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

PROPUESTA PARA LA IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE RIESGOS DE TI PARA LA COOPERATIVA YUYAY LTDA

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

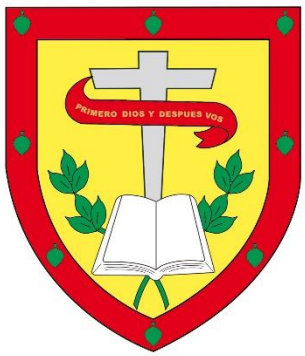
AUTORA: VERÓNICA JANETH YUPA CHIMBO

DIRECTOR: ING. JOSÉ ANTONIO CARRILLO ZENTENO.

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PROPUESTA PARA LA IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE RIESGOS DE TI PARA LA COOPERATIVA YUYAY LTDA

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

AUTORA: VERÓNICA JANETH YUPA CHIMBO

DIRECTOR: ING. JOSÉ ANTONIO CARRILLO ZENTENO.

CAÑAR - ECUADOR

2024

PATRIA, CULTURA Y DESARROLLO

DEDICATORIA

A Dios, porque ha estado conmigo en todo momento, guiándome y dándome fortaleza para continuar, y permitirme llegar hasta este ciclo de mi formación profesional.

A mi Madre quien, a lo largo de mi vida ha velado por mi bienestar y educación siendo un apoyo en todo momento, depositando su entera confianza en cada reto que se me ha presentado, sin dudar ni un solo momento de mi capacidad.

Por último, dedico a toda mi familia, por sus consejos, apoyo y compresión que me alertaron a lograr esta hermosa realidad.

AGRADECIMIENTO

“A MI MADRE”

Un agradecimiento especial a mi madre, mi amiga, mi confidente. Gracias por cada sacrificio que has hecho por mí, por ser mi guía en este camino, Por tus sabios consejos y por siempre estar presente en los momentos más importantes ya que este logro es más tuyo que mío.

A mis abuelos y tía por apoyarme de alguna u otra manera gracias por su cariño y apoyo incondicional y por siempre creer en mí.

“A MI TUTOR”

De manera especial al “ING. JOSE CARRILLO. Docente de la formación, director de mi trabajo de titulación por el tiempo asignado a mi persona, su gran apoyo y compresión y ser un guía para la formación de mi carrera, gracias por compartir sus conocimientos que han sido fundamentales para el éxito de esta investigación.

De la misma manera a todos los catedráticos de la Facultad de Sistemas, que, gracias a sus conocimientos y enseñanzas, su paciencia y su disposición para compartir sus conocimientos han sido fundamentales para mi formación académica.

CERTIFICACIÓN PREVIA REVISIÓN DE LECTORES

Cañar, 19 de septiembre del 2024

En mi calidad de director del Trabajo de Titulación: **"Propuesta para la Implementación de Sistemas de Gestión de Riesgos de TI para la Cooperativa Yuyay Ltda.",** elaborado por **Veronica Janeth Yupa Chimbo,** con Cl. **0350152534**, estudiante de la Carrera de Ingeniería en Sistemas en la Unidad Académica de Información, Ciencia de la Computación, e Innovación Tecnológica.

Certifico:

Que, el trabajo de Titulación esta apto para el proceso de revisión de los lectores dignados por Dirección de Carrera.

0103304531
JOSE ANTONIO
CARRILLO
ZENTENO

Firmado digitalmente por 0103304531 JOSE ANTONIO CARRILLO ZENTENO

Fecha: 2024.11.25

Ing. José Antonio Carrillo Zenteno, MSIG, MTI.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Veronica Janeth Yupa Chimbo portadora de la cédula de ciudadanía N^{O} **0350152534.**

Declaro ser el autor de la obra: **Propuesta para la Implementación de Sistemas de Gestión de Riesgos de TI para la Cooperativa Yuyay Ltda.**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas, Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto.

Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto,

Cañar, 22 de noviembre de 2024

Veronica Janeth Yupa Chimbo
C.I. 0350152534

INDICE

RESUMEN 11
ABSTRACT 12
INTRODUCCIÓN 13
CAPÍTULO I 15
1. Planteamiento del problema 15
1.1. Formulación del problema 16
1.2. Antecedentes de la Investigación 16
1.3. Justificación de la investigación 18
1.4. Objetivos 19
1.4.1. Objetivo General 19
1.4.2. Objetivos Específicos 19
1.5. Limitaciones 20
1.6. Delimitaciones 20
CAPÍTULO II 21
MARCO TEÓRICO 21
2.2. Gestión de riesgos 21
2.2.1. Vulnerabilidades, Amenazas y Riesgos Informáticos 21
2.2.2. Análisis de Impacto en el Negocio (BIA) 23
2.3. Sistema de Gestión de Riesgos 24
2.4. Metodologías de Evaluación de Riesgos Informáticos 24
2.4.1. COBIT 5 24
2.4.2. MAGERIT 26
2.4.3. MEHARI 27
2.4.4. ISO 27001 y Gestión de la Seguridad de la Información 29
2.4.5. ISO 31000 en la Gestión de Riesgos 29
2.7. Gestión de Incidentes de Seguridad de TI 30
2.7.1. Beneficios de la Gestión de Incidentes de Seguridad de TI 30
2.8. Controles Informáticos 30

2.9. Impacto Regulatorio en la Gestión de Riesgos de TI 32
2.9.1. Importancia del Impacto Regulatorio en Tecnologías de la Información 32
CAPÍTULO III 34
3.1. Enfoque de la investigación 34
3.3. Población y muestra 34
3.4. Técnicas e instrumentos de recolección 35
3.5. Tratamiento de la información 35
3.6. Resultados de la entrevista al jefe de TI 35
3.7. Análisis de la entrevista 36
CAPÍTULO IV 38
4.1. Título de la propuesta 38
4.3. Desarrollo de la propuesta 39
4.3.1. Fase 1: Establecimiento del contexto 39
4.3.2. FASE 2: Identificación de riesgos 41
Conclusiones 79
Recomendaciones 80
Bibliografía 81
ANEXOS 1

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Principios de COBIT 5. Fuente: (ISACA, 2012) 25
Ilustración 2. Estructura organizacional COAC. Yuyay Ltda. Fuente: Autoría Propia . 40

ÍNDICE DE TABLAS

Tabla 1. Identificación de activos. Fuente: Autoría Propia ---------- 42
Tabla 2. Identificación de Activos críticos. Fuente: Autoría Propia---------- 47
Tabla 3. Escala de probabilidad. Fuente: Autoría Propia ---------- 47
Tabla 4. Escala de impacto. Fuente: Autoría Propia ---------- 48
Tabla 5. Calificación de activos. Fuente: Autoría Propia.---------- 49
Tabla 6. Identificación de amenazas. Fuente: Autoría Propia ---------- 53
Tabla 7. Impacto/Probabilidad. Fuente: Autoría Propia---------- 60
Tabla 8. Escala de riesgos. Fuente: Autoría Propia ---------- 61
Tabla 9. Calificación del riesgo de los activos críticos. Fuente: Autoría Propia. -------- 61
Tabla 10. Controles. Fuente: Autoría Propia---------- 69
Tabla 11. Formación del equipo de trabajo. Fuente: Autoría Propia ---------- 73
Tabla 12. Cronograma del proyecto. Fuente: Autoría Propia---------- 74

RESUMEN

La presente tesis propone la implementación de Sistemas de Gestión de Riesgos de TI para la Cooperativa YUYAY Ltda., con el objetivo de fortalecer la seguridad de la información y asegurar la continuidad operativa de la cooperativa en un entorno cada vez más digitalizado. A través de un marco teórico sólido, se identifican los conceptos clave de la gestión de riesgos de TI, además se diagnostica el estado actual de los sistemas de información y la infraestructura tecnológica de la cooperativa. La metodología utilizada en esta investigación sigue un enfoque mixto, combinando tanto análisis cualitativo como cuantitativo. Se recopila información mediante entrevistas con el personal clave y se utilizan matrices de análisis de riesgos para evaluar las vulnerabilidades y amenazas que afectan a los activos críticos. Posteriormente, se diseñan estrategias de mitigación basadas en los principios de la norma ISO 31000, proponiendo controles de seguridad, planes de respuesta ante incidentes y recomendaciones para el monitoreo continuo de los riesgos. La tesis busca proporcionar una solución integral que permita a la cooperativa gestionar eficientemente sus riesgos tecnológicos, garantizando la protección de sus activos de información y manteniendo la alineación con sus objetivos estratégicos. Esto asegura la integridad, confidencialidad y disponibilidad de sus sistemas, fortaleciendo su capacidad para enfrentar incidentes de seguridad y salvaguardar su operación.

Palabras Clave: *activos, ISO 31000; gestión de riesgos, amenazas*

ABSTRACT

This thesis proposes the implementation of an IT Risk Management System in the YUYAY Ltda. savings and loan union to strengthen information security and ensure the operational continuity of the cooperative in an increasingly digitized environment. Through a solid theoretical framework, the critical concepts of IT risk management are identified, and the current state of the information systems and the technological infrastructure of the cooperative is also diagnosed. The methodology used in this research follows a mixed approach, combining both qualitative and quantitative analysis. Information is collected through key personnel interviews, and risk analysis matrices are used to assess vulnerabilities and threats affecting critical assets. Subsequently, mitigation strategies are designed based on the principles of the ISO 31000 standard, proposing security controls, incident response plans, and recommendations for continuous risk monitoring. The thesis aims to provide a comprehensive solution that allows the cooperative to efficiently manage its technological risks, guaranteeing the protection of its information assets and maintaining alignment with its strategic objectives. It ensures the integrity, confidentiality, and availability of the systems, strengthening the ability to face security incidents and safeguard the operation.

Keywords: assets, ISO 31000, risk management, threats

INTRODUCCIÓN

En un entorno cada vez más dependiente de la tecnología, las organizaciones enfrentan desafíos significativos relacionados con la seguridad y la gestión de riesgos en sus sistemas de TI. Las cooperativas, como la Cooperativa Yuyay Ltda., no son ajenas a esta problemática, ya que manejan información crítica y recursos tecnológicos que, si no son protegidos adecuadamente, pueden comprometer sus operaciones y la confianza de sus socios. La gestión de riesgos de TI, bajo estándares reconocidos como ISO 31000, se convierte en una herramienta indispensable para garantizar la seguridad, continuidad y resiliencia de sus procesos.

Actualmente, la Cooperativa Yuyay Ltda. no cuenta con un sistema formalizado para identificar, analizar y mitigar riesgos en sus sistemas de TI, lo que expone a la organización a posibles incidentes que podrían afectar tanto su desempeño operativo como su reputación. Ante esta necesidad, el presente trabajo tiene como objetivo desarrollar una propuesta integral de gestión de riesgos basada en la norma ISO 31000, adaptada a las características y necesidades de la cooperativa.

El presente trabajo de titulación se estructura de la siguiente manera:

Capítulo I: Se expone la problemática de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda., analizando la situación actual y justificando la necesidad de un sistema formalizado de gestión de riesgos. Se incluyen los antecedentes, los objetivos generales y específicos, y las delimitaciones del estudio, estableciendo el marco dentro del cual se desarrollará la investigación.

Capítulo II: Se detalla el marco teórico que abarca los conceptos fundamentales de la gestión de riesgos de TI, incluyendo metodologías como ISO 31000, COBIT y

MAGERIT. Este capítulo proporciona la base conceptual necesaria para entender los riesgos y la implementación de controles en un entorno cooperativo.

Capítulo III: Presenta el marco metodológico utilizado, describiendo la metodología descriptiva y evaluativa aplicada. Se incluye el proceso de recolección de datos a través de encuestas y análisis, lo que sustenta el diagnóstico de los riesgos actuales en los sistemas de TI de la cooperativa.

Capítulo IV: Desarrolla la propuesta de implementación de sistemas de gestión de riesgos de TI para la Cooperativa Yuyay Ltda. bajo la norma ISO 31000. Se incluyen estrategias de mitigación, planes de respuesta a incidentes, y recomendaciones para el monitoreo continuo. Además, se describen las fases de implementación y se priorizan los activos críticos para garantizar la seguridad y resiliencia operativa de la cooperativa.

CAPÍTULO I

1. Planteamiento del problema

En la era digital actual, la dependencia de las tecnologías de la información (TI) es crucial para la operación y el crecimiento sostenible de las organizaciones. Sin embargo, esta dependencia también expone a las organizaciones a una variedad de riesgos inherentes que pueden comprometer la seguridad, la eficiencia y la integridad de sus operaciones. En el caso de la Cooperativa Yuyay Ltda., una entidad que desempeña un papel vital en el desarrollo económico y social del cantón Cañar, la gestión de riesgos de TI no ha sido completamente formalizada ni estructurada. Esto representa una vulnerabilidad significativa, especialmente en un contexto donde las amenazas cibernéticas y los fallos tecnológicos están en aumento.

Actualmente, la cooperativa enfrenta desafíos significativos relacionados con la seguridad de la información, la continuidad del negocio y la conformidad con regulaciones nacionales e internacionales. La falta de un sistema formal de gestión de riesgos de TI impide que la cooperativa identifique, evalúe y mitigue adecuadamente los riesgos potenciales, lo que podría resultar en interrupciones operativas, pérdidas financieras, o daños a su reputación.

La necesidad de implementar un sistema de gestión de riesgos de TI en la Cooperativa Yuyay Ltda. es evidente, y la ausencia de dicho sistema plantea preguntas críticas sobre la capacidad de la cooperativa para manejar efectivamente los riesgos tecnológicos en un entorno cada vez más digitalizado y regulado. Por lo tanto, esta tesis buscará desarrollar una propuesta para la implementación de un sistema de gestión de riesgos de TI que sea

robusto, escalable y adaptado a las necesidades específicas de la cooperativa, asegurando así la resiliencia y la sostenibilidad de sus operaciones en el futuro.

1.1.**Formulación del problema**

En la actualidad, la Cooperativa Yuyay Ltda. enfrenta desafíos significativos relacionados con la gestión de riesgos de tecnologías de la información (TI), que pueden impactar su operatividad y seguridad. A pesar de la creciente dependencia de las soluciones tecnológicas para sus operaciones diarias, no existe un sistema formal y estructurado que permita identificar, evaluar y gestionar eficazmente los riesgos asociados a la TI. Esta falta de un sistema de gestión de riesgos integral puede exponer a la cooperativa a vulnerabilidades y amenazas que podrían comprometer la integridad de la información, la continuidad del negocio y la confianza de los socios y clientes.

- ¿Cómo se puede diseñar e implementar un sistema de gestión de riesgo de TI en la Cooperativa Yuyay Ltda. que permita identificar, evaluar y mitigar eficazmente los riesgos tecnológicos, mejorando así la seguridad y la resiliencia operacional de la organización?

1.2.**Antecedentes de la Investigación**

En el año (2022) en el trabajo de titulación, realiza una investigación sobre los riesgos operativos en la cooperativa de Ahorro y crédito CACEC Ltda., a través de un modelo computacional para evaluar la gestión de riesgos de TI COBIT en los cuales se a utilizado técnicas de DM mediante la implementación de una herramienta llamada weka. Además, ayuda a que mediante la tecnología se proteja la información con la que cuenta las entidades bancarias y disminuye los factores de riego.

Este estudio anterior demostró cómo la tecnología puede ser utilizada eficazmente para proteger la información en entidades bancarias y reducir los factores de riesgo asociados. La adaptación y aplicación de enfoques similares en Yuyay Ltda. no solo pueden mejorar la seguridad y eficacia de sus sistemas de información, sino también ofrecer una estrategia probada para la mitigación de riesgos, capitalizando en la experiencia y resultados obtenidos en CACEC Ltda.

Santolla (2022) afirma que la investigación reveló una deficiencia en la gestión de los procedimientos tecnológicos, los cuales carecen de una metodología efectiva para una

gestión adecuada de TI. Esta falta de metodología obstaculiza la optimización de los recursos tecnológicos disponibles para los usuarios. Por lo tanto, se propone la aplicación de la metodología COBIT como solución para mejorar estos procedimientos y garantizar un control de las buenas prácticas en TI.

El estudio de Santolla destaca la importancia de adoptar un marco estructurado y probado como COBIT, que no solo optimiza los recursos tecnológicos mediante una gestión efectiva, sino que también mejora la gobernanza de TI y el control de riesgos. Para la Cooperativa Yuyay Ltda., la adopción de COBIT puede proporcionar un enfoque sistemático para identificar, evaluar y mitigar riesgos de TI, garantizando que los procedimientos tecnológicos sean manejados con las mejores prácticas y de acuerdo a estándares internacionales.

Zapata (2021) resalta la importancia estratégica de gestionar los riesgos de TI y la continuidad de los procesos del negocio para asegurar la efectividad y eficacia de los sistemas de gestión de la seguridad de la información. Se argumenta que la falta de estas herramientas en entidades financieras locales justifica la realización del trabajo de tesis. La investigación evidencia que la implementación de un modelo de gestión de riesgos, basado en estándares como ISO/IEC 27001 e ISO 17799 y la metodología MAGERIT, puede mejorar la evaluación y tratamiento de los riesgos de los activos de TI, cumpliendo con los requisitos de la SBS. Se tomó como estudio de caso la Agencia Metro Santa Elena del Banco Scotiabank en Chiclayo. Analizando los riesgos de TI que puede tener el sector financiero demostrando que tan eficiente es la seguridad TI.

Este documento es una herramienta valiosa para comprender la metodología MAGERIT y aplicarla al desarrollo de un SGIT para la Cooperativa Yuyay Ltda.

Barbosa (2020) manifiesta en su estudio la búsqueda de desarrollar un recurso que simplifique la adopción de un Modelo de ciberseguridad en consonancia con los marcos de gestión y gobierno de Tecnologías de la Información (TI), con el propósito de mejorar las deficiencias presentes en los sistemas de seguridad de la información de las instituciones financieras. Esto se realizará en cumplimiento de las regulaciones vigentes, con la intención de ser evaluado más adelante en el Banco Serfinanza ubicado en la ciudad de Barranquilla.

Este estudio aborda las deficiencias en los sistemas de seguridad de la información en instituciones financieras y propone una solución que no solo mejora estas deficiencias, sino que también cumple con las regulaciones vigentes. La aplicación de un modelo similar en la Cooperativa Yuyay Ltda. podría proporcionar una estructura robusta para fortalecer la seguridad de la información, alinear las prácticas de TI con los marcos de gestión reconocidos y garantizar el cumplimiento normativo.

Moncada en el año (2018) en su trabajo de investigación, tuvo como objetivo preparar a la cooperativa de ahorro y crédito ABC para una gestión efectiva de riesgos y para cumplir con los requisitos regulatorios de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS). En primer lugar, la implementación de un sistema de gestión permitirá mejoras en la seguridad de la información, lo que beneficiará a todas las cooperativas de crédito y ahorro al mejorar el manejo de los procesos de negocio. En segundo lugar, la gestión efectiva de riesgos puede conducir a una reducción de costos mediante la optimización de recursos y un tratamiento adecuado de los riesgos. Finalmente, al mejorar la eficacia y reducir los costos, las cooperativas pueden generar beneficios adicionales en términos de marketing, lo que les permitirá diferenciarse en el mercado y fortalecer las relaciones con los clientes y proveedores.

En base a que este documento proporciona ejemplos de controles de seguridad que se utilizan para la protección de los activos de TI de la cooperativa; servirá como una guía para establecer el sistema de gestión de riesgos de TI a través de las buenas prácticas

1.3.**Justificación de la investigación**

La gestión eficiente de los riesgos de Tecnologías de la Información (TI) es crucial para la sostenibilidad y el crecimiento estratégico de cualquier organización en el contexto actual, donde la tecnología desempeña un papel central en todas las actividades empresariales. En el caso de la Cooperativa Yuyay Ltda., una entidad clave en el desarrollo económico y social del cantón Cañar, la adopción de un sistema formalizado de gestión de riesgos de TI no es solo una necesidad operativa, sino también una estrategia crítica para su evolución y protección en el ambiente digital.

Implementar un sistema de gestión de riesgos de TI robusto ayudará a la cooperativa a protegerse contra las vulnerabilidades de seguridad cibernética y los fallos tecnológicos, asegurando la integridad, disponibilidad y confidencialidad de la información crítica. Esto

es fundamental para mantener la continuidad de las operaciones y minimizar el impacto financiero y operativo de cualquier incidente de seguridad. A medida que aumentan las regulaciones sobre protección de datos y seguridad cibernética, la Cooperativa Yuyay Ltda. debe asegurarse de cumplir con estos requerimientos legales. La implementación de un sistema de gestión de riesgos de TI no solo ayudará a cumplir con estas normativas, sino que también mejorará la reputación de la cooperativa como una entidad segura y confiable, esencial para atraer y retener a los socios y clientes.

Al establecer un entorno de TI seguro y gestionado, la Cooperativa Yuyay Ltda. estará mejor equipada para adoptar nuevas tecnologías que pueden ofrecer ventajas competitivas, como mejoras en la eficiencia operativa, nuevas capacidades de servicio al cliente y expansión a nuevos mercados. Este enfoque proactivo en la gestión de riesgos de TI también fomenta una cultura de innovación y mejora continua. En resumen, la propuesta para implementar un sistema de gestión de riesgos de TI en la Cooperativa Yuyay Ltda. es esencial no solo para la protección contra riesgos y amenazas actuales, sino también para asegurar un crecimiento estratégico y sostenible en el futuro. Esta inversión en la gestión de riesgos de TI es, por lo tanto, una decisión estratégica que fortalecerá la posición de la cooperativa en un mercado cada vez más tecnológico y regulado.

1.4. **Objetivos**

1.4.1. **Objetivo General**

Desarrollar una propuesta para la implementación de un sistema de gestión de riesgos de TI que permita a la Cooperativa Yuyay Ltda.

1.4.2. **Objetivos Específicos**

- Elaborar un marco teórico que describa los conceptos fundamentales y las metodologías existentes sobre la gestión de riesgos de TI.
- Diagnosticar el estado actual de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda. mediante una evaluación detallada de sus sistemas de información y tecnologías empleadas.
- Diseñar una propuesta detallada para la implementación de un sistema de gestión de riesgos de TI que incluya estrategias de mitigación, planes de respuesta a incidentes y recomendaciones para el monitoreo continuo.

1.5. **Limitaciones**

- La disponibilidad limitada de recursos financieros, técnicos y humanos puede restringir la profundidad y amplitud de la implementación y evaluación del sistema propuesto.
- Falta de colaboración por parte de los empleados de la cooperativa.
- Tiempo limitado de 3 meses para la elaboración del presente trabajo de investigación.

1.6. **Delimitaciones**

- La investigación se centrará exclusivamente en la Cooperativa Yuyay Ltda., ubicada en el cantón Cañar.
- El estudio se limitará a los sistemas de información y tecnologías actualmente en uso en la Cooperativa. No se explorarán tecnologías emergentes o sistemas no implementados en la cooperativa.
- La implementación y evaluación del sistema de gestión de riesgo se delimitará a un período de tiempo específico durante la fase de investigación, sin incluir un seguimiento a largo plazo.
- La investigación involucrará a los empleados y gestores de TI de la cooperativa, excluyendo a otras partes interesadas como clientes.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. La seguridad de la información es importante para todas las organizaciones, independientemente de su tamaño o industria. Sin embargo, es especialmente importante para las organizaciones que manejan datos sensibles, como datos financieros o de salud (Rodríguez, Fernández, & Santos, 2023).

2.2. Gestión de riesgos

La gestión de riesgos es un proceso general que se aplica en diversas áreas de una organización, no solo en TI. Involucra la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos potenciales que podrían afectar a la organización. La gestión de riesgos tiene como objetivo minimizar los efectos negativos de los riesgos en los objetivos de la organización y maximizar las oportunidades. Se basa en principios universales aplicables a cualquier tipo de riesgo, incluyendo, pero no limitándose a riesgos financieros, operacionales, de reputación, legales, y de seguridad de la información (Grishaeva & Borzov, 2020).

2.2.1. Vulnerabilidades, Amenazas y Riesgos Informáticos

2.2.1.1. Vulnerabilidades de TI

Una vulnerabilidad en (TI) se refiere a una debilidad en un sistema, software, hardware o proceso que puede ser explotada por una amenaza para causar daño o interrumpir el funcionamiento normal. Estas vulnerabilidades pueden surgir de diversos orígenes, como errores de software, configuraciones inadecuadas, actualizaciones incompletas o políticas de seguridad deficientes (Dand & Chudasama, 2021).

La identificación de vulnerabilidades es crítica porque permiten a los atacantes obtener acceso no autorizado, robar datos, instalar malware o interrumpir servicios. Ejemplos comunes incluyen fallos en la encriptación, deficiencias en los protocolos de autenticación, o errores de programación que permiten inyecciones de SQL o ataques de cross-site scripting (XSS).

La gestión de estas vulnerabilidades implica su detección mediante herramientas de escaneo de vulnerabilidades, la evaluación de su criticidad, y la implementación de

parches o remedios. Este proceso es un componente esencial de la gestión de riesgos de TI, ya que reduce significativamente la probabilidad de incidentes de seguridad y fortalece la postura de seguridad de la organización (Riggs, y otros, 2023).

2.2.1.2. Amenazas de TI

De acuerdo con Mata (2023):

> "Las amenazas de TI representan cualquier potencial de daño que pueda explotar una vulnerabilidad en el sistema de información de una organización. Estas amenazas pueden ser internas o externas, intencionadas o accidentales, y varían ampliamente en su naturaleza y origen".

Las amenazas intencionadas incluyen actores maliciosos como hackers, grupos de ciberdelincuencia, y ataques patrocinados por estados que buscan robar información, interrumpir operaciones o comprometer infraestructuras críticas. Por otro lado, las amenazas accidentales pueden incluir errores humanos, fallos de software o hardware, y desastres naturales que también ponen en riesgo la integridad, disponibilidad y confidencialidad de los sistemas de información (Payá Santos & Luque Juárez, 2021).

Identificar y clasificar las amenazas es fundamental para desarrollar estrategias efectivas de mitigación y respuesta. Esto incluye la realización de evaluaciones de riesgos, el establecimiento de sistemas de alerta temprana, y la implementación de políticas de seguridad rigurosas. Comprender el panorama de amenazas permite a las organizaciones prepararse mejor contra ataques potenciales y gestionar de manera proactiva sus defensas de seguridad (Moya, 2023).

2.2.1.3. Riesgos de TI

El riesgo de TI se refiere a la combinación de la probabilidad de que ocurra un evento dañino y el impacto que dicho evento tendría en la organización. Este riesgo surge cuando las amenazas encuentran vulnerabilidades sin las salvaguardas adecuadas, llevando a potenciales pérdidas o daños (Velthuis, 2008).

La gestión de riesgos de TI implica procesos sistemáticos para identificar, evaluar, y tratar riesgos para asegurar que permanezcan dentro de un nivel aceptable. Esto incluye el desarrollo de un plan de manejo de riesgos que detalla cómo se deben abordar los riesgos identificados a través de la mitigación, transferencia, aceptación o evitación (Ismagilova, Laurie Hughes, & Dwivedi, 2020).

Una parte crucial de la gestión de riesgos es su evaluación, que determina la severidad y la probabilidad de riesgos basándose en el análisis de las vulnerabilidades existentes y las amenazas potenciales. Los resultados de estas evaluaciones ayudan a priorizar las respuestas y a asignar recursos de manera efectiva, asegurando que los riesgos más críticos sean tratados con la urgencia que requieren. El objetivo final es minimizar el impacto negativo en las operaciones de la organización y proteger los activos de información de manera efectiva.

2.2.2. Análisis de Impacto en el Negocio (BIA)

De acuerdo con Liendo (2023), el Análisis de Impacto en el Negocio (BIA, por sus siglas en inglés) es una herramienta fundamental dentro del marco de la gestión de riesgos y la continuidad del negocio. El objetivo principal del BIA es identificar y evaluar los efectos potenciales que una interrupción en las operaciones puede tener sobre las actividades críticas del negocio. Este análisis permite a las organizaciones priorizar los procesos y recursos que deben ser restaurados rápidamente para minimizar el impacto de un incidente y garantizar la resiliencia operativa.

Entre los objetivos del BIA se encuentran:

- **Identificar Procesos Críticos**: Determinar qué procesos son esenciales para las operaciones diarias y el cumplimiento de los objetivos estratégicos de la organización.
- **Evaluar Impactos**: Analizar el impacto financiero, operativo, legal, y reputacional que podría resultar de la interrupción de estos procesos.
- **Establecer Prioridades de Recuperación**: Priorizar los procesos y recursos en función de su criticidad y el tiempo máximo tolerable de inactividad (MTD).
- **Determinar Requisitos de Recuperación**: Identificar los recursos necesarios, tales como personal, tecnología, datos e infraestructura, para restaurar las operaciones críticas en el menor tiempo posible.

Por ello, el Análisis de Impacto en el Negocio es una herramienta esencial para la gestión de riesgos de TI y la comunidad operativa, permitiendo a las empresas prepararse y responder de forma efectiva ante interrupciones, garantizando que los procesos críticos se mantengan funcionando y que los impactos de minimicen (pág. 26).

2.3. Sistema de Gestión de Riesgos

Un sistema de gestión de riesgos de TI es un conjunto de políticas, procedimientos y prácticas integradas destinadas a identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos de TI dentro de una organización. Este sistema ayuda a tomar decisiones informadas sobre cómo 'tratar' los riesgos identificados, ya sea a través de la mitigación, la transferencia, la aceptación o la evasión (Avila Irigoin & Caloggero Sangama, 2022).

Es considerado también como un marco específicamente diseñado para manejar los riesgos asociados con la tecnología de la información.

2.4. Metodologías de Evaluación de Riesgos Informáticos

Para la elaboración de una gestión de riesgos de TI, existen diversas metodologías que permiten seguir pasos determinados con el fin de lograr mitigar los riesgos de un activo informático.

2.4.1. COBIT 5

COBIT es un marco de referencia para la gestión y la gobernanza de las tecnologías de la información (TI), desarrollado por ISACA (Information Systems Audit and Control Association) (ISACA, 2012). COBIT proporciona un enfoque integral para la gobernanza y gestión de TI en las organizaciones, ofreciendo prácticas, herramientas analíticas, y modelos de madurez que pueden ser utilizados para aumentar la eficiencia y efectividad de las operaciones de TI. COBIT 5, una de las versiones más recientes, presenta varios componentes claves (ISACA, 2013).

4.4.1.1. Principios de COBIT 5

COBIT 5 se basa en cinco principios fundamentales para la gobernanza y gestión de TI empresarial:

1. **Satisfacer las necesidades de las partes interesadas**: COBIT 5 ayuda a las organizaciones a alinear sus objetivos de TI con las necesidades del negocio, asegurando que la tecnología aporte valor a la empresa.
2. **Cubrir la empresa de extremo a extremo**: Integra todos los procesos y aspectos de la organización, asegurando una cobertura completa de la empresa, desde el nivel ejecutivo hasta las operaciones.

3. **Aplicar un marco único integrado**: COBIT 5 se alinea y puede integrarse con otros estándares y buenas prácticas, como ITIL, ISO 27001, y más, proporcionando un enfoque consolidado para la gobernanza y gestión de TI.
4. **Habilitar un enfoque holístico**: El marco identifica y conecta los recursos y las capacidades de TI necesarias para garantizar que la tecnología funcione de manera eficiente y efectiva.
5. **Separar la gobernanza de la gestión**: Distingue claramente entre las responsabilidades de gobernanza y las funciones de gestión para asegurar la claridad y eficiencia en las operaciones (ISACA, 2012).

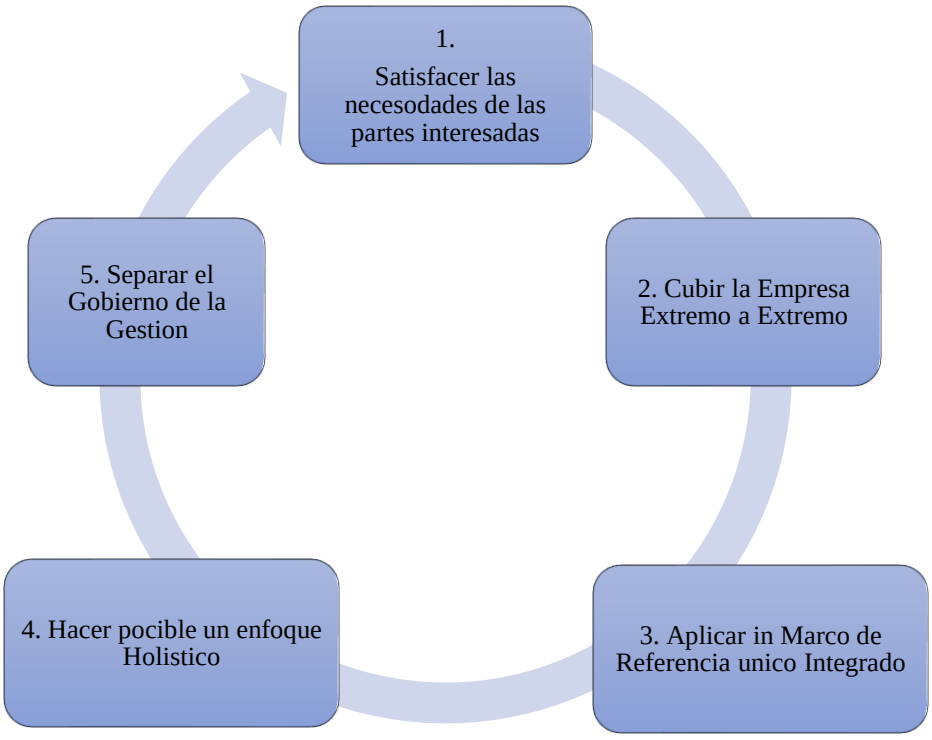


Ilustración 1. Principios de COBIT 5. Fuente: (ISACA, 2012)

Componentes de COBIT 5

COBIT 5 incluye varios componentes que ayudan en la implementación y mantenimiento de una gobernanza efectiva de TI:

- **Objetivos de control**: Proporciona prácticas específicas y actividades para lograr los objetivos de control relacionados con la calidad, la seguridad y el control de las informaciones y los sistemas de TI.

- **Habilitadores**: Identifica diferentes recursos como políticas, procesos, estructuras organizativas, y tecnologías que ayudan a alcanzar los objetivos de gobernanza y gestión.
- **Modelo de Madurez**: Ofrece un camino para la mejora continua, permitiendo a las organizaciones desarrollar capacidades en etapas hacia niveles más altos de madurez.
- **Mapas de Ruta de Implementación**: Guías y herramientas para ayudar en la implementación efectiva de las prácticas de gobernanza de TI (ISACA, 2012).

2.4.2. MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica de España. Es una herramienta oficialmente reconocida y utilizada ampliamente por las administraciones públicas en España para la gestión de riesgos en los sistemas de información, aunque también es aplicable a entornos empresariales privados. El objetivo principal de MAGERIT es identificar, analizar y gestionar los riesgos relacionados con la información y las tecnologías de información, garantizando la protección adecuada de los activos (Montalbán, Gómez, & Borré, 2020).

Esta metodología destaca por su MAGERIT destaca por su flexibilidad y adaptabilidad a diferentes tipos de organizaciones y necesidades. Está diseñada para ser independiente de tecnologías específicas y proporciona un marco sistemático para entender los riesgos, evaluar su impacto y probabilidad, y determinar las medidas de control más adecuadas para mitigarlos (Avila-Torres & Tapia, 2021).

2.4.2.1. Proceso de MAGERIT

El proceso de gestión de riesgos de MAGERIT se estructura en varias fases:

1. **Inicio**: Definición del alcance del análisis, los sistemas involucrados, y los recursos disponibles. Se establecen los objetivos y se identifican las restricciones y requisitos.
2. **Identificación de Activos**: Catalogación de los activos de información que necesitan protección, incluyendo datos, procesos y sistemas que son críticos para la organización.

3. **Evaluación de Riesgos**:
    - **Identificación de Amenazas**: Determinación de las diferentes amenazas que pueden afectar a cada uno de los activos.
    - **Identificación de Vulnerabilidades**: Análisis de las debilidades que podrían ser explotadas por las amenazas para comprometer los activos.
    - **Estimación del Riesgo**: Evaluación de la potencialidad de que una amenaza explote una vulnerabilidad y cause un daño.
4. **Análisis de Riesgos**: Este análisis detalla el impacto y la probabilidad de los riesgos identificados, proporcionando una base para la priorización de los mismos.
5. **Gestión de Riesgos**:
    - **Planificación de Tratamiento**: Definición de las estrategias y medidas para tratar los riesgos identificados.
    - **Implementación de Controles**: Aplicación de las medidas decididas para reducir, transferir o aceptar los riesgos.
6. **Mantenimiento y Revisión**: Monitorización continua de los riesgos y revisión de las estrategias de gestión para asegurar que sigan siendo efectivas ante cambios en el entorno o en la organización (Gobierno de España, 2012).

2.4.3. MEHARI

Es una metodología de análisis y gestión de riesgos de seguridad de la información, desarrollada y mantenida por el CLUSIF (Club de la Sécurité de l'Information Français). Esta metodología es reconocida principalmente en el ámbito francófono, pero es aplicable a nivel internacional. MEHARI ofrece un marco comprensivo para la evaluación de los riesgos asociados a la información y las tecnologías de la información (TI), y para el desarrollo de estrategias adecuadas de gestión de estos riesgos. Se caracteriza por su enfoque estructurado y detallado para identificar, analizar, evaluar y gestionar los riesgos de seguridad de la información. Está diseñada para ser adaptable a cualquier tipo de organización y para integrarse fácilmente con otros estándares y frameworks, como ISO/IEC 27001, ITIL, o COBIT (CLUSIF, 2010).

2.4.3.1. Proceso de MEHARI

El proceso de gestión de riesgos según MEHARI se organiza en varias etapas clave:

1. **Preparación y Contexto**:
    - **Definición de alcance**: Establecer los límites y la profundidad del análisis de riesgos.
    - **Comprensión del contexto organizacional**: Analizar el contexto operativo, legal y de negocio en el que se sitúa la gestión de riesgos.
2. **Evaluación de Riesgos**:
    - **Identificación de activos de información**: Determinar qué recursos de información necesitan protección.
    - **Evaluación de amenazas y vulnerabilidades**: Identificar amenazas potenciales y vulnerabilidades que puedan afectar a estos activos.
    - **Análisis del impacto de los riesgos**: Determinar el impacto potencial que tendrían los incidentes de seguridad sobre la organización.
    - **Estimación del nivel de riesgo**: Calcular la probabilidad y el impacto de los distintos escenarios de riesgo.
3. **Gestión de Riesgos**:
    - **Decisión sobre el tratamiento de riesgos**: Optar por mitigar, transferir, evitar o aceptar los riesgos, basándose en los criterios de aceptación de la organización.
    - **Planificación e implementación de controles**: Desarrollar e implementar las medidas de seguridad necesarias para tratar los riesgos identificados.
4. **Monitoreo y Revisión**:
    - **Revisión periódica y monitoreo de los riesgos**: Evaluar la efectividad de las medidas de tratamiento y hacer ajustes cuando sea necesario.
    - **Auditoría y actualización del análisis de riesgos**: Realizar auditorías de seguridad regulares y actualizar el análisis de riesgos conforme cambien las amenazas o el negocio (ENISA, 2024).

2.4.4. ISO 27001 y Gestión de la Seguridad de la Información

ISO 27001 es una norma internacional establecida por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), dedicada a la gestión de seguridad de la información. Este estándar forma parte de la familia de normas ISO/IEC 27000 y es reconocido mundialmente como un referente en la implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información (SGSI) (ISO / IEC, 2022).

Esta norma proporciona un marco sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. La norma utiliza un enfoque basado en el riesgo para asegurar que la seguridad de la información sea integral y conforme a las necesidades de la información y los procesos de la organización. En cuanto a la evaluación de riesgos, uno de los elementos centrales de la ISO 27001, es la obligatoriedad de realizar evaluaciones de riesgos de seguridad de la información, en donde la organización debería identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, y debe determinar las amenazas y los riesgos (Colegio Oficial de Ingenieros de Telecomunicación, 2016).

Según Yungán & Narváez (2022), la norma ISO 27001 enfatiza la importancia de un enfoque de mejora continua basado en el ciclo Plan-Do-Check-Act (PDCA). Este ciclo permite a las organizaciones ser proactivas en lugar de simplemente reactivas, fortaleciendo los controles de seguridad con el tiempo y adaptándose a los cambios en el entorno de seguridad.

2.4.5. ISO 31000 en la Gestión de Riesgos

ISO 31000 es una norma internacional publicada por la Organización Internacional de Normalización (ISO), que proporciona principios y directrices sobre la gestión de riesgos. Diseñada para ser utilizada por cualquier organización independientemente de su tamaño, sector o ubicación geográfica, ISO 31000 ayuda a estas a identificar, analizar, evaluar, tratar y monitorear los riesgos que podrían impactar sus operaciones, objetivos y proyectos. A diferencia de ISO 27001, que se centra específicamente en la seguridad de la información, ISO 31000 aborda la gestión de riesgos en un contexto más amplio (Harefa & Hartomo, 2022).

2.7. Gestión de Incidentes de Seguridad de TI

La gestión de incidentes de seguridad de TI es un proceso crítico diseñado para identificar, manejar, registrar y analizar amenazas o vulnerabilidades de seguridad que pueden causar incidentes en las tecnologías de la información. Este proceso es esencial para proteger los activos de información y mantener la continuidad del negocio. Se centra en la preparación, detección rápida de los incidentes, respuesta efectiva y, finalmente, la recuperación de la funcionalidad normal de los sistemas (Marín Hernández, 2021).

2.7.1. Beneficios de la Gestión de Incidentes de Seguridad de TI

- **Minimización de Interrupciones**: Una gestión efectiva de incidentes ayuda a reducir el tiempo de inactividad de los sistemas, asegurando que las operaciones críticas de negocio puedan continuar con la menor interrupción posible.
- **Reducción de Daños**: Una respuesta rápida y eficaz puede limitar significativamente los daños causados por incidentes de seguridad, protegiendo tanto los activos de información como la reputación de la organización.
- **Cumplimiento Regulatorio**: Muchas normativas de seguridad de datos requieren un proceso formal de gestión de incidentes. La capacidad de responder adecuadamente a incidentes es a menudo un requisito para cumplir con estas regulaciones.
- **Mejora de la Seguridad**: El análisis de incidentes proporciona información valiosa que puede usarse para fortalecer las medidas de seguridad y prevenir futuros incidentes (Iparraguirre-Villanueva, Obregon-Palomino, Pujay-Iglesias, & Cabanillas-Carbonell, 2023).

Implementar un enfoque estructurado para la gestión de incidentes de seguridad de TI es crucial para cualquier organización que dependa de la tecnología para sus operaciones diarias. Esto no sólo protege los recursos de información, sino que también fortalece la postura general de seguridad de la organización (Linares Vasquez, 2023).

2.8. Controles Informáticos

Los controles informáticos son herramientas y técnicas diseñadas para asegurar la integridad, confidencialidad y disponibilidad de los datos. Estas tecnologías son cruciales en un entorno de seguridad de la información moderno, dado que los datos son uno de los activos más valiosos que una organización posee (Aguirre Sánchez, 2021).

1. Cifrado

El cifrado es una de las medidas de seguridad más efectivas y esenciales. Consiste en convertir datos de un formato legible a un formato codificado que solo puede ser leído o procesado después de ser descifrado. El cifrado se puede aplicar tanto a datos en reposo como a datos en tránsito (Mamami, Ancco, & Argollo, 2023).

2. Control de Acceso

Los controles de acceso son medidas que se utilizan para asegurar que solo las personas autorizadas tengan acceso a recursos digitales específicos. (Mamami, Ancco, & Argollo, 2023)

3. Gestión de Claves

La gestión de claves es el proceso de manejar claves criptográficas de una organización. Incluye la generación, distribución, almacenamiento, uso, rotación y revocación de claves. Es esencial para la seguridad del cifrado, ya que asegura que las claves utilizadas para cifrar y descifrar datos sean manejadas de manera segura y eficaz (Mamami, Ancco, & Argollo, 2023).

4. Firewalls

Los firewalls son dispositivos de seguridad que monitorizan y controlan el tráfico entrante y saliente basado en reglas de seguridad predeterminadas. Son una primera línea de defensa en la seguridad de la red que puede ayudar a prevenir accesos no autorizados a o desde una red privada (Ramírez Loría, 2021).

5. Detección y Prevención de Intrusiones (IDS/IPS)

- **IDS (Sistema de Detección de Intrusiones)**: Monitoriza el tráfico de la red para detectar actividades sospechosas que podrían indicar un intento de compromiso (Kumar, Abhishek, Ghalib, & Shankar, 2022).
- **IPS (Sistema de Prevención de Intrusiones)**: Actúa sobre los incidentes detectados por el IDS, bloqueando el tráfico y previniendo posibles ataques (Möller, 2023).

6. Backup y Recuperación

Las estrategias de backup y recuperación son fundamentales para la protección de datos, asegurando que los datos importantes puedan ser restaurados en caso de pérdida de datos por desastres, errores técnicos o ataques cibernéticos (Hernández Benítez, 2021).

7. Gestión de Vulnerabilidades

Esta tecnología implica la identificación, clasificación, remediación y mitigación de vulnerabilidades en el software o hardware que podría ser explotado por los atacantes (Syed, 2020).

8. Protección contra Malware

Incluye software como antivirus y anti-malware que ayuda a proteger las computadoras y redes detectando, previniendo y eliminando software malicioso.

Cada una de estas tecnologías juega un papel crítico en la estrategia de protección de datos de una organización, y a menudo, su uso combinado es necesario para lograr una postura de seguridad robusta (Alsmadi & Alqudah, 2021).

2.9. Impacto Regulatorio en la Gestión de Riesgos de TI

El impacto regulatorio en la gestión de riesgos de TI es una dimensión crítica que toda organización debe considerar cuidadosamente. La conformidad con regulaciones relevantes no solo es fundamental para evitar penalizaciones legales y financieras, sino también esencial para mantener la confianza de clientes, socios y otras partes interesadas. Este cumplimiento involucra adaptar las prácticas de gestión de riesgos de TI para satisfacer los requerimientos legales, normativos y contractuales específicos que afectan a la organización (ARCOTEL, 2023).

2.9.1. Importancia del Impacto Regulatorio en Tecnologías de la Información

- **Cumplimiento Normativo**: En Ecuador, existen varias leyes y regulaciones que exigen que las organizaciones gestionen activamente los riesgos asociados con la

información y las tecnologías de la información. Algunas de las normativas más relevantes incluyen:

- **Ley Orgánica de Protección de Datos Personales (LOPDP)**: Establece los principios, derechos y obligaciones relacionados con la protección de datos personales y requiere que las organizaciones implementen medidas de seguridad adecuadas para proteger dichos datos.
- **Reglamento de Seguridad de la Información**: Impone requisitos específicos para la protección de la información en entidades del sector público y privado, incluyendo la implementación de sistemas de gestión de seguridad de la información.
- **Normas de la Superintendencia de Bancos**: Establecen directrices para la gestión de riesgos de TI en instituciones financieras, asegurando la protección y seguridad de los datos financieros.

- **Reputación y Confianza de la Empresa**: El cumplimiento de las normativas puede tener un gran impacto en la percepción de la empresa por parte de clientes y otras entidades. Las organizaciones que demuestran un compromiso con la conformidad regulatoria mejoran su reputación y fortalecen la confianza de los clientes y socios.

- **Reducción de Riesgos Financieros**: Las violaciones de las normativas pueden conllevar sanciones financieras significativas. Por ejemplo, la LOPDP puede imponer multas sustanciales por incumplimientos relacionados con la protección de datos personales (ARCOTEL, 2023).

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de la investigación

El enfoque de la investigación es mixto, se combinan métodos cuantitativos y cualitativos con el objetivo de proporcionar una visión completa y detallada del problema. El componente cuantitativo se utilizará para evaluar datos numéricos, como la frecuencia y el impacto de incidentes de seguridad pasados, y para analizar la efectividad de los controles de seguridad actuales. Por otro lado, el componente cualitativo involucrará entrevistas y análisis de documentos para obtener una comprensión más profunda de las percepciones, experiencias y actitudes de los empleados y directivos respecto a la gestión de riesgos de TI.

De esta manera, este enfoque permite triangulación de datos, lo que mejora la validez y confiabilidad de los hallazgos, asegurando que tanto aspectos técnicos como humanos de la gestión de riesgos sean abordados de manera integral.

3.2. Nivel de la investigación

El nivel de la investigación es de carácter descriptivo y exploratorio, se detallarán las características clave de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda., con el objetivo de identificar y analizar las vulnerabilidades, amenazas y riesgos específicos. Para ello, se evaluará la infraestructura tecnológica, los controles de seguridad y los procesos internos, aplicando marcos de referencia como ISO 27001 o MAGERIT. Estos marcos guiarán el diagnóstico de las vulnerabilidades existentes, permitiendo una comparación con los estándares de seguridad y facilitando la identificación de debilidades que podrían ser explotadas por amenazas tecnológicas o humanas.

3.3. Población y muestra

El universo de la investigación, se centra en el personal del área del departamento de tecnologías de la Información de la Cooperativa Yuyay Ltda.

3.4. Técnicas e instrumentos de recolección

En esta investigación se emplearán diversas técnicas e instrumentos para recolectar datos esenciales sobre la gestión de riesgos de TI en la Cooperativa Yuyay Ltda. Inicialmente, se realizará un levantamiento exhaustivo de los activos del área de TI, identificando y catalogando todos los sistemas, datos, aplicaciones y hardware críticos que requieren protección. Posteriormente, estos activos serán evaluados y valorados mediante matrices de análisis de riesgos, permitiendo una comprensión detallada de las vulnerabilidades y amenazas específicas que enfrenta la cooperativa.

3.5. Tratamiento de la información

La información obtenida mediante el levantamiento de activos será organizada y analizada a través de matrices específicas que faciliten la identificación de riesgos. Cada activo será evaluado en términos de su criticidad y valor para la cooperativa, lo que permitirá identificar y priorizar las vulnerabilidades y amenazas. El análisis de riesgos se realizará considerando variables como la probabilidad de ocurrencia de las amenazas y el impacto que podrían tener en los activos críticos, garantizando una evaluación detallada para la toma de decisiones en la gestión de riesgos.

3.6. Resultados de la entrevista al jefe de TI

¿Qué tipo de tecnologías utiliza actualmente la cooperativa para garantizar la seguridad de la información?

- La cooperativa utiliza firewalls, sistemas de control de acceso, cifrado de datos y sistemas de prevención de intrusiones (IPS) para proteger la red y los datos de los usuarios. También se cuenta con antivirus instalados en todos los equipos.

¿Cómo evalúan las vulnerabilidades en los sistemas de TI?

- Realizamos auditorías periódicas para evaluar el estado de los sistemas y corregir cualquier problema que pueda surgir.

¿Qué amenazas son las más comunes en la cooperativa y cómo las gestionan?

- Las amenazas más comunes incluyen ataques de phishing, malware y accesos no autorizados.

¿Cómo manejan la continuidad del negocio en caso de una interrupción importante del sistema?

- Actualmente contamos con copias de seguridad regulares de los datos.

¿Existen procedimientos establecidos para la gestión de incidentes de seguridad?

- Sí, tenemos un proceso formal de gestión de incidentes. En caso de una brecha de seguridad, se notifica inmediatamente al equipo de TI, se aísla el sistema afectado y se investiga el incidente. Luego se aplican las correcciones necesarias y se actualizan los procedimientos para evitar que vuelva a ocurrir.

¿Qué sugerencias harían para mejorar la actual gestión de riesgos de TI en la cooperativa?

- Sería beneficioso actualizar algunos equipos que ya están quedándose obsoletos y aumentar la frecuencia de las auditorías de seguridad. También creo que podríamos invertir en una herramienta más avanzada de gestión de incidentes para mejorar nuestra capacidad de respuesta.

3.7. Análisis de la entrevista

El análisis de la entrevista realizada al jefe de TI revela que la Cooperativa YUYAY Ltda. ha implementado diversas tecnologías de seguridad como firewalls, sistemas de control de acceso, cifrado de datos y sistemas de prevención de intrusiones (IPS), lo que demuestra un enfoque proactivo en la protección de la red y la información de los usuarios. Además, la utilización de antivirus en todos los equipos asegura una defensa básica contra amenazas comunes.

En cuanto a la evaluación de vulnerabilidades, se menciona que se realizan auditorías periódicas, lo cual es una práctica importante para mantener la infraestructura de TI actualizada y corregir posibles brechas de seguridad. Sin embargo, no se hace referencia a herramientas automáticas de detección de vulnerabilidades, lo que podría indicar una oportunidad de mejora en la automatización de este proceso.

Las amenazas más comunes identificadas incluyen phishing, malware, y accesos no autorizados, todas amenazas recurrentes en el ámbito digital. Aunque la cooperativa cuenta con mecanismos para gestionarlas, como la protección de red mediante controles de acceso y antivirus, es fundamental implementar un sistema más robusto para detectar y prevenir estos ataques, especialmente los de phishing, que a menudo dependen de la capacitación y conciencia de los empleados.

Respecto a la continuidad del negocio, se destaca la realización de copias de seguridad regulares de los datos, lo cual es una medida esencial para garantizar la disponibilidad de la información en caso de una interrupción importante del sistema. No obstante, no se menciona un plan más completo de recuperación ante desastres, lo que podría representar un área a mejorar para asegurar la restauración rápida de los sistemas críticos.

El proceso de gestión de incidentes está formalizado, lo que indica un enfoque estructurado para responder a incidentes de seguridad. El aislamiento inmediato de los sistemas comprometidos y la investigación posterior son medidas esenciales para limitar los daños. Sin embargo, el jefe de TI sugiere que la capacidad de respuesta podría mejorarse invirtiendo en una herramienta más avanzada de gestión de incidentes, lo que permitiría una reacción más rápida y eficiente ante incidentes futuros.

Finalmente, se sugiere actualizar equipos obsoletos y aumentar la frecuencia de las auditorías de seguridad. Estos puntos reflejan una necesidad de mantener la infraestructura tecnológica al día y realizar evaluaciones más frecuentes para asegurar que las vulnerabilidades sean detectadas y corregidas antes de que puedan ser explotadas.

En resumen, aunque la cooperativa ha implementado medidas sólidas para la seguridad de la información, el análisis sugiere que existen oportunidades para mejorar en áreas como la actualización tecnológica, la automatización de la detección de vulnerabilidades, y la implementación de herramientas avanzadas para la gestión de incidentes. Estas mejoras podrían fortalecer aún más la postura de seguridad de la cooperativa y asegurar una gestión de riesgos más eficiente y proactiva.

CAPÍTULO IV

4.1. Título de la propuesta

"Propuesta para la Implementación de Sistema de Gestión de Riesgos de TI para la Cooperativa YUYAY LTDA."

4.2. Presentación

En el presente capítulo se expone la propuesta para la implementación de un Sistema de Gestión de Riesgo de TI en la Cooperativa YUYAY LTDA. El objetivo principal de esta propuesta es establecer un marco integral que permita gestionar de manera efectiva los riesgos asociados a las Tecnologías de la Información (TI) en la cooperativa, garantizando así la continuidad operativa, la seguridad de la información y la alineación con los objetivos estratégicos de la organización.

La propuesta está fundamentada en un análisis exhaustivo de la situación actual de la cooperativa, el cual ha permitido identificar las principales amenazas y vulnerabilidades que podrían afectar la integridad, confidencialidad y disponibilidad de la información. A partir de este diagnóstico, se ha diseñado un conjunto de controles y estrategias que buscan mitigar los riesgos identificados, asegurando una gestión proactiva y eficiente de los mismos.

Este capítulo se estructura en varias secciones, comenzando con una descripción detallada del marco teórico y metodológico utilizado para la identificación y valoración de los riesgos. Posteriormente, se presenta el modelo de gestión propuesto, el cual incluye políticas, procedimientos y herramientas específicas que se recomiendan implementar en la cooperativa para gestionar los riesgos de TI. Finalmente, se plantean las acciones necesarias para la implementación y seguimiento del sistema propuesto, asegurando su sostenibilidad en el tiempo y su adaptación a los cambios en el entorno tecnológico y normativo.

Esta propuesta no solo busca fortalecer la capacidad de la cooperativa para enfrentar los riesgos de TI, sino también impulsar una cultura organizacional orientada a la seguridad y la gestión de riesgos, aspectos fundamentales para el crecimiento y la competitividad en el sector financiero.

4.3. Desarrollo de la propuesta

Para realizar este apartado se utilizará la norma ISO 31000, ya que establece un marco para la gestión de riesgos que puede ser aplicado a cualquier tipo de organización, incluyendo la gestión de riesgos de TI en una cooperativa.

4.3.1. Fase 1: Establecimiento del contexto

La Cooperativa de Ahorro y Crédito YUYAY Ltda., ubicada en el cantón Cañar, fue fundada en 1996 y tiene como objetivo principal apoyar el desarrollo económico de las comunidades indígenas y campesinas del pueblo Cañari. La cooperativa cuenta con una estructura organizacional orientada a ofrecer productos financieros accesibles, como cuentas de ahorro y microcréditos, dirigidos principalmente a su comunidad.

En cuanto a la estructura organizacional, YUYAY Ltda. se organiza en diferentes áreas funcionales que incluyen finanzas, tecnología, atención al cliente, y operaciones, con un enfoque en la inclusión financiera y el servicio comunitario. La cultura organizacional está fuertemente ligada a los valores de cooperación, confianza, y desarrollo social, lo que influye en la manera en que la cooperativa aborda la gestión de riesgos y la seguridad de la información.

Los recursos disponibles para la gestión de riesgos incluyen un equipo técnico capacitado y una infraestructura tecnológica que soporta servicios digitales como Yuyay Móvil y Yuyay Web, que facilitan transacciones y pagos a sus usuarios. Esto pone de manifiesto la importancia de gestionar eficazmente los riesgos asociados con la seguridad de la información y la continuidad del negocio.

4.3.1.1. Estructura organizacional

Ilustración 2. Estructura organizacional COAC. Yuyay Ltda. Fuente: Autoría Propia

4.3.1.2. Contexto Externo

La cooperativa opera en un **entorno regulatorio** que incluye la supervisión de la Superintendencia de Economía Popular y Solidaria (SEPS), cumpliendo con normativas específicas para el sector cooperativo en Ecuador. Además, el **entorno económico** del cantón Cañar, caracterizado por una economía rural y agrícola, presenta desafíos y oportunidades para la gestión de riesgos de TI, ya que la cooperativa debe equilibrar la inclusión financiera con la seguridad tecnológica.

El **entorno tecnológico** también juega un papel crucial, con un aumento en el uso de servicios digitales por parte de sus clientes, lo que eleva la necesidad de implementar medidas de seguridad robustas contra amenazas cibernéticas. La cooperativa mantiene relaciones con proveedores de tecnología y servicios financieros que también influyen en la gestión de riesgos.

4.3.1.3. Establecimiento de los Criterios de Riesgo

Dado su compromiso con la inclusión financiera y la confianza depositada por sus miembros, la cooperativa YUYAY Ltda. establece criterios de riesgo que priorizan la **confidencialidad**, **integridad**, y **disponibilidad** de la información. La tolerancia al riesgo es baja, particularmente en lo que respecta a la seguridad de los datos personales y financieros de sus socios.

4.3.1.4. Alcance y Objetivos del Proceso de Gestión de Riesgos

El proceso de gestión de riesgos de TI en la cooperativa se enfoca en asegurar la continuidad operativa y la protección de los activos de información, abarcando áreas críticas como la infraestructura tecnológica, los sistemas de gestión de clientes, y los servicios digitales.

Objetivo General:

- Elaborar la propuesta de gestión de riesgos tecnológicos de la COAC. Yuyay Ltda.

Objetivos Específicos:

- Identificar los activos críticos de TI de la COAC. Yuyay Ltda.
- Determinar las vulnerabilidades y amenazas que afectan a los activos críticos.
- Proponer controles de protección para mitigar las amenazas.

4.3.2. FASE 2: Identificación de riesgos

En esta fase, se lleva a cabo un proceso sistemático para identificar los riesgos que podrían afectar la integridad, confidencialidad y disponibilidad de los activos de TI de la Cooperativa YUYAY Ltda. El objetivo es reconocer todas las amenazas potenciales que podrían comprometer los sistemas de información y la infraestructura tecnológica de la cooperativa.

4.3.2.1. Identificación de Activos Tecnológicos

En el contexto de la gestión de la (TI), la identificación y gestión de los activos de TI constituyen un pilar fundamental para la protección y optimización de los recursos tecnológicos de una organización. En un entorno cada vez más digitalizado, donde la dependencia de la tecnología es crítica para la operación diaria, la gestión adecuada de los activos de TI se vuelve esencial no solo para garantizar la continuidad operativa, sino también para asegurar la integridad, confidencialidad y disponibilidad de la información.

Este apartado se enfoca en la primera fase del ciclo de vida de la gestión de activos: la identificación y el inventario de todos los activos de TI, un proceso clave para el desarrollo de estrategias de seguridad y gestión de riesgos eficientes.

Tabla 1. Identificación de activos. Fuente: Autoría Propia

ID	ACTIVO	CUSTODIO	CARACTERIZACIÓN
ACT-01	Switch TP-LINK	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-02	Router MIKROTIK	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-03	InBio ZK Teco	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-04	GrandStream IP GRANDSTREAM	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-05	Switch TP-LINK	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-06	NVR HIKVISION	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-07	CPU GENÉRICO	Cajas	[HW]Equipamiento informático (hardware)
ACT-08	Impresora de Tickets EPSON	Cajas	[HW]Equipamiento informático (hardware)
ACT-09	Teléfono IP GRANDSTREAM	Cajas	[HW]Equipamiento informático (hardware)
ACT-10	Intercomunicador ZHUDELE	Cajas	[HW]Equipamiento informático (hardware)
ACT-11	Acceso Biométrico ZKTeco	Cajas	[HW]Equipamiento informático (hardware)
ACT-12	Yuyay Móvil	Ingeniero de Sistemas	Software
ACT-13	Scanner EPSON	Asesor de Crédito	[HW]Equipamiento informático (hardware)

ACT-14	Laptop	Gerencia	[HW]Equipamiento informático (hardware)
ACT-15	Teléfono IP	Asesor de Crédito	[HW]Equipamiento informático (hardware)
ACT-16	Impresora de Tickets	Asesor de Crédito	[HW]Equipamiento informático (hardware)
ACT-17	Base de Ventilación	Responsable de Oficina	[HW]Equipamiento informático (hardware)
ACT-18	Regulador/UPS QUASAD	Responsable de Oficina	[HW]Equipamiento informático (hardware)
ACT-19	Router MIKROTIK	Responsable de Oficina	[HW]Equipamiento informático (hardware)
ACT-20	Router DLINK	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-21	NVR	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-22	Monitor	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)
ACT-23	Intercomunicador	Cajas	[HW]Equipamiento informático (hardware)
ACT-24	Teléfono IP	Cajas	[HW]Equipamiento informático (hardware)
ACT-25	Scanner	Cajas	[HW]Equipamiento informático (hardware)
ACT-26	Regulador/UPS	Créditos	[HW]Equipamiento informático (hardware)
ACT-27	Router MIKROTIK	Créditos	[HW]Equipamiento informático (hardware)
ACT-28	Switch DLINK	Cajas	[HW]Equipamiento informático (hardware)
ACT-29	NVR	Ingeniero de Sistemas	[HW]Equipamiento informático (hardware)

ACT-30	Contador Billetes	Cajas	[HW]Equipamiento informático (hardware)
ACT-31	Intercomunicador	Cajas	[HW]Equipamiento informático (hardware)
ACT-32	Laptop	Cajas	[HW]Equipamiento informático (hardware)
ACT-33	Regulador/Ups	Cajas	[HW]Equipamiento informático (hardware)
ACT-34	Oficial de Seguridad de la Información	TI	[P]Personal
ACT-35	Auditor Informativo	TI	[P]Personal
ACT-36	Oficial de Seguridad Física y Electrónica	TI	[P]Personal
ACT-37	Coordinador de Sistemas	TI	[P]Personal
ACT-38	Teléfono IP	Cajas	[HW]Equipamiento informático (hardware)
ACT-39	Monitor	AREA DE CREDITO 2	[HW]Equipamiento informático (hardware)
ACT-40	CPU	AREA DE CREDITO 2	[HW]Equipamiento informático (hardware)
ACT-41	Teléfono IP	AREA DE CREDITO	[HW]Equipamiento informático (hardware)
ACT-42	Scanner	AREA DE CREDITO 3	[HW]Equipamiento informático (hardware)
ACT-43	Impresora	AREA DE CREDITO 3	[HW]Equipamiento informático (hardware)
ACT-44	Periféricos	ÁREA DE INFORMACIÓN	[HW]Equipamiento informático (hardware)
ACT-45	Impresora	ÁREA DE INFORMACIÓN	[HW]Equipamiento informático (hardware)

ACT-46	Teléfono IP	ÁREA DE INFORMACIÓN	[HW]Equipamiento informático (hardware)
ACT-47	Regulador	ÁREA DE INFORMACIÓN	[HW]Equipamiento informático (hardware)
ACT-48	Monitor	ÁREA DE INFORMACIÓN	[HW]Equipamiento informático (hardware)
ACT-49	CPU	COORDINADOR CREDITO	[HW]Equipamiento informático (hardware)
ACT-50	Impresora	COORDINADOR CREDITO	[HW]Equipamiento informático (hardware)
ACT-51	Teléfono IP	COORDINADOR CREDITO	[HW]Equipamiento informático (hardware)
ACT-52	Teléfono Inalámbrico	CONTABILIDAD	[HW]Equipamiento informático (hardware)
ACT-53	CPU	CONTABILIDAD	[HW]Equipamiento informático (hardware)
ACT-54	Teléfono IP	CONTABILIDAD	[HW]Equipamiento informático (hardware)
ACT-55	Switch	CONTABILIDAD	[HW]Equipamiento informático (hardware)
ACT-56	Router HP	CONTABILIDAD	[HW]Equipamiento informático (hardware)
ACT-57	GrandStrem	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-58	Switch	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-59	Convertidor de Fibra	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-60	NVR	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-61	CPU	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)

ACT-62	FIREWALL	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-63	UPS	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-64	ROUTER	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-65	Receptor GSM	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)
ACT-66	DISCO DURO	CENTRO DE DATOS	[HW]Equipamiento informático (hardware)

.3.2.2. Identificación de Activos Críticos

La identificación de los activos críticos es un paso esencial en la gestión de riesgos de TI, ya que estos activos representan los recursos más valiosos y vulnerables de la cooperativa YUYAY Ltda. Estos activos incluyen sistemas, datos y tecnologías que son fundamentales para el funcionamiento diario y la prestación de servicios financieros. Reconocer estos activos permite priorizar la protección y establecer medidas de seguridad adecuadas para mitigar los riesgos asociados.

En la Tabla 2, se describe los valores asignados a los criterios de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad de los activos críticos de TI en la Cooperativa Yuyay Ltda. Estos criterios se utilizan para evaluar la criticidad de cada activo en función del impacto que tendría una alteración o vulnerabilidad en alguno de estos aspectos. Cada valor refleja el nivel de importancia y el grado de protección necesario para asegurar que los activos mantengan su operatividad y seguridad dentro de la organización.

Valor	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
1	Información de mínima importancia	Integridad de poca relevancia	No se requiere disponibilidad constante	No se requiere autenticidad estricta	No es necesario rastrear las acciones
2	Información que puede ser pública	Integridad deseada pero no crítica	Disponibilidad necesaria pero no urgente	Se requiere autenticidad en ocasiones	Es útil rastrear algunas

	o de bajo riesgo				acciones, pero no es obligatorio
3	Información interna que debe protegerse moderadamente	Integridad importante para evitar errores	Disponibilidad deseada, pero puede tolerar interrupciones cortas	Autenticidad requerida para proteger el acceso	Se necesita registro de acciones importantes
4	Información confidencial o personal	Integridad crítica para evitar alteraciones	Disponibilidad constante para operaciones críticas	Autenticidad esencial para evitar accesos no autorizados	Es obligatorio rastrear todas las acciones
5	Información altamente sensible o clasificada	Integridad extremadamente crítica	Disponibilidad ininterrumpida es obligatoria	Autenticidad imprescindible para acceso seguro	Trazabilidad completa y exhaustiva de todas las acciones

Tabla 2. Identificación de Activos críticos. Fuente: Autoría Propia

Criterio de probabilidad

El criterio de probabilidad es un componente esencial en la gestión de riesgos, ya que permite evaluar la probabilidad de que una amenaza se materialice en un incidente. Este criterio se utiliza para asignar un valor a la probabilidad basada en la frecuencia o la posibilidad de ocurrencia, lo que facilita priorizar los riesgos y enfocar los esfuerzos de mitigación en aquellas amenazas que presentan una mayor probabilidad de afectar los activos de la organización.

Tabla 3. Escala de probabilidad. Fuente: Autoría Propia

Nivel de probabilidad	Descripción	Valor
Muy Alto	El riesgo es casi seguro que ocurra	5
Alto	El riesgo es probable que ocurra	4
Medio	El riesgo podría ocurrir en algún momento.	3
Bajo	El riesgo es poco probable que ocurra.	2

Muy bajo	El riesgo es altamente improbable.	1

Criterio de Impacto

El criterio de impacto se refiere a la evaluación de las consecuencias que un incidente puede tener sobre los activos críticos y la operatividad de la organización. Este criterio mide el nivel de daño o interrupción que podría causar una amenaza si se concretara, permitiendo clasificar los riesgos en función de su severidad. Comprender el impacto potencial es crucial para desarrollar estrategias de mitigación efectivas que protejan los activos más valiosos de la organización.

Tabla 4. Escala de impacto. Fuente: Autoría Propia

Nivel de Impacto	Descripción	Valor
Catastrófico	Impacto extremo, causando una interrupción severa de los servicios críticos.	5
Grave	Impacto significativo, causando disrupciones importantes en los servicios.	4
Moderado	Impacto moderado, con algunas interrupciones en el servicio.	3
Menor	Impacto leve, con disrupciones menores en el servicio.	2
Insignificante	Impacto mínimo, sin disrupciones notables en el servicio.	1

A continuación, se expone la calificación final en base a los siguientes criterios:

- **Muy Alto (21-25)**: Este rango indica que el activo es extremadamente crítico en términos de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Estos activos generalmente requieren las medidas de seguridad y gestión más estrictas.
- **Alto (16-20)**: Activos importantes, que requieren un nivel considerable de protección y gestión, pero que no son tan críticos como los del rango Muy Alto.
- **Medio (11-15)**: Activos moderadamente importantes, que necesitan un nivel estándar de protección y gestión.
- **Bajo (6-10)**: Activos de menor importancia, con requerimientos básicos de protección y gestión.
- **Muy Bajo (1-5)**: Activos de mínima importancia, que requieren poca o ninguna medida de protección o gestión específica.

Tabla 5. Calificación de activos. Fuente: Autoría Propia.

ID	Activo	Caracterización	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Total
ACT-01	Switch TP-LINK	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-02	Router MIKROTIK	[HW]Equipamiento informático (hardware)	4	4	5	4	4	21
ACT-03	InBio ZK Teco	[HW]Equipamiento informático (hardware)	5	5	4	5	4	24
ACT-04	GrandStream IP GRANDSTREAM	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-05	Switch TP-LINK	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-06	NVR HIKVISION	[HW]Equipamiento informático (hardware)	4	5	5	4	5	23
ACT-07	CPU GENÉRICO	[HW]Equipamiento informático (hardware)	3	4	4	3	3	17
ACT-08	Impresora de Tickets EPSON	[HW]Equipamiento informático (hardware)	2	3	4	2	2	13
ACT-09	Teléfono IP GRANDSTREAM	[HW]Equipamiento informático (hardware)	2	2	3	3	2	12
ACT-10	Intercomunicador ZHUDELE	[HW]Equipamiento informático (hardware)	3	4	4	3	3	17

ACT-11	Acceso Biométrico ZKTeco	[HW]Equipamiento informático (hardware)	3	5	4	3	3	18
ACT-12	Yuyay Móvil	Software	4	5	4	4	4	21
ACT-13	Scanner EPSON	[HW]Equipamiento informático (hardware)	3	4	3	2	2	14
ACT-14	Laptop	[HW]Equipamiento informático (hardware)	4	4	3	4	3	18
ACT-15	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-16	Impresora de Tickets	[HW]Equipamiento informático (hardware)	2	3	4	2	2	13
ACT-17	Base de Ventilación	[HW]Equipamiento informático (hardware)	1	2	2	1	1	7
ACT-18	Regulador/UPS QUASAD	[HW]Equipamiento informático (hardware)	2	4	5	1	2	14
ACT-19	Router MIKROTIK	[HW]Equipamiento informático (hardware)	4	4	5	4	4	21
ACT-20	Router DLINK	[HW]Equipamiento informático (hardware)	4	4	5	5	4	22
ACT-21	NVR	[HW]Equipamiento informático (hardware)	4	5	5	4	5	23
ACT-22	Monitor	[HW]Equipamiento informático (hardware)	2	3	4	1	1	11
ACT-23	Intercomunicador	[HW]Equipamiento informático (hardware)	3	4	4	3	3	17
ACT-24	Teléfono IP	[HW]Equipamiento informático (hardware)	3	3	4	2	2	14
ACT-25	Scanner	[HW]Equipamiento informático (hardware)	3	4	3	2	2	14
ACT-26	Regulador/UPS	[HW]Equipamiento informático (hardware)	2	4	5	1	2	14

ACT-27	Router MIKROTIK	[HW]Equipamiento informático (hardware)	4	4	5	4	4	21
ACT-28	Switch DLINK	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-29	NVR	[HW]Equipamiento informático (hardware)	4	5	5	4	5	23
ACT-30	Contador Billetes	[HW]Equipamiento informático (hardware)	3	4	4	3	3	17
ACT-31	Intercomunicador	[HW]Equipamiento informático (hardware)	3	4	4	2	3	16
ACT-32	Laptop	[HW]Equipamiento informático (hardware)	4	4	4	4	3	19
ACT-33	Regulador/Ups	[HW]Equipamiento informático (hardware)	2	4	5	1	2	14
ACT-34	Oficial de Seguridad de la Información	[P]Personal	5	5	4	5	5	24
ACT-35	Auditor Informativo	[P]Personal	5	5	4	5	5	24
ACT-36	Oficial de Seguridad Física y Electrónica	[P]Personal	4	5	4	5	4	22
ACT-37	Coordinador de Sistemas	[P]Personal	5	5	4	5	5	24
ACT-38	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-39	Monitor	[HW]Equipamiento informático (hardware)	2	3	4	1	1	11
ACT-40	CPU	[HW]Equipamiento informático (hardware)	4	4	4	3	3	18

ACT-41	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-42	Scanner	[HW]Equipamiento informático (hardware)	3	4	3	2	2	14
ACT-43	Impresora	[HW]Equipamiento informático (hardware)	2	3	4	2	2	13
ACT-44	Periféricos	[HW]Equipamiento informático (hardware)	2	3	3	2	1	11
ACT-45	Impresora	[HW]Equipamiento informático (hardware)	2	3	4	2	2	13
ACT-46	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-47	Regulador	[HW]Equipamiento informático (hardware)	2	4	5	1	2	14
ACT-48	Monitor	[HW]Equipamiento informático (hardware)	2	3	4	1	1	11
ACT-49	CPU	[HW]Equipamiento informático (hardware)	4	4	4	3	3	18
ACT-50	Impresora	[HW]Equipamiento informático (hardware)	2	3	4	2	2	13
ACT-51	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-52	Teléfono Inalámbrico	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-53	CPU	[HW]Equipamiento informático (hardware)	4	4	4	4	3	19
ACT-54	Teléfono IP	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-55	Switch	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-56	Router HP	[HW]Equipamiento informático (hardware)	4	4	5	4	4	21

ACT-57	GrandStrem	[HW]Equipamiento informático (hardware)	3	4	5	4	3	19
ACT-58	Switch	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-59	Convertidor de Fibra	[HW]Equipamiento informático (hardware)	3	4	5	3	3	18
ACT-60	NVR	[HW]Equipamiento informático (hardware)	4	5	5	4	5	23
ACT-61	CPU	[HW]Equipamiento informático (hardware)	4	4	4	4	3	19
ACT-62	FIREWALL	[HW]Equipamiento informático (hardware)	5	5	5	5	5	25
ACT-63	UPS	[HW]Equipamiento informático (hardware)	2	4	5	1	2	14
ACT-64	ROUTER	[HW]Equipamiento informático (hardware)	4	4	5	4	4	21
ACT-65	Receptor GSM	[HW]Equipamiento informático (hardware)	3	4	4	3	3	17
ACT-66	DISCO DURO	[HW]Equipamiento informático (hardware)	4	5	4	4	4	21

a) 4.3.2.2. Identificación de Amenazas

Tabla 6. Identificación de amenazas. Fuente: Autoría Propia

ID	Activo	Caracterización	Amenaza
ACT-01	Switch TP-LINK (Área de TI)	[HW]Equipamiento informático (hardware)	Ataques DDoS
			Fallas de Hardware
			Errores de configuración
			Interferencia electromagnética
ACT-02	Router MIKROTIK (Área de TI)	[HW]Equipamiento informático (hardware)	Acceso no autorizado
			Ataques de enrutamiento
			Configuración incorrecta
			Fallos en la actualización de firmware

ACT-03	InBio ZK Teco (Área de TI)	[HW]Equipamiento informático (hardware)	Ataques de fuerza bruta
			Pérdida de datos
			Malware
ACT-04	GrandStream IP GRANDSTREAM (Área de TI)	[HW]Equipamiento informático (hardware)	Intercepción de llamadas
			Vulnerabilidades de firmware
			Phishing
			Fallas de hardware
ACT-05	Switch TP-LINK (Área de TI)	[HW]Equipamiento informático (hardware)	Sobrecarga de red
			Ataques DDoS
			Errores de configuración
ACT-06	NVR HIKVISION (Área de TI)	[HW]Equipamiento informático (hardware)	Pérdida de grabaciones
			Ataques a la red
			Manipulación de videos
			Fallas de hardware
			Acceso no autorizado
ACT-07	CPU GENÉRICO (Área de Cajas)	[HW]Equipamiento informático (hardware)	Pérdida de datos financieros
			Fallas en disco duro
			Malware
			Errores humanos
			Acceso no autorizado
ACT-10	Intercomunicador ZHUDELE (Área de Cajas)	[HW]Equipamiento informático (hardware)	Fallas de hardware
			Interferencia en la comunicación
			Sabotaje físico
			Errores de configuración
			Pérdida de funcionalidad

ACT-11	Acceso Biometrico ZKTeco (Área de Cajas)	[HW]Equipamiento informático (hardware)	Compromiso de datos biométricos
			Fallas en la autenticación
ACT-12	Yuyay Móvil (Área de TI)	Software	Vulnerabilidades en la aplicación
			Robo de datos personales
			Acceso no autorizado
			Ataques de phishing
			Interrupciones de servicio
ACT-14	Laptop (Gerencia)	[HW]Equipamiento informático (hardware)	Pérdida de datos sensibles
			Malware
			Robo físico
			Ataques de phishing
			Fallas de hardware
ACT-15	Teléfono IP ()	[HW]Equipamiento informático (hardware)	Intercepción de llamadas
			Vulnerabilidades de firmware
			Fallas de hardware
ACT-19	Router MIKROTIK (responsable de oficina)	[HW]Equipamiento informático (hardware)	Acceso no autorizado
			Configuración incorrecta
			Ataques de enrutamiento
ACT-20	Router DLINK (responsable de oficina)	[HW]Equipamiento informático (hardware)	Acceso no autorizado
			Configuración incorrecta
			Ataques de enrutamiento
			Fallos en la actualización de firmware
ACT-21	NVR (Área de TI)	[HW]Equipamiento informático (hardware)	Pérdida de grabaciones
			Ataques a la red
			Manipulación de videos
			Acceso no autorizado
ACT-23	Intercomunicador	[HW]Equipamiento informático (hardware)	Fallas de hardware
			Interferencia en la comunicación
			Sabotaje físico

	(Área de Cajas)		Errores de configuración
			Pérdida de funcionalidad
ACT-27	Router MIKROTIK (Área de Créditos)	[HW]Equipamiento informático (hardware)	Acceso no autorizado
			Ataques de enrutamiento
			Configuración incorrecta
			Fallos en la actualización de firmware
ACT-28	Switch DLINK (Área de Cajas)	[HW]Equipamiento informático (hardware)	Sobrecarga de red
			Fallas de hardware
			Ataques DDoS
			Errores de configuración
ACT-29	NVR (Área de Cajas)	[HW]Equipamiento informático (hardware)	Pérdida de grabaciones
			Ataques a la red
			Manipulación de videos
			Acceso no autorizado
ACT-30	Contador Billetes (Área de Cajas)	[HW]Equipamiento informático (hardware)	Fallas mecánicas
			Sabotaje
			Interferencia electromagnética
			Robo físico
			Mal uso del equipo
ACT-31	Intercomunicador (Área de Cajas)	[HW]Equipamiento informático (hardware)	Fallas de hardware
			Interferencia en la comunicación
			Sabotaje físico
			Errores de configuración
ACT-32	Laptop (Área de Cajas)	[HW]Equipamiento informático (hardware)	Pérdida de datos sensibles
			Malware
			Robo físico
			Falta de actualización

ACT-34	Oficial de Seguridad de la Información (Área de TI)	[P]Personal	Errores humanos
			Acceso no autorizado a sistemas
			Sobrecarga de trabajo
			Extorsión
			Falta de formación
			Compromiso de credenciales
			Ingeniería social
ACT-35	Auditor Informativo (Área de TI)	[P]Personal	Acceso no autorizado a información
			Filtración de datos
			Errores en la auditoría
			Robo de información
ACT-36	Oficial de Seguridad Física y Electrónica (Área de TI)	[P]Personal	Sabotaje físico
			Errores humanos
			Acceso no autorizado a sistemas
			Extorsión
			Falta de formación
ACT-37	Coordinador de Sistemas (Área de TI)	[P]Personal	Errores humanos
			Acceso no autorizado a Sistemas
			Falta de formación
			Fallos en la toma de decisiones
ACT-38	Teléfono IP (Área de Cajas)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Vulnerabilidades de firmware
			Ataques de denegación de servicio

			Fallas de hardware
ACT-40	CPU (Área de Crédito 2)	[HW]Equipamiento informático (hardware)	Pérdida de datos financieros
			Fallas en disco duro
			Errores humanos
			Acceso no autorizado
ACT-41	Teléfono IP (Área de Crédito 2)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Ataques de denegación de servicio
			Fallas de hardware
ACT-46	Teléfono IP (Área de información)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Ataques de denegación de servicio
			Fallas de hardware
ACT-49	CPU (Coordinador de crédito)	[HW]Equipamiento informático (hardware)	Pérdida de datos financieros
			Fallas en disco duro
			Errores humanos
			Acceso no autorizado
ACT-51	Teléfono IP (Coordinador de crédito)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Ataques DoS
ACT-52	Teléfono Inalámbrico (Contabilidad)	[HW]Equipamiento informático (hardware)	Fallas en la señal
			Pérdida de conectividad
			Robo físico
ACT-53	CPU (Contabilidad)	[HW]Equipamiento informático (hardware)	Pérdida de datos financieros
			Fallas en disco duro
			Errores humanos
			Acceso no autorizado
ACT-54	Teléfono IP (Contabilidad)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Ataques DoS
ACT-55	Switch (Contabilidad)	[HW]Equipamiento informático (hardware)	Sobrecarga de red
			Fallas de hardware

			Ataques DDoS
			Errores de configuración
ACT-56	Router HP (Contabilidad)	[HW]Equipamiento informático (hardware)	Acceso no autorizado
			Ataques de enrutamiento
			Configuración incorrecta
			Fallos de actualización
ACT-57	GrandStrem (Centro de datos)	[HW]Equipamiento informático (hardware)	Interceptación de llamadas
			Vulnerabilidades de firmware
			Ataques de denegación de servicio
ACT-58	Switch (Centro de datos)	[HW]Equipamiento informático (hardware)	Sobrecarga de red
			Fallas de hardware
			Ataques DDoS
ACT-59	Convertidor de Fibra (Centro de datos)	[HW]Equipamiento informático (hardware)	Fallas en la transmisión de datos
			Vulnerabilidades en el hardware
			Sabotaje físico
			Errores en la configuración
			Pérdida de conectividad
ACT-60	NVR (Centro de datos)	[HW]Equipamiento informático (hardware)	Pérdida de grabaciones
			Ataques a la red
			Manipulación de videos
			Acceso no autorizado
ACT-61	CPU (Centro de datos)	[HW]Equipamiento informático (hardware)	Pérdida de datos críticos
			Fallas en disco duro
			Malware
			Acceso no autorizado
ACT-62	FIREWALL (Centro de datos)	[HW]Equipamiento informático (hardware)	Fallos en la configuración
			Ataques de desbordamiento
			Vulnerabilidades en el firmware
			Sobrecarga de tráfico
			Acceso no autorizado
ACT-64	ROUTER	[HW]Equipamiento informático (hardware)	Ataques de enrutamiento
			Configuración incorrecta

	(Centro de datos)		Acceso no autorizado
ACT-65	Receptor GSM (Centro de datos)	[HW]Equipamiento informático (hardware)	Interferencia en la señal
			Acceso no autorizado
			Sabotaje físico
ACT-66	**DISCO DURO (Centro de datos)**	[HW]Equipamiento informático (hardware)	Pérdida de datos
			Sobrecarga de almacenamiento
			Fallas mecánicas
			Malware
			Robo Físico

4.3.2.3. Análisis de riesgos

El análisis de riesgos es una etapa crucial dentro del proceso de gestión de riesgos, cuyo objetivo es evaluar la probabilidad de ocurrencia y el impacto potencial de las amenazas identificadas sobre los activos críticos de la organización. Este análisis no solo permite priorizar los riesgos según su severidad, sino que también proporciona una base sólida para el desarrollo de estrategias de mitigación y control. A través de este proceso, la entidad financiera puede anticiparse a los posibles incidentes, optimizando la asignación de recursos y fortaleciendo su capacidad de respuesta ante contingencias. Además, el análisis de riesgos facilita la toma de decisiones informadas, al ofrecer una visión integral de los escenarios de riesgo que podrían comprometer la continuidad operativa y la seguridad de la información.

Matriz de riesgo

Esta matriz permite cruzar la probabilidad de ocurrencia de un riesgo (Muy Bajo a Muy Alto) con el impacto potencial (Insignificante a Catastrófico). Los resultados se clasifican en diferentes niveles de severidad, desde "Bajo" hasta "Muy Alto", lo que facilita la priorización de los riesgos a gestionar.

Tabla 7. Impacto/Probabilidad. Fuente: Autoría Propia

Impacto/ Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Catastrófico (5)	Moderado	Alto	Muy Alto	Muy Alto	Muy Alto

Grave (4)	Moderado	Alto	Muy Alto	Muy Alto	Muy Alto
Moderado (3)	Bajo	Moderado	Alto	Muy Alto	Muy Alto
Menor (2)	Bajo	Moderado	Moderado	Alto	Muy Alto
Insignificante (1)	Bajo	Bajo	Moderado	Moderado	Alto

La siguiente tabla, presenta la categorización de los riesgos en cuatro niveles:

- **Bajo (1-6)**: Riesgo aceptable, sin necesidad de acciones inmediatas.
- **Medio (7-12)**: Riesgo tolerable, con medidas de control recomendadas.
- **Alto (13-18)**: Riesgo inaceptable, que requiere atención urgente.
- **Crítico (19-25)**: Riesgo inadmisible, que demanda una acción inmediata para mitigar o eliminar el riesgo.

Tabla 8. Escala de riesgos. Fuente: Autoría Propia

Riesgo	Descripción	Valor
Bajo	Riesgo aceptable	**1-6**
Medio	Riesgo tolerable	**7-12**
Alto	Riesgo inaceptable	**13-18**
Crítico	Riesgo inadmisible	**19-25**

A continuación, se presenta el análisis de riesgos, tomando en cuenta los criterios mencionados anteriormente:

Tabla 9. Calificación del riesgo de los activos críticos. Fuente: Autoría Propia.

ID	Activo	Amenaza	Probabilidad	Impacto	Riesgo
ACT-01	Switch TP-LINK (Área de TI)	Ataques DDoS	4	5	20
		Fallas de Hardware	2	3	6
		Errores de configuración	1	3	3
		Interferencia electromagnética	2	3	6
		Acceso no autorizado	3	5	15

ACT-02	Router MIKROTIK (Área de TI)	Ataques de enrutamiento	2	4	8
		Configuración incorrecta	1	5	5
		Fallos en la actualización de firmware	1	5	5
ACT-03	InBio ZK Teco (Área de TI)	Ataques de fuerza bruta	1	4	4
		Pérdida de datos	1	5	5
		Malware	1	5	5
ACT-04	GrandStream IP GRANDSTREAM (Área de TI)	Intercepción de llamadas	2	5	10
		Vulnerabilidades de firmware	1	4	4
		Phishing	1	3	3
		Fallas de hardware	2	3	6
ACT-05	Switch TP-LINK (Área de TI)	Sobrecarga de red	2	4	8
		Ataques DoS	1	5	5
		Errores de configuración	2	5	10
ACT-06	NVR HIKVISION (Área de TI)	Pérdida de grabaciones	2	5	10
		Ataques a la red	3	5	15
		Manipulación de videos	1	5	5
		Fallas de hardware	1	5	5
		Acceso no autorizado	2	5	10
ACT-07	CPU GENÉRICO (Área de Cajas)	Pérdida de datos financieros	2	5	10
		Fallas en disco duro	1	5	5
		Malware	1	5	5
		Errores humanos	3	5	15
		Acceso no autorizado	1	5	5
ACT-10	Intercomunicador ZHUDELE (Área de Cajas)	Fallas de hardware	1	3	3
		Interferencia en la comunicación	1	5	5

		Sabotaje físico	1	4	4
		Errores de configuración	2	4	8
		Pérdida de funcionalidad	1	4	4
ACT-11	Acceso Biométrico ZKTeco (Área de Cajas)	Compromiso de datos biométricos	2	5	10
		Fallas en la autenticación	2	5	10
ACT-12	Yuyay Móvil (Área de TI)	Vulnerabilidades en la aplicación	1	5	5
		Robo de datos personales	3	5	15
		Acceso no autorizado	2	5	10
		Ataques de phishing	2	4	8
		Interrupciones de servicio	3	5	15
ACT-14	Laptop (Gerencia)	Pérdida de datos sensibles	2	5	10
		Malware	1	5	5
		Robo físico	2	5	10
		Ataques de phishing	3	5	15
		Acceso no autorizado	3	5	15
		Fallas de hardware	1	3	3
ACT-15	Teléfono IP (responsable de oficina)	Intercepción de llamadas	1	4	4
		Vulnerabilidades de firmware	1	3	3
		Fallas de hardware	1	4	4
ACT-19	Router MIKROTIK (responsable de oficina)	Acceso no autorizado	2	5	10
		Configuración incorrecta	2	5	10
		Ataques de enrutamiento	3	5	15
ACT-20	Router DLINK (responsable de oficina)	Acceso no autorizado	2	5	10
		Configuración incorrecta	1	5	5
		Ataques de enrutamiento	2	5	10
		Fallos en la actualización de firmware	1	5	5
	NVR	Pérdida de grabaciones	1	5	5

ACT-21	(Área de TI)	Ataques a la red	2	5	10
		Manipulación de videos	1	5	5
		Acceso no autorizado	3	5	15
ACT-23	Intercomunicador (Área de Cajas)	Fallas de hardware	1	4	4
		Interferencia en la comunicación	2	5	10
		Sabotaje físico	1	4	4
		Errores de configuración	1	5	5
		Pérdida de funcionalidad	1	4	4
ACT-27	Router MIKROTIK (Área de Créditos)	Acceso no autorizado	3	4	12
		Ataques de enrutamiento	2	3	6
		Configuración incorrecta	2	4	8
		Fallos en la actualización de firmware	2	4	8
ACT-28	Switch DLINK (Área de Cajas)	Sobrecarga de red	2	3	6
		Fallas de hardware	2	3	6
		Ataques DDoS	3	3	9
		Errores de configuración	2	4	8
ACT-29	NVR (Área de Cajas)	Pérdida de grabaciones	2	5	10
		Ataques a la red	3	5	15
		Manipulación de videos	2	5	10
		Acceso no autorizado	3	4	12
ACT-30	Contador Billetes (Área de Cajas)	Fallas mecánicas	2	3	6
		Sabotaje	2	2	4
		Interferencia electromagnética	2	2	4
		Robo físico	1	3	3
		Mal uso del equipo	1	3	3
		Fallas de hardware	2	2	4

ACT-31	Intercomunicador (Área de Cajas)	Interferencia en la comunicación	2	2	4
		Sabotaje físico	1	3	3
		Errores de configuración	2	2	4
ACT-32	Laptop (Área de Cajas)	Pérdida de datos sensibles	3	4	12
		Malware	2	3	6
		Robo físico	3	3	9
		Falta de actualización	2	2	4
ACT-34	Oficial de Seguridad de la Información (Área de TI)	Errores humanos	2	5	10
		Acceso no autorizado a sistemas	1	5	5
		Extorsión	4	5	20
		Sobrecarga de trabajo	2	3	6
		Falta de formación	1	5	5
		Compromiso de credenciales	2	5	10
		Ingeniería social	2	5	10
ACT-35	Auditor Informativo (Área de TI)	Acceso no autorizado a información	1	4	4
		Filtración de datos	2	5	10
		Errores en la auditoría	3	5	15
		Robo de información	1	5	5
ACT-36	Oficial de Seguridad Física y Electrónica (Área de TI)	Sabotaje físico	2	2	4
		Errores humanos	2	3	6
		Acceso no autorizado a sistemas	2	2	4
		Extorsión	4	5	20
		Falta de formación	2	3	6
ACT-37	Coordinador de Sistemas (Área de TI)	Errores humanos	2	4	8
		Acceso no autorizado a Sistemas	1	3	3
		Ingeniería Social	3	5	15

		Falta de formación	1	4	4
		Fallos en la toma de decisiones	2	4	8
ACT-38	Teléfono IP (Área de Cajas)	Interceptación de llamadas	2	2	4
		Vulnerabilidades de firmware	2	3	6
		Ataques de denegación de servicio	2	2	4
		Fallas de hardware	2	2	4
ACT-40	CPU (Área de Crédito 2)	Pérdida de datos financieros	3	3	9
		Fallas en disco duro	3	2	6
		Errores humanos	3	3	9
		Acceso no autorizado	2	2	4
ACT-41	teléfono IP (Área de Crédito 2)	Interceptación de llamadas	2	2	4
		Ataques de denegación de servicio	2	2	4
		Fallas de hardware	1	2	2
ACT-46	teléfono IP (Área de información)	Interceptación de llamadas	2	2	4
		Ataques de denegación de servicio	2	2	4
		Fallas de hardware	2	2	4
ACT-49	CPU (Coordinador de crédito)	Pérdida de datos financieros	2	5	10
		Fallas en disco duro	2	3	6
		Errores humanos	2	2	4
		Acceso no autorizado	2	3	6
ACT-51	Teléfono IP (Coordinador de crédito)	Interceptación de llamadas	2	2	4
		Ataques DoS	2	3	6
ACT-52	Teléfono Inalámbrico (Contabilidad)	Fallas en la señal	1	2	2
		Pérdida de conectividad	2	2	4
		Robo físico	2	2	4
ACT-53	CPU (Contabilidad)	Pérdida de datos financieros	2	3	6
		Fallas en disco duro	2	4	8
		Errores humanos	2	2	4
		Acceso no autorizado	3	4	12

ACT-54	Teléfono IP (Contabilidad)	Interceptación de llamadas	1	4	4
		Ataques DoS	2	4	8
ACT-55	Switch (Contabilidad)	Sobrecarga de red	3	3	9
		Fallas de hardware	1	4	4
		Ataques DDoS	2	5	10
		Errores de configuración	2	5	10
ACT-56	Router HP (Contabilidad)	Acceso no autorizado	3	5	15
		Ataques de enrutamiento	2	5	10
		Configuración incorrecta	1	5	5
		Fallos de actualización	2	5	10
ACT-57	GrandStrem (Centro de datos)	Interceptación de llamadas	2	2	4
		Vulnerabilidades de firmware	3	2	6
		Ataques de denegación de servicio	2	2	4
ACT-58	Switch (Centro de datos)	Sobrecarga de red	2	4	8
		Fallas de hardware	1	3	3
		Ataques DDoS	2	4	8
ACT-59	Convertidor de Fibra (Centro de datos)	Fallas en la transmisión de datos	1	3	3
		Vulnerabilidades en el hardware	2	3	6
		Sabotaje físico	2	3	6
		Errores en la configuración	1	2	2
		Pérdida de conectividad	2	1	2
ACT-60	NVR (Centro de datos)	Pérdida de grabaciones	1	5	5
		Ataques a la red	3	5	15
		Manipulación de videos	1	5	5
		Acceso no autorizado	4	5	20
ACT-61	CPU (Centro de datos)	Pérdida de datos críticos	2	5	10
		Fallas en disco duro	2	5	10
		Malware	1	5	5
		Acceso no autorizado	2	5	10
	FIREWALL	Fallos en la configuración	2	4	8

ACT-62	(Centro de datos)	Ataques de desbordamiento	3	5	15
		Vulnerabilidades en el firmware	2	3	6
		Sobrecarga de tráfico	3	4	12
		Acceso no autorizado	3	4	12
ACT-64	Servidor	Interrupción por pérdida de alimentación	3	5	15
		Configuración incorrecta	2	3	6
		Acceso no autorizado	3	3	9
ACT-65	Receptor GSM (Centro de datos)	Interferencia en la señal	2	2	4
		Acceso no autorizado	2	4	8
		Sabotaje físico	1	3	3
ACT-66	DISCO DURO (Centro de datos)	Pérdida de datos	2	3	6
		Sobrecarga de almacenamiento	2	3	6
		Fallas mecánicas	1	3	3
		Ransomware	2	4	8
		Robo Físico	3	5	15

El análisis de riesgos presentado revela una matriz de amenazas críticas que afectan principalmente a los activos del Área de TI y el Centro de Datos. Los riesgos más severos, con valores de 15 a 20, se concentran en equipos de red, sistemas de almacenamiento y personal clave. Destacan los ataques DDoS al switch TP-LINK y la posible extorsión a los oficiales de seguridad, ambos con un riesgo máximo de 20. Los dispositivos NVR, routers y firewalls presentan vulnerabilidades significativas ante accesos no autorizados y ataques de red, con riesgos de 15. La infraestructura de almacenamiento, incluyendo CPUs y discos duros, muestra susceptibilidad a pérdidas de datos y robos físicos. El factor humano emerge como un punto crítico, evidenciado por los altos riesgos asociados a errores en auditorías y manipulación de datos financieros.

La seguridad de las comunicaciones también se ve comprometida, con amenazas de interceptación en sistemas VoIP. Este panorama subraya la necesidad de implementar medidas robustas de ciberseguridad, incluyendo sistemas avanzados de detección y prevención de intrusiones, políticas estrictas de control de acceso, cifrado de datos sensibles, y programas intensivos de capacitación en seguridad para el personal. Además,

se requiere fortalecer la seguridad física de los activos críticos y establecer protocolos de respuesta a incidentes para mitigar el impacto de posibles brechas de seguridad. Es crucial implementar un enfoque de seguridad en capas, que abarque desde la protección perimetral hasta la seguridad a nivel de aplicación, complementado con auditorías regulares de seguridad y pruebas de penetración para identificar y corregir vulnerabilidades de manera proactiva. La gestión de riesgos debe ser un proceso continuo y dinámico, adaptándose a las nuevas amenazas emergentes en el panorama de la ciberseguridad.

4.3.2.4. Controles/Salvaguardas

En respuesta al análisis de riesgos detallado, es imperativo establecer un conjunto robusto de controles y salvaguardas para mitigar las amenazas identificadas y proteger los activos críticos de la organización. Estos mecanismos de seguridad se diseñan para abordar las vulnerabilidades específicas reveladas en el análisis, con un enfoque en la prevención, detección y respuesta a incidentes de seguridad. Los controles propuestos abarcan medidas técnicas, procedimentales y organizativas, creando un marco de seguridad integral que se alinea con las mejores prácticas de la industria y los estándares regulatorios aplicables.

A continuación, se presenta una serie de controles estratégicos destinados a fortalecer la postura de seguridad de la organización y reducir significativamente los niveles de riesgo identificados.

Tabla 10. Controles. Fuente: Autoría Propia

ID	Activo	Amenaza	Riesgo	Control
ACT-01	Switch TP-LINK (Área de TI)	Ataques DDoS	20	Implementar firewalls con filtrado de tráfico y limitar el ancho de banda para mitigar DDoS.
ACT-02	Router MIKROTIK (Área de TI)	Acceso no autorizado	15	Configurar autenticación multifactorial y utilizar contraseñas robustas para acceso al router.

ACT-06	NVR HIKVISION (Área de TI)	Ataques a la red	15	Segmentar la red y aplicar cifrado en las comunicaciones del NVR para prevenir accesos no autorizados.
ACT-07	CPU GENÉRICO (Área de Cajas)	Errores humanos	15	Capacitar al personal en prácticas de seguridad y realizar auditorías periódicas de acceso.
ACT-11	Acceso Biométrico ZKTeco (Área de Cajas)	Robo de datos personales	15	Implementar cifrado de datos biométricos y monitoreo continuo de accesos para detectar anomalías.
		Interrupciones de servicio	15	Implementar redundancia en el hardware y sistemas de respaldo para garantizar la continuidad del servicio.
ACT-14	Laptop (Gerencia)	Ataques de phishing	15	Capacitar al personal sobre el reconocimiento de correos de phishing y utilizar filtros antispam avanzados.
		Acceso no autorizado	15	Capacitar al personal sobre el reconocimiento de correos de phishing y utilizar filtros antispam avanzados.
ACT-19	Router MIKROTIK (responsable de oficina)	Ataques de enrutamiento	15	Configurar políticas de enrutamiento seguras y mantener el firmware actualizado.
ACT-20	Router DLINK (responsable de oficina)	Acceso no autorizado	15	Implementar control de acceso basado en roles y autenticación multifactorial.
ACT-23	Intercomunicador (Área de Cajas)	Ataques de enrutamiento	15	Segmentar la red y actualizar las configuraciones de seguridad en el enrutador del intercomunicador.

		Ataques a la red	15	Utilizar VPNs y cifrado en las comunicaciones del intercomunicador para proteger la integridad de la red.
ACT-29	NVR (Área de Cajas)	Acceso a la red	20	Implementar políticas estrictas de acceso a datos sensibles y monitoreo continuo de las actividades del NVR.
ACT-32	Laptop (Área de Cajas)	Errores en la auditoría	15	
ACT-34	Oficial de Seguridad de la Información (Área de TI)	Extorsión	20	Establecer procedimientos de respuesta a incidentes y capacitar al personal sobre técnicas de manipulación social.
ACT-35	Auditor Informativo (Área de TI)	Errores en la auditoría	15	Automatizar procesos de auditoría y utilizar herramientas de verificación de consistencia de datos.
ACT-36	Oficial de Seguridad Física y Electrónica (Área de TI)	Extorsión	20	Implementar protocolos de respuesta a incidentes y capacitación en prevención de extorsión.
ACT-37	Coordinador de Sistemas (Área de TI)	Ingeniería Social	15	Capacitación continua en seguridad para evitar ataques de ingeniería social y manipulación.
ACT-56	Router HP (Contabilidad)	Acceso no autorizado	15	Uso de autenticación multifactorial y monitoreo constante de accesos para detectar anomalías.
ACT-60	NVR (Centro de datos)	Acceso no autorizado	20	Implementar cifrado de datos y controles de acceso robustos con autenticación multifactorial.

ACT-61	CPU (Centro de datos)	Acceso no autorizado	15	Uso de contraseñas seguras y cifrado de datos almacenados en la CPU.
ACT-62	FIREWALL (Centro de datos)	Ataques de desbordamiento	15	Configurar límites de tráfico y realizar auditorías regulares de reglas y configuraciones.
ACT-64	Servidor	Interrupción por pérdida de alimentación	15	Implementar sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo.
ACT-66	DISCOS DUROS (Centro de datos)	Robo físico	15	Uso de seguridad física, como cerraduras y cámaras, y cifrado de datos en caso de robo.

La implementación de controles efectivos es esencial para mitigar los riesgos identificados en la infraestructura de TI de la Cooperativa de Ahorro y Crédito Yuyay Ltda. Una de las ventajas significativas que posee la COAC Yuyay es contar con profesionales capacitados en ciberseguridad, lo que facilita la formación continua del personal en prácticas de seguridad y la implementación adecuada de los controles propuestos.

Cada control ha sido seleccionado en función de su capacidad para abordar las amenazas específicas identificadas en el análisis de riesgos. Por ejemplo, para mitigar los riesgos de acceso no autorizado en routers, se propone la implementación de autenticación multifactorial (MFA), un control reconocido por su eficacia en fortalecer la seguridad del acceso a sistemas críticos. Cabe mencionar que, dado que la COAC Yuyay cuenta con profesionales especializados en ciberseguridad, estos expertos liderarán la implementación de los controles, asegurando que se apliquen correctamente y que todos los empleados reciban la capacitación necesaria. El proceso de implementación incluirá la configuración técnica del MFA en los routers y sesiones de formación para que el personal aprenda a utilizar este sistema de manera efectiva.

La implementación de estos controles no solo reducirá el riesgo asociado con el acceso no autorizado, sino que también fomentará una cultura organizacional más

consciente de la seguridad. La capacitación continua del personal y la presencia de un equipo de ciberseguridad dedicado aseguran que la cooperativa esté preparada para responder de manera efectiva a cualquier amenaza futura.

4.3.2.5. Plan de implementación

El presente apartado detalla las etapas necesarias para llevar a cabo de manera efectiva los controles propuestos en la gestión de riesgos de TI. Este plan se organiza en fases, desde la preparación inicial y la planificación, hasta la implementación técnica, la capacitación del personal, y el monitoreo continuo de los controles. Cada fase está diseñada para asegurar que la Cooperativa Yuyay Ltda. integre los nuevos controles de manera estructurada, garantizando la seguridad y resiliencia de su infraestructura tecnológica.

1. **Fase 1: Preparación y planeación**

Formación del equipo de proyecto:

La formación del equipo de proyecto es un paso crucial en la fase de preparación y planeación, ya que el éxito de la implementación depende de contar con un equipo multidisciplinario con las habilidades y conocimientos necesarios. A continuación, se detalla la estructura del equipo y las responsabilidades de cada miembro:

Tabla 11. Formación del equipo de trabajo. Fuente: Autoría Propia

Rol	Responsabilidades	Perfil requerido
Líder de Proyecto	Coordinar todas las actividades del proyecto, asegurar el cumplimiento de plazos y objetivos, y servir como enlace entre el equipo y la alta dirección.	Experiencia en gestión de proyectos de TI y liderazgo.
Especialista en Ciberseguridad	Implementar los controles técnicos, realizar auditorías de seguridad y capacitar al personal en ciberseguridad.	Certificaciones en ciberseguridad (CISSP, CISM) y experiencia en seguridad de redes y sistemas.
Administrador de Sistemas	Gestionar la infraestructura tecnológica, implementar cambios en	Experiencia en administración de sistemas y gestión de servidores.

	los sistemas y asegurar la continuidad operativa durante la implementación.	
Analista de Riesgos	Evaluar los riesgos asociados con la implementación, realizar análisis de impacto y apoyar en la priorización de actividades.	Conocimiento en gestión de riesgos y análisis de impacto.
Responsable de Capacitación	Desarrollar y coordinar programas de capacitación para el personal, asegurando que comprendan y apliquen los nuevos controles.	Experiencia en desarrollo de programas de formación y habilidades de comunicación.
Soporte Técnico	Proveer asistencia técnica durante la implementación, resolver problemas técnicos y asegurar el correcto funcionamiento de las soluciones implementadas.	Experiencia en soporte técnico y resolución de problemas de hardware/software.

Cronograma del Proyecto

El cronograma es un componente esencial que detalla las actividades a realizar durante la implementación, asignando tiempos específicos para cada tarea y estableciendo hitos importantes.

Tabla 12. Cronograma del proyecto. Fuente: Autoría Propia

Actividad	Duración	Fecha Inicio	Fecha de Finalización	Responsable
Formación del Equipo de Proyecto	1 semana	01-10-2024	07-10-2024	Líder de Proyecto
Revisión y Ajuste de Políticas Internas	2 semanas	08-10-2024	21-10-2024	Especialista en Ciberseguridad

Identificación y Adquisición de Recursos	2 semanas	22-10-2024	05-11-2024	Administrador de Sistemas
Desarrollo del Cronograma Detallado	1 semana	06-11-2024	12-11-2024	Líder de Proyecto
Evaluación de Riesgos Previos a la Implementación	1 semana	13-11-2024	19-11-2024	Analista de Riesgos
Preparación de Programas de Capacitación	2 semanas	20-11-2024	02-12-2024	Responsable de Capacitación
Revisión Final y Aprobación del Plan	1 semana	03-12-2024	09-12-2024	Líder de Proyecto

Identificación de recursos

Para la implementación efectiva del sistema de gestión de riesgos de TI en la Cooperativa Yuyay Ltda., es esencial identificar y asegurar los recursos necesarios que permitirán la ejecución de cada fase del proyecto. Estos recursos pueden clasificarse en humanos, tecnológicos, y financieros.

1. Recursos Humanos

- **Profesionales de Ciberseguridad**: Especialistas en seguridad informática que liderarán la implementación de controles y realizarán auditorías de seguridad.
- **Personal de TI**: Administradores de sistemas y soporte técnico encargados de la implementación técnica y mantenimiento de la infraestructura.
- **Capacitadores**: Responsables de desarrollar e impartir programas de formación para el personal.

2. Recursos Tecnológicos

- **Software de Seguridad**: Herramientas de autenticación multifactorial, firewalls, y sistemas de detección de intrusos (IDS) para reforzar la seguridad de la red y los sistemas.

- **Hardware**: Equipos adicionales como servidores, routers, y dispositivos de almacenamiento seguros, necesarios para implementar y respaldar los controles.
- **Plataformas de Capacitación**: Herramientas y sistemas de gestión de aprendizaje (LMS) para la formación del personal, que permitan la creación de módulos interactivos y seguimiento del progreso.

3. Recursos Financieros

- **Presupuesto para Adquisiciones**: Fondos necesarios para la compra de software, hardware, y otros recursos tecnológicos.
- **Presupuesto para Capacitación**: Recursos destinados a la formación del personal, incluyendo costos de materiales, herramientas educativas y contratación de expertos externos si es necesario.
- **Presupuesto para Consultoría**: Fondos destinados a la contratación de consultores especializados en ciberseguridad y gestión de riesgos para asesorar en la implementación.

4. Recursos Organizacionales

- **Políticas y Procedimientos**: Documentación existente que debe revisarse y ajustarse para alinearse con los nuevos controles de seguridad.
- **Infraestructura de TI**: Sistemas y redes actuales que servirán como base para la implementación de los controles propuestos.

La identificación y aseguramiento de los recursos antes mencionados, es crucial para garantizar que el proyecto se ejecute sin contratiempos, permitiendo que la Cooperativa Yuyay Ltda. logre una implementación exitosa del sistema de gestión de riesgos de TI.

2. **Fase 2: Implementación Técnica**

- **Objetivo**: Desplegar los controles técnicos en la infraestructura de TI de la cooperativa.
- **Actividades**:
    - Configuración e implementación de la autenticación multifactorial en todos los sistemas críticos.

- Segmentación de la red para aislar y proteger los activos más sensibles.
- Instalación y configuración de firewalls y sistemas de detección de intrusos (IDS).
- Implementación de sistemas de respaldo automatizado para los datos críticos.
- Capacitación técnica para el personal de TI sobre los nuevos sistemas y herramientas.

3. Fase 3: Capacitación y Concienciación

- **Objetivo**: Asegurar que todos los empleados comprendan y puedan cumplir con los nuevos controles de seguridad.
- **Actividades**:
  - Desarrollo e implementación de un programa de capacitación sobre ciberseguridad, dirigido a todo el personal.
  - Realización de talleres específicos para la alta dirección y los responsables de áreas críticas.
  - Distribución de materiales educativos, como guías y manuales de uso, para apoyar el aprendizaje continuo.
  - Evaluación del nivel de comprensión de los empleados mediante pruebas y simulaciones.

4. Fase 4: Monitoreo y Evaluación Inicial

- **Objetivo**: Evaluar la efectividad de los controles recién implementados y ajustar según sea necesario.
- **Actividades**:
  - Monitoreo continuo del tráfico de red y accesos a los sistemas críticos.
  - Realización de auditorías de seguridad para evaluar la eficacia de los controles implementados.
  - Revisión de incidentes de seguridad para identificar áreas de mejora.

- Ajuste de las configuraciones de seguridad en función de los resultados de las auditorías y monitoreos.

5. Fase 5: Revisión y Optimización Continua

- **Objetivo**: Garantizar que los controles de seguridad sigan siendo efectivos ante nuevas amenazas y cambios en la infraestructura.
- **Actividades**:
  - Establecimiento de un ciclo de revisión trimestral para evaluar y actualizar los controles de seguridad.
  - Integración de nuevos controles o tecnologías según sea necesario.
  - Capacitación continua del personal en nuevas amenazas y mejores prácticas de seguridad.
  - Documentación y comunicación de cualquier cambio en las políticas o procedimientos de seguridad.

CONCLUSIONES

A través del desarrollo de un marco teórico sólido, se logró establecer una comprensión sólida de los conceptos clave y las metodologías más relevantes en la gestión de riesgos de TI. Al explorar y analizar estándares como ISO 31000, COBIT y MAGERIT, se ofreció un panorama exhaustivo de las prácticas actuales en el manejo de riesgos tecnológicos. Este análisis no solo sirvió como base conceptual para la propuesta, sino que también facilitó la identificación de las metodologías más adecuadas para ser implementadas en el contexto de la Cooperativa Yuyay Ltda.

Además, el diagnóstico realizado reveló la situación actual de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda., mostrando tanto fortalezas como debilidades en su infraestructura tecnológica y sistemas de información. A través de un análisis detallado, se identificaron vulnerabilidades críticas que podrían comprometer la seguridad y continuidad operativa de la cooperativa. Este diagnóstico subrayó la falta de un sistema formalizado de gestión de riesgos y la necesidad urgente de establecer controles y procesos adecuados para mitigar los riesgos identificados.

Finalmente, con base en los hallazgos del diagnóstico, se diseñó una propuesta integral para la implementación de un sistema de gestión de riesgos de TI, adaptado específicamente a las necesidades y capacidades de la Cooperativa Yuyay Ltda. La propuesta incluye estrategias de mitigación efectivas, como la implementación de controles de seguridad tecnológica, y planes de respuesta a incidentes que aseguran una reacción oportuna ante posibles eventos adversos. Además, se recomendó un enfoque continuo de monitoreo y revisión, garantizando que el sistema de gestión de riesgos evolucione con las nuevas amenazas y cambios en el entorno tecnológico.

RECOMENDACIONES

Se recomienda a la COAC. Yuyay Ltda.:

- Priorizar la implementación de los controles propuestos en la tesis, como la autenticación multifactorial y la segmentación de redes, para mitigar los riesgos identificados y fortalecer la seguridad de la infraestructura tecnológica.
- Aprovechar la ventaja de contar con profesionales en ciberseguridad para desarrollar programas de capacitación continua para todos los empleados, enfocándose en la concientización sobre ciberseguridad y en la correcta aplicación de los controles.
- Establecer un sistema de monitoreo continuo que permita la revisión periódica de los controles implementados, asegurando que se mantengan efectivos ante posibles nuevas amenazas y cambios tecnológicos.
- Considerar la inversión en tecnologías de última generación que refuercen la protección de los sistemas críticos y mejoren la capacidad de respuesta ante incidentes.

A la Universidad Católica de Cuenca, Extensión Cañar, Carrera de Ingeniería en Sistemas de Información:

- Incentivar la realización de proyectos prácticos que aborden problemas reales de empresas locales, como lo realizado en esta tesis, fortaleciendo así la relación entre la teoría y la práctica.
- Se recomienda incentivar a los estudiantes a realizar investigaciones sobre ciberseguridad y gestión de riesgos de TI, abordando problemas locales y globales. Creando laboratorios especializados donde se pueda practicar la gestión de riesgos en entornos controlados.

BIBLIOGRAFÍA

Aguirre Sánchez, M. J. (01 de 01 de 2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/handle/123456789/20566

Alsmadi, T., & Alqudah, N. (2021). Encuesta sobre técnicas de detección de malware. *Conferencia internacional sobre tecnología de la información (ICIT)*, 371-376.

ARCOTEL. (18 de 12 de 2023). *www.arcotel.gob.ec.* Obtenido de www.arcotel.gob.ec: https://www.arcotel.gob.ec/wp-content/uploads/2023/12/2.2-181223-OFICIO-DR-1095-2023-OBSERVACIONES-PRI-2024-signed.pdf

Avila Irigoin, J. P., & Caloggero Sangama, C. T. (01 de 01 de 2022). *repositorio.ucv.edu.pe.* Obtenido de repositorio.ucv.edu.pe: https://repositorio.ucv.edu.pe/handle/20.500.12692/93690

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

Cazar, J. C., & Contero, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *ominio De Las Ciencias*, 1025-1041.

CLUSIF. (01 de 01 de 2010). *clusif.fr.* Obtenido de clusif.fr: https://clusif.fr/wp-content/uploads/2015/10/mehari-2010-introduccion.pdf

Colegio Oficial de Ingenieros de Telecomunicación. (05 de 09 de 2016). *www.coit.es.* Obtenido de www.coit.es: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Dand, P., & Chudasama, D. (2021). Vulnerability . *International Journal of Wireless Network Security* , 1-6.

ENISA. (25 de 05 de 2024). *www.enisa.europa.eu*. Obtenido de www.enisa.europa.eu: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

Enrique, M. G. (2023). *Seguridad de Equipos Informáticos. Edición 2024.* Ra-Ma S.A. Editorial y Publicaciones.

Gobierno de España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Grishaeva, S. A., & Borzov, V. I. (2020). Gestión de riesgos de seguridad de la información. *Congreso internacional gestión de calidad, transporte y seguridad de la información, tecnologías de la información (IT&QM&IS)*, 96-98.

Harefa, W., & Hartomo, K. D. (2022). Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang. *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Kompute*, 389-396.

Hernández Benítez, J. M. (01 de 06 de 2021). *openaccess.uoc.edu.* Obtenido de openaccess.uoc.edu: https://openaccess.uoc.edu/handle/10609/132629

Iparraguirre-Villanueva, O., Obregon-Palomino, L., Pujay-Iglesias, W., & Cabanillas-Carbonell, M. (2023). Agente inteligente para la gestión de incidencias. *Revista Ibérica de Sistemas de Tecnologias de Información*, 99-115.

ISACA. (2012). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.* ISACA.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* ISACA.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* ISACA.

ISACA. (2013). *COBIT 5 for Assurance.* ISACA.

Ismagilova, E., Laurie Hughes, N. P., & Dwivedi, Y. K. (2020). Seguridad, privacidad y riesgos dentro de las ciudades inteligentes: revisión de la literatura y desarrollo de un marco de interacción de ciudades inteligentes. *Fronteras de los sistemas de información*, 393-414.

ISO / IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

Kumar, A., Abhishek, K., Ghalib, S., & Shankar, A. (2022). Sistema de detección y prevención de intrusiones para un entorno IoT. *Comunicaciones y redes digitales*, 540-551.

Liendo Afonso, L. C. (01 de 07 de 2023). *titula.universidadeuropea.com.* Obtenido de titula.universidadeuropea.com: https://titula.universidadeuropea.com/handle/20.500.12880/5414

Linares Vasquez, W. E. (01 de 01 de 2023). *tesis.usat.edu.pe.* Obtenido de tesis.usat.edu.pe: https://tesis.usat.edu.pe/handle/20.500.12423/6364

Mamami, R. G., Ancco, R. C., & Argollo, R. R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innov. softw.*, 96-106.

Marín Hernández, H. S. (31 de 05 de 2021). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/handle/46000/5867

Möller, D. P. (2023). Detección y prevención de intrusiones. En D. P. Möller, *Guía de Ciberseguridad en la Transformación Digital. Avances en seguridad de la información* (págs. 131-179).

Montalbán, E. A., Gómez, R. J., & Borré, D. A. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Uninunez*, 227-245.

Moya, J. G. (2023). La importancia de la seguridad informática en la educación digital, retos y soluciones. *RECIMUNDO: Revista Científica de la Investigación y el Conocimiento*, 609-616.

Payá Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova*, 1122-1136.

Ramírez Loría, L. (01 de 03 de 2021). *repositorio.usam.ac.cr.* Obtenido de repositorio.usam.ac.cr: https://repositorio.usam.ac.cr/xmlui/handle/11506/2365

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., . . . Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensores*, 4060.

Rodríguez, G. R., Fernández, R. A., & Santos, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Innov. softw*, 219-236.

Syed, R. (2020). Gestión de vulnerabilidades en ciberseguridad: una ontología conceptual y un sistema de alerta de ciberinteligencia. *Información y gestión*, 103334.

Velthuis, M. G. (2008). *Auditoría de Tecnologías y Sistemas de Información.* RA-MA.

ANEXOS

A. TÍTULO

Propuesta para la Implementación de Sistemas de Gestión de Riesgos de TI para la Cooperativa Yuyay Ltda.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN

Tecnología de información y comunicación	Energía eléctrica y tecnologías de información para la innovación y el desarrollo sostenible	Inteligencia de negocio	
		Auditoria y seguridad informática	
		Gobierno de TI	
		Gestión de riesgo de TI	X
		Redes y comunicación	
		Inteligencia de requerimientos	
		Arquitectura de Desarrollo de Software	

C. PLANTEAMIENTO DEL PROBLEMA

En la era digital actual, la dependencia de las tecnologías de la información (TI) es crucial para la operación y el crecimiento sostenible de las organizaciones. Sin embargo, esta dependencia también expone a las organizaciones a una variedad de riesgos inherentes que pueden comprometer la seguridad, la eficiencia y la integridad de sus operaciones. En el caso de la Cooperativa Yuyay Ltda., una entidad que desempeña un papel vital en el desarrollo económico y social del cantón Cañar, la gestión de riesgos de TI no ha sido completamente formalizada ni estructurada. Esto representa una vulnerabilidad significativa, especialmente en un contexto donde las amenazas cibernéticas y los fallos tecnológicos están en aumento.

Actualmente, la cooperativa enfrenta desafíos significativos relacionados con la seguridad de la información, la continuidad del negocio y la conformidad con regulaciones nacionales e internacionales. La falta de un sistema formal de gestión de riesgos de TI impide que la cooperativa identifique, evalúe y mitigue adecuadamente los riesgos potenciales, lo que podría resultar en interrupciones operativas, pérdidas financieras, o daños a su reputación.

La necesidad de implementar un sistema de gestión de riesgos de TI en la Cooperativa Yuyay

Ltda. es evidente, y la ausencia de dicho sistema plantea preguntas críticas sobre la capacidad de la cooperativa para manejar efectivamente los riesgos tecnológicos en un entorno cada vez más digitalizado y regulado. Por lo tanto, esta tesis buscará desarrollar una propuesta para la implementación de un sistema de gestión de riesgos de TI que sea robusto, escalable y adaptado a las necesidades específicas de la cooperativa, asegurando así la resiliencia y la sostenibilidad de sus operaciones en el futuro.

D. OBJETIVO GENERAL

Desarrollar una propuesta para la implementación de un sistema de gestión de riesgo de TI que permita a la Cooperativa Yuyay Ltda.

E. OBJETIVOS ESPECÍFICOS

1. Elaborar un marco teórico que describa los conceptos fundamentales y las metodologías existentes sobre la gestión de riesgos de TI.
2. Diagnosticar el estado actual de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda. mediante una evaluación detallada de sus sistemas de información y tecnologías empleadas.
3. Diseñar una propuesta detallada para la implementación de un sistema de gestión de riesgos de TI que incluya estrategias de mitigación, planes de respuesta a incidentes y recomendaciones para el monitoreo continuo.

F. JUSTIFICACIÓN

La gestión eficiente de los riesgos de Tecnologías de la Información (TI) es crucial para la sostenibilidad y el crecimiento estratégico de cualquier organización en el contexto actual, donde la tecnología desempeña un papel central en todas las actividades empresariales. En el caso de la Cooperativa Yuyay Ltda., una entidad clave en el desarrollo económico y social del cantón Cañar, la adopción de un sistema formalizado de gestión de riesgos de TI no es solo una necesidad operativa, sino también una estrategia crítica para su evolución y protección en el ambiente digital.

Implementar un sistema de gestión de riesgos de TI robusto ayudará a la cooperativa a protegerse contra las vulnerabilidades de seguridad cibernética y los fallos tecnológicos, asegurando la integridad, disponibilidad y confidencialidad de la información crítica. Esto es fundamental para mantener la continuidad de las operaciones y minimizar el impacto financiero y operativo de cualquier incidente de seguridad. A medida que aumentan las regulaciones sobre protección de datos y seguridad cibernética, la Cooperativa Yuyay Ltda. debe asegurarse de cumplir con estos requerimientos legales. La implementación de un sistema de gestión de riesgos de TI no solo ayudará a cumplir con estas normativas, sino que también mejorará la reputación de la cooperativa como una entidad segura y confiable, esencial para atraer y retener a los socios y clientes.

Al establecer un entorno de TI seguro y gestionado, la Cooperativa Yuyay Ltda. estará mejor equipada para adoptar nuevas tecnologías que pueden ofrecer ventajas competitivas, como mejoras en la eficiencia operativa, nuevas capacidades de servicio al cliente y expansión a nuevos mercados. Este enfoque proactivo en la gestión de riesgos de TI también fomenta una

cultura de innovación y mejora continua. En resumen, la propuesta para implementar un sistema de gestión de riesgos de TI en la Cooperativa Yuyay Ltda. es esencial no solo para la protección contra riesgos y amenazas actuales, sino también para asegurar un crecimiento estratégico y sostenible en el futuro. Esta inversión en la gestión de riesgos de TI es, por lo tanto, una decisión estratégica que fortalecerá la posición de la cooperativa en un mercado cada vez más tecnológico y regulado.

G. ALCANCE

El estudio se centrará exclusivamente en la Cooperativa Yuyay Ltda., ubicada en el cantón Cañar. Las actividades de investigación, evaluación de riesgos y propuestas de implementación se realizarán dentro de las instalaciones y sistemas informáticos que opera la cooperativa.
El estudio no abordará:

- La implementación física y operacional completa del sistema de gestión de riesgos de TI; se centrará en la fase de diseño y propuesta.
- Aspectos de gestión de riesgos no relacionados directamente con las TI, como riesgos financieros, legales o de mercado, a menos que estén directamente relacionados con la gestión de las tecnologías de la información.
- Evaluaciones de riesgo en áreas que no están directamente bajo el control o influencia de la infraestructura TI de la cooperativa

H. CONCEPTOS RELACIONADOS

Gestión de Riesgos de TI

Se refiere al proceso de identificación, evaluación, mitigación y control de los riesgos asociados con el entorno de tecnología de la información de una organización. Esto incluye la protección de la infraestructura, los datos y las operaciones contra posibles amenazas que podrían afectar la continuidad y eficiencia de los servicios de TI (Flores Cortez, 2023).

Riesgo

De acuerdo con Colina & Túa (2020):

En el contexto de TI, un riesgo es la posibilidad de que ocurra un evento que tenga un impacto negativo en los objetivos y operaciones de la organización. Esto puede incluir riesgos relacionados con la seguridad cibernética, fallos de hardware o software, pérdidas de datos, entre otros.

Vulnerabilidad

Una debilidad en un sistema que puede ser explotada por una amenaza para causar daño a la organización. Las vulnerabilidades pueden ser técnicas, como un software sin actualizar, o procesales, como la falta de capacitación en seguridad para los empleados (Gómez, 2022).

Amenaza

Cualquier circunstancia o evento con el potencial de causar daño a un sistema de TI o a la información que maneja. Las amenazas pueden ser internas (por ejemplo, empleados descontentos) o externas (por ejemplo, hackers, desastres naturales) (Arango Gomez, 2023).

Impacto

Es la consecuencia de un evento de riesgo si este llega a materializarse. El impacto puede ser medido en términos financieros, de reputación, legales, entre otros, y es clave para determinar la gravedad del riesgo.

Mitigación de Riesgos

Las acciones que se toman para reducir la probabilidad o el impacto de un riesgo. Esto puede incluir la implementación de nuevas tecnologías de seguridad, cambios en los procesos o capacitaciones para los empleados (Ordinola Del Castillo, 2021).

Evaluación de Riesgos

El proceso de determinar la probabilidad y el impacto de un evento de riesgo, lo que ayuda a priorizar los riesgos según su severidad potencial. Es un paso crítico en el proceso de gestión de riesgos. **ISO 27001**

Una norma internacional que describe cómo gestionar la seguridad de la información. Proporciona un marco de políticas y procedimientos que incluye todos los controles legales, físicos y técnicos implicados en la gestión de riesgos de seguridad de la información de una organización (Sánchez, Carrillo, & Campuzano, 2022) (nqa, 2019).

ISO 31000

Norma internacional que proporciona directrices para la gestión de riesgos. Ofrece un enfoque estructurado para la implementación de la gestión de riesgos en una organización, independientemente de su tamaño, tipo o sector (ISO, 2018).

COBIT

Un marco de referencia para la gestión y gobernanza de las TI empresariales que ayuda a las organizaciones a crear valor óptimo de TI mediante el mantenimiento de un equilibrio entre la realización de beneficios y la optimización de niveles de riesgo y uso de recursos (ISACA, 2023).

I. TRABAJOS RELACIONADOS

En el año (2022) en el trabajo de titulación, realiza una investigación sobre los riesgos operativos en la cooperativa de Ahorro y crédito CACEC Ltda., a través de un modelo computacional para evaluar la gestión de riesgos de TI COBIT en los cuales se ha utilizado técnicas de DM mediante la implementación de una herramienta llamada weka. Además, ayuda a que mediante la

tecnología se proteja la información con la que cuenta las entidades bancarias y disminuye los factores de riego.

Este estudio anterior demostró cómo la tecnología puede ser utilizada eficazmente para proteger la información en entidades bancarias y reducir los factores de riesgo asociados. La adaptación y aplicación de enfoques similares en Yuyay Ltda. no solo pueden mejorar la seguridad y eficacia de sus sistemas de información, sino también ofrecer una estrategia probada para la mitigación de riesgos, capitalizando en la experiencia y resultados obtenidos en CACEC Ltda.

Santolla (2022) afirma que la investigación reveló una deficiencia en la gestión de los procedimientos tecnológicos, los cuales carecen de una metodología efectiva para una gestión adecuada de TI. Esta falta de metodología obstaculiza la optimización de los recursos tecnológicos disponibles para los usuarios. Por lo tanto, se propone la aplicación de la metodología COBIT como solución para mejorar estos procedimientos y garantizar un control de las buenas prácticas en TI.

El estudio de Santolla destaca la importancia de adoptar un marco estructurado y probado como COBIT, que no solo optimiza los recursos tecnológicos mediante una gestión efectiva, sino que también mejora la gobernanza de TI y el control de riesgos. Para la Cooperativa Yuyay Ltda., la adopción de COBIT puede proporcionar un enfoque sistemático para identificar, evaluar y mitigar riesgos de TI, garantizando que los procedimientos tecnológicos sean manejados con las mejores prácticas y de acuerdo a estándares internacionales.

Zapata (2021) resalta la importancia estratégica de gestionar los riesgos de TI y la continuidad de los procesos del negocio para asegurar la efectividad y eficacia de los sistemas de gestión de la seguridad de la información. Se argumenta que la falta de estas herramientas en entidades financieras locales justifica la realización del trabajo de tesis. La investigación evidencia que la implementación de un modelo de gestión de riesgos, basado en estándares como ISO/IEC 27001 e ISO 17799 y la metodología MAGERIT, puede mejorar la evaluación y tratamiento de los riesgos de los activos de TI, cumpliendo con los requisitos de la SBS. Se tomó como estudio de caso la Agencia Metro Santa Elena del Banco Scotiabank en Chiclayo. Analizando los riesgos de TI que puede tener el sector financiero demostrando que tan eficiente es la seguridad TI.

Este documento es una herramienta valiosa para comprender la metodología MAGERIT y aplicarla al desarrollo de un SGIT para la Cooperativa Yuyay Ltda.

Barbosa (2020) manifiesta en su estudio la búsqueda de desarrollar un recurso que simplifique la adopción de un Modelo de ciberseguridad en consonancia con los marcos de gestión y gobierno de Tecnologías de la Información (TI), con el propósito de mejorar las deficiencias presentes en los sistemas de seguridad de la información de las instituciones financieras. Esto se realizará en cumplimiento de las regulaciones vigentes, con la intención de ser evaluado más adelante en el Banco Serfinanza ubicado en la ciudad de Barranquilla.

Este estudio aborda las deficiencias en los sistemas de seguridad de la información en instituciones financieras y propone una solución que no solo mejora estas deficiencias, sino que también cumple con las regulaciones vigentes. La aplicación de un modelo similar en la Cooperativa Yuyay Ltda. podría proporcionar una estructura robusta para fortalecer la seguridad de la información, alinear las prácticas de TI con los marcos de gestión reconocidos y garantizar el cumplimiento normativo.

Moncada en el año (2018) en su trabajo de investigación, tuvo como objetivo preparar a la cooperativa de ahorro y crédito ABC para una gestión efectiva de riesgos y para cumplir con los

requisitos regulatorios de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS). En primer lugar, la implementación de un sistema de gestión permitirá mejoras en la seguridad de la información, lo que beneficiará a todas las cooperativas de crédito y ahorro al mejorar el manejo de los procesos de negocio. En segundo lugar, la gestión efectiva de riesgos puede conducir a una reducción de costos mediante la optimización de recursos y un tratamiento adecuado de los riesgos. Finalmente, al mejorar la eficacia y reducir los costos, las cooperativas pueden generar beneficios adicionales en términos de marketing, lo que les permitirá diferenciarse en el mercado y fortalecer las relaciones con los clientes y proveedores.

En base a que este documento proporciona ejemplos de controles de seguridad que se utilizan para la protección de los activos de TI de la cooperativa; servirá como una guía para establecer el sistema de gestión de riesgos de TI a través de las buenas prácticas.

J. METODOLOGÍA

Esta investigación utilizará un enfoque mixto, combinando métodos cuantitativos y cualitativos. Esto permitirá no solo recolectar y analizar datos numéricos relacionados con incidentes de seguridad, fallos técnicos y otras métricas de riesgo, sino también entender las percepciones, experiencias y actitudes del personal y la gestión frente a los riesgos de TI. La combinación de ambos métodos proporcionará una comprensión más completa y profunda de los riesgos de TI que enfrenta la cooperativa y cómo abordarlos eficazmente. A través de un enfoque descriptivo, en el que se detallará las condiciones actuales y las prácticas de gestión de riesgos de TI en la Cooperativo Yuyay Ltda., estableciendo una línea base desde la cual se pueden realizar mejoras.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES			
		I	II	III	MEDIOS DE VERIFICACIÓN
1.	Elaborar un marco teórico que describa los conceptos fundamentales y las **metodologías** existentes sobre la gestión de riesgos de TI.				
1.1.	Investigar y analizar las teorías y modelos previos sobre gestión de riesgos de TI, incluyendo normativas internacionales como ISO 27001 e ISO 31000, así como metodologías específicas de la industria, como COBIT y ITIL.	X	X		Lista de documentos almacenados en la herramienta Zotero

1.2.	Análisis comparativo de las metodologías de gestión de riesgos de TI para identificar las más adecuadas para la cooperativa, basado en factores como relevancia, eficacia probada, y adaptabilidad.		X		Tabla comparativa de metodologías
2.	Diagnosticar el estado actual de la gestión de riesgos de TI en la Cooperativa Yuyay Ltda. mediante una evaluación detallada de sus sistemas de información y tecnologías empleadas.				
2.1.	Realizar encuestas al personal de TI		X		Encuestas/Entrevistas
2.2.	Evaluar la percepción de riesgos a través de matrices		X	X	Matriz
3.	Diseñar una propuesta detallada para la implementación de un sistema de gestión de riesgos de TI que incluya estrategias de mitigación, planes de respuesta a incidentes y recomendaciones para el monitoreo continuo.				
3.1.	Documento del plan de mitigación, listado de herramientas y tecnologías seleccionadas, descripción de procedimientos			X	Documento pdf
	operativos y políticas de seguridad.				
3.2.	Creación de planes de respuesta ante incidentes y protocolos de recuperación de desastres		X	X	Documento pdf

L. DECLARACIÓN FINAL

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

M. PARTICIPANTES

DIRECTOR:	Ing. José Antonio Carrillo Zenteno
ESTUDIANTE 1	Verónica Janeth Yupa Chimbo

N. FIRMAS DE RESPONSABILIDAD

Lugar:	Cañar
Fecha:	29-04-2024

Firmas:

Nombre: José Antonio Carrillo Zenteno CC:0103304531 **Director del Proyecto**	Nombre: Verónica Janeth Yupa Chimbo C.C.: 0350152534 **Estudiante / Egresado**

O. APROBACIÓN

Firmas:

Nombre:	**Nombre:**
CC:	**C.C:**
Primer Par revisor	**Segundo Par Revisor**

P. REFERENCIAS

Referencias

Arango Gomez, O. D. (2023). *El ABC de la seguridad informática: guía práctica para entender la seguridad digital.*

Flores Cortez, R. A. (01 de 01 de 2023). *repositorio.ucv.edu.pe.* Obtenido de repositorio.ucv.edu.pe: https://repositorio.ucv.edu.pe/handle/20.500.12692/107946

Gómez, Á. (2022). *Auditoría de seguridad informática.* Ediciones de la U.

ISACA. (01 de 01 de 2023). *www.isaca.org.* Obtenido de www.isaca.org: https://www.isaca.org/

ISO. (01 de 01 de 2018). *www.ramajudicial.gov.co.* Obtenido de www.ramajudicial.gov.co: https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486

nqa. (11 de 10 de 2019). *www.nqa.com.* Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-deimplantacion.pdf

Ordinola Del Castillo, D. L. (01 de 01 de 2021). *tesis.usat.edu.pe.* Obtenido de tesis.usat.edu.pe: https://tesis.usat.edu.pe/handle/20.500.12423/3859

Sánchez, M. A., Carrillo, J. M., & Campuzano, M. F. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. *Revista de Tecnologías de la Informática y las Telecomunicaciones*, 63-78.

Vargas, A. M., & Ollarves, J. J. (2020). Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI. *INNOVA Research Journal*, 196-213.

Universidad Católica de Cuenca

TERCER NIVEL
TN- 0023557

CAMBRIDGE UNIVERSITY PRESS

UC-CID-CAÑAR-2024-06.B1
17 de septiembre del 2024

UNIVERSIDAD CATÓLICA DE CUENCA
LA SECRETARÍA GENERAL Y LA DIRECCIÓN DEL CENTRO DE IDIOMAS

OTORGAN EL PRESENTE

CERTIFICADO

YUPA CHIMBO VERONICA JANETH

Quien ha cumplido con los requerimientos legales de suficiencia en Español como segunda lengua con el siguiente resultado:

Nivel de acuerdo al Marco Común Europeo de Referencia para las Lenguas (MCRL):
B1

Abg. Cristian Gavilanes B. Mgs.
CAÑAR SECRETARY

Lic. María José Carrión. Mgs.
CAÑAR CENTER COORDINATOR

Typed by	Lic. María José Carrión. Mgs.
Reviewed by	Lic. María José Carrión. Mgs.
Authorized by	Cañar Secretary

Universidad Católica de Cuenca
EXTENSIÓN CAÑAR
SECRETARÍA

Universidad Católica de Cuenca
Coordinación Cañar
Centro de Idiomas

TERCER NIVEL Universidad Católica de Cuenca

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Veronica Janeth Yupa Chimbo portador(a) de la cédula de ciudadanía Nº **0350152534** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Propuesta para la Implementación de Sistemas de Gestión de Riesgos de TI para la Cooperativa Yuyay Ltda"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **22 de noviembre del 2024**

F: .....

Veronica Janeth Yupa Chimbo

C.I. **0350152534**