahorro y Crédito Yuyay Ltda. no se limita únicamente a mitigar amenazas identificadas mediante la metodología MAGERIT, sino que se fundamenta en estándares internacionales reconocidos. En particular, se ha establecido una alineación explícita con los controles descritos en la norma ISO/IEC 27002:2022, considerada la guía de referencia global para la implementación de medidas de seguridad de la información.

- El objetivo de esta alineación es asegurar la compatibilidad normativa, garantizando que las medidas propuestas sean coherentes con buenas prácticas ampliamente aceptadas en el sector financiero.
- Fortalecer la gestión de riesgos, al estructurar las salvaguardas bajo controles que cubren los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (CIA).

En la tabla 9 se detalla el análisis de riesgos identificados en los principales activos críticos de la organización. En ella se especifican las amenazas más relevantes, el nivel de riesgo asociado y los controles de seguridad recomendados conforme a la norma ISO/IEC 27002, así como las salvaguardas propuestas para su mitigación.

Tabla 9 Salvaguardas para los activos críticos

Activo	Código de Amenaza	Amenaza	Nivel de Riesgo	Control ISO/IEC 27002	Salvaguarda
	[A.11]	Acceso no Autorizado	Critico	9.2.3 – Gestión de privilegios de acceso	Implementar autenticación multifactor (MFA) y control de accesos privilegiados.
Core Financiero	[A.24]	Denegación de servicio	Critico	12.1.4 – Protección contra ataques	Sistemas IDS/IPS y balanceadores de carga para mitigar ataques.
	[E.4]	Errores de configuración	Critico	12.1.2 – Gestión de cambios	Establecer procedimientos de gestión de cambios y auditorías de configuración periódicas.
	[I.8]	Fallo de servicios de comunicaciones	Critico	17.2.1 – Continuidad de servicios TIC	Contratar proveedores con SLA robustos y establecer redundancia de enlaces.

Orquestador de Servicios	[E.8]	Difusión de software dañino	Critico	12.2.1 – Protección contra malware	Implementar soluciones antimalware, parches regulares y control de integridad en el software
	[A.4]	Manipulación de la configuración	Critico	9.4.3 – Gestión de credenciales de usuario	Aplicar segregación de funciones y controles de acceso basados en roles (RBAC).
	[I.5]	Avería de origen físico o lógico	Critico	11.1.2 – Seguridad física de equipos 11.2.1 – Protección contra sabotaje	Mantenimiento preventivo, monitoreo remoto y contratos de soporte técnico inmediato
	[A.5]	Suplantación de la identidad del usuario	Critico	7.2.2 – Concienciación en seguridad 9.4.3 – Gestión de credenciales	Implementar autenticación biométrica y validación de PIN cifrado.
	[A.23]	Manipulación de los equipos	Critico	11.1.2 – Seguridad física de equipos	Video vigilancia, alarmas, sellado físico de puertos y sensores de apertura.

ATM1	[A.26]	Ataque destructivo	Critico	11.2.1 – Protección contra sabotaje	Refuerzo físico de cajeros (acero reforzado), monitoreo en tiempo real y protocolos de respuesta rápida
	[A.5]	Suplantación de la identidad del usuario	Critico	9.4.3 – Gestión de credenciales de usuario	Autenticación reforzada, validaciones biométricas y cifrado de transacciones.
ATM2	[A.5]	Suplantación de la identidad del usuario	Critico	9.4.3 – Gestión de credenciales de usuario	Autenticación reforzada, validaciones biométricas y cifrado de transacciones.
	[A.30]	Ingeniería social	Critico	7.2.2 – Concienciación en seguridad	Capacitación continua a usuarios y personal sobre fraudes electrónicos.
	[A.11]	Acceso no autorizado	Critico	9.4.2 – Control de acceso a sistemas	Segmentación de red, VPN seguras y control de sesiones remotas.
Aplicaciones	[E.28]	Indisponibilidad del sistema	Critico	17.1.1 – Continuidad de negocio	Implementar alta disponibilidad, servidores redundantes y plan de

		recuperación ante desastres (DRP).

b. **Plan de tratamiento de riesgos**

El plan de tratamiento de riesgos se fundamenta en los resultados de la matriz de valoración, que evidenció activos críticos con un nivel alto o crítico. Para su gestión se adopta la metodología MAGERIT, complementada con las buenas prácticas de la ISO/IEC 27002:2022, lo que asegura un enfoque sistemático y alineado a estándares internacionales del sector financiero.

El plan se estructura en tres ejes:

- **Estrategias de mitigación:** aplicación de controles preventivos, detectivos y correctivos para proteger la confidencialidad, integridad y disponibilidad (CIA) de los activos.
- **Protocolos de respuesta:** procedimientos de contención, erradicación y recuperación para reducir tiempos de indisponibilidad y evitar recurrencias.
- **Políticas de continuidad (DRP/BCP):** mecanismos de resiliencia operativa basados en redundancia tecnológica, replicación de servicios y planes de recuperación ante desastres.

En la siguiente tabla 11 se presenta el análisis de riesgos asociados a los principales activos críticos de la organización. En ella se identifican las amenazas relevantes según el catálogo MAGERIT, las salvaguardas correspondientes alineadas a la norma ISO/IEC 27002.

Tabla 10 Plan de tratamiento de riesgos Fuente: Autor Propio

Activo Critico	Amenaza (Catálogo MAGERIT)	Salvaguarda (ISO/IEC 27002)	Estrategia de Mitigación	Protocolo de Respuesta	Política de Continuidad (DRP/BCP)
Core Financiero	[A.11] Acceso no Autorizado	MFA, control de accesos privilegiados	Prevención mediante autenticación reforzada y segregación de funciones	Aislamiento inmediato del sistema comprometido, bloqueo de credenciales	. Restauración desde backups cifrados, reanudación prioritaria de operaciones
	[A.24] Denegación de servicio	IDS/IPS y balanceadores de carga	Mitigación técnica con sistemas de detección y balanceo de tráfico	Contención del ataque DDoS con reglas dinámicas en firewall	Redundancia de servidores y plan de recuperación rápida
	[E.4] Errores de configuración	Gestión de cambios y auditorías periódicas	Procedimientos formales de revisión y control de configuraciones	Reversión inmediata de cambios erróneos, activación de versión estable	Procedimientos documentados de fallback en sistemas críticos

Orquestador de Servicios	[I.8] Fallo de servicios de comunicaciones	Contratar proveedores con SLA robustos y establecer redundancia de enlaces.	Contratación de proveedores con SLA garantizados y enlaces alternos.	Derivación automática a enlaces redundantes, activación de plan de soporte	Continuidad operativa con enlaces secundarios
	[E.8] Difusión de software dañino	Antimalware, parches regulares, control de integridad	Endurecimiento de sistemas y validación de software seguro	Eliminación de software malicioso, cuarentena de equipos	Restauración de imágenes seguras y monitoreo continuo
	[A.4] Manipulación de la configuración	Aplicar segregación de funciones y controles de acceso	Aplicación de privilegios mínimos y revisión de cambios críticos	Bloqueo de cuentas sospechosas y restauración de configuración confiable	Respaldo de configuraciones seguras y rollback automático

		basados en roles (RBAC			
ATM1	[I.5] Avería de origen físico o lógico	Mantenimiento preventivo, monitoreo remoto y contratos de soporte técnico inmediato	Prevención mediante revisiones programadas y monitoreo activo	Activación inmediata de soporte técnico y derivación a otro cajero	Disponibilidad de ATM redundantes y reemplazo rápido
	[A.5] Suplantación de la identidad del usuario	Autenticación biométrica y cifrado de PIN/transacciones	Validación robusta de usuario y cifrado extremo a extremo	Bloqueo automático ante intentos fallidos y reporte en tiempo real	Mantenimiento de ATM redundantes y reposición inmediata
	[A.23] Manipulación de los equipos	Videovigilancia, alarmas, sellado físico	Prevención mediante control físico y sensores	Alerta inmediata a seguridad física y desconexión del ATM afectado	Sustitución de equipos comprometidos y respaldo de operaciones

	[A.26] Ataque destructivo				
ATM2	[A.5] Suplantación de la identidad del usuario	Autenticación biométrica y cifrado de PIN/transacciones	Validación robusta de usuario y cifrado extremo a extremo	Bloqueo automático ante intentos fallidos y reporte en tiempo real	Mantenimiento de ATM redundantes y reposición inmediata
	[A.30] Ingeniería social	Capacitación en fraudes electrónicos	Concienciación de usuarios y personal de soporte	Registro y análisis de incidentes reportado	Inclusión en plan de comunicación de crisis
	[A.11] Acceso no autorizado	MFA, control de accesos privilegiados	Prevención mediante autenticación reforzada y segregación de funciones	Bloqueo de sesiones no autorizadas y monitoreo reforzado	Restauración inmediata y continuidad con sistemas de respaldo

Aplicaciones	[E.28] Indisponibilidad del sistema	Alta disponibilidad y plan de recuperación ante desastres (DRP)	Prevención con redundancia y monitoreo de sistemas	Activación de servidores de respaldo y restauración desde backups	Ejecución del DRP con servidores alternos y replicación en la nube

c. Planificación de implementación de controles

La tabla 11 presenta la planificación para la implementación de los controles y se convierte en una guía práctica que ordena de manera clara y coherente la ejecución del Plan de Tratamiento de Riesgos. Su propósito es asegurar que los controles definidos se apliquen paso a paso, siguiendo un orden lógico de prioridades, lo que facilita un mejor uso de los recursos disponibles y aumenta la efectividad en la reducción de los riesgos detectados.

Las actividades están distribuidas en cuatro fases secuenciales:

- **Fase 1 (Controles preventivos):** orientada a reducir la probabilidad de ocurrencia de amenazas mediante autenticación robusta, segmentación de red y refuerzo físico de la infraestructura más expuesta.
- **Fase 2 (Controles detectivos):** incorpora capacidades de monitoreo y detección de incidentes en tiempo real, fortaleciendo la capacidad de identificar anomalías y responder de forma temprana.
- **Fase 3 (Controles correctivos y pruebas):** incluye simulacros de incidentes, recuperación ante desastres y restauración de copias de seguridad, lo que permite evaluar la eficacia de los mecanismos de respuesta.
- **Fase 4 (Mejora continua):** establece actividades permanentes de auditoría, capacitación y actualización de políticas, asegurando la sostenibilidad del modelo de gestión de riesgos en el tiempo.

Tabla 11 Matriz de fases de implementación

Fase	Periodo estimado	Actividades principales	Responsables
Fase1: Controles preventivos	Mes 1 – Mes 2	- Implementación de autenticación multifactor (MFA) - Configuración de firewalls y segmentación de red - Aplicación de políticas RBAC - Refuerzo físico y videovigilancia en ATMs	Jefe de TI, Equipo de Seguridad Informática
Fase2: Controles detectivos	Mes 3 – Mes 4	- Implementación de IDS/IPS y monitoreo en tiempo real (SIEM) - Auditorías de configuración periódicas - Instalación de sistemas antimalware y gestión de parches - Monitoreo de aplicaciones críticas (Core Financiero, Web Transaccional, App Yuyay)	Equipo de Seguridad Informática, Soporte Técnico
Fase3: Controles correctivos y pruebas	Mes 5 – Mes 6	- Ejecución de simulacros de respuesta a incidentes - Activación de servidores redundantes y pruebas de DRP	Jefe de TI, Operaciones Financieras, Alta Dirección

		- Restauración de copias de seguridad cifradas - Protocolos de escalamiento y comunicación en crisi	
Fase4: Mejora continua	Permanente (a partir del Mes 7)	- Evaluaciones periódicas de riesgos (MAGERIT) - Auditorías de cumplimiento ISO/IEC 27002 - Programas de capacitación en seguridad - Actualización de políticas y protocolos	Alta Dirección, Jefe de TI

Riesgo residual

El caculo de riesgo residual se realizó a partir del riesgo inherente identificado en cada activo, el cual resulta de la combinación entre probabilidad de ocurrencia de la amenaza y el impacto asociado implementados mediante las escalas cualitativas mostradas.

En la tabla 12 se define la escala de riesgo residual empleada para priorizar el tratamiento de riesgos tras la implementación de controles. Se definen los niveles cualitativos entre 1–4.

Tabla 12Escala de valores de eficiencia del control

EFICIENCIA DEL CONTROL	
Cualitativo	**Cuantitativo**
Bajo	1
Medio	2
Alto	3
Optimo	4

En la Tabla 13 expone lo valores asignados al riesgo residual, los cuales se clasifican en un rango que vea desde el nivel Bajo hasta el nivel Muy Alto.

Tabla 13 Valores para el Riesgo Residual

ESCALA DE RIESGO RESIDUAL		
Nivel	**Escala**	**Descripción**
Bajo	1	Exposición mínima
Medio-bajo	2	Riesgo controlado
Medio	3	Puede afectar objetivos relacionados que tenga fallas similares
Alto	4	Probable afectación
Muy Alto	5	Riesgo inaceptable

En la Tabla 14 donde se detalla las salvaguardas a implementar seguidas del riesgo inherente, eficiencia del control y el riesgo residual, para ello se utilizan los siguientes cálculos:

Riesgo Inherente (RI): Es el nivel de riesgo antes de aplicar controles, calculado como:

RI=Probabilidad×Impacto

Eficacia del Control (Ef): Es el porcentaje en que un control reduce la probabilidad o el impacto de la amenaza (ej. 80% = 0.8).

Riesgo Residual (RR): Es el riesgo que permanece después de aplicar los controles.

Fórmula del Riesgo Residual

$$RR = RI \times (1 - Ef)$$

donde:

RI = valor del riesgo inherente (en escala numérica, ej. 1–5).

Ef = eficacia del control expresada en fracción (ej. 80% = 0.8).

Tabla 14 Matriz de riesgo residual

Activo / Proceso afectado	Amenaza	Probabilidad	Impacto	Riesgo Inherente	Salvaguarda	Tipo de -control	Eficiencia de controles	Riesgo Residual
ATMs	Acceso no autorizado	Alta	Alta	Critico	Autenticación multifactor (MFA), configuración de firewalls y segmentación de red, aplicación de políticas RBAC, refuerzo físico y videovigilancia en ATMs	Preventivo	80%	Medio
Aplicaciones críticas (Core Financiero, Web Transaccional, App Yuyay)	Denegación de Servicio (DoS), malware, fallas de configuración	Alta	Medio	Alto	IDS/IPS y monitoreo en tiempo real (SIEM), auditorías de configuración periódicas, instalación de sistemas antimalware y gestión de parches, monitoreo de aplicaciones críticas (Core Financiero, Web Transaccional, App Yuyay)	Preventivo/dtectivo	60%	Medio-Bajo

Infraestructura general de TI	Interrupción del servicio, pérdida de dato	Alta	Critica	Muy Alto	Simulacros de respuesta a incidentes, activación de servidores redundantes y pruebas de DRP, restauración de copias de seguridad cifradas, protocolos de escalamiento y comunicación en crisis	Correctivos	90%	Bajo

La tabla 14 expone la evaluación y calculación del riesgo residual, ya que permite identificar el nivel de exposición que persiste incluso después de aplicar las salvaguardas. Los resultados reflejan que, aunque algunos riesgos iniciales eran críticos altos, la implementación de controles efectivos logro reducirlos a niveles medios y bajos, lo que demuestra la eficacia de la gestión de riesgos realizada.

Como resultado de la aplicación de las salvaguardas y controles propuestos, se observa una reducción significativa de los niveles de riesgo. En los activos más críticos, como los ATMs y las aplicaciones financieras, el riesgo pasó de ser clasificado como *Crítico* o *Alto* a niveles *Medio* y *Medio-Bajo*, gracias a la implementación de controles preventivos y detectivos con eficiencias del 60% al 80%. Por su parte, en la infraestructura general de TI**,** los riesgos catalogados inicialmente como *Muy Altos* se redujeron a un nivel *Bajo*, con una efectividad del 90% en los controles correctivos aplicados. En términos globales, se logró una reducción aproximada del 80% de los riesgos críticos y muy altos**,** migrándolos hacia categorías aceptables (Medio o Bajo), lo que evidencia la efectividad de la estrategia de seguridad implementada y refuerza la resiliencia organizacional frente a incidentes de ciberseguridad.

Plan de Implementación de Salvaguardas

Con el fin de garantizar la puesta en marcha efectiva de las medidas de seguridad propuestas, se plantea un plan de implementación que incluye fases, actividades y responsables. Este plan busca integrar tanto la adquisición de tecnologías como la capacitación del personal, alineando los recursos disponibles con las prioridades estratégicas de la cooperativa.

Cronograma propuesto (6 meses):

Tabla 15 Implementación de las salvaguardas.

	Actividades principales	Responsable	Duración estimada
1. Planificación inicial	Presentación del plan al Directorio, asignación de presupuesto, definición de responsables	Gerencia + TI	2 semanas
2. Adquisición de tecnologías	Compra de soluciones de MFA, firewalls, SIEM, servidores redundantes	Área de TI	1 mes
3. Implementación técnica	Instalación y configuración de firewalls, IDS/IPS, SIEM, redundancia de servidores	Área de TI + Proveedor externo	2 meses
4. Capacitación del personal	Talleres de concienciación en ciberseguridad, formación en protocolos de respuesta	RRHH + TI	1 mes
5. Pruebas y simulacros	Ejecución de pruebas de DRP, simulacros de incidentes, auditoría interna	TI + Auditoría	1 mes

6. Evaluación final	Medición de reducción de riesgos, entrega de informe final al Directorio	TI + Auditoría externa	2 semanas

Presupuesto estimado

Tabla 16 Presupuesto Estimado para la implementación.

Categoría	Descripción	Costo estimado (USD)
Tecnologías de seguridad	Firewalls, SIEM, IDS/IPS, licencias antimalware, MFA	25,000
Infraestructura redundante	Servidores, almacenamiento cifrado, respaldo en la nube	15,000
Capacitación y sensibilización	Talleres para personal administrativo y técnico	5,000
Auditoría y consultoría externa	Evaluación inicial y auditoría de implementación	8,000
Total, estimado		53,000

CONCLUSIONES

- La revisión de la teoría permitió la identificación de marcos y metodologías relevantes aplicables a la gestión de riesgos del sector financiero, como MAGERIT, ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 27002. La comparación demostró que la metodología MAGERIT es particularmente relevante para la Cooperativa Yuyay Ltda., ya que proporciona una descripción rica y técnica que ayuda en la identificación de activos, amenazas y vulnerabilidades dentro de los canales de percepción electrónica, al tiempo que garantiza el cumplimiento de las buenas normas internacionales.

- La evaluación realizada con respecto a los canales electrónicos de la cooperativa pudo identificar activos críticos como el Núcleo Financiero, los Cajeros Automáticos, las Transacciones por Web y la aplicación móvil Yuyay. Estos activos tienen una calificación de riesgo alta o crítica, principalmente debido a algunas de las siguientes amenazas: acceso no autorizado, ataques de denegación de servicio, manipulación física de dispositivos y ingeniería social. Tal diagnóstico señaló la necesidad de mejorar las medidas de control de seguridad para garantizar la Confidencialidad, Integridad y Disponibilidad (CIA) de los servicios digitales.

- El uso de MAGERIT complementado con las directrices de ISO/IEC 27002 permitió la formulación de un plan de tratamiento de riesgos estructurado que integra estrategias de mitigación priorizadas, protocolos de respuesta a incidentes y políticas de continuidad del negocio (DRP/BCP). El plan aborda múltiples dimensiones que mejoran la resiliencia operativa de la cooperativa, aumentan la confianza de los miembros en los servicios digitales y también ayudan a construir una base a largo plazo para futuras innovaciones tecnológicas

RECOMENDACIONES

- Se recomienda a Yuyay Ltda. implementar gradualmente el plan de tratamiento de riesgos diseñado. Se debe poner un énfasis especial en los activos críticos encontrados. La gobernanza del marco que estructura la adopción de los controles alineados debe ser codificada como políticas internas y como procedimientos que se mantengan bajo control de versiones a intervalos definidos, garantizando que la actividad de gestión de riesgos sea etérea, continua y revisada en los intervalos definidos.

- Se recomienda a Yuyay Ltda. implementar gradualmente el plan de tratamiento de riesgos diseñado. Se debe poner un énfasis especial en los activos críticos encontrados. La gobernanza del marco que estructura la adopción de los controles alineados debe ser codificada como políticas internas y como procedimientos que se mantengan bajo control de versiones a intervalos definidos, garantizando que la actividad de gestión de riesgos sea etérea, continua y revisada en los intervalos definidos.

- Se recomienda que, durante la estrategia a medio plazo de la cooperativa, la imagen y credibilidad de la institución hacia socios y organismos reguladores se vean positivamente impactadas por la obtención de la certificación ISO/IEC 27001. Este proceso integrará, por primera vez, los aprendizajes continuos y posteriores a los talleres, marcos para la mejora continua, auditorías externas e indicadores de rendimiento claros en la consolidación del Sistema de Gestión de Seguridad de la Información (SGSI).

5. REFERENCIAS

Alvarado Véliz, M. J. (01 de 2024). *repositorio.puce.edu.ec.* Obtenido de repositorio.puce.edu.ec: https://repositorio.puce.edu.ec/server/api/core/bitstreams/3a66057a-e0bc-4393-8dcd-bed7515ce423/content

Campo Cucunuba , L. M. (2024). *ciencia.lasalle.edu.co.* Obtenido de ciencia.lasalle.edu.co: https://ciencia.lasalle.edu.co/server/api/core/bitstreams/2a97f3ed-687a-45da-9e16-2f34d8407bf8/content

Molina, A. V., & Chacon , N. C. (2022). *repository.ucatolica.edu.co.* Obtenido de repository.ucatolica.edu.co: https://repository.ucatolica.edu.co/server/api/core/bitstreams/d14a100b-b3ea-46f4-b9f6-53a0765e91f7/content

Sánchez Paredes, C. E. (08 de 2021). *biblioteca.uteg.edu.ec:8080.* Obtenido de biblioteca.uteg.edu.ec:8080: http://biblioteca.uteg.edu.ec:8080/bitstream/handle/123456789/1533/Modelo%20de%20Gesti%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%20adaptado%20a%20las%20Cooperativas%20de%20Ahorro%20y%20Cr%C3%A9dito%20de%20la%20ciudad%20de%20Guayaquil..pdf?

Álvarez Veintimilla , E. P. (2022). *repositorio.utc.edu.ec.* Obtenido de repositorio.utc.edu.ec: https://repositorio.utc.edu.ec/server/api/core/bitstreams/8b520822-8fc7-40cb-8090-9f05dedec66b/content

Álvaro, G. (06 de 4 de 2023). *repositorio.comillas.edu.* Obtenido de repositorio.comillas.edu: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/74737/TFG%20-%20Guerrero%20Gallego%2c%20Alvaro%20.pdf?sequence=1&isAllowed=y

Amparo Ortiz, A. (2021). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/41960/aortizari.pdf?sequence=3

Arellano Veloz, C. E. (01 de 2023). *repositorio.puce.edu.ec.* Obtenido de repositorio.puce.edu.ec: https://repositorio.puce.edu.ec/server/api/core/bitstreams/75d06c01-781e-49b7-aba0-b87b258deea8/content

Avila Ruiz, J. F., & Jara Guarnizo , P. A. (02 de 2022). *repository.ucc.edu.co.* Obtenido de repository.ucc.edu.co: https://repository.ucc.edu.co/server/api/core/bitstreams/0ae5f6b8-cd1c-4fd8-bf49-90cdd8a6480a/content

Borbor Tumbaco, A. S. (2024). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/bitstream/46000/11828/1/UPSE-TTI-2024-0026.pdf

Braga Calderon, I. M. (2021). *repositorio.uchile.cl.* Obtenido de repositorio.uchile.cl: https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?sequence=1&isAllowed=y

Calderón Morán, M. J. (2024). *dspace.unach.edu.ec.* Obtenido de dspace.unach.edu.ec: http://dspace.unach.edu.ec/bitstream/51000/12420/1/PLAN%20INTEGRAL%20DE%20GESTION%20DE%20RIESGOS%20ADPEC.S.A.S.pdf

García Bravo , M. E., Hurtado García , K., Torres Briones , R. M., & Moreno Tapia, L. M. (2021). FACTORES INFLUYENTES EN EL INCUMPLIMIENTO DE. *Revista electrónica TAMBARA*, 1160-1170.

Garzon Quito, E. M. (2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/21396/1/UPS-CT009402.pdf

González, M. (01 de 03 de 2023). *repositorio.comillas.edu.* Obtenido de repositorio.comillas.edu: https://repositorio.comillas.edu/jspui/retrieve/619887/TFG%20-%20Gonzalez%20Hernandez%2C%20Mar.pdf

Guaman Zaruma, L. A. (2022). *dspace.ucacue.edu.ec.* Obtenido de dspace.ucacue.edu.ec: https://dspace.ucacue.edu.ec/server/api/core/bitstreams/8ee91783-351e-4691-8de6-931dce9a9028/content

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

Jiménez, J. (01 de 02 de 2023). *oa.upm.es.* Obtenido de oa.upm.es: https://oa.upm.es/75099/1/TFG_JUAN_JIMENEZ_PEREZ.pdf

Larrauri , I. (21 de 10 de 2021). *upcommons.upc.edu.* Obtenido de upcommons.upc.edu: https://upcommons.upc.edu/bitstream/handle/2117/356501/memoria.pdf?sequence=1&isAllowed=y

Ortiz Alulema , I. D. (2020). *repositorio.uasb.edu.ec.* Obtenido de repositorio.uasb.edu.ec: https://repositorio.uasb.edu.ec/bitstream/10644/7760/1/T3349-MAE-Ortiz-Implementacion.pdf

Quinde Uyaguari, K. E. (2023). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/24314/1/UPS-CT010340.pdf

Rivadeneira Aguirre, M. V. (2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/21031/1/TTQ446.pdf

Rodríguez, I. O. (01 de 04 de 2022). *51.143.95.221.* Obtenido de 51.143.95.221: http://51.143.95.221/bitstream/TecNM/5601/1/G14071343_donacion_tesis_bib.pdf

Santos Camas, J. (2020). *dspace.espoch.edu.ec:8080.* Obtenido de dspace.espoch.edu.ec:8080: https://dspace.espoch.edu.ec:8080/server/api/core/bitstreams/2a96e9c6-1ad6-4392-aec7-bc1ca3ae6ee5/content

Sapper, N. E., Capli, A. G., & Legal, H. (2023). Propuesta de un plan de continuidad del negocio para el registro del dominiio de primer nivel de internet del Paraguay(NIC-PY). *Revista sobre estudios e investigaciones del saber académico, 17*(17), 7.

ANEXOS

Anexo 1: Protocolo de Investigación

Anexo 2 Controles y Políticas de seguridad

Introducción

Debido a la amenaza del ciberespacio, hay un aumento en la dependencia de sistemas prácticos y lógicos. Es una era decisiva para cada organización. El recurso vital, 'Información', puede verse comprometido debido a un ataque, un fallo técnico o un error humano. Este documento propone políticas de seguridad de la información y directrices administrativas para minimizar los riesgos identificados y preservar la confidencialidad, integridad y disponibilidad de la información.

La propuesta utiliza la información de los riesgos, donde la probabilidad, impacto y el riesgo son residuales, los niveles están organizados. A partir de esos resultados, se identifican qué son los restantes y qué políticas y controles de seguridad se reformulan, así como qué aspectos administrativos, organizacionales y técnicos se sugieren. Las políticas están diseñadas para guiar a cada institución de manera integral y coherente.

Controles de seguridad propuestos

Controles preventivos

Los controles preventivos (o controles proactivos) tienen como objetivo minimizar las posibilidades de que la amenaza se materialice, y los más relevantes de estos son:

- Uso de Autenticación Multifactor (MFA) para proteger puntos de acceso críticos y sensibles

- Implementación de cortafuegos y segmentación de red para restringir los movimientos laterales de un atacante
- Aplicación de políticas de Control de Acceso, Control de Acceso Basado en Roles (RBAC) para garantizar el acceso mínimo de los usuarios a datos sensibles y críticos para realizar funciones
- Refuerzo de la vigilancia física y por video en los Cajeros Automáticos (ATM) y cajas fuertes sensibles y críticas

Estos controles son efectivos para reducir las posibilidades de acceso no autorizado y violaciones físicas.

Controles correctivos

Estos son controles que se centran en la identificación de incidentes de seguridad en tiempo real con el fin de proporcionar mitigación oportuna:

- Uso de sistemas IDS/IPS y monitoreo centralizado a través de sistemas SIEM
- Auditorías programadas de configuraciones de cambios no autorizados
- Soluciones antimalware y sistemas de gestión de parches
- Monitoreo continuo de sistemas críticos como Finanzas Centrales y Web Transaccional.

Estos controles son efectivos para reducir el riesgo al aumentar las capacidades de detección y reacción ante la amenaza.

Controles detectivos

Los controles detectivos se centran en identificar incidentes de seguridad en tiempo real para permitir acciones de respuesta oportunas.

- Instalación de IDS/IPS y monitoreo central de SIEM.
- Auditorías de configuración regulares para descubrir cambios no autorizados.
- Implementación de soluciones anti-malware y políticas de gestión de parches.
- Monitoreo continuo de sistemas clave como el núcleo financiero y la web transaccional.

Estos controles proporcionan mayores capacidades de respuesta y recuperación que, a su vez, reducen el riesgo general.

Controles de mejora continua

La mejora continua asegura que la seguridad se mantenga a lo largo del tiempo.

- Sesiones de evaluación de riesgos enfocadas, p. ej., utilizando MAGERIT.
- Auditorías de cumplimiento de estándares internacionales (ISO/IEC 27002).
- Programas continuos para capacitar al personal.
- Revisión de políticas y procedimientos, incluyendo seguridad y protección de datos.

Estos ayudarán a la organización a abordar nuevos desafíos mientras aseguran un crecimiento sostenido.

Políticas de seguridad

Política de acceso y autenticación

Establece que todos los accesos a sistemas críticos deben estar protegidos con autenticación multifactor (MFA). Se aplicará el principio de privilegios mínimos, garantizando que cada usuario disponga únicamente de los permisos necesarios.

Política de seguridad física

Define controles para restringir el acceso a áreas críticas, incluyendo videovigilancia, cerraduras electrónicas y supervisión de visitantes. Su propósito es reducir el riesgo de sabotaje o acceso no autorizado a equipos sensibles.

Política de continuidad del negocio

Incluye la implementación de planes de continuidad (BCP) y recuperación ante desastres (DRP). Garantiza la disponibilidad de copias de seguridad cifradas y servidores redundantes para asegurar la reanudación rápida de operaciones.

Política de concienciación en seguridad

Dispone de programas de capacitación periódicos para empleados, con el fin de prevenir incidentes derivados de fraudes electrónicos, phishing o ingeniería social. La concienciación de los usuarios es clave para reducir los riesgos humanos**.**

Política de gestión de cambios

Regula la introducción de modificaciones en los sistemas críticos. Todo cambio deberá ser evaluado, aprobado y documentado formalmente, minimizando así errores de configuración o vulnerabilidades introducidas accidentalmente**.**

Conclusiones

La propuesta de controles y políticas de seguridad presentada constituye una herramienta esencial para fortalecer la postura de seguridad de la organización. Los controles preventivos, detectivos, correctivos y de mejora continua permiten reducir la probabilidad e impacto de incidentes, mientras que las políticas establecen lineamientos claros que garantizan la coherencia en la gestión de la seguridad.

Universidad Católica de Cuenca	AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Gloria Mercedes Guartacho Tenesaca portador(a) de la cédula de ciudadanía Nº 0302487624 En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación "Gestión de riesgos de los canales electrónicos de la Cooperativa Yuyay Ltda basado en normas y estándares internacionales" de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 6 de noviembre de 2025

F: .....
Gloria Mercedes Guartacho Tenesaca
C.I. 0302487624