UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA DE COMPUTACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"ACTUALIZACIÓN DEL ANÁLISIS DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN DE LA UNIDAD DE TECNOLOGÍA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO, BASADO EN EL INVENTARIO LEVANTADO POR LA UNIDAD DE SEGURIDAD LÓGICA EN EL AÑO 2022"

Trabajo de titulación previo a la obtención del título de Magíster en Computación con Mención en Seguridad Informática

Línea de investigación: Seguridad de la Información

AUTOR:

Andrés Patricio Mena Ger

DIRECTOR:

Ángel Gabriel Jaramillo Alcázar

Ibarra – Ecuador

2026

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
APELLIDOS Y NOMBRES:	Mena Ger Andrés Patricio

DATOS DE LA OBRA	
TÍTULO:	Actualización del análisis de riesgo de los activos de información de la unidad de tecnología de una Cooperativa de Ahorro y Crédito, basado en el inventario levantado por la unidad de seguridad lógica en el año 2022
AUTOR (ES):	Mena Ger Andrés Patricio
FECHA: DD/MM/AAAA	05/06/2026

SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	Magister en computación con mención en Seguridad Informática
DIRECTOR /ASESOR:	PhD. Ángel Gabriel Jaramillo Alcázar

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 5 días del mes de junio de 2026

EL AUTOR:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ANDRES PATRICIO MENA GER

Nombre: Andrés Patricio Mena Ger

CERTIFICACIÓN DEL DIRECTOR Y ASESOR DEL TRABAJO DE TITULACIÓN

Nos permitimos informar que revisado el Trabajo final de Grado "ACTUALIZACIÓN DEL ANÁLISIS DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN DE LA UNIDAD DE TECNOLOGÍA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO, BASADO EN EL INVENTARIO LEVANTADO POR LA UNIDAD DE SEGURIDAD LÓGICA EN EL AÑO 2022", del Maestrante: Andrés Patricio Mena Ger de la Maestría en Computación con Mención en Seguridad Informática, certificamos que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizamos su presentación para los fines legales pertinentes.

Ibarra, a los 15 días del mes de abril del 2026

	Nombres y Apellidos	**Firma**
Director	PhD. Ángel Jaramillo Alcázar	Validar únicamente en FirmaEC. Firmado electrónicamente por: ANGEL GABRIEL JARAMILLO ALCAZAR
Asesor	Msc. Diego Trejo España	Validar únicamente en FirmaEC. Firmado electrónicamente por: DIEGO JAVIER TREJO ESPAÑA

DEDICATORIA

Principalmente se lo dedico a mi madre, quien con su fuerza, lucha diaria, ejemplo de trabajo y constancia, me ha sabido inspirar siempre, y de la misma manera me ha sabido motivar en cada momento de mi vida, a ser un mejor ser humano, un mejor hijo, un mejor padre, se lo dedico madre por ese amor incondicional que me entrega cada día.

A mis hijos Jeannine y Samuel, quienes con solo su existencia me han dado fortaleza en este proceso académico, y me han motivado a alcanzar un peldaño más en mi vida.

A mi familia, quienes me han acompañado en este proceso con sus palabras de aliento.

Andrés Patricio Mena Ger

AGRADECIMIENTO

Agradezco a Dios, por hacer posible este proyecto académico, y abrir las puertas necesarias para que todo haya salido de la mejor manera con su bendición.

Agradezco a mi familia por esos momentos de apoyo incondicional, cuando el tiempo o la distancia, ha sido el mayor desafío en cada paso que he dado.

Agradezco a la institución que me permitió realizar este trabajo de posgrado, a través de su Gerente General y las áreas de Tecnología y Seguridad, quienes han brindado las facilidades para el correcto desarrollo de este trabajo académico.

Al director de tesis Phd. Ángel Jaramillo y Msc. Diego Trejo, por la paciencia y la generosidad en compartir sus conocimientos para el cumplimiento del presente estudio.

Gracias a la Universidad Técnica del Norte, por sus enseñanzas y aprendizajes adquiridos.

Andrés Patricio Mena Ger

ÍNDICE DE CONTENIDOS

PORTADA I
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA II
UNIVERSIDAD TÉCNICA DEL NORTE II
CERTIFICACIÓN DEL DIRECTOR Y ASESOR DEL TRABAJO DE TITULACIÓN IV
DEDICATORIA V
AGRADECIMIENTO VI
ÍNDICE DE CONTENIDOS VII
ÍNDICE DE TABLAS XI
ÍNDICE DE FIGURAS XII
ÍNDICE DE ANEXOS XIII
RESUMEN XIV
ABSTRACT XV
CAPÍTULO I 1
EL PROBLEMA DE INVESTIGACIÓN 1
1.1 Problema de investigación 1
1.1.1 Contextualización 1
1.1.2 Planteamiento del problema 2
1.2 Interrogantes de la investigación 5
1.3 Objetivos de la investigación 5
1.3.1 Objetivo general 5
1.3.2 Objetivos específicos 5
1.4 Hipótesis 6
1.5 Categorización de variables 6

1.6 Justificación 6
CAPÍTULO II 9
MARCO REFERENCIAL 9
2.1 Antecedentes 9
2.2 Marco Teórico 13
2.2.1 Seguridad de la información y ciberseguridad 13
2.2.1.1 Política de seguridad de la información 15
2.2.1.2 Gestión del ciclo de vida de los datos 15
2.2.1.3 Base de datos 16
2.2.2 Tipos de activos 17
2.2.2.1 Actividades y procesos del negocio 17
2.2.2.2 Activos de información 17
2.2.2.3 Hardware 19
2.2.2.4 Software 20
2.2.2.5 Redes 20
2.2.2.6 Personal 21
2.2.2.7 Sitio 21
2.2.3 Análisis de riesgos 22
2.2.3.1 Componentes del riesgo 23
2.2.3.2 Metodologías de Análisis de Riesgo 26
2.2.3.3 Gestión del riesgo 28
2.2.3.4 MAGERIT 28
2.2.3.5 ISO 27005 28
2.2.4 Método del Ciclo PDCA 29

2.3 Marco Legal 31
CAPÍTULO III 33
MARCO METODOLÓGICO 33
3.1 Descripción del área de estudio 33
3.2 Modelo metodológico 34
3.3 Tipo de investigación 35
3.3.1 Investigación bibliográfica 35
3.3.2 Investigación de campo 36
3.3.3 Investigación descriptiva 36
3.4 Metodología de análisis de riesgo fundamentados en ISO 27005 37
3.5 Procedimiento de investigación 37
3.5.1 Fase 1. Levantamiento de información de los activos 38
3.5.2 Fase 2. Priorización de los activos 39
3.5.3 Fase 3. Establecimiento de un inventario actualizado de activos de seguridad 39
3.6 Consideraciones bioéticas 40
CAPÍTULO IV 41
RESULTADOS Y DISCUSIÓN 41
4.1 Resultados de diagnóstico de la encuesta 41
4.1.1 Determinación del Alfa de Cronbach 43
4.1.2 Determinación del Chi-Cuadrado 45
4.1.3 Análisis de correlación 46
4.2 Resultados de diagnóstico de la entrevista 47
4.2.1 Entrevista a la Jefatura de la Tecnología de la Información 47
4.2.2 Entrevista a la Jefatura de Seguridad Física 48

4.2.3 Entrevista a la Jefatura de Seguridad Lógica 48
4.3 Diseñar un inventario 50
CAPÍTULO V 54
CONCLUSIONES Y RECOMENDACIONES 54
5.1 Conclusiones 54
5.2 Recomendaciones 55
REFERENCIAS 57
ANEXOS 65

ÍNDICE DE TABLAS

Tabla 1 Procesos de SGSI 30

Tabla 2 Estadística de elementos 44

Tabla 3 Estadística de fiabilidad 44

Tabla 4 Chi-Cuadrado 45

Tabla 5 Análisis de correlación 46

Tabla 6 Resumen de análisis de riesgo de activos de TI 51

ÍNDICE DE FIGURAS

Figura 1 Formas de las buenas prácticas de seguridad de datos 14

Figura 2 Gestión del Ciclo de Vida de los Datos 16

Figura 3 Tipos de activos primarios 17

Figura 4 Tipos de activos de soporte 19

Figura 5 Ejemplos de amenazas o peligrosidades comunes 23

Figura 6 Ejemplos de vulnerabilidades comunes 25

Figura 7 Ciclo PDCA 29

Figura 8 Ubicación de la Cooperativa de Ahorro y Crédito en Tulcán 33

Figura 9 Fases de investigación 38

Figura 10 Escala de interpretación del Alfa de Cronbach 43

ÍNDICE DE ANEXOS

Anexo 1. Resultado de los encuestados 65

Anexo 2. Explicación de activo por activo sobre la calificación de las amenazas, vulnerabilidades y riesgos detalladamente. 76

RESUMEN

El presente estudio se enfoca en la renovación del análisis de riesgos sobre los activos de datos de la Unidad de Tecnología de una entidad de ahorro y crédito, en un entorno en el que cada vez se observa una mayor digitalización del ámbito financiero. Este proceso, aunque mejora la eficiencia operativa, también eleva la vulnerabilidad ante amenazas tales como ataques cibernéticos, fraudes y colapsos tecnológicos, lo que implica reforzar los sistemas de protección y gestión de riesgos. El estudio se realizó desde una perspectiva mixta, empleando como herramienta fundamental, en la parte cuantitativa la información de las encuestas. Para evaluar la confiabilidad de la herramienta se utilizó el Alfa de Cronbach de 0.717, lo cual indica que existe una consistencia interna adecuada para investigaciones de tipo descriptivo; mientras que la parte cualitativa señala que el personal tiene percepciones críticas sobre la gestión de la seguridad de la información, destacando limitaciones en capacitación, políticas claras y gestión de riesgos. Se enfatiza la necesidad de reforzar la cultura organizacional en materia de seguridad y optimizar los procedimientos de control, así como la imperiosa urgencia de adoptar estrategias integrales para salvaguardar los activos de información. Los resultados evidencian que los recursos tecnológicos presentan niveles similares de evaluación en promedio, no obstante, existen fluctuaciones internas relacionadas con debilidades y amenazas concretas. Esto reafirma la necesidad de implementar métodos de análisis de riesgos recientes que permitan una correcta priorización de las acciones de seguridad. En conclusión, el análisis efectuado permite evidenciar la importancia de aplicar técnicas innovadoras en materia de protección de datos, dirigidas a fortalecer la seguridad de los recursos tecnológicos y disminuir potenciales incidentes que impacten la funcionalidad de la organización. El estudio constituye una sólida base para la toma de resoluciones en el ámbito de la gestión de riesgos y la seguridad informática.

PALABRAS CLAVES: análisis de riesgos; efectividad operativa; vulnerabilidad; recursos tecnológicos; seguridad informática

ABSTRACT

The present study focuses on the renewal of risk analysis on the data assets of the Technology Unit of a savings and credit entity, in an environment where there is an increasing digitalization of the financial sector. This process, although it improves operational effectiveness, also increases vulnerability to threats such as cyberattacks, fraud, and technological collapses, which implies strengthening protection and risk management systems. The study was conducted from a mixed perspective, using survey information as the fundamental tool in the quantitative part. To evaluate the reliability of the tool, a Cronbach's Alpha of 0.717 was used, indicating an adequate internal consistency for descriptive-type research; while the qualitative part indicates that the staff has critical perceptions about information security management, highlighting limitations in training, clear policies, and risk management. It is important to strengthen the culture of an organization in security and improve control processes. It is also important to act quickly to protect assets of information with comprehensive strategies. The results show that, on average, technological assets are valued the same. However, there are differences within the company based on specific threats and vulnerabilities. This reinforces the necessity for the implementation of contemporary hazard analysis methods that facilitate the proper prioritization of precautionary measures. In conclusion, the conducted analysis highlights the importance of applying innovative techniques in data protection, aimed at strengthening the security of technological resources and reducing potential incidents that could impact the organization's functionality. The study constitutes a solid foundation for decision-making in the field of risk management and cybersecurity.

KEYWORDS: risk analysis; operational effectiveness; vulnerability; technological resources; cybersecurity

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

Actualización del análisis de riesgo de los activos de información de la unidad de tecnología de una Cooperativa de Ahorro y Crédito, basado en el inventario levantado por la unidad de seguridad lógica en el año 2022.

1.1 Problema de investigación

La transformación digital está revolucionando el sector financiero global a través de la banca en línea, la banca en la nube y la automatización. Estos avances mejoran la eficiencia operativa, pero también amplían la superficie de ataque, sometiendo a bancos y cooperativas de crédito a amenazas cada vez más sofisticadas.

1.1.1 Contextualización

A nivel mundial la digitalización financiera comenzó de manera más notable en Estados Unidos, Japón y el Reino Unido, donde las autoridades implementaron estrategias para promover la banca en línea, los pagos electrónicos y la innovación regulatoria. Las innovaciones introducidas tempranamente desarrollaron nuevos riesgos, incluyendo ciberataques, fraudes y fallos tecnológicos exacerbados por una mayor interconexión digital (Azura et al., 2025).

Los países de Noruega, Corea del Sur y Singapur impulsaron la digitalización mediante la introducción de los pagos móviles, los servicios sin efectivo y los avanzados ecosistemas Fintech. Su adopción temprana de la tecnología intensificó la dependencia digital y puso a las infraestructuras financieras en riesgo de amenazas tales como malware, piratería y ciberterrorismo, lo que obliga a implementar estrategias sólidas de defensa ante los ataques cibernéticos (Waliullah et al., 2025).

Mientras que en Latinoamérica Brasil ha estado a la vanguardia en banca en línea, pagos electrónicos y un ecosistema Fintech avanzado desde la década de 2000 en América Latina. Hoy, Brasil sigue siendo el número uno con regulaciones sólidas y un sistema de pago electrónico llamado PIX. Mientras tanto, México se ha convertido en el segundo jugador en América Latina

con la ayuda de la Ley Fintech del país y el creciente número de Servicios Digitales (Navarro et al., 2025).

Tres naciones de América Latina, Chile, Colombia y Argentina han tenido como meta fortalecer sus procesos de digitalización con billeteras electrónicas, códigos QR para pagos, banca móvil y nueva reglamentación. Estos avances han reducido la diferencia tecnológica y mejorado la experiencia de los clientes en el ámbito financiero, lo que ha derivado en un progreso regional importante de los servicios digitales (Bakker et al., 2023).

Ecuador ha realizado importantes avances en digitalización geográfica en donde primero se encontraban Pichincha y Guayas donde nació el banco electrónico y los pagos digitales. Azuay fortaleció estos procesos en cooperativas innovadoras, mientras que Manabí, Tungurahua, El Oro y Loja hicieron avances graduales. En Carchi, Esmeraldas y la Amazonía, la modernización avanza lentamente debido a limitaciones tecnológicas (Giler et al., 2024).

1.1.2 Planteamiento del problema

En el Ecuador el ente que regula a las cooperativas de ahorro y crédito es la Secretaría de Economía Popular y Solidaria, que en base a su resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 en su Capítulo I – Artículo 2, menciona que "Los niveles mínimos de seguridad se deben definir e implementar con el fin de resguardar y proteger los activos la información, preservando su confidencialidad, disponibilidad e integridad". En esta resolución se categorizan los tipos de servicios que se deben tratar de acuerdo con el tamaño de la institución financiera. En lo que respecta a las cooperativas de ahorro y crédito del segmento 1 están consideradas en el "Régimen General", para este régimen se detallan los siguientes servicios (página 4):

- Software financiero y computación
- Transaccionales y de pago
- Red de cajeros automáticos
- Generadores de cartera
- Administradoras de tarjetas

De acuerdo con Chng et al. (2022) las motivaciones para que los ciberdelincuentes ataquen son: delictivas, políticas o personales, pero el 96% de los ataques tienen fines financieros/económicos, además que el 95% de las causas son por el factor "error humano", y entre el 75% - 90% de los ataques inician con un correo electrónico. Otros datos importantes y muy comunes, es la reutilización de contraseñas al navegar en internet donde cerca del 82% lo hacen, tomando en cuenta que el robo de datos de acceso está en el 20%.

Tomando en cuenta que todas las empresas se encuentran expuestas a todo tipo de ataques, donde se comprometen sus activos y principalmente su información institucional, Aguilar y Balseca (2024) menciona que de acuerdo con un informe de delitos internacionales del FBI se han perdido 12300 millones de dólares debido a incidentes de ciberataques en 2023. En 2024 el costo promedio por filtración de datos alcanzó un máximo histórico de 4.88 millones de dólares. Además, que la empresa que es víctima de un ataque adicional sufre pérdida de productividad, daño reputacional, responsabilidad legal y problemas en la continuidad del negocio.

Por ello la importancia de mantener a los diferentes activos de información, con sus respectivas salvaguardas y poder fortalecer la seguridad en los mismos, tal como se indica en la resolución del ente regulador, anteriormente mencionada.

Bonderud (2024) menciona en su publicación que en el sector de Finanzas y Seguros se exponen aproximadamente 450 000 archivos sensibles de los cuales 36 000 son accesibles para los miembros de la organización. Este tipo de organizaciones tardan en promedio 233 días en detectar y contener una violación de datos y que el 74% de los ataques comprometieron datos personales de clientes.

Actualmente la organización en estudio ha crecido en los últimos 4 años en tamaño, tanto con sus activos como en su información y personal operativo- administrativo, es por ello necesario identificar los activos de información importantes para la institución.

La institución financiera en su oficina principal (Matriz), dispone de un Data Center implementado y en este edificio se encuentran todas las áreas operativas de la misma (gerencia, subgerencias, contabilidad, cartera, captaciones, seguridad, tecnología, operaciones, riesgos, auditoría, etc.). Desde la oficina matriz se generan la toma de decisiones para todas las agencias

involucradas y es donde se centraliza toda la información del día a día, de cada uno de los socios y clientes.

Por tanto, es relevante recalcar que la COAC tiene su inventario de activos de información y los riesgos que presenta, el que se encuentra desactualizado por más de cinco años. Esta situación perjudica e impide la correcta identificación y valoración de los nuevos activos y de los nuevos riesgos que emergen, afectando así a la confidencialidad, integridad y disponibilidad de la información. La falta de un análisis de riesgo contemporáneo, así como de las salvaguardas adecuadas, descontextualiza los elementos de la seguridad de la información y los controles necesarios para disminuir la probabilidad del riesgo.

La cooperativa de ahorro y crédito, con su sede Matriz ubicada en la ciudad de Tulcán, cuenta con aproximadamente 15 agencias, distribuidas en las provincias de Carchi, Imbabura, Pichincha, Sucumbíos, Nueva Loja y Azuay, con una trayectoria de más de 60 años, lo que la ha posicionado en el norte del país y su pertenencia al Segmento 1 de la Economía Popular y Solidaria.

Las unidades de Seguridad Lógica, Seguridad Física, y de Tecnologías de la Información de la institución crediticia, brindan el asesoramiento técnico y el análisis respectivo sobre la seguridad de los activos de información, con el fin de salvaguardar los datos sensibles o críticos de la institución, de sus socios y clientes.

La última actualización de los activos de seguridad levantada en la organización se realizó a finales del año 2021, tomando en cuenta que durante estos años hubo un incremento de áreas, personas y agencias, por lo que es posible que existan activos de información que no tengan un registro formal que permita fortalecer su seguridad.

Al ser una institución financiera, siempre es un blanco “ideal” para los delincuentes, ya que en la misma se alojan recursos, e información confidencial, que en manos de personas que intentan causar daño o para lucro personal de la competencia, lo que sería un peligro para la reputación de esta. Es por ello por lo que se debe mantener una búsqueda constante sobre cómo fortalecer la seguridad de estos activos de información, con el fin de garantizar a los socios y clientes, la confidencialidad, integridad y disponibilidad de sus datos.

Otro de los factores importantes para la cooperativa de ahorro y crédito, es que se debe

asegurar la continuidad del negocio, ya que los servicios deben estar disponibles 24 horas al día y 7 días a la semana; todo esto al tratarse de recursos económicos que se manejan por canales físicos y electrónicos.

Por todo lo que antecede, es primordial tener un inventario de activos de la información actualizado de manera periódica, para determinar su seguridad y tratamiento frente a las actividades que se realizan en la institución financiera, tanto internas como externas.

1.2 Interrogantes de la investigación

¿Cuáles son los activos sensibles a vulneraciones de seguridad de la Unidad de Tecnología de una Cooperativa de Ahorro y Crédito?

¿Qué metodología de análisis de riesgo permitirá priorizar los activos de seguridad de acuerdo con su orden de importancia?

¿Cómo diseñar un inventario actualizado de activos de seguridad, considerando la metodología del último análisis de riesgo de los activos de la Cooperativa de Ahorro y Crédito?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Actualizar el inventario de activos de información de la Unidad de Tecnología de una Cooperativa de Ahorro y Crédito, mediante la aplicación de una metodología de análisis de riesgos, para fortalecer la confidencialidad, integridad y disponibilidad de la información crítica.

1.3.2 Objetivos específicos

- Realizar el levantamiento de información de los activos sensibles a vulneraciones de seguridad en cada área de una Cooperativa de Ahorro y Crédito.
- Priorizar los activos de seguridad de acuerdo con su orden de importancia utilizando una metodología de análisis de riesgos.
- Diseñar un inventario actualizado de activos de seguridad, considerando la metodología

del último análisis de riesgo de los activos de la Cooperativa de Ahorro y Crédito o de ser necesario adaptar una nueva metodología.

1.4 Hipótesis

Al actualizar el inventario de activos de información de la Unidad de Tecnología de una Cooperativa de Ahorro y Crédito, mediante la aplicación de una metodología de análisis de riesgos, se fortalecerá la confidencialidad, integridad y disponibilidad de la información crítica.

1.5 Categorización de variables

Variable independiente: inventario de activos de información de la Unidad de Tecnología de una Cooperativa de Ahorro y Crédito, mediante la aplicación de una metodología de análisis de riesgos.

Variable dependiente: confidencialidad, integridad y disponibilidad de la información crítica.

1.6 Justificación

La resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 de la Secretaría de Economía Popular y Solidaria, busca regular los aspectos mínimos para la administración de la seguridad de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad.

Con esta resolución se tendrá un inventario de activos de seguridad de la información actualizado, y adaptable al crecimiento de la cooperativa de ahorro y crédito. Esto con el fin de dar un mayor alcance, al control de posibles riesgos o amenazas que puedan afectar el correcto funcionamiento de la institución y a la continuidad del negocio.

Las entidades financieras deben contar con las salvaguardas necesarias para mitigar o controlar, los diferentes riesgos tanto en el perímetro interno como externo. Estos perímetros están compuestos por instalaciones físicas, ubicación geográfica, hardware, software, personas y/o procedimientos; lo que permite tener un amplio campo para cualquier tipo de amenaza o por descuido generar alguna vulnerabilidad de la cual puedan aprovecharse.

Las empresas u organizaciones por más pequeñas que sean se deben implementar medidas de seguridad efectivas para salvaguardar activos valiosos y así evitar pérdidas y mantener la confianza de los clientes. Las medidas de seguridad aportan a mitigar los riesgos, pero también garantizan la seguridad y satisfacción en sus clientes (Chang et al., 2025).

Arteaga (2025) indica que para tener estrategias de seguridad y protección eficaces se deben tomar en cuenta inicialmente la compresión de los activos, tomando en cuenta que los activos se presentan en diferentes formas y para lo cual cada activo requiere medidas de seguridad específicas de acuerdo con su naturaleza y valor. Y por otro lado la evaluación de los riesgos, con el fin de identificar las amenazas y vulnerabilidades de los activos, con esto se avalúa también la probabilidad y el impacto de los diversos riesgos ante los robos físicos, ciberataques, desastres naturales y amenazas internas.

En la institución financiera que se aplicará este estudio, se ejecutará el análisis de riesgo en los activos de la Unidad de Tecnologías de la Información, lo que permitirá evaluar cuales son los activos prioritarios y por ende saber en qué nivel de riesgo se encuentra cada activo en base a la probabilidad de ocurrencia de amenazas y sus vulnerabilidades.

Este análisis contribuirá a mejorar y fortalecer la seguridad en los activos de información, con el fin de mantener o asegurar la confidencialidad, integridad y disponibilidad, para que los socios y clientes tengan esa confianza en la institución, frente a salvaguardar sus datos personales y financieros.

En la institución financiera, se dispone de un conjunto de activos que requieren medidas de seguridad adecuadas para garantizar su protección. Entre estos activos se incluyen los físicos (edificaciones y archivos de información), el software informático (programas o plataformas adquiridos para el desarrollo de tareas, así como para la protección de equipos e información), el hardware informático (computadores, switches, enrutadores, servidores, teléfonos, etc.) y el talento humano responsable de ingresar, procesar y proteger la información.

Al existir una variedad de activos de información, su tratamiento debe analizarse de manera particular a fin de determinar las salvaguardas necesarias y adecuadas para cada uno. Por ejemplo, en el caso de un computador perteneciente a un empleado del área de negocios o cartera, dicho

equipo debe permitir el acceso únicamente al usuario asignado, mediante su usuario y contraseña personal y secreta. Asimismo, internamente debe contar con protección antivirus, control de puertos USB para evitar filtraciones de información por parte de empleados que no cumplan las políticas de uso de equipos, acceso correcto al correo institucional y una contraseña confidencial y de uso personal para el Core Financiero.

Los controles son propios para cada situación, porque si hablamos de un espacio físico, por ejemplo, el archivo de crédito, ubicado en una habitación o cuarto físico dentro de la institución, su protección estaría dirigida a que el lugar no tenga humedad, exista una cámara de seguridad, posea un control de acceso, cuente con un extintor, cuente con la instalación de sensores de humo, su ubicación esté libre de posibles inundaciones, protección antisísmica, entre otros.

CAPÍTULO II

MARCO REFERENCIAL

El capítulo describe los fundamentos teóricos y conceptuales que justifican la actualización del análisis de riesgo de los activos de información de una cooperativa de ahorros y crédito. El capítulo revisa principios, normas y metodologías que hacen posible entender la relevancia de la protección de los sistemas tecnológicos institucionales y su información.

Además, se analizan los marcos regulatorios, técnicos y contextuales que guían la gestión del riesgo. Este capítulo proporciona la base para comprender adecuadamente las realidades de la organización y para justificar la metodología utilizada con el fin de identificar, evaluar y mitigar los riesgos informáticos.

2.1 Antecedentes

Según Mungabusi (2022) en su investigación con la temática "Modelo de gestión de seguridad de la información en entidades financieras cooperativas", dice que la Cooperativa de Ahorro y Crédito Ambato Ltda. ilustra lo importante que es para las entidades realizar un diagnóstico en seguridad de la información. La evaluación indica que pese a que tenemos varios procesos que son favorables, el dar crédito es esencial para el negocio. Las debilidades inciden en la administración de activos informáticos, especialmente por intervenciones externas. La ISO 27001 es una norma que permite optimizar la gestión de seguridad de los datos, útil para cualquier entidad. En el área de crédito mejora la disponibilidad, integridad y confidencialidad de la información. Esto permite una mayor seguridad tanto para la entidad como para el cliente.

Mientras que Angulo (2024) en su investigación "Análisis de un sistema de gestión de seguridad de la información para la PUCE-E basado en la norma ISO 27001", dice que a través de entrevistas y una evaluación detallada, se logró determinar los activos informativos en la PUCE-E, lo que da como resultado un inventario de recursos esenciales. Se examinó su efecto en la reputación, la economía y la integridad de la universidad, resaltando que se necesita un sistema para gestionar la seguridad de la información, particularmente en TI y diferentes departamentos. Para preservar la integridad de las instituciones, es esencial proteger los datos personales y

sensibles. La recolección de datos se benefició en gran medida de la metodología ISO 27002, y a pesar de que todavía no se han establecido varias regulaciones de la ISO 27001, su formalización podría reducir considerablemente los riesgos.

En tanto que Aguilar (2022) en su proyecto de investigación titulado como "Plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC27001:2013", dice que la norma ISO/IEC 27001:2013 y el método MAGERIT han determinado el estado del arte en la administración de amenazas en infraestructuras tecnológicas. En una empresa se han identificado 32 activos y el 41%, el 22% y el 19% son esenciales para la disponibilidad, la integridad y la confidencialidad. Los recursos humanos, la gestión de incidentes y la continuidad del negocio son los principales riesgos que enfrenta el organismo. En cuanto a las debilidades se refiere a la falta de políticas criptográficas y la administración de activos. La estrategia de gestión de seguridad de la estadística se evaluó con un 4,2 sobre 5 por los expertos, esto muestra que es viable, aunque tenga algunas debilidades organizativas.

De igual manera Núñez (2025) en su trabajo de titulación "Modelo para la Gestión de Seguridad de la Información en Cooperativas de Ahorro y Crédito del Segmento 1 Basada en ISO/IEC 27001:2022", dice que la puesta en marcha de un "Sistema de Gestión de Seguridad de la Información (SGSI)" en entidades cooperativas necesita una perspectiva interdisciplinaria y el involucramiento de toda la organización. Los líderes deben ser conscientes del valor que tiene la protección de datos en virtud de la normativa vigente. Es fundamental determinar responsabilidades y definir medidas que disminuyan los riesgos, lo cual se alcanza mediante el estudio organizativo de activos importantes. La aplicación del marco normativo correspondientes a la norma ISO 27001:2022 permite que el SGSI se alinee con las metas a largo plazo. Es indispensable contar con los expertos en seguridad que verifiquen y pulan la metodología para garantizar una protección adecuada frente a los riesgos.

Según Mera (2022) en su trabajo de titulación "Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: empresa ALTAC", menciona que después de analizar el estado de la compañía en términos de Seguridad de la Información, se detectaron tanto actividades positivas como deficiencias que necesitan ser atendidas. Es importante enmendar las vulnerabilidades para prevenir la repercusión de las amenazas detectadas, a pesar de

que la compañía gestiona información apropiadamente en ciertos aspectos. Se propuso optimizar los procedimientos internos vinculados con el manejo de la información, lo que incluye definir políticas que se transmitan a los trabajadores para que entiendan sus obligaciones en materia de seguridad. También se detectaron riesgos para los activos de la firma, lo que permitió resaltar la importancia de disminuir o atenuar las amenazas y sus vulnerabilidades con el fin de garantizar el funcionamiento normal del negocio.

Según Arellano (2023) en su proyecto de titulación "Modelo de gestión de la seguridad de la información en una institución financiera cooperativa" dice que la confirmación de la normativa ISO 27001 posibilita que se implemente un sistema de manejo de seguridad de la información, el cual está en consonancia con el gobierno de seguridad fundamentado en Cobit 2019. Se ha determinado que la entidad financiera se ha enfocado en la seguridad informática, lo cual le permite vincular las normas de protección, integridad y accesibilidad de los datos con el cubo de McCumber. Asimismo, al emplear CIS Controls se hace más sencillo examinar las vulnerabilidades y redactar un manual de directrices de seguridad de la información que documente las políticas requeridas para administrar la seguridad de los datos conforme a la norma ISO 27001.

En tanto que León y Murillo (2021), en su artículo titulado "Análisis Financiero: Gestionar los riesgos en las Cooperativas de Ahorro y Crédito segmento 1", dice que el análisis de riesgos y el financiero contribuyen a que las compañías organicen los datos contables y sugieran tácticas para reducir los riesgos. El crecimiento económico se ha visto ralentizado por la pandemia de covid-19, lo que ha causado que los hogares tengan menos liquidez, además de generar desempleo y el cierre de empresas emergentes. Los organismos cooperativos de ahorro y crédito, entre otras instituciones financieras, afrontan riesgos a medio y largo plazo como consecuencia de factores negativos en la economía a nivel macro y micro. Para conservar la salud del sistema financiero y su propia salud financiera, es esencial que sigan teniendo planes de contingencia.

Mientras que Doris (2023) en su artículo titulado como "Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS)", dice que el estudio sobre los riesgos informáticos en la cooperativa mostró diferentes debilidades en sus servicios vitales, así mismo

que detectó numerosos grados de riesgo que ponen en peligro la seguridad de la información. Se resaltó la relevancia de acelerar la capacidad de respuesta del personal mediante la formación de los empleados y el refuerzo de herramientas de trabajo. Con el fin de aminorar estas amenazas, se enfatizó que debe primar el establecimiento de reglamentos de seguridad, capacitación permanente y formalización de procesos que implique una gestión global de la seguridad informática, en base a lo que refiere la “Superintendencia de Economía Popular y Solidaria (SEPS)”.

En tanto que Cárdenas et al. (2023), en su artículo titulado "Evaluación de la Efectividad del Control Interno en Cooperativas de Crédito: Un Estudio Basado en COSO", menciona que las seis entidades de cooperativas de crédito analizadas, presentaron niveles elevados de confianza y riesgos bajos en varios componentes. La credibilidad fue de un 87% y el riesgo del 13% en el perímetro de control. En la valoración de riesgos, se establecieron los niveles en 4% de riesgo y 96% de confianza. Las operaciones de control lograron una seguridad del 93% y un riesgo del 7%. La información y la comunicación presentaron un 95 % de confianza y un 5 % de riesgo. Finalmente, el seguimiento y monitoreo también alcanzaron un 95% de seguridad con un 5% de riesgo, lo cual indica un firme compromiso con la gestión y la mejora constante de la organización.

Mientras que Nikhil y Sreevidya (2025), en su artículo titulado como "Gestión de riesgos cibernéticos en el sector financiero: Una evaluación de las prácticas actuales en escenarios modernos", manifiesta que el proceso de digitalización del sector económico ha cambiado tanto en la forma de ofrecer servicios como en los riesgos cibernéticos. A pesar de los adelantos en gobernanza y controles tecnológicos, permanecen las brechas en la gestión del riesgo de terceros, resiliencia cibernética y seguridad en la nube. Los ejemplos del Banco Central de Bangladesh y de Capital One demuestran que la tecnología, por sí sola, no es importante sin no hay una cultura de protección y buena gobernanza. El enfoque debe ser holístico en la combinación de procesos y gobernanza, tecnología y personas. Para mejorar la seguridad, es importante realizar cooperaciones regulatorias junto con iniciativas sectoriales a fin de abordar riesgos integrales y examinar tecnologías emergentes. Estos hallazgos subrayan la necesidad de marcos complejos y culturas eficaces en materia de riesgo dentro del sector industrial.

En el artículo “Ciberseguridad en Instituciones Financieras: Riesgos y Salvaguardias”, Reji (2024), expresa que en el área de la seguridad cibernética de las corporaciones financieras, resulta necesario incrementar la defensa frente a distintos tipos de riesgos. Este trabajo destaca la necesidad de implementar tácticas adaptativas y acciones proactivas a fin de resguardar la información externa de riesgos complejos, que comprenden los daños de ransomware hasta las amenazas más sofisticadas. Colaborar en el sector en cuanto a formación continua dirigida a los empleados e implementar protecciones sólidas, constituyen ejemplos de obligación con la resiliencia. Para poder amoldarse a un contexto que seguirá cambiando, se debe compartir información y acogerse a las tecnologías. Las entidades deben promover una cultura de perfeccionamiento constante que proteja la estabilidad global del sistema financiero y el respaldo de los clientes.

2.2 Marco Teórico

2.2.1 Seguridad de la información y ciberseguridad

La seguridad de la información resguarda los datos confidenciales frente a actividades no permitidas, tales como el registro, la modificación, la inspección y cualquier alteración o eliminación. La finalidad es asegurar la privacidad y la seguridad de datos fundamentales, como los financieros, los relacionados con las cuentas de clientes o los relativos a la propiedad intelectual (Rodríguez y Moreno, 2024).

La ciberseguridad comprende los procesos y políticas que protegen a las personas, sistemas y a la información, de los ataques cibernéticos. Las empresas deben implementar un manejo de riesgos que se ajuste a la ciberseguridad, lo que se vuelve fundamental para su correcto desarrollo. Tales son las amenazas sobre las que advierte el gobierno español ante el incremento de los ciberataques, citados por el periódico español El País. Según la International Data Corporation (IDC), ante la complejidad de estos ataques las organizaciones están incrementando sus inversiones y se estima que en 2028 la inversión en seguridad alcanzará los 377 mil millones de dólares (Lucio y Campaña, 2024).

Figura 1

Formas de las buenas prácticas de seguridad de datos



Nota: Son las formas que integran las buenas prácticas de seguridad de datos. Tomado de Ávila (2024)

La seguridad de la información se desarrolla bajo tres factores importantes, los que determinan el nivel de impacto y riesgo a los cuales los activos se encuentran expuestos, estos factores son: confidencialidad, integridad y disponibilidad.

a) Confidencialidad. De acuerdo con el Esquema Gubernamental de Seguridad de la Información (EGSI), la información únicamente debe ser divulgada o accesible para aquellos que tienen autorización. De igual manera, MAGERIT considera la confidencialidad como una cualidad difícil de recuperar, ya que en ella está en juego la confianza que los demás depositan en la organización. Si no se gestiona con diligencia el secreto de la información, puede incurrirse en el incumplimiento de principios, contratos y leyes relacionados con la preservación de los datos.

b) Este factor se refiere a la veracidad de la información, la cual debe mantenerse correcta y en su estado original desde su origen, sin ningún tipo de manipulación por parte de personas no autorizadas, tal como lo señala el Registro Oficial de EGSI. Por su parte,

MAGERIT considera la integridad como la preservación completa y fidedigna de los datos, la cual debe mantenerse íntegra bajo el principio de honestidad, sin ser manipulada ni corrompida. La vulneración de la integridad afecta directamente la continuidad del negocio o de la organización.

c) Disponibilidad. En el Registro Oficial del EGSI la información tiene que permanecer accesible, para aquellos que están facultados. Esto se encuentra relacionado con la disponibilidad de los servicios para ser utilizados cuando se requieran. Si este factor se llega a vulnerar o es escaso, se ve interrumpido el servicio como tal, y MAGERIT expresa que esto ocasiona una baja en la eficiencia de la organización.

2.2.1.1 Política de seguridad de la información

Constituye un conjunto de normas que orientan a los individuos en el uso de los activos de tecnologías de la información (TI). Las organizaciones tienen la facultad de establecer políticas orientadas a proteger la información, con el fin de garantizar que tanto los empleados como otros usuarios cumplan con los procedimientos y protocolos de seguridad establecidos. Dichas políticas de seguridad se definen para asegurar que únicamente los usuarios debidamente autorizados accedan a datos e información de carácter confidencial.

Es fundamental establecer una estrategia de seguridad efectiva y velar por su cumplimiento, pues ello resulta clave para prevenir y reducir las vulnerabilidades en la seguridad de la información. Para que dicha normativa sea verdaderamente eficaz, debe actualizarse periódicamente en función de los cambios organizacionales, las nuevas amenazas, las lecciones derivadas de incidentes pasados y las modificaciones en los sistemas y herramientas de seguridad (Llano et al., 2022).

2.2.1.2 Gestión del ciclo de vida de los datos

La administración o gestión del ciclo de vida de los datos, también llamada "Database Lifecycle Management (DLM)", implica la creación y/o optimización de una base de datos y todo lo que ella incluye desde una perspectiva técnica y organizacional. Esto permite que los datos sean procesados y manejados de manera específica, otorgándoles un valor y utilidad que puede ser implementado en compañías y organizaciones.

Un DLM (Data Lifecycle Management) se centra en los diferentes elementos relacionados con los datos, incluyendo la arquitectura de diseño, la creación de la estructura de datos, los procedimientos que un dato atraviesa dentro de una empresa específica, su seguridad y su método de almacenamiento (Ige et al., 2024).

Figura 2

Gestión del Ciclo de Vida de los Datos



Nota: Gestión del ciclo de vida de los datos. Tomado de Ige et al. (2024).

2.2.1.3 Base de datos

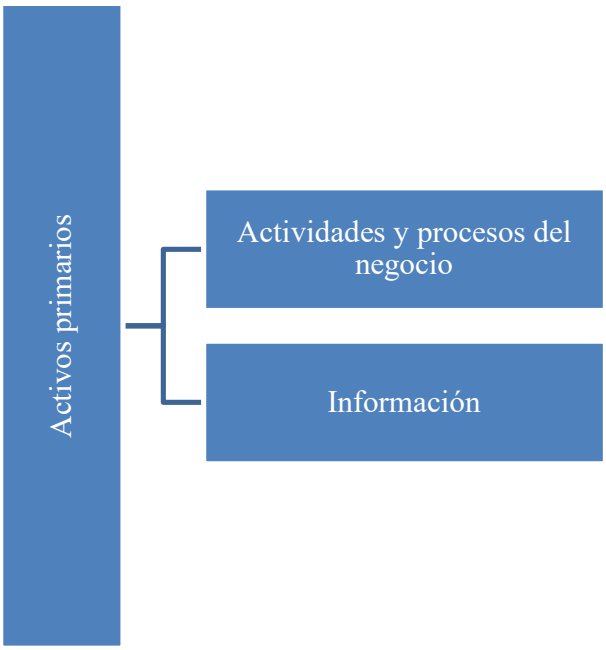
Constituye un repositorio informático que administra y resguarda conjuntos de datos organizados por diversos enfoques, tales como tablas en archivos vinculados o estructuras distintas en bases no relacionadas. Estas bases posibilitan que las organizaciones gestionen datos sin estructura como los archivos multimedia, y datos estructurados como los registros financieros. Es esencial estructurar grandes cantidades de datos en una configuración de datos consistente. Las bases de datos no solo guardan datos, sino que también simplifican el acceso, aseguran la confidencialidad y su protección, así como también apoyan proyectos de inteligencia artificial, empresarial y aprendizaje automático (Mariño, 2022).

2.2.2 Tipos de activos

En la ISO 27005 en su Anexo B menciona a la identificación y valoración de activos, así como también la valoración del impacto, diferenciando a los activos en dos grupos: los activos primarios y los activos de soporte.

Figura 3

Tipos de activos primarios



Nota: En la figura están los diferentes tipos de activos. Tomado de Colina y Túa (2020).

Por lo que estos se definen de la siguiente manera:

2.2.2.1 Actividades y procesos del negocio

A través de ellos se sigue una ruta o un camino, mediante los procesos que van encaminados al cumplimiento de las actividades del negocio, así como también con el correcto cumplimiento de los compromisos con terceros (contratos, proveedores, servicios externos) como lo indica la ISO 27005.

2.2.2.2 Activos de información

Son todos los datos o conjuntos de datos que tienen un valor para una organización o

sistema y que, por lo tanto, deben ser protegidos. Esto implica la información, ya sea digital o física, como bases de datos, documentos, registros, credenciales, archivos y cualquier contenido de interés para su funcionamiento, toma de decisiones o cumplimiento de disposiciones legales de la entidad. La preservación de la confidencialidad, integridad y disponibilidad de estos activos es de vital importancia, ya que la pérdida, alteración o divulgación no autorizada de la información puede ocasionar daños de carácter técnico, económico o reputacional (Páez y Portilla, 2024).

Un activo de información, que incluye documentos, imágenes, videos y bases de datos, constituye cualquier dato o contenido informático que un organismo tiene y administra. Estos activos son relevantes para brindar información acerca de los procesos internos y el comportamiento del cliente, así como para tomar decisiones e innovar. Se administran por medio de sistemas de administración de activos informáticos (SGA), que se ocupan del análisis y la conservación de los datos, y deben estar protegidos para impedir que personas no autorizadas tengan acceso a ellos o que se pierdan (Colina y Túa, 2020).

Dentro de este tipo de activo se maneja diferente tipo de información como datos exclusivos de cada usuario, que incluyen información personal, detalles sobre la conducta, preferencias y ubicación, entre otros (Ceci, 2025).

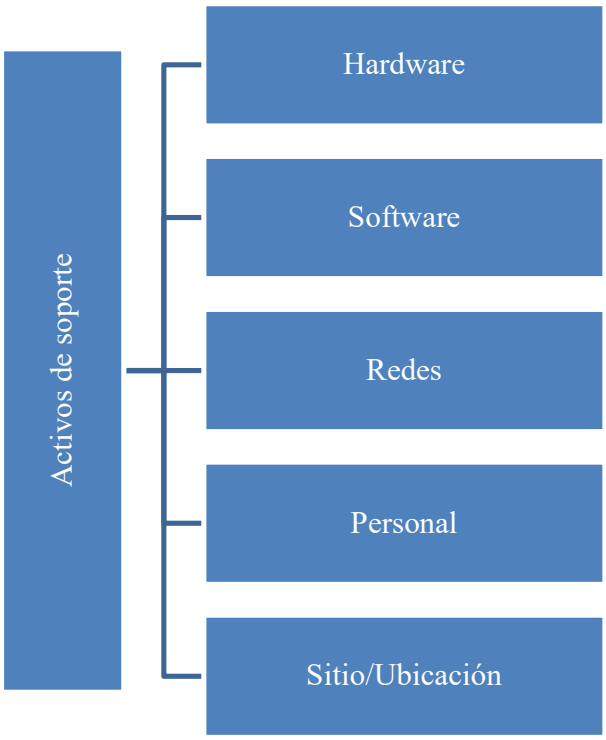
También datos financieros como las utilidades, los ingresos generados por las operaciones, los cargos por servicios, los costos por servicios y otras contraprestaciones se registran en los libros de la organización. La gerencia usa los fragmentos vinculados a la estabilidad económica para usarlo como un medio de estudio del desempeño de la empresa para ver si se requiere ajustar la estrategia y/ o táctica que se tiene. La información que tienen los usuarios de la empresa para la toma de decisiones será cualitativa y cuantitativa. Dicha información incluye los ingresos, los costes, el capital, los activos y los pasivos. Para posibilitar una adopción de decisiones táctica y rentable, es esencial tener información financiera precisa (Aimacaña et al., 2024).

En la organización se maneja también información confidencial, los cuales pueden ser documentos en formato digital o en soporte físico. Con el fin de resguardarlos y salvaguardarlos de ser leídos por individuos no autorizados, las organizaciones tienen que aplicar ciertas medidas de seguridad (Dove, 2023).

La ISO 27005 considera que este tipo de activos comprenden la información vital, personal, estratégica, y de alto costo para el cumplimiento de los objetivos, misión y visión de la organización.

Figura 4

Tipos de activos de soporte



2.2.2.3 Hardware

Son los componentes físicos de un sistema informático o computadora. Esto comprende cualquier parte que sea manipulable y tocable. Por ejemplo: ratón, teclado, disco duro, pantalla y memoria RAM.

Para que cualquier sistema computacional funcione, es indispensable la entrada, procesamiento, almacenamiento y salida de datos, todos ellos proporcionados por los componentes de hardware. Como fundamento físico de la ejecución del software, el hardware es utilizado. La computadora no podrá emplear sus elementos de hardware sin un sistema operativo (Monterrubio, 2024).

Este tipo de activos de acuerdo con la ISO 27005 en su Anexo B, indica que está compuesto por los elementos físicos que brindan soporte a los procesos.

2.2.2.4 Software

El software consiste en una serie de instrucciones que indican a una computadora, una aplicación web u otro tipo de dispositivo, qué acciones debe tomar, así asiste al dispositivo en comprender, qué debe hacer y cómo. Por medio del software, se tiene la posibilidad de interactuar con el dispositivo de una forma que antes no era posible. Para poner una ilustración, con el software se tiene la posibilidad de emplear una computadora para editar videos, elaborar música, hacer gráficos e incluso jugar juegos sin necesidad de comprender cómo trabaja el hardware. El software posibilita que se interactúe con las plataformas computacionales y da la oportunidad de acceder a nuevas funcionalidades y habilidades que no serían factibles sin él (Veloz, 2022).

Por ejemplo, un servidor es considerado como un dispositivo o conjunto de equipos en un sistema de red, que gestiona las capacidades de la red. Es capaz de guardar aplicaciones y archivos, brindar acceso a ellos y gestionar peticiones de múltiples dispositivos o usuarios simultáneamente (Shafiei et al., 2022).

En esta categorización se encuentran las aplicaciones que operan en los navegadores web, tales como Google Chrome o Firefox. Dichas aplicaciones no se instalan en nuestros dispositivos, sino que funcionan en una plataforma y se envían a nuestro navegador por medio de Internet (Veloz, 2022).

La ISO 27005 contribuye con la definición de este activo, como los programas que aportan al procesamiento de datos en conjunto, como por ejemplo el sistema operativo o paquetes de software de uso institucional.

2.2.2.5 Redes

Este tipo de activos lo integran los dispositivos de telecomunicaciones con el fin de que varios elementos de la infraestructura tecnológica se puedan comunicar entre sí, para dar continuidad a las tareas o labores diarias. La ISO 27005 se refiere a algunos activos de este tipo como: enlaces, protocolos de comunicación, equipos de enrutamiento, interfaz de comunicación,

entre otros.

Hacen referencia al hardware y a los dispositivos, que crean y sostienen las redes de computación. Incorporan módems, conmutadores, routers, adaptadores de red, conexiones de acceso sin hilos y cables de red (Reyna et al., 2023).

2.2.2.6 Personal

El personal es un recurso crucial para la seguridad de los sistemas organizacionales, donde su experiencia y sus habilidades son irreemplazables. Sobre todo, a los miembros del personal que son administradores de sistemas, analistas de TI, usuarios operacionales, personal administrativo, gerentes y proveedores externos autorizados.

Constituyen los miembros de una entidad que por sus competencias, habilidades, roles y responsabilidades participan en la operación y defensa de los sistemas e información. Abarca a colaboradores, jefes, técnicos, dirigentes y a aquellos que de forma activa constituyen parte de la gestión de las herramientas tecnológicas o de los datos. Por esta razón se considera un activo, porque su desempeño, educación y nivel de ingreso pueden afectar directamente la protección, la efectividad y la sostenibilidad operativa de la organización (Álvarez-López, 2023).

Este activo es un factor relevante porque existe la posibilidad de que se presenten vulnerabilidades críticas debido a fallos humanos, falta de capacitación o cumplimiento de políticas, tales como incidentes de seguridad desafortunados, exposición de datos, ingreso no autorizado o configuraciones erróneas del sistema. Por lo tanto, la gestión del personal incluye capacitación, asignaciones de roles adecuados y manejo de privilegios (Kaulwar, 2024).

Este tipo de activo se refiere a todos los grupos de personas involucradas en el sistema de información (ISO 27005).

2.2.2.7 Sitio

La ISO 27005 menciona a este tipo de activo, como el que permite tener un alcance sobre todos los lugares en los que la organización puede tener un control directo y en los que depende de otros organismos o entidades, así como también los medios físicos que se requieren para su funcionamiento. Entre ellos se pueden ejemplificar con los siguientes: instalaciones, áreas

externas, zona de ubicación, servicios básicos, servicios de comunicación.

2.2.3 Análisis de riesgos

Un riesgo es la posibilidad de perder algo de valor, comparado con la posibilidad de ganar algo de valor. El riesgo también puede definirse como la interacción intencional con la incertidumbre. Los riesgos pueden resultar en la pérdida de confidencialidad, integridad o disponibilidad, el riesgo podría convertirse en un evento adverso grave o catastrófico en las operaciones de la organización, los activos de la organización y las personas (Camacho y Carranco, 2025).

Según Sánchez (2025), el análisis de riesgos es la estimación de la probabilidad de que ocurra un evento y la probabilidad de pérdida o falla en caso de que ocurra. Cuando existe una modificación de un activo en particular, existe la presencia de vulnerabilidades en este activo. Este autor también determina que la gestión de riesgos puede vincular 4 cuatro objetivos: eliminar los riesgos, reducir los que no pueden ser eliminados (aceptable), convivir con ellos y ejercer o transferir cuidadosamente los controles que los mantienen "aceptables".

De acuerdo con lo publicado por Bermeo et al. (2025), la gestión de riesgos se define como el proceso que consiste en comparar los riesgos evaluados con los beneficios y costos de las salvaguardas, para luego derivar una estrategia de implementación y una política de seguridad del sistema que sean coherentes tanto con la política de seguridad de TI organizacional como con los objetivos del negocio.

En el Libro I de MAGERIT en su versión 3.0, el análisis de riesgos permite el análisis metódico de estos componentes para llegar a conclusiones sólidas y pasar a la fase de tratamiento. Este análisis permite determinar con qué recursos cuenta la organización y con esta información puede estimar los resultados potenciales.

Según la ISO 31000:2018, el objetivo del análisis de riesgo es reconocer y entender la naturaleza de los riesgos y sus atributos, con esto la organización identifica contra que se enfrenta.

2.2.3.1 Componentes del riesgo

Los componentes del riesgo son:

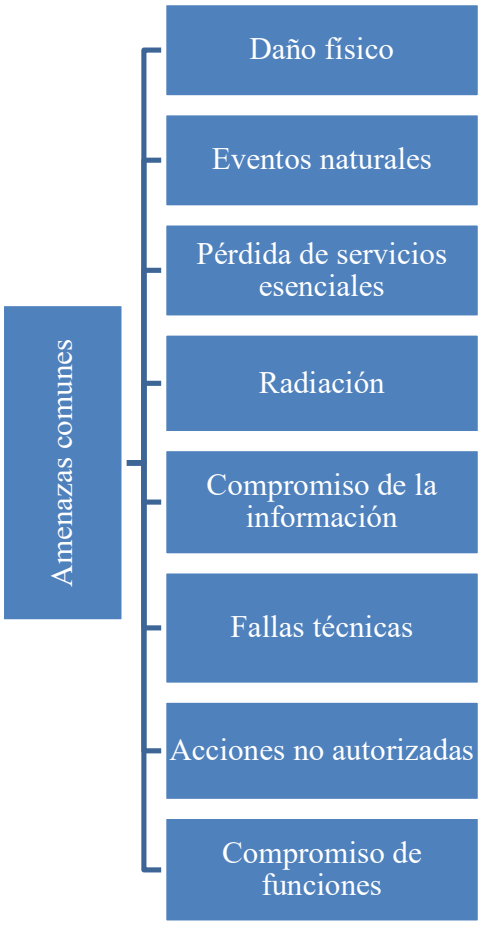
a) Amenazas o peligrosidades

La peligrosidad o amenaza hace referencia a sucesos de origen natural o antropogénico que tienen el potencial de provocar la pérdida de vidas y perjuicios materiales. Supone un riesgo latente, ya que está fuera de las personas y la infraestructura. Las amenazas naturales se incrementan y preocupan a las autoridades, debido a que la pobreza, la vulnerabilidad de los pobladores y el cambio climático aumentan los peligros en las ciudades (Aven, 2023).

Las amenazas o peligrosidades se clasifican en:

Figura 5

Ejemplos de amenazas o peligrosidades comunes



Nota: En la figura están los tipos de amenazas. Tomado de (Anexo C, ISO 27005).

Según el Anexo C, presentado por la ISO 27005:

- **Daño físico.** Que pueden ser causados por fuego, agua, contaminación, accidente, destrucción, polvo, corrosión o congelamiento.

- **Eventos naturales.** Eventos climáticos, sísmicos, volcánicos, meteorológicos, inundaciones.

- **Pérdida de servicios esenciales.** Pérdida o fallo en suministro de agua, climatización, energía, telecomunicaciones.

- **Irradiación.** Son radiación de tipo electromagnético, calor, pulsaciones.

- **Compromiso de la información.** Interferencia, infiltración, robo, apropiación de medios reciclables o de diseño, revelación, fuentes poco confiables, empleo de hardware o software, distribución de la posición.

- **Fallas técnicas.** Fallo o mal funcionamiento de equipo o programa operativo, saturación del sistema, falta de mantenimiento.

- **Actos no autorizados.** Utilización no autorizada, copias engañosas, software no confiable, manipulación de datos, procesamiento ilegal de datos.

- **Compromiso de funciones.** Error de uso, abuso o falsificación de derechos, negación de acciones, incumplimiento en disponibilidad del personal.

b) Vulnerabilidad

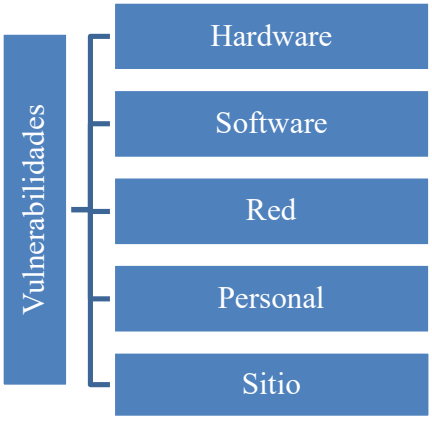
La vulnerabilidad se entiende como la propensión de una comunidad a sufrir consecuencias adversas derivadas de fenómenos de origen natural o antropogénico. Dicho riesgo depende tanto de la forma en que se ha ocupado y construido el territorio como de las condiciones sociales, económicas, culturales y educativas imperantes. La vulnerabilidad aumenta o disminuye en función del grado de exposición a amenazas, los niveles de pobreza, las desigualdades sociales, el uso inadecuado del suelo, las políticas públicas vigentes, la explotación del medio ambiente, el

acceso a la información y a la participación en los procesos de toma de decisiones (Sacoto y Sánchez, 2023).

Las vulnerabilidades según el Anexo C de la ISO 27005, menciona las siguientes vulnerabilidades que podrían considerarse.

Figura 6

Ejemplos de vulnerabilidades comunes



Nota: En la figura están los tipos de vulnerabilidades. Tomado del Anexo C de la ISO 27005.

La ISO 27005, los define de la siguiente manera:

- **Hardware.** En este tipo se refiere a falta de mantenimiento, falta de reemplazo periódico de equipos, susceptibilidad a humedad/polvo/suciedad/radiación/variaciones de voltaje, falta de cuidado, almacenamiento sin protección.
- **Software.** Menciona la falta de pruebas de calidad, defectos de software, no cerrar sesión en la estación de trabajo, reutilizar medios de almacenamiento sin borrado seguro, asignación errónea de derechos de acceso, mala parametrización, falta de controles de autenticación, contraseñas sin protección, falta de copias de seguridad, fallos en las protecciones físicas de la edificación.
- **Red.** Se identifican las conexiones deficientes, cableado incorrecto o de mala calidad, arquitectura insegura, no proteger contraseñas, tráfico sensible y conexiones de red sin protección.

- **Personal.** Las vulnerabilidades que podrían presentarse son la ausencia del personal, contratación inadecuada, falta de entrenamiento, falta de conciencia en seguridad, ausencia de monitoreo, trabajo no supervisado a personal externo y de limpieza.
- **Sitio.** Descuido en controles de acceso, ubicación e áreas susceptibles a eventos naturales, energía inestable, falta de protección en instalaciones físicas.

c) Incertidumbre

El riesgo se convierte en incertidumbre cuando no puede ser medido. La dificultad de las situaciones aumenta con el nivel de dificultad, y es proporcional a la cantidad de variables requeridas para entenderlas. La incertidumbre está vinculada a las restricciones en el estado del conocimiento y a las indeterminaciones respecto a las competencias de la institución y los aspectos normativos. Estas restricciones y lo complejo de la manifestación en cuestión, a la vez, hacen imposible gestionar todas las variables implicadas. Esto crea incertidumbre en los procedimientos de toma de decisiones (Salinas, 2025).

d) Exposición

Alude a la existencia de personas, servicios ambientales, bienes culturales e infraestructura, medios de subsistencia o recursos económicos y sociales, que debido a su ubicación geográfica pueden ser impactados por la aparición de una amenaza. Constituye una creación histórica donde se vinculan los procesos económicos y sociales con los físicos naturales, y el resultado de esto se manifiesta en la edificación, los asentamientos humanos, el uso del suelo y los recursos públicos, entre otros (Pérez y León, 2021).

2.2.3.2 Metodologías de Análisis de Riesgo

El análisis de riesgo es una herramienta metodológica de la seguridad de la información, que apoya a determinar el nivel de riesgo frente a un activo de una organización y de esa manera la efectividad de sus controles de mitigación, con el fin de asegurar la disponibilidad, integridad y confidencialidad.

En lo que respecta a la seguridad lógica existe la metodología MAGERIT, la misma que fue desarrollado por el Consejo Superior de Administración Electrónica (CSAE). La publicación de Guamán et al. (2023) menciona que esta metodología determina: activos más relevantes de la

organización, amenazas a los activos, estimación del impacto, costo para recuperar la integridad, confidencialidad, disponibilidad o autenticidad. Y que debido a su convergencia MAGERIT cumple con las cláusulas 4.2.1.d (Identificar Riesgos) y 4.2.1.e (Analizar y Evaluar Riesgos) de la norma ISO 27005.

En la publicación de Páez y Portilla (2024) determina que la metodología MAGERIT está conformada por cinco fases, las cuales se fundamentan en los siguientes elementos: activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas. Para fomentar la confianza de los clientes, tanto internos como externos, de la organización, es esencial reducir al mínimo los riesgos relacionados con el uso de sistemas asegurando su autenticidad, confidencialidad, honestidad, disponibilidad y trazabilidad.

La metodología NIST800-30 ha sido desarrollada por el NIST (National Institute of Standards and Technology) en cumplimiento de sus responsabilidades legales de la Ley de Seguridad Informática de 1987 y la Ley de Reforma de la Gestión de la Tecnología de la Información de 1996. Los documentos son para uso de organizaciones federales que procesan información confidencial (Prabawa y Soewito, 2023).

La metodología NIST SP 800:30, compuesta por nueve etapas: caracterización del sistema, que permite establecer la extensión y los límites operativos de la valoración de riesgos en la compañía; identificación de amenazas, donde se determinan las fuentes de motivación para estas; identificación de fragilidades, en esta etapa se elabora una lista con fallos o debilidades del sistema que pueden ser usadas por una amenaza potencial; análisis de controles; estimación de la probabilidad; evaluación del impacto; fase de cálculo del riesgo, facilita la evaluación del riesgo en el sistema informático; sugerencias de control, donde se indican los controles que podrían reducir el riesgo detectado a un nivel aceptable. Por último, está el reporte de resultados, que produce un informe con la descripción tanto de las amenazas como de las vulnerabilidades y mide el riesgo al tiempo que formula recomendaciones para implementar controles (Padua, 2025).

El Esquema Gubernamental de Seguridad de la Información (EGSI), plantea una metodología de análisis de riesgo, basada en la ISO 27005 y MAGERIT, considerando la valoración del activo bajo la confidencialidad, integridad y disponibilidad, para una vez que se obtenga el valor del activo, se pueda medir la probabilidad de ocurrencia de las amenazas y

vulnerabilidades a las que se encuentra expuesto cada activo. Con esto se llega a determinar el nivel de riesgo que asume cada activo con los controles implementados.

2.2.3.3 Gestión del riesgo

Consiste en identificar, analizar y gestionar estas amenazas potenciales al objetivo de la organización o proyecto. Existen procesos apropiados de planificación, organización, dirección y control para gestionar riesgos en eventos como desastres naturales, riesgos empresariales y tecnológicos, así como en las personas, la propiedad y el medio ambiente (Vásquez y Delgado, 2021).

2.2.3.4 MAGERIT

Se utiliza el MAGERIT que es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que estudia y trata los riesgos en el ámbito tecnológico. El enfoque consiste en identificar activos de información, así como amenazas y vulnerabilidades, estimando tanto el impacto como la probabilidad de que se produzcan riesgos. En el marco de EGSI, esta metodología permite organizar sistemáticamente la evaluación de riesgos para la toma de decisiones sobre controles de seguridad y protección de recursos informacionales de la organización.

MAGERIT establece una estructura de modelos para representar los activos, las amenazas y las salvaguardas que permiten entender todo el entorno del riesgo. Mediante la aplicación de esta metodología, se priorizan los riesgos que hayan sido identificados, de acuerdo a su nivel de criticidad, para optimizar el uso de recursos de su mitigación. Su aplicación en contexto organizacional ayuda a reforzar la gestión de la seguridad de la información, promoviendo la creación de una cultura de prevención y control (Guamán et al., 2023).

2.2.3.5 ISO 27005

De acuerdo con la norma ISO/IEC 27005 trata sobre gestiones de riesgo en materia de seguridad de la información. Por lo que establece un proceso cíclico donde se incluye la identificación, el análisis, la evaluación y el tratamiento de los riesgos, tanto internos como externos que afectan a los activos de información En el marco del esquema EGSI, esta norma es una referencia para la organización del análisis de riesgos, garantizando que este proceso se realice

de forma estructurada, documentada y conforme a estándares internacionales.

La norma ISO/IEC 27005 recalca la importancia de la mejora continua en la gestión de riesgos, como parte de la planificación organizativa, que se integra en el planeamiento estratégico. El monitoreo y la posterior evaluación de los riesgos implican, entre otras cosas, el registro sistemático de los riesgos identificados y acciones adoptadas para su tratamiento. En el esquema EGSI, la aplicación tiene que ser utilizada permanentemente en un proceso dinámico, capaz de cambiar junto con las condiciones del entorno (Angulo, 2024).

2.2.4 Método del Ciclo PDCA

Es una técnica cíclica de cuatro etapas que las organizaciones usan para mejorar continuamente sus procesos. Cada fase del ciclo PDCA ayuda a determinar qué procesos de la empresa son efectivos y cuáles necesitan mejorarse. Para prevenir errores que se repiten en las operaciones, también se aplica este método (Chen et al., 2022).

Figura 7

Ciclo PDCA



Nota: En la figura están las etapas que conforma el Ciclo PDCA. Tomado de (Chen et al., 2022).

Según Chen et al. (2022), las etapas del Método o Plan-Do-Check-Ac (PDCA) son:

- **Planificar.** Ejecuta las actividades previamente determinadas con la frecuencia requerida. Por ejemplo, la supervisión mensual sobre las medidas de control establecidas en una evaluación de riesgos constituye un tipo de actividad impulsada mediante la capacidad funcional de las tareas dentro del sistema.

- **Hacer.** Es la etapa en la que se implementarán las soluciones que han sido detectadas en el primer paso. Implementar los cambios únicamente en una reducida escala o en un entorno controlado, como un área determinada, una tarea o solo con una población demográfica particular. Esto es para garantizar que, si alguna vez las modificaciones no fueron efectivos o tuvieron un efecto negativo en su procedimiento o negocio, el daño será mínimo, utilizándose escasos recursos.

  Según la norma ISO 27005, esta fase aplica controles y acciones necesarias para disminuir el riesgo a un nivel admisible, conforme al plan de tratamiento del riesgo.

- **Consultar.** Esta fase es la de análisis, donde se determina la efectividad de las soluciones implementadas utilizando los resultados de la etapa anterior. Comparlos con los parámetros de éxito que se incorporaron durante la etapa de planificación. Determinar si el resultado resulta gratificante y las soluciones están funcionando de acuerdo con la meta, o si requieren más mejoras para llegar al objetivo general.

- **Actuar.** Esta fase corresponde a la implementación integral de las soluciones como parte del proceso empresarial, una vez que se ha comprobado su efectividad. En la etapa de "Actuar" se ejecutan las acciones necesarias para materializar las mejoras y consolidar los cambios dentro de la organización.

De acuerdo con la ISO 27005, menciona los procesos identificados en la fase de planificar, hacer, verificar y actuar, a través de la siguiente tabla del proceso del SGSI:

Tabla 1

Procesos de SGSI

Proceso de SGSI	Proceso de gestión del riesgo de la seguridad de la información
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continua del riesgo
Actuar	Mantener y mejorar el proceso de gestión del riesgo de la seguridad de la información

Nota: En la figura está el Alineamiento del SGSI y el proceso de Gestión del Riesgo (ISO 27005).

2.3 Marco Legal

La investigación que aquí se presenta, tiene como base la normativa vigente en materia de protección de la información personal y gestión de riesgos en entidades financieras, con el fin de garantizar la seguridad del contenido y el resguardo de los activos informáticos de la entidad.

La Ley Orgánica de Protección de Datos Personales (2021), aprobada por la Asamblea Nacional, crea el marco legal para asegurar la protección y el debido tratamiento de los datos particulares en las entidades públicas y privadas.

En el Capítulo VI, referente a la seguridad de datos personales, la ley prescribe que las organizaciones tienen que poner en marcha las herramientas técnicas y organizativas que posibiliten resguardar la información particular que manejen.

El artículo 40, manifiesta que el análisis de riesgo, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de datos personales, deberán aplicar un método para el este análisis, que incluya entre otras cosas:

1) Las características específicas del procedimiento.
2) Las características particulares de las partes implicadas.
3) La cantidad y la categoría de los datos personales que se están tratando.

Esta norma resulta de gran importancia para el presente estudio, pues sustenta la exigencia de implementar medidas de seguridad del conocimiento y administración de riesgos en el interior de la cooperativa, afín de salvaguardar los activos de datos y cumplir con la normativa vigente.

La Resolución SEPS-IGT-2025-0113 - "Norma de control para la prevención, detección y combate del delito de lavado de activos y la financiación de otros delitos en las entidades del sector financiero popular y solidario" (2025), establece que

Art. 8.- Para reconocer y analizar el riesgo relacionado con el lavado de activos y financiamiento de ilícitos de sus contrapartes, las entidades tienen que desarrollar metodologías fundamentadas en riesgos para dividir las variables y criterios de riesgo. El hallazgo de perfiles transaccionales y de comportamiento, así como la valoración completa del riesgo asociado, se verá favorecida por esta metodología. Esto es posible gracias a que los factores se definen y ponderan, lo que permite establecer el perfil de peligro total de cada contraparte.

Art. 10.- Los organismos deberán desarrollar, documentar y aplicar una administración del peligro de sustracción de medios y financiamiento de diversos delitos, mediante un enfoque sistemático que incluya, como mínimo.

Estas disposiciones son importantes para la investigación, pues ponen de relieve la necesidad de aplicar metodologías de investigación y manejo de riesgos en los organismos financieros, a fin de incrementar la seguridad de la información y la protección de los activos de la organización.

CAPÍTULO III

MARCO METODOLÓGICO

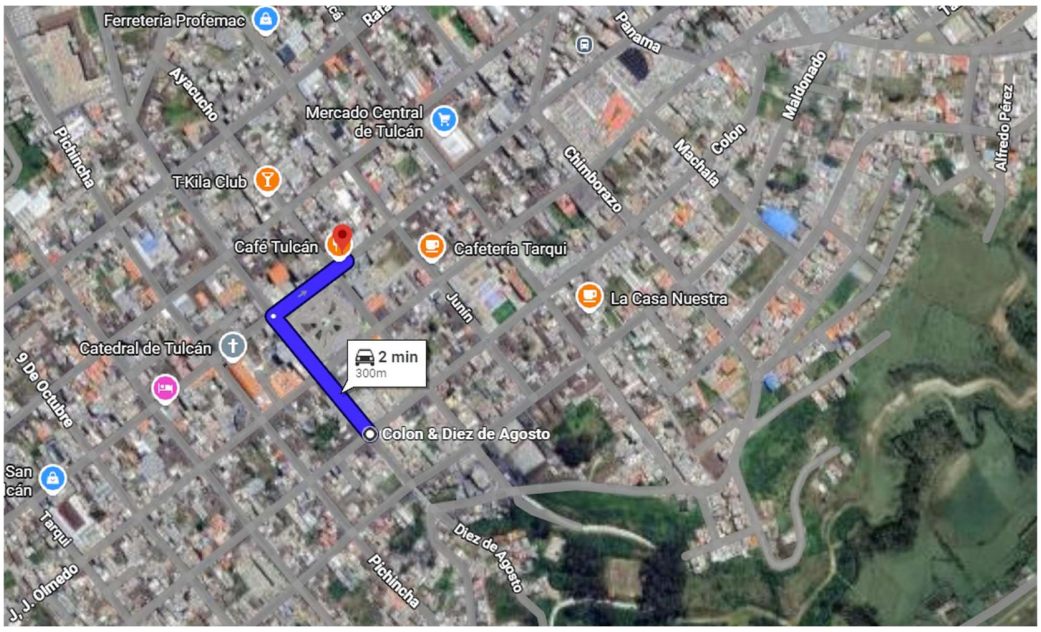
La metodología que respalda esta investigación se describe a fondo en este capítulo, así como el enfoque, el tipo de estudio, las técnicas e instrumentos, la población, la muestra y los procedimientos.

3.1 Descripción del área de estudio

El estudio se llevó a cabo en una cooperativa de ahorro y crédito que no tenía un inventario actual ni un análisis de sus activos, y al ser una institución financiera, podría ser un objetivo para varios atacantes, tanto internos como externos, dañando la reputación de la organización frente a más de 140,000 miembros y clientes. La cooperativa está ubicada en la ciudad de Tulcán, en la provincia de Carchi, parroquia Gonzáles Suárez, en la calle Colón y 10 de Agosto, diagonalmente frente a la Dirección Distrital de Educación Huaca-Tulcán D01.

Figura 8

Ubicación de la Cooperativa de Ahorro y Crédito en Tulcán



Nota: En la figura está la ubicación de la cooperativa de ahorro y crédito en Tulcán. Tomado de https://acortar.link/N02eaL

Esta institución financiera cuenta con un Data Center, cuyas instalaciones están bajo la responsabilidad de la unidad de Tecnología de la Información, así como las seguridades de las jefaturas de Seguridad Lógica y Seguridad Física. El Administrador de Infraestructura es el responsable del Data Center.

Es esencial analizar y evaluar este espacio que contiene hardware y software que permite la operabilidad institucional. Sin embargo, también es necesario evaluar las condiciones físicas y los riesgos a los que se somete este espacio, en caso de que ocurra un evento adverso que comprometa la integridad del equipo.

3.2 Modelo metodológico

La metodología mixta busca integrar las fortalezas de los métodos cualitativo y cuantitativo, combinando sus componentes, con el fin de lograr un entendimiento de mayor inmersión de los fenómenos que se estudian. Esta perspectiva posibilita la recopilación, el análisis y la conexión de datos cualitativos y cuantitativos en una sola investigación. Para enseñar métodos mixtos, se requiere de tácticas multifacéticas que promuevan la formación reflexiva y la colaboración (Álvarez y Rodríguez, 2025).

La investigación adopta un enfoque de métodos mixtos debido a la necesidad de primero identificar y describir los activos informativos, amenazas y vulnerabilidades situadas dentro del contexto organizacional de la cooperativa. Esto implica un análisis interpretativo, revisión de documentos y comprensión contextual de la institución, lo cual es típico de la investigación cualitativa.

El modelo metodológico del estudio se fundamenta en un enfoque descriptivo cuantitativo, empleando una encuesta organizada con interrogantes cerradas y niveles tipo Likert. Este cuestionario está orientado a liderazgos de la cooperativa, con el fin de recolectar datos medibles sobre interpretaciones y prácticas de protección del contenido, que serán considerados estadísticamente para reconocer situaciones y demandas en la institución.

Conjuntamente, el estudio utiliza un análisis de riesgo para la estimación de la probabilidad y el impacto, la clasificación de los niveles de riesgo y la priorización de los activos críticos. Esta

forma de evaluación estructurada implica medición y análisis de datos, típicos del enfoque cuantitativo, lo que permite la justificación de la combinación de los métodos en una investigación mixta.

Por lo que las técnicas empleadas son:

- La encuesta. El motivo de emplear la encuesta en este diseño que consiste en facilitar, la recolección de la información de forma sistemática, veloz y estandarizada de un conjunto particular de personas, facilitando lograr datos cuantificables acerca de sus percepciones, saberes o prácticas. En este caso, su utilización resulta apropiada porque las preguntas específicas y dimensiones tipo Likert posibilitan medir y comparar hallazgos de manera objetiva, lo cual ayuda a evaluar la situación presente, y respaldar la adopción de decisiones fundamentada en evidencia.

- La entrevista. La entrevista se usa en este diseño, ya que permite recolectar información más detallada, minuciosa y cualitativa sobre las perspectivas, experiencias e ideas de los entrevistados, mejorando los resultados cuantitativos correspondientes a las encuestas. Mediante el contacto directo, el investigador es capaz de aclarar respuestas, ahondar más en los temas y entender mejor el entorno, lo que enriquece la investigación y ayuda a interpretar más íntegramente los resultados obtenidos.

3.3 Tipo de investigación

Los tipos de investigación empleados son:

3.3.1 Investigación bibliográfica

Se trata de una de las metodologías cualitativas de investigación que tiene la función de recolectar, compilar y elegir información proveniente del análisis de documentos, libros, grabaciones, filmaciones, revistas, periódicos, artículos derivados de investigaciones y memorias de eventos. En este proceso se incluye la observación en el análisis de datos para identificarla, seleccionarla y relacionarla con el objeto estudiado (Zorrilla, 2021).

En el presente trabajo, se recurre a la bibliográfica debido a la necesidad de fundamentar teóricamente el análisis de riesgos y la gestión de la seguridad de la información, mediante la revisión de textos, artículos científicos, reglamento ISO 27005, ISO 31000, MAGERIT, Ley de Protección de Datos Personales, Esquema Gubernamental de Seguridad de la Información (EGSI) y normativa de la SEPS. Esta revisión ofrece los fundamentos conceptuales, metodológicos y legales sobre los que se sustenta el estudio y que encaminan el desarrollo del plan.

3.3.2 Investigación de campo

Es un método de recolección de datos que tiene como objetivo entender, analizar e interactuar con los individuos en su ambiente natural. La observación conlleva más que la mera observación en el marco de la investigación, significa observar con un objetivo, de manera estratégica y planificada (Bastis, 2024).

En esta investigación se utiliza la investigación de campo porque el levantamiento de información se efectúa directamente en la cooperativa de ahorro y crédito, donde se van a identificar los activos de información, amenazas y vulnerabilidades en su contexto real. Esto, permite analizar la situación actual de la institución y posteriormente aplicar la metodología de análisis de riesgos, que se basa en la información obtenida.

3.3.3 Investigación descriptiva

Se caracteriza por el análisis, la interpretación y la documentación de fenómenos, enfocándose en los rasgos de la población analizada y en su comportamiento actual. Esta visión se complementa al definir el análisis descriptivo como aquella que tiene el propósito de describir las características esenciales de fenómenos homogéneos, usando criterios sistemáticos para establecer su estructura y comportamiento, y ofreciendo información que puede ser comparada con otras fuentes (Guevara et al., 2020).

Los investigadores emplean la interpretación de tipo descriptivo, dado que se busca caracterizar y documentar la situación actual de la información activa, así como también de las amenazas y vulnerabilidades en la cooperativa de ahorro y crédito. Aquí se caracterizan las situaciones en una organización, puesto que no se busca la manipulación de variables.

3.4 Metodología de análisis de riesgo fundamentados en ISO 27005

El presente trabajo de investigación se lleva a cabo con un enfoque centrado al análisis y manejo de riesgos de los activos de la organización. Con la finalidad de desarrollar el estudio, se utilizan las fases del análisis de riesgo: identificación de activos, valoración de activos y análisis de riesgo, esto con el objetivo de identificar las vulnerabilidades, amenazas y si existen las herramientas utilizadas para su control.

El análisis de riesgos se lleva a cabo según los lineamientos de la norma ISO/IEC 27005, que establece normativas para la administración de riesgos de seguridad de los datos. Esta norma permite reconocer riesgos, debilidades y las consecuencias potenciales acerca de los activos de datos, y fomenta el cumplimiento de normativas y medidas de gestión del riesgo.

Esta metodología permite establecer un método riguroso con el fin de reconocer, valorar y tratar las amenazas que permite fortalecer la seguridad de la información y salvaguardar los activos de la organización.

El Esquema Gubernamental de Seguridad de la Información (EGSI) define un método basado en los principios de MAGERIT e ISO 27005, mediante el cual se clasifican los activos según su valor en base a ala atribución de una calificación en términos de bajo, medio o alto. Esto se hace con el objetivo de otorgarles un valor cualitativo y luego proceder a su análisis por medio las amenazas, las vulnerabilidades, el riesgo y los controles.

3.5 Procedimiento de investigación

Una metodología de análisis de riesgo establecida y aplicada para levantar un inventario de activos, permite conocer si existen o se deben implementar controles de seguridad efectivos que apoyen la adecuada toma de decisiones sobre la seguridad de la información. Con respecto a lo mencionado y a fin de fortalecer la propuesta de mejora para la organización, el presente estudio se estructura en tres fases que se describen a continuación:

Figura 9

Fases de investigación



Nota: En la figura están las fases de la investigación.

3.5.1 Fase 1. Levantamiento de información de los activos

La ISO 31000 nos expone que al identificar los activos logramos reconocer su valor institucional, su ubicación y de esta manera los riesgos que podrían ayudar o dificultar, encaminarse en la misión de la organización. El tener un inventario de activos actualizado, nos permite tener un análisis real y actual de los riesgos a los que se encuentran expuestos cada uno de los activos. Las organizaciones tienen la posibilidad de emplear una variedad de métodos para detectar incertidumbres que podrían impactar uno o múltiples objetivos.

Para profundizar en estos aspectos se lleva a cabo entrevistas individuales, para precisar los elementos con los que se encuentran a cargo o que a su juicio son relevantes, con el objetivo de apreciar la trascendencia de los datos que poseen, en función a la actividad del área o el rol que desempeñan en la continuidad del negocio.

Se realiza la entrevista con el jefe de Tecnología, el oficial en Seguridad Lógica y al oficial en Seguridad Física. La interdependencia de los recursos y activos que manejan los profesionales mencionados permiten afirmar que estos especialistas colaboran de modo más estrecho. La colaboración mencionada permite explicar de forma más integral el análisis de los activos de información que se identifiquen, para determinar los niveles de riesgo y de impacto.

La correcta identificación de la información de los activos permite la optimización de recursos, ya que, si el procedimiento falla se habrá perdido tiempo en la identificación errónea de los activos más relevantes de la institución.

3.5.2 Fase 2. Priorización de los activos

El objetivo del análisis de riesgos es entender la naturaleza de estos y sus atributos, incluyendo si corresponde, el nivel de riesgo. El estudio de los riesgos conlleva un examen minucioso de situaciones inciertas, orígenes del riesgo, efectos, probabilidades, acontecimientos, escenarios y controles, así como su eficacia. Las técnicas de análisis podrían ser cualitativas, cuantitativas o una mezcla de ambas, en función del contexto y del uso que se les quiera dar. (ISO 31000).

Se realiza un análisis de riesgos para identificar el valor de los activos, ofreciéndoles una nota cualitativa de Alto (A), Medio Alto (MA), Medio (MB), y Bajo (B). Las calificaciones se tradujeron a una escala de 1 a 4, donde 1 es Bajo (B) y 4 es Alto (A), respecto a los criterios de protección, integridad y accesibilidad, a fin de analizar el impacto de cualquier activo.

Luego de esto se determina para cada activo las potenciales amenazas/vulnerabilidad en un rango de 1 a 4 para evaluar la probabilidad de ocurrencia tal como se mencionó previamente, obteniendo bajo estos dos factores, el cálculo de valoración del riesgo.

El siguiente paso después de identificar las amenazas y vulnerabilidades, es determinar el riesgo que representarían si sucedieran (probabilidad). De esta manera se obtiene una calificación en base al riesgo que experimenta cada activo.

Así, se lleva a cabo una categorización de cada activo, de acuerdo con su puntaje dentro de la escala de calificación previamente establecida.

3.5.3 Fase 3. Establecimiento de un inventario actualizado de activos de seguridad

El objetivo del análisis de los riesgos consiste en asistir a tomar decisiones. La evaluación de riesgos consiste en cotejar los hallazgos del análisis de riesgo con los indicadores para riesgos establecidos, con el fin de determinar, cuándo es necesaria una medida complementaria (ISO 31000).

En esta fase, se documenta el análisis realizado con el propósito de actualizar el inventario de activos para el adecuado tratamiento de la información, la cual se presenta al departamento de Seguridad de la cooperativa de ahorro y crédito, para su correspondiente evaluación.

Este análisis de riesgo propuesto tiene como objetivo calificar los activos de la unidad de Tecnología en función de la importancia de la información, para fortalecer los controles apropiados y la reducción del riesgo de cada activo.

La institución financiera, para asegurar la confidencialidad, integridad y disponibilidad de la información, debe contar con un inventario de activos actualizado para poder implementar medidas de seguridad, de acuerdo con la evaluación de riesgo y el impacto que cada activo tiene frente a las distintas amenazas. Se lleva a cabo el análisis real para cada activo, teniendo en cuenta las amenazas de diferentes tipos (naturales, industriales, de personas, entre otras), con las cuales se pueden evaluar los controles existentes o se pueden proponer nuevos controles a implementar que traten de disminuir el impacto de las amenazas/vulnerabilidades que puedan surgir.

3.6 Consideraciones bioéticas

La investigación actual se basa en los principios de la bioética y los valores relacionados con la ética, la autonomía y la responsabilidad.

La ética constituye una disciplina filosófica que investiga la naturaleza y los reglamentos del progreso moral, tanto en la sociedad como en el mundo interior de cada persona. Además, se trata de un conjunto de normas, principios, costumbres y convicciones sobre lo favorable y lo adverso, ideales que guían y regulan cómo actúan y se comportan los seres humanos (Espinoza-Freire & Calva-Nagua, 2020)

La investigación debe resguardar la confidencialidad respecto a la información institucional y datos personales relacionados a socios, clientes y colaboradores. La información recabada en las entrevistas y en la recolección de activos, debe ser estrictamente utilizada para fines académicos y no debe ser divulgada ni mal utilizada.

Así que es importante conseguir el consentimiento informado de los participantes, con la cual se prueba que su participación es voluntaria y que están conscientes del estudio. En último término, la conducta de la investigación observará las disposiciones de la Ley Orgánica de Protección de Datos Personales y de la normativa vigente de la SEPS, promoviendo la cultura de la responsabilidad.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Este capítulo incluye los resultados de la recolección y análisis de los activos de información de la Unidad de Tecnología de la Información, incluyendo la identificación de amenazas, vulnerabilidades, niveles de riesgo y la priorización de activos críticos. Además, interpreta estos resultados en base a las regulaciones y metodologías aplicables y describe los resultados sobre el impacto en la confidencialidad y la integridad.

El análisis de la encuesta es una etapa esencial dentro del estudio, puesto que puede analizar y entender la situación real de la entidad en lo referente a la seguridad de los datos y la administración de los recursos institucionales. Con la implementación de encuestas a los empleados se lograría detectar el grado de entendimiento, las prácticas vigentes y la valoración sobre los sistemas de seguridad establecidos, evidenciando igualmente a las fortalezas como a las limitaciones en la seguridad de los datos. Los resultados obtenidos servirían para establecer una perspectiva global de la gestión de la información, indicando la necesidad de reforzar la formación, mejorar los controles y los procedimientos de seguridad.

4.1 Resultados de diagnóstico de la encuesta

Los resultados correspondientes a la encuesta efectuada a los trabajadores de la entidad posibilitan reconocer el grado de entendimiento, las estrategias vigentes y la valoración del personal, en relación con la protección de los datos y el manejo de los recursos institucionales. Los resultados obtenidos permiten un diagnóstico general sobre la forma en que la entidad gestiona las herramientas tecnológicas, los controles de salvaguarda y la seguridad de los datos.

Los resultados vinculados con el conocimiento sobre la protección de los datos muestran que una parte importante del personal tiene bajos o escasos niveles de entendimiento acerca de este asunto. La mayor parte de los participantes indican que tienen poco entendimiento o poca formación en la protección de la información empresarial. Este escenario pone en relieve la exigencia de reforzar los procedimientos de enseñanza y concienciación de los empleados, ya que la correcta comprensión de la protección de los datos resulta fundamental para prevenir incidentes,

disminuir las debilidades y promover prácticas adecuadas dentro de la institución.

Asimismo, los resultados que se obtienen señalan que el personal comprende la importancia de la seguridad lógica y corporal dentro de la institución, considerándolas como componentes fundamentales para salvaguardar los sistemas, los registros administrativos, así como sus recursos. Esa visión positiva refleja que existe conciencia acerca de la exigencia de implementar estrategias de seguridad que faciliten el acceso conservar tanto la infraestructura tangible como los recursos informáticos que se utilizan en las actividades cotidianas de la organización.

El diagnóstico, sin embargo, permite también identificar diversas complicaciones en los sistemas de seguridad vigentes, en especial, en aspectos vinculados al dominio de acceso a zonas establecidas, la utilización de dispositivos externos, así como la implementación de procesos formales con el fin de la destrucción de datos. Estas situaciones pueden implicar riesgos susceptibles para la institución, en caso de no existir políticas concretas y controles individualizados que posibiliten garantizar una correcta administración de los datos y de los recursos tecnológicos.

De igual manera los resultados indican que el personal estima que la información que gestiona dentro de sus áreas laborales es sensible, crítica o privada, lo cual evidencia que se observa una percepción clara acerca de la relevancia de salvaguardar los datos institucionales. Este reconocimiento es beneficioso para la entidad, ya que permite implementar normativas de seguridad y cumplir con las normas vinculadas con la seguridad de la información.

En el diagnóstico también se identifica como un punto importante la percepción de los empleados sobre los riesgos que podrían afectar a la entidad, sobre todo los que tienen que ver con el componente humano. El mayor número de encuestados cree que los fallos, descuidos o acciones incorrectas por parte de los individuos son capaces de transformarse en una de las causas principales de vulnerabilidad de la organización. Esto pone de relieve la significación de reforzar la cultura de la seguridad institucional a través de iniciativas de formación, monitoreo y aplicación de prácticas adecuadas en la gestión de la información.

Por último, en cuanto a la gestión de los bienes institucionales, los resultados muestran que

el personal valora la relevancia del mantenimiento y seguridad de los recursos tecnológicos e informativos, aunque también se considera que las medidas de seguridad establecidas serían capaces de reforzarse para asegurar una mejor protección de los bienes esenciales de la entidad. De esta manera, el diagnóstico que se realiza mediante la encuesta permite reconocer la exigencia de implementar innovaciones en los sistemas de seguridad, gestión de riesgos y estrategias de salvaguardia de la información, con el fin de reforzar la seguridad corporativa y disminuir posibles incidentes que podrían afectar la operación de la organización.

4.1.1 Determinación del Alfa de Cronbach

El Alfa de Cronbach constituye una medida estadística que sirve para medir la confiabilidad o solidez interna de una herramienta de medida, como un cuestionario. El coeficiente permite saber qué tan consistentes son los resultados de los ítems que forman parte de una escala, de manera que se tenga la seguridad de que todos están midiendo de forma uniforme un concepto idéntico o variable. Su valor varía de 0 a 1, y cuanto más cercano a 1, mayor será la fiabilidad del instrumento. Este análisis resulta esencial en estudios, ya que asegura la fiabilidad de los datos obtenidos y apoya la exactitud de los resultados.

Se suele emplear la siguiente escala para la interpretación:

Figura 10

Escala de interpretación del Alfa de Cronbach



Nota: En la figura están las escalas que conforman el Alfa de Cronbach

En función de los resultados se tiene que la estadística de los elementos es:

Tabla 2

Estadística de elementos

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza	N de elementos
Medias de elemento	2.541	2.273	2.655	.382	1.168	.032	4
Varianzas de elemento	.663	.077	1.255	1.178	16.293	.438	4

Nota: En la tabla se encuentra la estadística de elementos

La media de los elementos referenciados en la Tabla 2 es de 2,541 con un rango bajo (0,382) y una varianza baja (0,032) lo que indica que los cuatro elementos son valorados de forma bastante uniforme. Esto quiere decir que, en lo que respecta al análisis de riesgo que se ha asumido de los activos de la Unidad Tecnología, no hay diferencias significativas en su nivel promedio de importancia o criticidad. En el contexto de la investigación, indica que los activos relevantes tienen un valor de la entidad comparable a la entidad, además que es un ente financiero, y la información es muy oportuna para mantener la confidencialidad, integridad y disponibilidad.

Por su parte, las varianzas de los elementos cuentan con una mayor dispersión (media de 0.663 y rango de 1.178), lo que indica que, si bien los promedios son similares, hay activos que presentan diferencias internas que obedecen a amenazas o criterios de evaluación determinados. Esto significa que hay activos que pueden ser más vulnerables a ciertas cosas o causar más daño y riesgo que los demás, a pesar de que su valor no sea muy distinto. Como resultado, los hallazgos avalan la necesidad de tener actualizado el inventario y aplicar una metodología de análisis de riesgo que permita hacer frente a estas variaciones y priorizar convenientemente las salvaguardas de la cooperativa.

Tabla 3

Estadística de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
.659	.717	4

Nota: En la tabla se encuentra la estadística de fiabilidad dad en función del Alfa de Cronbach

La Tabla 3 muestra la estadística de fiabilidad del instrumento, el cual fue medido mediante el Alfa de Cronbach. El valor que se obtuvo es el correspondiente a 0.659, mientras que el Alfa de

Cronbach basado en elementos estandarizados es de 0.717 con un total de 4 elementos. Según las estadísticas un alfa mayor que 0.6 ya se considera aceptable en estudios exploratorios y mayor que 0.7 indica adecuada consistencia interna. En este caso, el resultado estandarizado (0.717) evidencia aceptabilidad; lo que denota que los ítems están en coherencia y que son complementarios al momento de medir el constructo.

En el ámbito del análisis, estos resultados evidencian la validez del análisis aplicado para evaluar los activos y riesgos de la Unidad de Tecnología. El adecuado nivel de consistencia interna indica que las preguntas o criterios utilizados para la valorización de los activos están referidos entre sí y dan lugar a resultados confiables para la toma de decisión. A pesar de que el alfa no es de un alto nivel, si se lo tiene suficientemente alto para estudios de tipo descriptivo, aplicado.

4.1.2 Determinación del Chi-Cuadrado

El Chi-cuadrado es un método estadístico muy usado para estudiar la asociación entre variables cualitativas y comprobar si son independientes entre sí. Esta prueba permite contrastar las frecuencias observadas en un estudio con las frecuencias esperadas bajo la hipótesis nula y detectar posibles diferencias significativas. Es de uso habitual en estudios sociales, educativos y científicos, ya que ayuda a tomar decisiones fundamentadas en evidencia al identificar si las diferencias encontradas se atribuyen al azar o a que realmente existe una relación entre las variables analizadas. En función de los resultados se tiene que el Chi-Cuadrado es:

Tabla 4

Chi-Cuadrado

	Valor	**gl**	**Significación asintótica (bilateral)**
Chi-cuadrado de Pearson	17.722[a]	9	.039
Razón de verosimilitud	18.069	9	.034
Asociación lineal por lineal	6.663	1	.010
N de casos válidos	11		

a. 16 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .36.

Nota: En la tabla se encuentra la estadística del Chi-Cuadrado

La tabla de Chi-cuadrado muestran el estadístico de Pearson 17.722; el valor de los grados

de libertad es 9 y la significación asintótica (bilateral) 0.039. Se sostiene que las variables están correlacionadas estadísticamente o que no se distinguen entre sí, dado que este valor es inferior a 0.05. En el mismo sentido, el valor de 18.069 y una significación de 0.034, de la razón de verosimilitud, refuerzan la existencia de asociación. De esta manera, la asociación lineal por lineal tiene un valor de 6.663 con significación de 0.010.

Sin embargo, hay que advertir que el 100 % de las celdas tiene un conteo esperado menor que 5, siendo este de 0.36 el más aceptable que se obtiene. Por lo tanto, en lo que respecta a los resultados de la investigación, se nota que si existe relación entre los factores analizados (probablemente por variables asociadas a los conceptos de seguridad o de riesgo).

4.1.3 Análisis de correlación

La correlación constituye una técnica estadística utilizada para medir y analizar el grado de asociación entre dos o más elementos. Mediante coeficientes como Pearson, Spearman o Kendall, este estudio mide la intensidad y la dirección de la asociación, señalando si las variables tienden a crecer o a decrecer al mismo tiempo. Su uso es esencial en múltiples campos del saber, ya que permite entender patrones, tendencias y potenciales relaciones entre distintos fenómenos, constituyendo una base para tomar decisiones y la realización de estudios más profundas.

Tabla 5

Análisis de correlación

		Media3	Media1
Media2	Correlación de Pearson	1	.816**
	Sig. (bilateral)		.002
	N	11	11
Media1	Correlación de Pearson	.816**	1
	Sig. (bilateral)	.002	
	N	11	11
**. La correlación es significativa en el nivel 0,01 (bilateral).			

Nota: En la tabla se encuentra la estadística del análisis de correlación

El análisis de la correlación de Pearson entre las variables Media1 y Media2 está en la Tabla 5. El coeficiente de correlación que se ha obtenido es r = 0.816 y tiene una significación bilateral de 0.002, con 11 casos válidos. Este valor indica que hay una correlación positiva muy

fuerte, es decir que, si una de las variables se incrementa, la otra también tiende a incrementarse. Asimismo, por tener un nivel de significancia menor a 0.01 se acepta que este vínculo fue significativo al nivel 1%, eliminando la probabilidad de que la relación se deba sólo al azar.

Las dimensiones que se analizan tienen una elevada relación entre sí, según el análisis de los datos, en el contexto de esta evaluación. Esto quiere decir que mejorar uno de los componentes como es el caso de la gestión o control de los activos puede afectar de forma directa a otro, como puede ser el caso de la percepción del riesgo o el impacto sobre la seguridad. Por lo tanto, el resultado refuerza la cohesión interna del análisis y subraya la necesidad de aplicar una metodología integral de gestión de riesgos en el seno de la cooperativa.

4.2 Resultados de diagnóstico de la entrevista

4.2.1 Entrevista a la Jefatura de la Tecnología de la Información

La primera entrevista se dirige a la Jefatura de Tecnología de la Información, donde se obtiene, que la cooperativa tiene un grado de madurez intermedio alto en controles tecnológicos y operativos. Desde el área de TI se observa que existen mecanismos para proteger los activos críticos, como la segmentación de red, controles de acceso físico y lógico, CSOC, backups, renovación del antivirus y clara definición de funciones y responsabilidades. Obsérvese que los activos más críticos para la continuidad de los negocios están adecuadamente identificados, lo que revela un correcto conocimiento técnico.

No obstante, hay debilidades en el manejo integral del riesgo y la formalización de procesos. A pesar de que se habla de la existencia de documentación y algo de metodologías, en ocasiones se da la ausencia de seguimiento continuo de la inteligencia y otra es que se da el escaso uso de fuentes externas. También se muestra que no todos los usuarios reportan incidentes, lo que evidencia una brecha cultural organizacional de seguridad y de sensibilización del personal.

En líneas generales, la cooperativa cuenta con una base tecnológica y controles implementados que funcionan adecuadamente; no obstante, es necesario robustecer aspectos en lo que se refiere a la gestión del riesgo de forma estratégica, el seguimiento permanente de metodologías, la capacitación integral del personal y la mejora en los procesos de evaluación y reporte de incidentes. Esto indica que la organización tiene un nivel de madurez aceptable, pero que hay oportunidades claras para implementar mejoras en la gestión que generen un mejor nivel de seguridad acorde a las buenas prácticas.

4.2.2 Entrevista a la Jefatura de Seguridad Física

La segunda entrevista tiene un nivel de madurez bastante más bajo que la primera, sobre todo en relación con la gestión formal de activos y análisis de riesgos. No existe evidencia de un inventario actualizado de activos críticos; los datos no están clasificados e inexistencia de un mapeo de flujo de la información (data Flow). También se observan distintas deficiencias, como la falta de un procedimiento formal para priorizar recursos y de una valoración estructurada de probabilidades e impactos. Estos elementos suponen debilidades relevantes en la base de la gestión de la seguridad de los datos.

No obstante, se evidencian fortalezas en las capacidades, tanto operativas como físicas. Están equipados con control de ingreso por vigilantes de seguridad, con monitoreo físico centralizada, control de la utilización de USB y colaboración de TI en la detección de fraudes electrónicos. Se incluye en el informe la utilización de la metodología Mosler para la evaluación de riesgos y que en el departamento de Riesgos hay procesos para atender vulnerabilidades. Esto quiere decir que, aunque la gestión documenta y la gestión estratégica son relativas, hay controles que de hecho si existen.

Otro aspecto que se destaca en varias respuestas es “no se tiene conocimiento”, lo que se puede interpretar como que hay falta de comunicación o no se conoce los procesos. Esto indica que, a pesar de que se implementan algunas medidas, no son discutidas formalmente dentro de la institución. La segunda entrevista indica que hay más medidas reactivas que proactivas con controles operativos presentes, pero con debilidades de planificación y de documentación.

4.2.3 Entrevista a la Jefatura de Seguridad Lógica

El análisis de la entrevista realizada para identificar los activos y controles de seguridad en la cooperativa de ahorro y crédito da cuenta del nivel actual de gestión de seguridad de la información que tiene la organización. De acuerdo con lo manifestado según el entrevistado, la entidad ya posee algunos controles fundamentales en algunas dimensiones. Sobre todo, estos controles se realizan sobre el control físico de seguridad y algunas tareas operativas de la tecnología. Sin embargo, se observarán diversas debilidades relevantes en la administración organizada de la ciberseguridad, al igual que en los procedimientos formales de manejo de riesgos.

El primer problema principal detectado es la falta de un inventario reciente de los activos críticos. Según lo que menciona el entrevistado, este proceso no se encuentra implementado, lo

que quiere decir que la organización no tiene plenamente identificados todos sus recursos tecnológicos, su información, sus sistemas o su personal clave. Esta circunstancia representa una gran debilidad por cuanto sin un inventario de activos resulta difícil definir prioridades de protección, identificar riesgos o asignar controles de seguridad.

Otra cosa por destacar es que la información no está clasificada según su grado de severidad o confidencialidad. La ausencia de clasificación no nos permite gestionar la información según su grado de sensibilidad, lo que podría acarrear riesgos de exposición o manipulación incorrecta de datos financieros o de clientes. También, la entrevista muestra que no se lleva a cabo un proceso formal de identificación y documentar vulnerabilidades.

Asimismo, hay que destacar que la gestión de riesgos presenta un punto débil importante, que es el de no medir formalmente los impactos y las probabilidades de los incidentes de seguridad. Esto es indicativo de que la organización no hace uso de metodologías estructuradas para el análisis de riesgos, como marcos de referencia de carácter internacional. La falta de una metodología formal complica las decisiones estratégicas en seguridad de la información e impide la planificación de medidas preventivas.

A pesar de sus debilidades, tiene algunas fortalezas en aspectos concretos. Se observan controles físicos instalados en el acceso a las áreas críticas con personal de seguridad y controles de acceso. También se indica que hay una política de ciberseguridad y que hay unos roles y responsabilidades para la ciberseguridad. Los trabajadores de la construcción reciben capacitaciones que permiten crear conciencia sobre la seguridad y la importancia de aplicar buenas prácticas, como la planificación de tareas en función de sus riesgos.

Dentro del área tecnológica, se pueden ubicar unos controles que realiza el departamento de TI. Lo primero es que hay una segmentación de redes, un control de acceso y el manejo de mecanismos que logran detectar el fraude electrónico. Además, el uso de USB será controlado por el área de tecnología, a fin de minimizar ciertos riesgos.

En la entrevista también se encuentran limitaciones en el uso de copias de seguridad y el conocimiento de herramientas contra código malicioso. El entrevistado señala que no tienen conocimiento de la realización de pruebas de respaldos ni de la implementación de herramientas antimalware, posiblemente por una falta de comunicación entre áreas o simplemente porque no hay procesos formales de monitoreo y control en estos aspectos.

Finalmente, los activos esenciales que surgen en la entrevista fueron, principalmente, los datos e información financiera; la tecnología e infraestructura; los procesos y operaciones de la cooperativa; el personal y la cadena de suministro de dinero. Estos elementos son esenciales para la continuidad del negocio y requieren una protección adecuada con controles de seguridad técnicos, organizacionales y físicos.

4.3 Diseñar un inventario

La cooperativa de ahorro y crédito modificó su inventario de activos de datos hasta marzo de 2026, basándose en la metodología que la institución aplicó a finales del año 2021. Esta metodología en su momento asignó un valor a cada activo de información de acuerdo con los parámetros de confidencialidad, integridad y disponibilidad con los pesos asignados del 40%, 35% y 25% respectivamente.

Del levantamiento ejecutado en 23 áreas operativas, fueron detectados 177 activos relacionados con la información. De ellos 79 fueron catalogados como información privada, 72 como restringida, 16 en calidad de uso interno y 10 de carácter público. Estos resultados muestran que una parte significativa de la información administrativa tiene un grado de sensibilidad alto, lo que requiere controles adecuados para su protección.

Para complementar esta clasificación se tomó como guía el proyecto del Esquema Gubernamental de Seguridad de la Información (EGSI), el mismo que se encuentra estructurado conforme a la ISO 27005 y la metodología de análisis de riesgo MAGERIT, para manifestar la valoración de los activos en niveles alto, medio y bajo. Con este criterio el inventario actualizado arrojó 75 activos con valoración Alta, 88 con valoración Media y 14 con valoración Baja. Esto permite determinar que la mayoría de los activos administrativos necesitan un nivel de seguridad medio-alto.

Para efectos de este estudio, se seleccionaron los activos más importantes de la Unidad de Tecnologías de la Información para el análisis de riesgos, teniendo en cuenta los activos primarios y de soporte de acuerdo con la clasificación propuesta por la norma ISO 27005. Los activos primarios comprendieron la base de datos institucional y sus copias de apoyo, y los activos de soporte fueron elementos de hardware, software, red, personal y sitio, por su directa incidencia en la continuidad operativa de la cooperativa.

Por lo que cada activo con la respectiva valoración de las amenazas, vulnerabilidades y

riesgos se dan en el Anexo 2 del presente documento. Con respecto a estos resultados, se resume lo más significativo en la siguiente tabla:

Tabla 6

Resumen de análisis de riesgo de activos de TI

Categoría de Activo	Nivel de Riesgo	Hallazgos Clave (Riesgos Altos)	Impacto en el Negocio
Información (Base de Datos)	Alto	• Falla en climatización.	• Pérdida de disponibilidad de datos críticos.
		• Error de configuración en la BD.	• Interrupción del servicio a socios.
		• Indisponibilidad de personal capacitado.	• Posible pérdida o corrupción de información financiera.
Hardware (Servidor de BDD, Servidor de Aplicaciones)	Alto	• Manipulación de hardware, espionaje, sabotaje	• Incidentes en la seguridad de hardware
Software (Core Financiero, AD)	Alto	• Fallo del dispositivo/sistema (denegación de servicio).	• Pare total de la operación (Core Financiero).
		• Políticas de AD no aplicadas (seguridad de equipos).	• Acceso inseguro a la red corporativa.
Redes (Switch Core, Firewall)	Alto	• Avería del Switch Core por problemas eléctricos.	• Caída de la red central, aislando todas las agencias.
		• Errores de administración en Firewall.	• Vulnerabilidad ante ciberataques.
		• Denegación de servicio por ataques externos.	• Indisponibilidad de servicios a socios.
Personas (Jefe TI, Asistentes de Soporte)	Alto	• Indisponibilidad de personal clave (Jefe TI).	• Cuello de botella en decisiones críticas.
		• Mal uso de control de acceso a áreas restringidas.	• Riesgo de incidentes de seguridad física y lógica.
Sitio/Ubicación (Eléctrico, Climatización, UPS, Generador)	Alto	• Múltiples riesgos: Fallo de proveedores, sobrecargas, cortocircuitos, falta de mantenimiento del generador, control de acceso deficiente al área de UPS.	• Es la categoría con mayor concentración de riesgos altos. Una falla aquí impacta a TODOS los demás activos (servidores, redes, personas).

Nota: En la tabla se encuentra un resumen de los riesgos y su impacto.

La evaluación de estos activos identificó que los elementos más críticos son la base de datos, copias de seguridad, core financiero, servidor de directorio activo, switch de core, firewall,

servidor de base de datos, servidor de aplicaciones y encargado de tecnología, todos los cuales alcanzaron una alta valoración. Por su parte, los activos de infraestructura tangible como el sistema eléctrico, sistema de climatización, generador de energía y sistema UPS fueron evaluados principalmente en nivel medio, considerando que su mayor repercusión se concentra en disponibilidad de los recursos tecnológicos.

Posteriormente, en relación con cada activo se detectaron las amenazas y vulnerabilidades significativas, tomando en calidad de referencia los catálogos propuestos por EGSI, MAGERIT e ISO 27005. El riesgo se evaluó basado en la relación entre la valoración del activo, el nivel de amenaza y el de vulnerabilidad, lo que permitió categorizar el riesgo como bajo, medio o alto.

En líneas generales, los resultados reflejan que los riesgos más importantes se encuentran en la operación continua de la plataforma tecnológica, el abastecimiento de servicios esenciales, la confianza del equipo de sitio y la probabilidad de errores de ajuste o administración. En los activos de información y software se destacan riesgos vinculados con interrupciones eléctricas, dificultades de climatización, errores de ajuste, indisponibilidad de los empleados y negación de servicio. En los activos de hardware se refiere más al incumplimiento de procesos por parte del factor persona o usuario, considerando aquí a los empleados de la institución. En los activos de red se identificaron riesgos altos asociados a fallas de hardware, fallos de administración y amenazas externas. En los activos del personal existen riesgos vinculados con la falta del capital humano y errores en actividades críticas. Por último, en los activos de sitio junto con la infraestructura se identifican elevados riesgos asociados al suministro eléctrico, al control de los accesos físicos y a la continuidad de la asistencia energética.

El análisis también pone en evidencia que la cooperativa cuenta con controles ya implementados, en los cuales se encuentran UPS de data center, UPS centralizado, fuente de energía, categorización de red, normativas de acceso, monitoreo de avisos, redes complementarias, apoyos de configuración, controles de acceso presencial y esquemas de personal backup. No obstante, se detectan oportunidades de reforzamiento fundamentalmente en la conservación preventiva, formalización de las obligaciones, validación regular de los respaldos, mejora del sistema de control de acceso físico, formación del personal y adopción de estrategias de emergencia complementarias.

En resumen, el estudio indica que la cooperativa situada en la ciudad de Tulcán gestiona

un significativo conjunto de activos que son de alto valor para la operación comercial y con una proporción considerable de riesgos medios y altos, especialmente en el departamento de Tecnologías de la Información. Por lo tanto, se hace necesario mantener y reforzar los controles existentes, teniendo en cuenta aquellos activos cuya afectación pudiera poner en riesgo la continuidad de la empresa, la seguridad de la información y la prestación de servicios a colaboradores y clientes.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se determina que la actualización del inventario de activos informáticos facilitó una identificación, valoración y gestión más exacta de los recursos esenciales de la "Unidad de Tecnología de la Cooperativa de Ahorro y Crédito". El uso de una metodología para el análisis de riesgos permitió fortalecer los principios de integridad, disponibilidad y confidencialidad. Se evidenció que la mayor parte de los activos tienen grados de peligro medio y alto, lo que hace necesaria la implementación de controles más sólidos y recientes.

Con respecto al primer objetivo específico, la recolección de datos permitió encontrar un total de 177 activos de información en diferentes partes de la cooperativa. De estos, una parte importante es información que se considera privada y restringida. Esto indica que la organización tiene información muy sensible y que es muy importante que sepa cómo manejarla para mantener la seguridad.

Respecto del segundo objetivo específico, se puede concluir que, al priorizar los activos a través de la aplicación de un análisis de riesgos, los elementos más esenciales están vinculados fundamentalmente a la base de datos, sistemas principales, infraestructura tecnológica y equipos de sitio. Igualmente se encontró que se encuentran riesgos significativos asociados a defectos técnicos, errores humanos y fallas en los procesos, lo que confirma la relevancia de implementar estrategias elaboradas para una correcta implementación de decisiones.

En relación con el tercer objetivo específico, la planificación del inventario actualizado facilitó la estructuración y clasificación de los activos en escalas relativos al valor (alto, medio y bajo), optimizando su gestión y tratamiento. La adaptación de métodos como EGSI, MAGERIT e ISO 27005 también facilitó el establecimiento de unos criterios claros con el fin de evaluar del impacto y el riesgo, lo que contribuyó a una mejor organización de controles y acciones de seguridad.

Se concluye que la identificación los activos de información y el análisis del riesgo aplicado a la organización, son un requisito para dar cumplimiento con la Ley Orgánica de

Protección de Datos Personales, como se lo indica en su artículo 37 y artículo 40, donde el delegado de esta función deberá garantizar la confidencialidad, integridad y disponibilidad de los datos, donde podrá basarse en una metodología para la gestión de riesgos.

Las encuestas aplicadas a las áreas operativas arrojaron datos importantes referentes a la falta de políticas bien establecidas, y sobre todo en determinar los controles adecuados al activo de personas, donde se requiere tener conciencia y formación en términos de seguridad de la información.

De acuerdo con las entrevistas generadas con los responsables de TI, Seguridad Física y Lógica, la organización necesita de un inventario de activos actualizado, con el fin de generar las alertas adecuadas en cuanto a seguridad, conociendo de esta manera los nuevos activos generados en cada área operativa, e identificar si se le da el tratamiento de seguridad adecuado.

Finalmente, la combinación de los dos métodos estadísticos permitió una visión esencial y confiable de los resultados de una investigación. El alfa de Cronbach apoyó la consistencia interna de los instrumentos empleados, el Chi-cuadrado hizo posible revelar las relaciones existentes entre las variables clasificadas y el coeficiente de Pearson midió la intensidad y dirección con respecto a las variables cuantitativas. La exactitud y la credibilidad del análisis estadístico mejoraron gracias a estas herramientas, lo que permitió conseguir resultados seguros y con una buena fundamentación.

5.2 Recomendaciones

Respecto de la actualización del inventario para reforzar la confidencialidad, integridad y disponibilidad, se recomienda la implementación de una metodología de análisis de riesgo que se ejecute de manera frecuente o ante cambios relevantes en la infraestructura tecnológica u organizacional. Asimismo, se requiere la implementación de un sistema de monitoreo y supervisión continuo que permita la identificación oportuna de nuevos riesgos y el ajuste de las salvaguardas respectivas.

En relación con la recolección de datos acerca de los activos, se recomienda crear un tratamiento oficial para reconocer y documentar los activos en cada uno de los departamentos, incluyendo la clasificación de la información según su nivel de protección. También se recomienda reforzar esta estrategia con iniciativas de capacitación y sensibilización de los empleados, con el

fin de mejorar la comprensión sobre protección de los datos y reducir vulnerabilidades asociadas al factor humano.

Se sugiere que la cooperativa efectúe formalmente un método estándar durante el proceso de análisis de peligros para priorizar y relacionar beneficio a los activos, asegurando que dicha implementación programada se aplique a todos los activos esenciales. También es crucial fortalecer la supervisión de los recursos más esenciales (redes, bases de datos, equipos clave, computadoras y activos informáticos), mediante auditorías, ambientes para pruebas regulares y administración de incidentes.

Se recomienda que el inventario actualizado de activos se incorpora a un Sistema de Gestión de Seguridad de los Datos (SGSI). Esto permitirá una gestión unificada, trazabilidad y mejoramiento continuo. De igual forma, se propone la implementación de plataformas tecnológicas que permitan la automatización del manejo, el ordenamiento y la valoración de activos, lo cual facilitará la toma de decisiones basada en los riesgos presentes.

Se recomienda nombrar formalmente a una persona encargada que vele por el cumplimiento de la Ley Orgánica de Protección de Datos Personales, y con ello pueda implementar las medidas técnicas necesarias y apropiadas, referentes a la seguridad de la información que maneja la organización.

Es recomendable dar continuidad al análisis de riesgo con el fin de mantener actualizado el inventario de los activos, y de esta manera identificar nuevos activos y que los controles implementados sean adecuados, así como también avanzar en el tratamiento de aquellos activos considerados con alto impacto con el fin de implementar nuevos controles que ayuden a disminuir el riesgo identificado.

Se recomienda completar estas técnicas estadísticas mediante una configuración adecuada del diseño de estudio y una elección apropiada de la muestra, a fin de garantizar la calidad de las observaciones desde el principio. Por otra parte, es fundamental analizar los resultados de forma holística y no de manera individual, considerando el contexto del estudio. De tal manera que el coeficiente alfa de Cronbach, Chi-cuadrado y correlación de Pearson, no solamente serán herramientas de análisis, sino también soporte en la toma de decisiones más exactas y fundamentadas.

REFERENCIAS

Aguilar, P. (2022). *Plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC27001:2013* [Proyecto de investigación, Pontificia Universidad Católica del Ecuador - Sede Ambato]. https://repositorio.puce.edu.ec/items/5887eac6-18b6-4c11-8743-927c81a27c73/full?utm_source

Aguilar, P., & Balseca, J. (2024). Tendencias, Desafíos y Vulnerabilidades de los Ataques Cibernéticos en Ambientes de Desarrollo. Revisión Sistemática. *Estudios y Perspectivas Revista Científica y Académica*, *4*(4), 517-539. https://doi.org/https://estudiosyperspectivas.org/index.php/EstudiosyPerspectivas/article/view/689

Aimacaña, V., Estrella, N. C., & Razo, C. (2024). Análisis de los indicadores financieros en las cooperativas de ahorro y crédito segmentación 3, de la provincia de Tungurahua, de la ciudad de Ambato 2021. *Boletín de Coyuntura*, (40), 15-27. https://doi.org/https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/2292

Álvarez, N., & Rodríguez, H. (2025). La filosofía como fundamento crítico de la investigación científica: Revisión de enfoques y corrientes. *Revista Arbitrada Investigación y Creatividad | Dirección de Investigación*, *22*(1), 7-22. https://doi.org/https://revistasuba.com/index.php/INVESTIGACIONYCREATIVIDAD/issue/view/91?utm_source

Alvarez-López, L. D. (2023). HUMANOS 5.0: El recurso humano, activo fundamental para la competitividad. *Revista Científica Internacional*, *6*(1), 41-50. https://doi.org/https://revista-cientifica-internacional.org/index.php/revista/article/view/63

Angulo, D. (2024). *Análisis de un sistema de gestión de seguridad de la información para la PUCEE basado en la norma ISO 27001* [Tesis de grado, Pontificia Universidad Católica del Ecuador - Sede Esmeraldas]. https://repositorio.puce.edu.ec/items/7248f114-244f-485c-a713-ad381ddbf052

Arellano, C. (2023). *Modelo de gestión de la seguridad de la información en una institución financiera*

cooperativa [Proyecto de investigación, Pontificia Universidad Católica del Ecuador - Sede Ambato]. https://repositorio.puce.edu.ec/items/33ccc110-78e3-4b72-a3ac-924d5bfcb414/full?utm_source

Arteaga, Y. (2025). Estrategias innovadoras en seguridad y tecnología para la prevención del crimen organizado y el narcotráfico. *Bastcorp International Journal*, *4*(1), 391-406. https://doi.org/https://editorialinnova.com/index.php/bij/article/view/257

Aven, T. (2023). A risk and safety science perspective on the precautionary principle. *Safety Science*, *165*, 106211. https://doi.org/https://linkinghub.elsevier.com/retrieve/pii/S0925753523001534

Ávila, A. (2024). Seguridad de la información en instituciones públicas: Desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, *4*(2), 140-156. https://doi.org/https://economicsocialresearch.com/index.php/home/article/view/96

Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, 1-20. https://doi.org/https://link.springer.com/10.1007/s42786-025-00056-3

Bakker, B., Garcia, B., Lian, W., Liu, Y., Perez, C., Siddiq, A., Sumlinski, M., Vasilyev, D., & Yang, Y. (2023). *Fintech note: The Rise and Impact of Fintech in Latin America* (p. 61) [Informe / Nota de política]. International Monetary Fund. https://www.imf.org/en/-/media/files/publications/ftn063/2023/english/ftnea2023003.pdf

Bastis. (2024, agosto 30). Investigación de Campo. *ONLINE-TESIS*. https://online-tesis.com/investigacion-de-campo/

Bermeo, E., Erazo, G., & Andrade, D. (2025). Análisis de Riesgos Laborales mediante Realidad Virtual: Estrategias para la Gestión de Proyectos. *Resistances. Journal of the Philosophy of History*, *6*(12), e250194. https://doi.org/https://resistances.religacion.com/index.php/about/article/view/194

Bonderud, D. (2024). Cost of a Data Breach 2024: Financial Industry Insights [Entrada de blog / Artículo informativo]. *IBM Think Blog – Insights*. https://www.ibm.com/think/insights/cost-of-a-data-

breach-2024-financial-industry

Camacho, M., & Carranco, S. (2025). Análisis de los sistemas de gestión riesgo laborales en las empresas. Una revisión sistemática. *RECIMUNDO*, *9*(1), 765-782. https://doi.org/https://recimundo.com/index.php/es/article/view/2544

Cárdenas, J., Reyes, J., & Rojas, M. (2023). Assessing Internal Control Effectiveness in Credit Unions: A Coso-Based Study. *International Journal of Professional Business Review*, *8*(11), e04006. https://doi.org/https://www.openaccessojs.com/JBReview/article/view/4006

Ceci, L. (2025, febrero 17). Tiempo diario dedicado a internet a través del móvil por usuarios de todo el mundo en 2024, por región. *statista*. https://www.statista.com/statistics/1288783/daily-time-spent-online-via-mobile/#statisticContainer

Chang, Y., Heller, O., Shlomo, Y., Bar-Noy, I., Bokobza, E., Grinstein, M., & Zhang, N. (2025). *Mind the Gap: Revealing Security Barriers through Situational Awareness of Small and Medium Business Key Decision-Makers* (arXiv:2506.10025). arXiv. https://doi.org/http://arxiv.org/abs/2506.10025

Chen, H., Wang, P., & Ji, Q. (2022). Analysis of the Application Effect of PDCA Cycle Management Combined With Risk Factor Management Nursing for Reducing Infection Rate in Operating Room. *Frontiers in Surgery*, *9*, 837014. https://doi.org/https://www.frontiersin.org/articles/10.3389/fsurg.2022.837014/full

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/https://linkinghub.elsevier.com/retrieve/pii/S245195882200001X

Colina, A., & Túa, J. (2020). Activos informáticos: Un referente en la caracterización de procesos de la gestión riesgos de TI. *INNOVA Research Journal*, *5*(3.2), 196-213. https://doi.org/https://revistas.uide.edu.ec/index.php/innova/article/view/1608

Doris, S. (2023). *Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria*

(SEPS) [Trabajo de Titulación, Universidad Estatal Península de Santa Elena]. https://repositorio.upse.edu.ec/items/31b5b3b5-0f9b-4212-860d-4ba596d1c8f4/full?utm_source

Dove, E. S. (2023). Confidentiality, public interest, and the human right to science: When can confidential information be used for the benefit of the wider community? *Journal of Law and the Biosciences*, *10*(1), lsad013-. https://doi.org/https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsad013/7197746

Espinoza-Freire, E. E., & Calva-Nagua, D. X. (2020). La ética en las investigaciones educativas. *Revista Científica de la Universidad de Cienfuegos*, *12*(4), 333-340. https://doi.org/http://scielo.sld.cu/pdf/rus/v12n4/2218-3620-rus-12-04-333.pdf

Giler, J., Alvarado, K. J., Yela, R., Choez, F., & Garcia, J. (2024). Impacto de la digitalización en el sector bancario ecuatoriano: Transformaciones, desafíos y oportunidades para el futuro financiero. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *5*(5), 936-953. https://doi.org/https://latam.redilat.org/index.php/lt/article/view/2658

Guamán, M., Carrillo, J., Flores, C., Flores, C., & Ron, M. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*(49), 139-165. https://doi.org/https://journalprosciences.com/index.php/ps/article/view/676/721

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO*, *3*(4), 163-173. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Ige, A., Chukwurah, N., Idemudia, C., & Adebayo, V. I. (2024). Managing Data Lifecycle Effectively: Best Practices for Data Retention and Archival Processes. *International Journal Of Engineering Research And Development*, *20*(7), 453-461. https://doi.org/https://www.researchgate.net/publication/388387603_Managing_Data_Lifecycle_Effectively_Best_Practices_for_Data_Retention_and_Archival_Processes

Kaulwar, P. (2024). Cybersecurity Risk Management in Financial Institutions: A Multi-Layered

Approach to Safeguarding Data, Preventing Breaches, and Enhancing Regulatory Compliance. *Journal of Electrical Systems (JES)*, *20*(10), 3866-3877. https://doi.org/https://journal.esrgroups.org/jes/article/view/8275/5579

León, S., & Murillo, D. (2021). Análisis Financiero: Gestionar los riesgos en las Cooperativas de Ahorro y Crédito segmento 1. *Revista Arbitrada Interdisciplinaria Koinonía*, *6*(12), 242. https://doi.org/https://fundacionkoinonia.com.ve/ojs/index.php/revistakoinonia/article/view/1289

Ley Orgánica de Protección de Datos Personales, Legislation No. Registro Oficial Suplemento No. 459, 38 (2021). https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf?utm_source=chatgpt.com Aprobada por la Asamblea Nacional del Ecuador, publicada en el Registro Oficial Suplemento 459 el 26 de mayo de 2021.

Llano, A., Gaibor, M., Cruz, C., & Cadena, J. (2022). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Revista Ciencias de la Ingeniería y Aplicadas*, *4*(1), 82-98. https://doi.org/https://investigacion.utc.edu.ec/index.php/ciya/article/view/374/361

Lucio, E., & Campaña, E. (2024). Desafíos y estrategias de ciberseguridad para pequeñas empresas. *Gestio et Productio. Revista Electrónica de Ciencias Gerenciales*, *6*(11), 18-36. https://doi.org/https://iieakoinonia.org/ojs3/index.php/gestioep/article/view/151

Mariño, E. (2022). *Obtención de una base de datos de temperatura, corriente y caída de tensión de la evolución de un falso contacto de un terminal en un circuito eléctrico energizado* [Trabajo de Integración Curricular, Escuela Superior Politécnica De Chimborazo]. https://dspace.espoch.edu.ec:8080/server/api/core/bitstreams/7a813877-ef73-4434-ae66-8d3fce481238/content

Mera, I. (2022). *Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: Empresa ALTAC* [Trabajo de Titulación, Pontificia Universidad Católica del Ecuador]. https://repositorio.puce.edu.ec/items/3ac14304-ef60-4eeb-a4e1-

0b4a0dd1aa8c?utm_source

Monterrubio, E. (2024). Hardware. *Con-Ciencia Serrana Boletín Científico de la Escuela Preparatoria Ixtlahuaco*, *6*(11), 6-8. https://doi.org/https://www.researchgate.net/publication/377201940_Hardware

Mungabusi, L. (2022). *Modelo de gestión de seguridad de la información en entidades financieras cooperativas* [Proyecto de investigación, Pontificia Universidad Católica del Ecuador - Sede Ambato]. https://repositorio.puce.edu.ec/items/3ef29e80-ea25-47f3-bc3c-8be539351190?utm_source

Navarro, D., Suárez, F., & Navajas, S. (2025). *Perspectivas sobre transformación digital, fintech e inclusión financiera: América Latina y el Caribe* (p. 59) [Informe técnico]. Banco Interamericano de Desarrollo (BID). https://publications.iadb.org/es/perspectivas-sobre-transformacion-digital-fintech-e-inclusion-financiera-america-latina-y-el-caribe?utm_source

Nikhil, M., & Sreevidya, U. (2025). Cyber risk management in the financial sector: An evaluation of current practices in modern scenarios. *International Journal of Research in Finance and Management*, *8*(1), 789-793. https://doi.org/https://www.allfinancejournal.com/article/view/508/8-1-101

Núñez, J. (2025). *Modelo para la Gestión de Seguridad de la Información en Cooperativas de Ahorro y Crédito del Segmento 1 Basada en ISO/IEC 27001:2022* [Proyecto de titulación, Universidad Tecnológica Israel]. https://doi.org/http://repositorio.uisrael.edu.ec/xmlui/handle/47000/4312

Padua, W. (2025). Metodología Cuantitativa para la Gestión del Riesgo Tecnológico y Cibernético en Entidades Financieras de la República Dominicana. *Revista Veritas de Difusão Científica*, *6*(2), 245-277. https://doi.org/https://revistaveritas.org/index.php/veritas/article/view/631

Páez, M., & Portilla, D. (2024). Metodología Magerit para la evaluación de riesgos de activos de información, caso Instituto Superior Tecnológico Nelson Torres. *Revista Nexos Científicos*, *8*(1), 1-11. https://doi.org/https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/88

Pérez, A., & León, R. (2021). Elementos que connotan la gestión de riesgo en emergencias sanitarias.

Retos de la Dirección, *15*(1), 97-121. https://doi.org/http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2306-91552021000300097

Prabawa, A., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4), 625-633. https://doi.org/http://thesai.org/Publications/ViewPaper?Volume=14&Issue=4&Code=IJACSA&SerialNo=68

Reji, J. (2024). Cybersecurity in Financial Institutions: Risks and Safeguards. *International Journal of Research Publication and Reviews*, *5*(3), 2758-2764. https://doi.org/https://ijrpr.com/uploads/V5ISSUE3/IJRPR23670.pdf

Resolución SEPS-IGT-2025-0113 - Norma de control para la prevención, detección y combate del delito de lavado de activos y la financiación de otros delitos en las entidades del sector financiero popular y solidario, Legislation No. Suplemento Nº 102 — Registro Oficial (Registro Oficial Suplemento Nº 102), 53 (2025). https://www.seps.gob.ec/wp-content/uploads/Resolucion-N%C2%B0-SEPS-IGT-2025-0113.pdf Emitida por SEPS como norma de control en cumplimiento de sus atribuciones de supervisión del sector financiero popular y solidario, en concordancia con el marco legal vigente del sector financiero y las normas de prevención de lavado de activos.

Reyna, J., Lema, S., & Freire, L. (2023). *Administración del ciclo de vida de un proyecto para el desarrollo de un portal web de monitoreo satelital utilizando la metodología PMI* [Guayaquil, Tesina de Seminario]. https://www.dspace.espol.edu.ec/handle/123456789/46019

Rodríguez, H., & Moreno, C. (2024). Seguridad de la información y ciberseguridad: Su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas Revista Científica y Académica*, *4*(1), 159-178. https://doi.org/https://estudiosyperspectivas.org/index.php/EstudiosyPerspectivas/article/view/90

Sacoto, M., & Sánchez, C. (2023). Vulnerabilidades de los elementos esenciales y evaluación integral del

riesgo de desastres para la planificación urbana y la gestión del riesgo en Azogues, Ecuador. *Cuadernos de Investigación Geográfica*, *49*(1), 163-190. https://doi.org/https://publicaciones.unirioja.es/ojs/index.php/cig/article/view/5628

Salinas, J. (2025). El tratamiento de la incertidumbre y la espera en la toma de decisiones y gestión del riesgo estratégicos. *Revista IECOS*, *26*(2), 1-25. https://doi.org/https://revistas.uni.edu.pe/index.php/iecos/article/view/2684

Sánchez, C. (2025). Análisis de riesgos de ejecución en proyectos de desarrollo institucional con componentes de tecnología de información. *Revista InveCom*, *5*(3), 1-13. https://doi.org/https://ve.scielo.org/scielo.php?pid=S2739-00632025000300168&script=sci_arttext

Shafiei, H., Khonsari, A., & Mousavi, P. (2022). Serverless Computing: A Survey of Opportunities, Challenges, and Applications. *ACM Computing Surveys*, *54*(11s), 1-32. https://doi.org/https://dl.acm.org/doi/10.1145/3510611

Vasquez, C., & Delgado, J. (2021). Gestión del riesgo de desastres para mejorar el ordenamiento territorial en municipalidades. *Ciencia Latina Revista Científica Multidisciplinar*, *5*(1), 165-186. https://doi.org/https://ciencialatina.org/index.php/cienciala/article/view/214

Veloz, E. (2022). Componentes de calidad software y su utilización en aplicaciones web. *Ciencia Latina Revista Científica Multidisciplinar*, *6*(3), 3193-3204. https://doi.org/https://ciencialatina.org/index.php/cienciala/article/view/2456

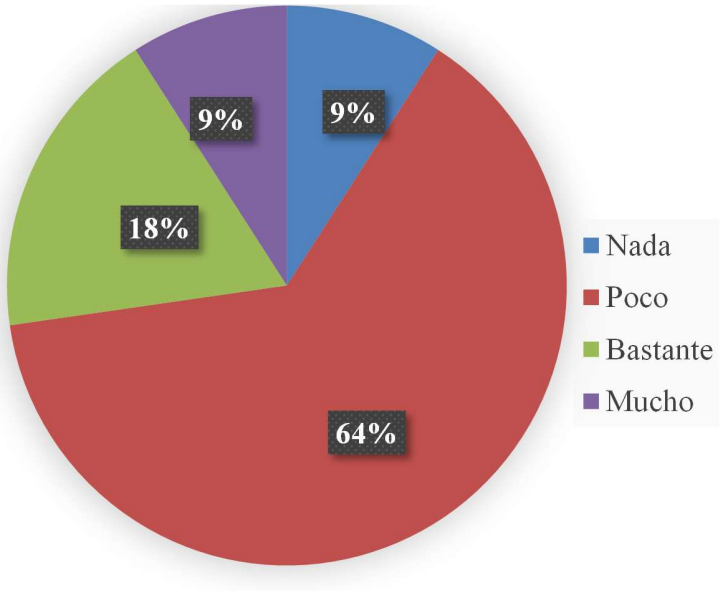
Waliullah, Hossain, Z., Hasan, T., Alam, K., Khatun, M., & Alam, N. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226-257. https://doi.org/https://ajates-scholarly.com/index.php/ajates/article/view/12

Zorrilla, A. (2021, enero 8). ¿Cómo se realiza una investigación documental o bibliográfica? *CAMPUS digital idyd*. https://campusidyd.com/investigacion-documental-o-bibliografica/

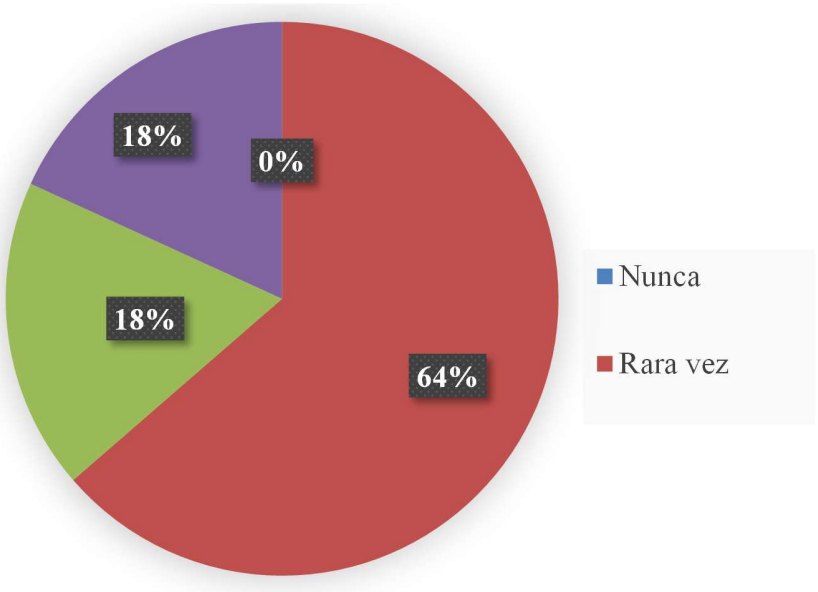
ANEXOS

Anexo 1. Resultado de los encuestados

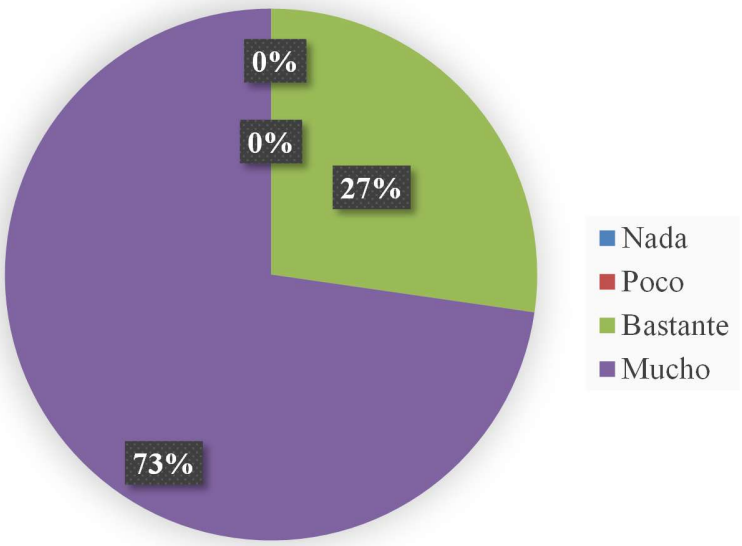
1. **¿Que tanto conoce sobre seguridad de la información?**



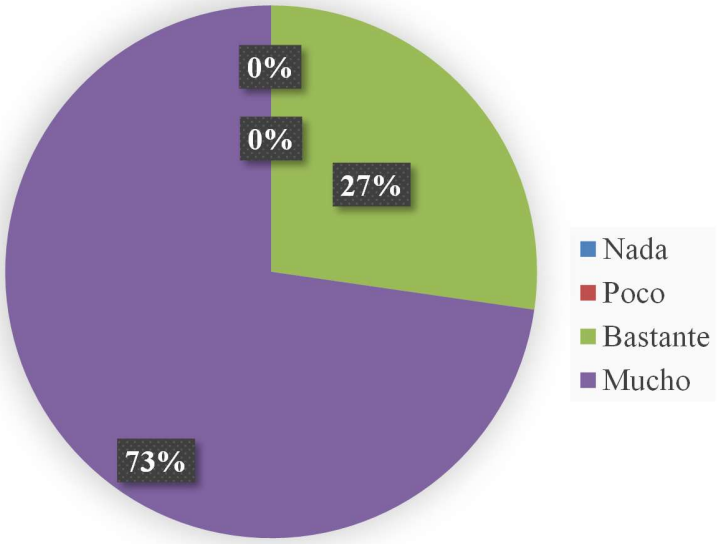
2. **Usted y/o su equipo de trabajo, ¿Han recibido capacitación sobre la protección de información institucional?**



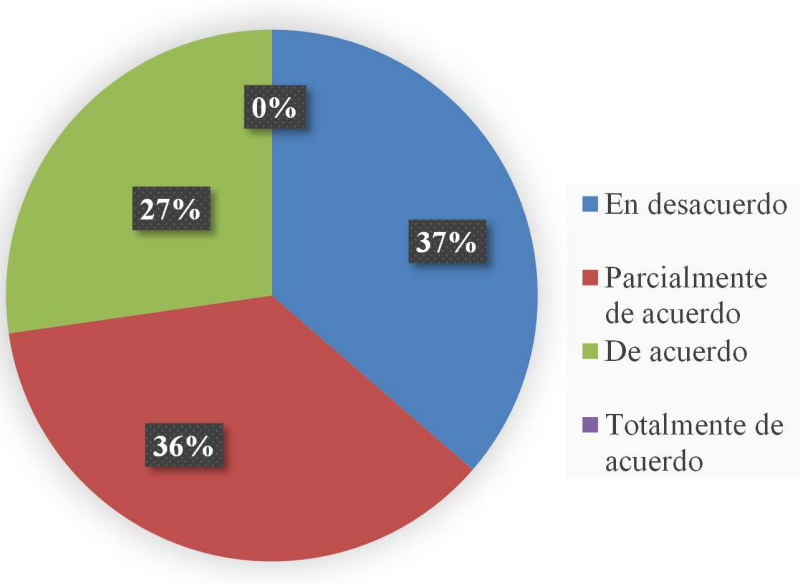
3. **¿Qué tan importante es para Usted, la seguridad física en la institución?**



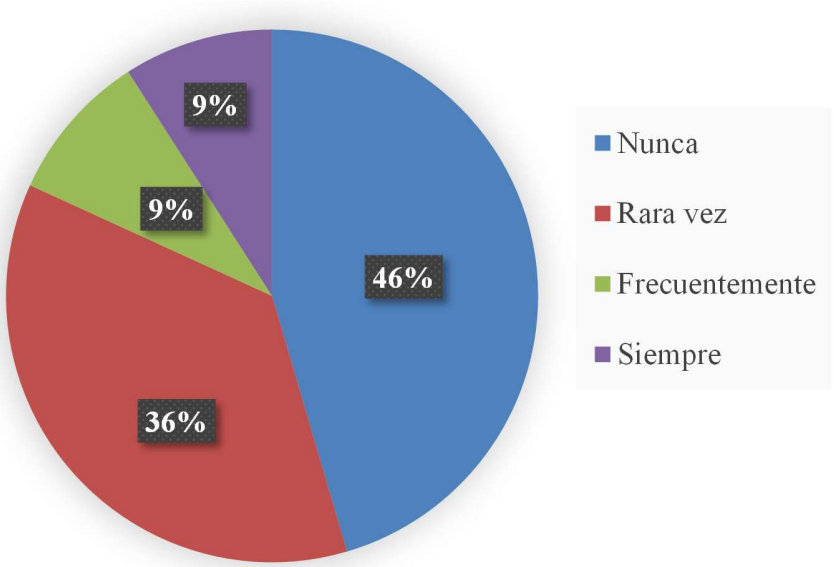
4. **¿Qué tan importante es para Usted, la seguridad lógica en la institución?**



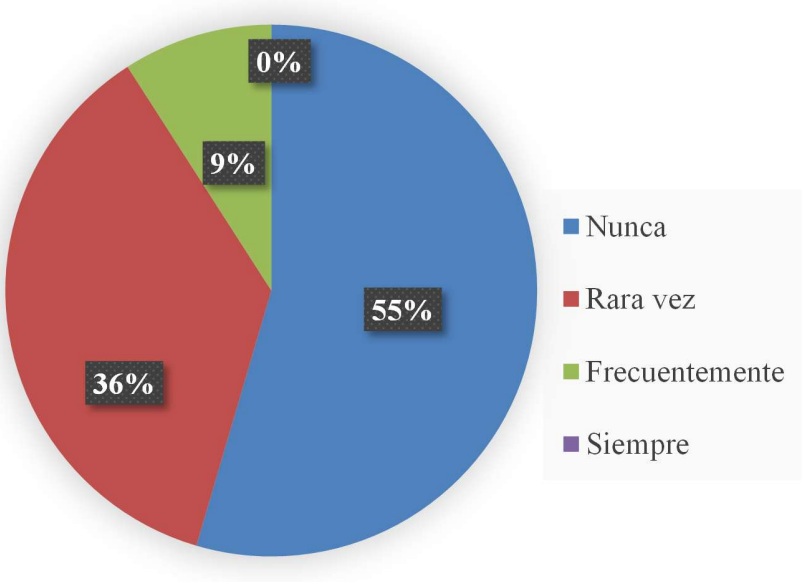
5. **¿Está de acuerdo con el número de personas que están a cargo de la seguridad en la institución?**



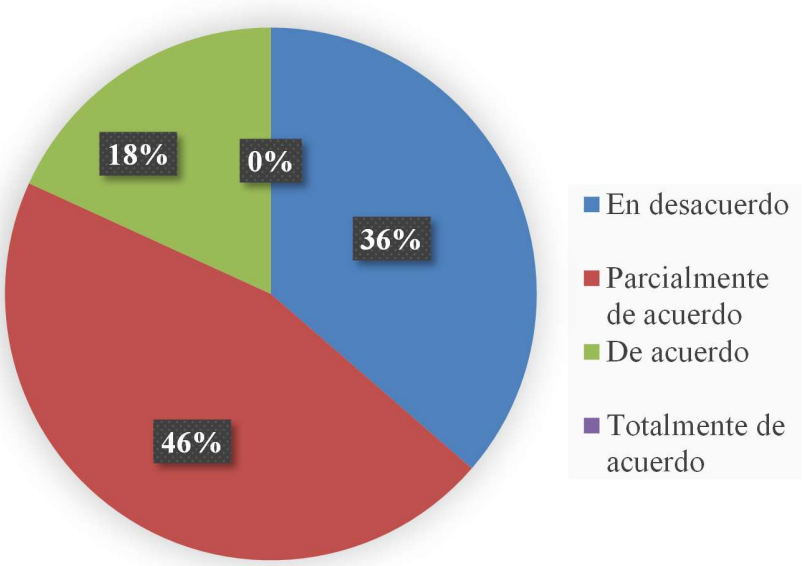
6. **¿Se realiza algún control, procedimiento o registro, cuando ingresan personas a su departamento?**



7. **¿Alguna vez, se ha presentado algún robo o alteración de información en su área?**

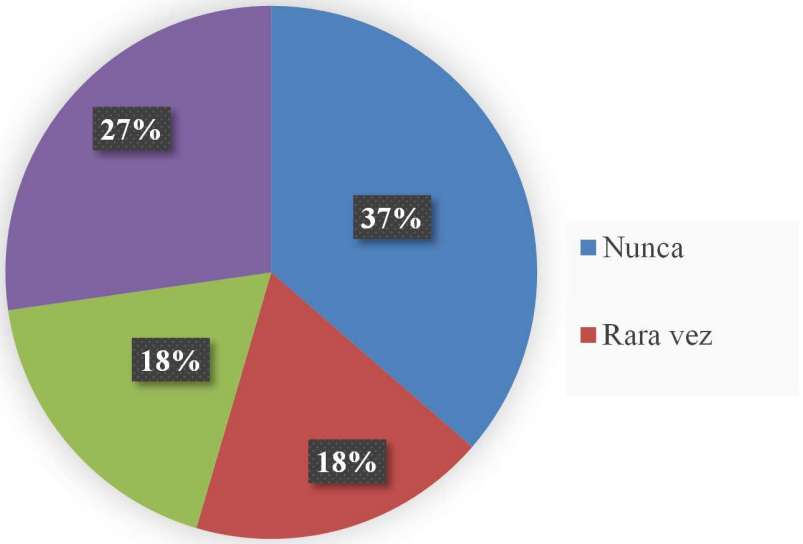


8. **En caso del robo de un activo (información/equipos) ¿Existen los suficientes procesos, mecanismos y/o dispositivos de alerta?**

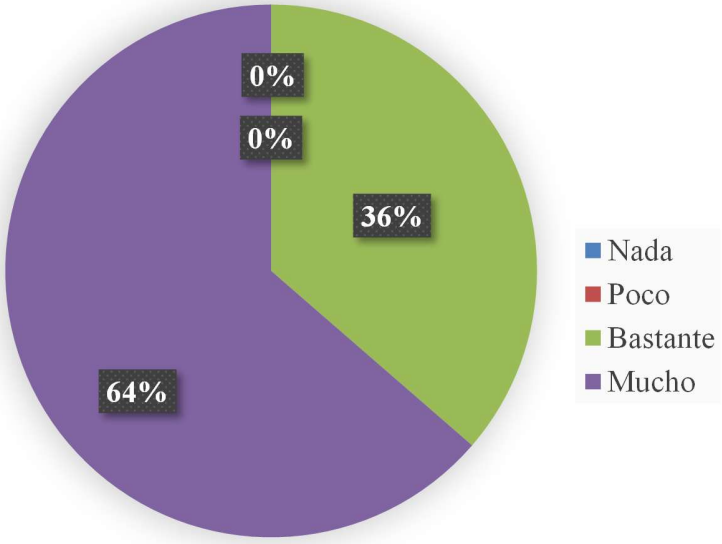


9. **Cuando conecta un dispositivo USB, ¿Lo revisa con el programa de seguridad, si tiene**

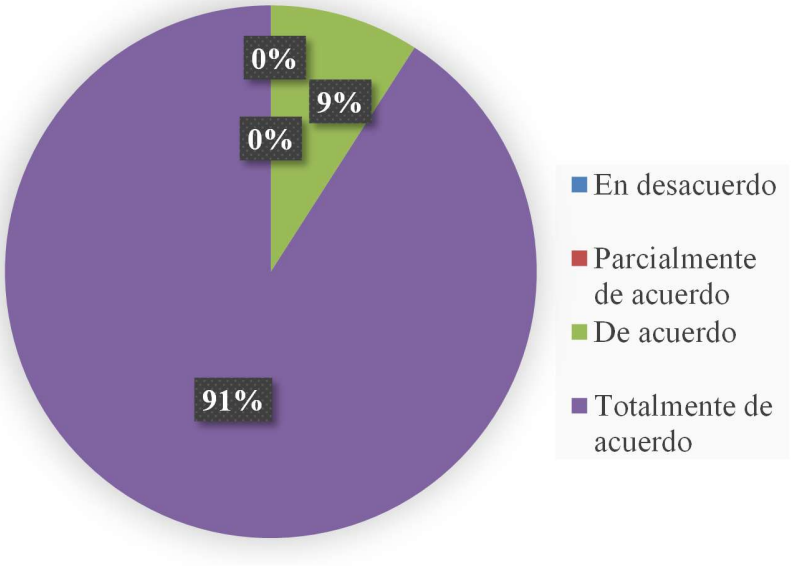
virus?



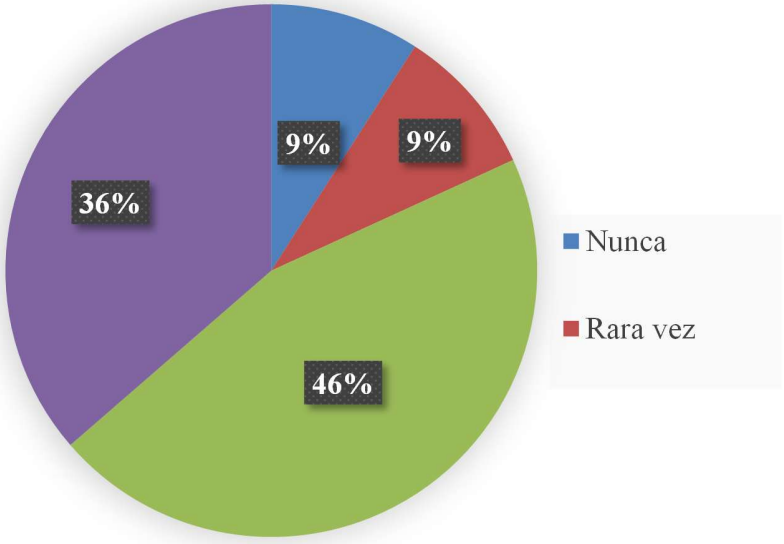
10. ¿Qué tan importante considera Usted, al mantenimiento de los activos a su cargo?



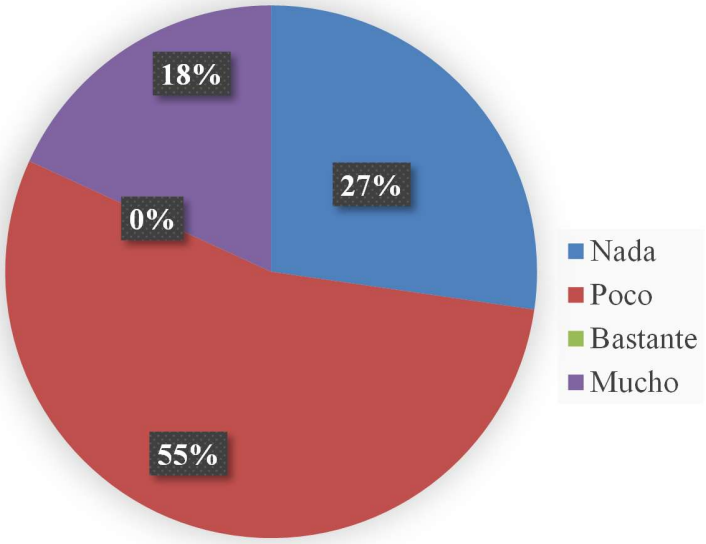
11. Considera que la información que se maneja en su área, ¿Es sensible, crítica y/o confidencial?



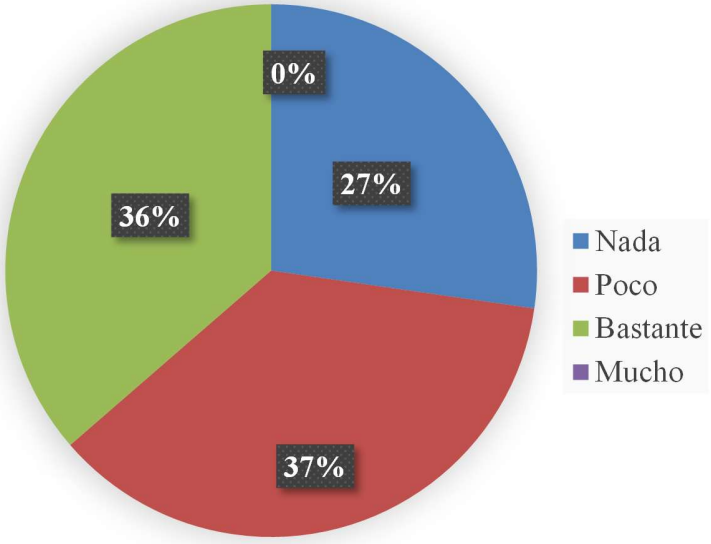
12. La cantidad de información que almacena diariamente en su área de trabajo, ¿La genera desde el sistema principal de operaciones financieras?



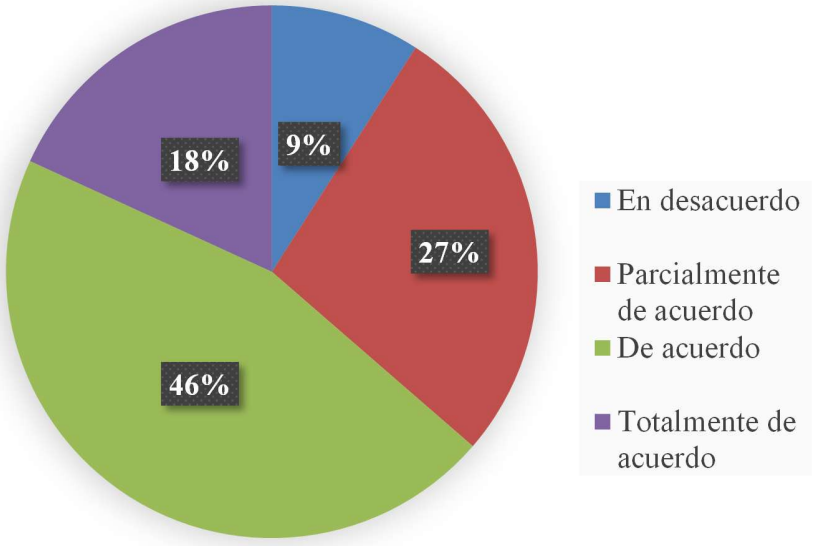
13. **¿Tiene conocimiento de los planes de seguridad de los activos (programas, equipos, personas) que tiene a su cargo?**



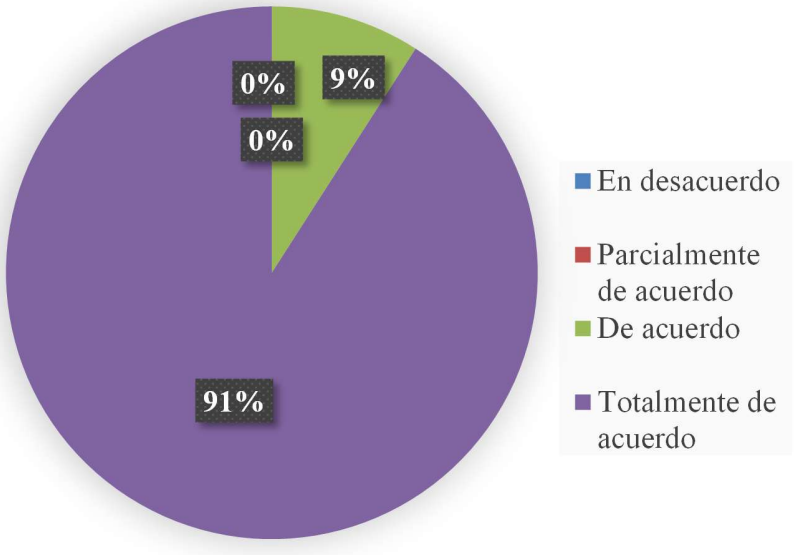
14. **En base a sus funciones laborales que tiene asignadas, ¿Estas le permiten ver información de otras áreas?**



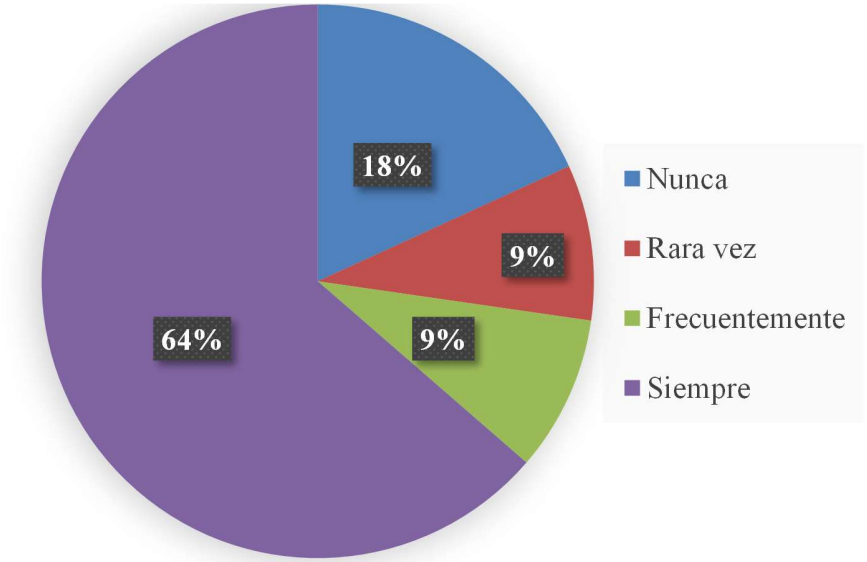
15. Considera que una situación de riesgo para la institución, ¿Se debe a una posible ocurrencia de desastre natural o ambiental?



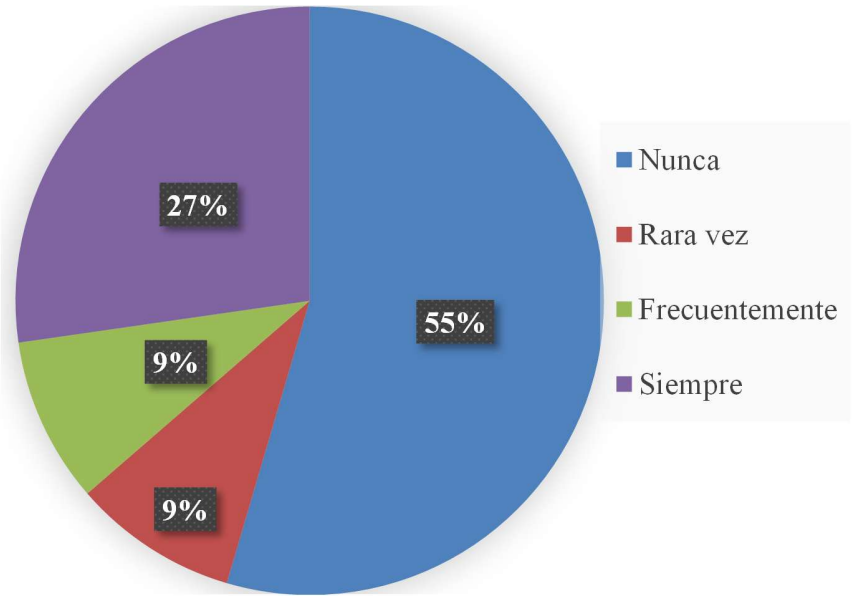
16. Considera que una situación de riesgo para la institución, ¿Se debe a la vulneración de la seguridad por parte del factor "Persona" (empleados, directivos, proveedores, socios)?



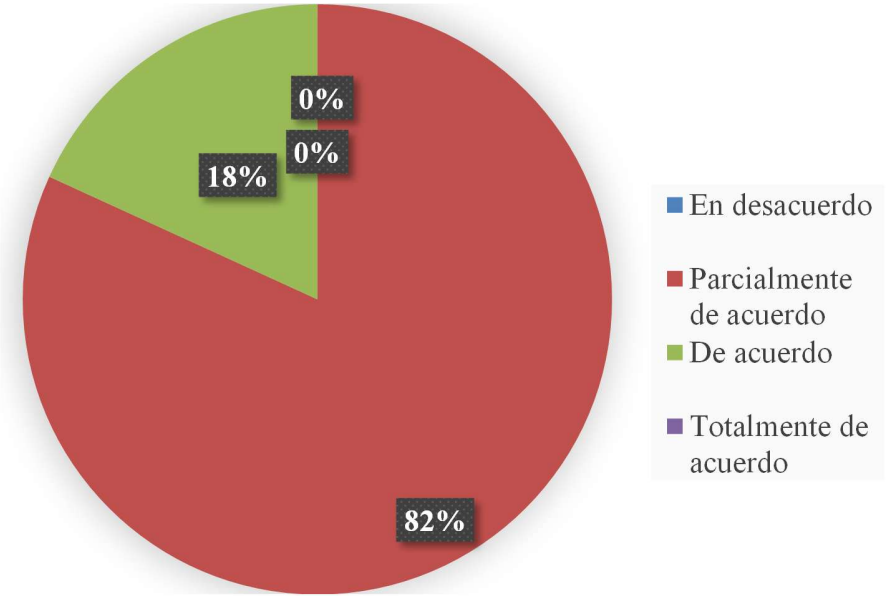
17. ¿Comparte la impresora con personas de otras áreas?



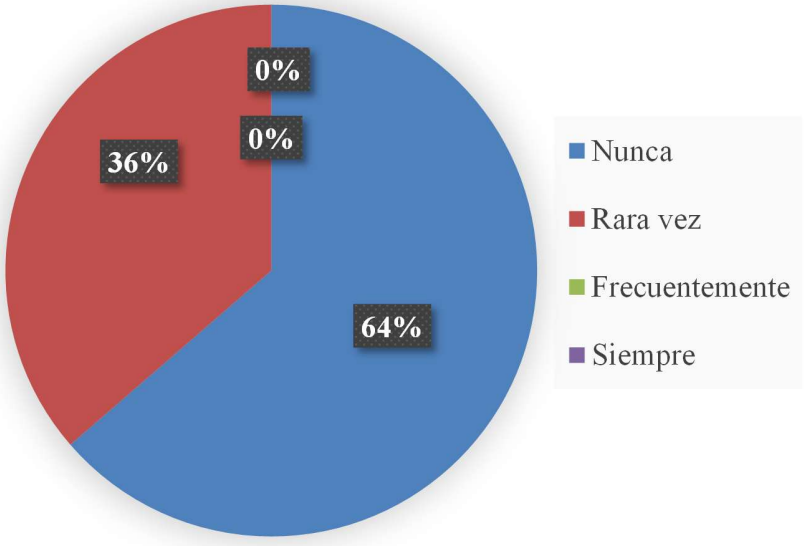
18. Para la destrucción de la información ¿Aplica algún protocolo o procedimiento establecido?



19. ¿Las medidas de seguridad que están implementadas en su área, son suficientes?



20. Cuando tiene que trabajar desde casa, ¿Traslada información en discos externos desde la oficina?



Anexo 2. Explicación de activo por activo sobre la calificación de las amenazas, vulnerabilidades y riesgos detalladamente.

La Cooperativa de Ahorro y Crédito de la ciudad de Tulcán, realizó la última actualización del inventario de activos de información a finales del año 2021, donde utilizó una metodología autónoma y adaptada a la institución para la valoración de cada uno de los activos en función de su confidencialidad, integridad y disponibilidad.

De esta manera se asignó una calificación con un valor de 1 como Bajo, 2 como Medio Bajo, 3 como Medio Alto y 4 como Alto.

Calificación	Valor
ALTA	4
MEDIA ALTA	3
MEDIA BAJA	2
BAJA	1

Adicional se asignó una ponderación, que se enmarca en una mayor importancia para la Confidencialidad asignándole el 40%, a la Integridad el 35% y a la Disponibilidad el 25%. Esta calificación genera una clasificación de la información que contiene cada activo, de la siguiente manera: Pública, Uso Interno, Restringida y Privada.

Puntaje mínimo	Puntaje máximo	CLASIFICACIÓN
> 340	400	PRIVADA
> 250	340	RESTRINGIDA
> 160	250	USO INTERNO
>=100	160	PÚBLICA

La calificación se la obtuvo del producto entre la valoración del activo y el porcentaje de ponderación, lo que le permite tener una clasificación del activo en base a su contenido como se puede apreciar a continuación, donde se ejemplifica el caso de la máxima calificación, donde categoriza a la información como PRIVADA en base a la calificación alcanzada:

Confidencialidad	40	Integridad	35	Disponibilidad	25	Total	Clasificación información
4	160	4	140	4	100	400	PRIVADA

De esta manera se realizó la actualización del inventario de activos de información de la Cooperativa de Ahorro y Crédito con corte a marzo de 2026, logrando obtener la valoración de

177 activos de información correspondientes a las jefaturas de la institución, con su respectiva calificación y clasificación de información. Las áreas a las que se realizó el levantamiento de la información son:

- Tecnología de la Información
- Seguridad de la Información
- Seguridad Física
- Gestión de Administración de Riesgos
- Gestión de Adquisiciones
- Gestión de Tesorería
- Gestión de la Contabilidad
- Gestión de Marketing y Mercadeo
- Gestión de Talento Humano
- Gestión de Auditoría Interna
- Gestión de la Calidad y Operaciones
- Gestión de la Calidad y Procesos
- Jefatura de Negocios
- Jefatura de Captaciones
- Oficiales de Crédito
- Cajas
- Trabajo Social
- Seguridad Ocupacional
- Salud Ocupacional
- Jurídico Judicial
- Jurídico Administrativo
- Gerencia General
- Innovación y Proyectos

De este inventario de activos de información, se identificaron los siguientes resultados, en cuanto a la clasificación de información:

CLASIFICACIÓN INFORMACIÓN	NÚMERO DE ACTIVOS
PRIVADA	79
RESTRINGIDA	72
PÚBLICA	10
USO INTERNO	16

Con esta metodología adaptada a la Cooperativa de Ahorro y Crédito, la valoración del activo no se encuentra expresada en un valor cualitativo que nos permita identificar aquellos activos considerados con un valor Alto, Medio o Bajo, por tal motivo se toma como referencia la propuesta de valoración de activos planteada por el Esquema Gubernamental de Seguridad de la Información (EGSI). Este esquema fue creado tomando como referencia la ISO 27005 y la Metodología de Análisis de Gestión Riesgos de los Sistemas de Información MAGERIT, desarrollada en España.

El EGSI identifica la valoración de los activos acorde a los lineamientos de la ISO 27005, tratando a la valoración del impacto sobre los factores de Confidencialidad, Integridad y Disponibilidad, en su propuesta determina al valor del activo como Alto (3), Medio (2) y Bajo (1).

A continuación el Esquema Gubernamental de Seguridad de la Información (EGSI), se presenta las consideraciones para calificar el impacto que tiene el activo en base a los términos de Confidencialidad, Integridad y Disponibilidad:

Valoración del impacto en términos de la perdida de la **confidencialidad**	**Criterio**
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Valoración del impacto en términos de la perdida de la **integridad**	**Criterio**
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Valoración del impacto en términos de la perdida de **disponibilidad**	**Criterio**
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Adaptando a este nuevo formato, en el que la calificación se realiza en una escala del 1 al 3, conforme se considere la Confidencialidad, Integridad y Disponibilidad por cada propietario del activo, se logran identificar la valoración de los siguientes activos en el rango de calificación como Alto, Medio y Bajo.

Cabe indicar que en esta valoración existen casos en la que la valoración del activo va a tener un valor con decimales, para lo cual se debe considerar que pasado al 0.5 se debe asumir al número inmediato superior y si es menor que 0.5 al inmediato inferior; por ejemplo si un activo llega a tener un valor de 2,33 se lo debe considerar como un activo con un valor cuantitativo de 2 que equivale a MEDIO, otro ejemplo sería si un activo tiene una calificación de 2,66 se lo debe considerar al inmediato superior 3 que equivale a ALTO, de esta manera la actualización del inventario de activos nos devuelve el siguiente resultado:

VALORACIÓN ACTIVO	NÚMERO DE ACTIVOS
ALTO	75
MEDIO	88
BAJO	14

Para el análisis de riesgo de los activos de este presente estudio se ha tomado como objeto a la unidad de TI de la Cooperativa de Ahorro y Crédito, donde se tomarán como referencia las categorías presentadas por la ISO 27005, teniendo en cuenta a los activos primarios: Actividades y procesos del negocio, e Información; así como también los activos de soporte: Hardware, Software, Redes, Personal, Ubicación y la estructura de la organización.

Dentro de esta clasificación se tomarán en cuenta los activos que se crean necesarios de acuerdo con las entrevistas levantadas a las Jefaturas de Tecnologías de la Información, Seguridad Lógica y Seguridad Física, así como también que sirvan como fuente de consulta o respaldo, las encuestas realizadas a las jefaturas de cada área operativa, donde se puedan identificar activos que dependan de la unidad de TI.

La ISO 27005 sugiere una clasificación de activos de acuerdo a dos tipos: Primarios y de Soporte, donde los incluye a los siguientes:

Primarios:

- Actividades y Procesos del Negocio
- Información

Y los de Soporte:

- Hardware
- Software
- Redes
- Personal
- Ubicación

Se tomó como referencia esta clasificación de la norma ISO, con el fin de poder analizar el riesgo de los siguientes activos considerados como primarios:

- Base de Datos: considerado el activo más importante, el mismo que contiene la

información operativa de toda la cooperativa y sus áreas que la conforman

- Copia de Base de Datos: es el respaldo de la base de datos, generando copias de esta.

Para los activos de soporte, se han relacionado los siguientes activos de la Unidad de Tecnologías de la Información, iniciando por los activos de Hardware se han considerado a:

- Servidor de Base de Datos: se considera al equipo en el cual se encuentra ejecutado las instancias de BDD disponibles.
- Servidor de Aplicaciones: se encarga de la ejecución de la aplicación o aplicaciones que tenga disponible la Cooperativa de Ahorro y Crédito.

En cuanto a los activos de software, se consideraron a los siguientes activos:

- Core Financiero: es el software mediante el cual se registran las operaciones realizadas en las áreas y agencias de la Cooperativa.
- Servidor de Directorio Activo: es el servidor centralizado de dominio institucional.

En cuanto a los activos de tipo red, se han identificado los siguientes:

- Switch de Core: activo mediante el cual se coordinan las operaciones entre los distintos switches de cada piso del edificio Matriz.
- Firewall: este activo se encarga del control del perímetro externo de la red institucional.

En lo que se refiere a los activos de personas, se han definido los siguientes:

- Jefe de Tecnología: este activo representa al responsable del área de TI de la cooperativa, quien tiene autoridad y toma de decisiones en la misma.
- Asistente de Soporte Técnico: asiste, apoya o ayuda a los usuarios de la cooperativa con el equipo asignado, configuraciones, instalación de software/aplicativos y dispositivos institucionales.

Y por último en los activos de ubicación/Sitio, se encuentran identificados los siguientes:

- Sistema Eléctrico
- Sistema de Climatización
- Generador de Energía
- Sistema de UPS

Una vez que se identificaron los activos prioritarios de acuerdo con los tipos de activos, se procedió con la "Valoración" de los mismos en base al impacto que este activo tendría en los factores de Confidencialidad, Integridad y Disponibilidad, dejando los siguientes resultados:

Nombre de Activo	Propietario del Activo	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
			C	I	D	VA
Base de datos	Jefe de Tecnología de la Información	Data Center de TI	3	3	3	3.00
Copias de BDD	Jefe de Tecnología de la Información	Data Center de TI	3	3	3	3.00
Plan de Contingencias del departamento de TI	Jefe de TI	Archivo de TI Computador Jefatura	1	1	3	1.67
Core Financiero	Jefe de Tecnología de la Información	Data Center de TI	3	3	3	3.00
Servidor de Directorio Activo	Jefe de Seguridad de la Información	Data Center de TI	3	3	3	3.00
Sistema Eléctrico	Sugerencia Administrativa	Edificio Matriz	1	3	3	2.33
Sistema de Climatización	Sugerencia Administrativa	Data Center de TI	1	3	3	2.33
Generador de energía	Sugerencia Administrativa	Patio Exterior Ed. Matriz	1	3	3	2.33
Sistema de UPS	Sugerencia Administrativa	Edificio Matriz	1	3	3	2.33
Switch de Core	Jefe de TI	Data Center de TI	3	3	3	3.00
Firewall	Jefe de TI	Data Center de TI	3	3	3	3.00
Jefe de Tecnología	Gerencia General	Oficina Matriz - Área de Tecnología	3	3	3	3.00
Asistente de Soporte Técnico	Jefe de TI	Oficina Matriz - Área de Tecnología	3	3	2	2.67
Servidor de Base de Datos	Jefe de TI	Data Center de TI	3	3	3	3.00
Servidor de Aplicaciones	Jefe de TI	Data Center de TI	3	3	3	3.00

Luego de realizada la valoración del activo, se procede a determinar por cada activo las Amenazas y Vulnerabilidades que este presenta, para ello tanto el esquema EGSI, MAGERIT y la ISO 27005, nos sugieren un catálogo de las mismas, para que sean consideradas en el análisis, tomando en cuenta que pueden existir amenazas en base a los factores ambientales, culturales, sociales, gubernamentales y/o de ubicación geográfica, que pueden ser considerados por la persona que realiza el análisis de los activos.

Basándonos en la metodología del EGSI, los valores a calificar en los factores de

probabilidad de ocurrencia como amenazas y vulnerabilidades mantienen la escala de Alto (3), Medio (2) y Bajo (1), lo que nos permite evaluar el riesgo de la siguiente manera:

Tabla de evaluación del activo										
Nivel de Amenaza		Bajo (1)			Medio (2)			Alto (3)		
Nivel de Vulnerabilidades		Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)
Valor del impacto en términos de la pérdida de (CID) en los activos	Bajo (1)	1	2	3	2	4	6	3	6	9
	Medio (2)	2	4	6	4	8	12	6	12	18
	Alto (3)	3	6	9	6	12	18	9	18	27

La evaluación del riesgo se obtiene con el producto del valor del activo de la información (CID) x Amenaza x Vulnerabilidad. El producto de estos valores determina si el Riesgo del activo es considerado como Alto, Medio o Bajo.

Nivel de Riesgo		
1	3	BAJO
4	8	MEDIO
9	27	ALTO

A continuación, el análisis realizado a los activos de información:

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad			
Base de datos	Pérdida de suministro de energía	Racionamiento energético por emergencia nacional, por parte del Gobierno Nacional	3.00	1	2	Generador de energía	6.00	MEDIO
Base de datos	Fallas en la climatización	Susceptibilidad a las variaciones de temperatura	3.00	2	2	Aire acondicionado	12.00	ALTO
Base de datos	Error de configuración	Dejar la BDD inaccesible para las operaciones del negocio	3.00	2	2	Control de acceso autorizado a la BDD	12.00	ALTO
Base de datos	Abuso de privilegio de acceso	Almacenamiento sin protección	3.00	1	1	IBM Guardium Firewall de BDD	3.00	BAJO
Copias de BDD	Indisponibilidad del personal	Entrenamiento insuficiente	3.00	2	2	Plan de capacitación Documentos guía para la ejecución de las copias	12.00	ALTO
Copias de BDD	Error de configuración	Falta de copias de seguridad o copias de seguridad incompletas o no verificadas	3.00	1	2	Plan de Respaldo de BDD establecido de manera clara.	6.00	MEDIO
Copias de BDD	Destrucción del equipo o los medios	Almacenamiento sin protección	3.00	1	1	Respaldo en sitio alterno	3.00	BAJO
Copias de BDD	Robo	Protección física insuficiente del edificio, puertas y ventanas	3.00	1	2	Control de acceso físico, Agentes de seguridad, ingreso restringido al área	6.00	MEDIO

La base de datos como un activo de información, presenta las siguientes amenazas y vulnerabilidades:

- Pérdida de suministro de energía / Racionamiento energético por emergencia Nacional: en este caso se valora como Bajo a la amenaza y como Medio a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), de tal manera obteniendo un cálculo de la evaluación del riesgo de 6 (seis), identificando al Riesgo como Medio. Para este activo se encuentran implementados controles como el UPS del Data Center, el UPS Centralizado y el Generador de Energía.

- Falla en la Climatización / Susceptibilidad a las variaciones de temperatura: la amenaza y la vulnerabilidad están consideradas con un valor de Medio, el riesgo se ha considerado como Alto y los controles para disminuir las probabilidades son el aire acondicionado de Data Center y un aire acondicionado empresarial de backup.

- Error de Configuración / Inoperatividad de la Base de Datos: la probabilidad de estos está considerada como Medio (2) y su riesgo está en nivel Alto, donde su control implementado a través de una política es el control de acceso a la base de datos, donde solamente el administrador de la Base de Datos está autorizado en realizar algún cambio, previo a la autorización de la Jefatura de Seguridad Lógica.

Las copias de la base de datos como activo de información presentan las siguientes amenazas y vulnerabilidades:

- Indisponibilidad de Personal / Entrenamiento Insuficiente: la amenaza y la vulnerabilidad están consideradas con un valor de Medio, el riesgo se ha considerado como Alto y los controles existentes se refieren al Plan de Capacitación y el Plan de Guía para Respaldo de BDD, así como también para este activo se implementa un proceso de empleado backup quien cumplirá las funciones del asistente en caso de ausencia del mismo.

- Error de Configuración / Falta de Copias de Seguridad o copias incompletas o no verificadas: el nivel de amenaza es de Bajo (1) y el nivel de vulnerabilidad es Medio (2), dando como resultado un riesgo Medio, el control, existente es el Plan Guía del paso a paso para generar la copia de seguridad; en este caso se podría implementar

un control adicional referente a la prueba periódica de validación sobre la fiabilidad de estas copias generadas.

- Destrucción del Equipo o los Medios / Almacenamiento Sin Protección: el nivel de amenaza y vulnerabilidad tiene una probabilidad de Bajo (1), obteniendo un riesgo de nivel Bajo, en este caso el control implementado se refiere al respaldo que se envía a un sitio alterno para su seguridad.

En el análisis realizado a los activos de soporte de tipo Hardware, se han considerado con un valor de activo Alto (3):

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad				
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Servidor de Base de Datos	Manipulación de hardware	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	3.00	1	2	Control de acceso físico y electrónico	6.00	MEDIO
Servidor de Base de Datos	Espionaje remoto	Conexiones de red pública no protegidas	3.00	2	1	Zona Desmilitarizada DMZ	6.00	MEDIO
Servidor de Base de Datos	Terrorismo, Ataque, sabotaje	Almacenamiento sin protección	3.00	2	2	Políticas de acceso a solo administrador y a equipo único.	12.00	ALTO
Servidor de Aplicaciones	Fallo de una red de telecomunicaciones	Activo inaccesible	3.00	2	2	Enlance redundante para mantener conectividad	12.00	ALTO
Servidor de Aplicaciones	Falta de mantenimiento y/o actualización	Servidor vulnerable a fallas o acceso no autorizado	3.00	3	3	Ejecución de proceso de Hardening	27.00	ALTO
Servidor de Aplicaciones	Falta de disponiblidad	Inexistencia de políticas de copias de seguridad	3.00	3	3	Respaldo de máquinas virtuales	27.00	ALTO

El Servidor de Base de Datos como un activo de hardware, presenta las siguientes amenazas y vulnerabilidades:

- Manipulación de hardware / Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones: en este caso se valora como Bajo a la amenaza y como Medio a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo de 6 (seis), identificando al riesgo como Medio. Para este activo se encuentran implementados controles como el control de acceso con tarjeta electrónica, aunque se podría mejorar con la instalación de un control biométrico.

- Espionaje remoto / Conexiones de red pública no protegidas: en este caso se valora como Medio a la amenaza y como Bajo a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo

de 6 (seis), identificando al riesgo como Medio. Para este activo se cuenta con una zona desmilitarizada (DMZ), así como la implementación de segmentación de la red a través de VLAN's.

- Terrorismo, Ataque, sabotaje / Almacenamiento sin protección: en este caso se valora como Medio a la amenaza y como Medio a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo de 12 (doce), identificando al riesgo como Alto. Se cuenta con políticas de acceso de solo Administrador y a equipo único, y en curso se tiene la implementación de un firewall de base de datos (IBM Guardium).

El Servidor de Aplicaciones como un activo de hardware, presenta las siguientes amenazas y vulnerabilidades:

- Fallo de una red de telecomunicaciones / Activo inaccesible: en este caso se valora como Medio a la amenaza y como Medio a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo de 12 (doce), identificando al riesgo como Alto. Para mantener la conectividad de este hardware se cuenta con la implementación de un enlace redundante, adicional se podría mantener un monitoreo periódico de enlaces para mantener el failover.

- Falta de mantenimiento o actualización / Servidor vulnerable a fallas o acceso no autorizado: en este caso se valora como Alto a la amenaza y como Alto a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo de 27 (veintisiete), identificando al riesgo como Alto. Como controles implementados se cuenta con la ejecución del proceso de hardening.

- Falta de disponibilidad / Inexistencia de políticas de copias de seguridad: en este caso se valora como Alto a la amenaza y como Alto a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), obteniendo un cálculo del riesgo de 27 (veintisiete), identificando al riesgo como Alto. Como controles implementados se mantienen los respaldos de máquinas virtuales, y

servidor de aplicaciones backup, como control a implementar se debe considerar testeo o pruebas periódicas del servidor backup para asegurar su correcto funcionamiento.

A continuación, el análisis realizado a los activos de soporte de tipo Software, los mismos que se ha considerado con un valor de activo Alto (3):

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad			
Core Financiero	Fallo en el suministro de energía	Detener la atención a socios y clientes que se encuentran en las agencias.	3,00	1	2	Sistema de UPS en la estación de trabajo	6,00	MEDIO
Core Financiero	Fallo en el sistema de red	Falla en la comunicación con agencias	3,00	1	2	Segmentos de red asignados para cada área y agencia.	6,00	MEDIO
Core Financiero	Fallo del dispositivo o sistema	Negación de servicio	3,00	2	2	Revisión de logs, donde se encuentra el serivicio	12,00	ALTO
Servidor de Directorio Activo	Información sin actualizar	No permitir el acceso a las cuentas de usuario	3,00	1	2	Políticas GPO, hacer parte a la persona del dominio	6,00	MEDIO
Servidor de Directorio Activo	Fallo en la comunicación	Servidor inaccesible	3,00	1	2	Enlace backup con proveedor alterno	6,00	MEDIO
Servidor de Directorio Activo	Que las políticas no se afecten en las cuentas de usuario	Equipos inseguros e información sin protección	3,00	2	2	Equipo BackUp	12,00	ALTO

El Core Financiero como un activo de software, presenta las siguientes amenazas y vulnerabilidades:

- Fallo de suministro de energía / Detener la atención a clientes-socios: en este caso se valora como Bajo a la amenaza y como Medio a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), de tal manera obteniendo un cálculo de la evaluación del riesgo de 6 (seis), identificando al Riesgo como Medio. Para este activo se encuentran implementados controles como el UPS del equipo de escritorio, así como controles que se están implementando que son tomas reguladas, provenientes del sistema central de UPS.

- Fallo en el Sistema de Red / Falta de Comunicación con agencias: la amenaza se ha considerado en un nivel Bajo y la vulnerabilidad está considerada con un valor de Medio, el riesgo se establece en un nivel Medio y el control implementado para disminuir las probabilidades es la segmentación de la red tanto para áreas como para agencias/sucursales.

- Fallo del Dispositivo o Sistema / Negación de Servicio: la probabilidad de estos está considerada como Medio (2) y su riesgo está en nivel Alto, mantiene un control implementado de revisión de logs, además de la capacidad del equipo de personas de TI para restablecer el sistema en el menor tiempo posible.

El Servidor de Directorio Activo como activo de software presenta las siguientes amenazas y vulnerabilidades:

- Información sin Actualizar / No permitir el acceso a las cuentas de usuarios: la amenaza está considerada en un nivel Bajo y la vulnerabilidad con un valor de Medio, el riesgo se ha considerado como Medio y el control existente son el cumplimiento y aplicación de políticas GPO.

- Fallo en la Comunicación / Servidor Inaccesible: el nivel de amenaza es de Bajo (1) y el nivel de vulnerabilidad es Medio (2), dando como resultado un riesgo Medio, el control existente es el correcto funcionamiento de un enlace con un proveedor alterno al existente.

- Políticas sin Afectar a Cuentas de Usuarios / Equipos Inseguros e Información sin Protección: el nivel de amenaza y vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, el control para esta amenaza y vulnerabilidad es un equipo de directorio activo backup, y adicional se aplican las políticas de manera manual.

A continuación, el análisis realizado a los activos de soporte de tipo Redes, los mismos que se ha considerado con un valor de activo Alto (3):

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad			
Switch de Core	Avería del harware	Cambio de tensión eléctrica	3,00	2	2	Sistema de UPS en el Datacenter	12,00	ALTO
Switch de Core	Errores del administrador	Mala administración en los parámetros	3,00	2	1	respaldo antes de ejcutar cambios, caso contrario se realiza rollback	6,00	MEDIO
Switch de Core	Errores de mantenimiento/actualizacion de equipos	Actualizaciones incompletas debido a error en conectividad	3,00	1	1	respaldo antes de ejcutar cambios, caso contrario se realiza rollback	3,00	BAJO
Switch de Core	Caída de enlace	Cableado de mala calidad o mala instalación	3,00	1	1	Certificación de red cableada	3,00	BAJO
Firewall	Avería del harware	Cambio de tensión eléctrica	3,00	2	2	Sistema de UPS en el Datacenter	12,00	ALTO
Firewall	Errores del administrador	Mala administración en los parámetros	3,00	2	2	respaldo antes de ejcutar cambios, caso contrario se realiza rollback	12,00	ALTO
Firewall	Errores de mantenimiento/actualizacion de equipos	Actualizaciones incompletas debido a error en conectividad	3,00	1	1	respaldo antes de ejcutar cambios, caso contrario se realiza rollback	3,00	BAJO
Firewall	Denegación de servicio	Atque externo	3,00	2	2	Implementación de SOC	12,00	ALTO

El Switch de Core como un activo de Red, presenta las siguientes amenazas y vulnerabilidades:

- Avería del Hardware / Cambio de Tensión Eléctrica: en este caso se valora como Medio (2) a la amenaza y como Medio (2) a la vulnerabilidad, sobre la probabilidad de ocurrencia. El valor de este activo es Alto (3), de tal manera obteniendo un cálculo de la evaluación del riesgo de 12 (doce), identificando al Riesgo como Alto. El control para este activo es el UPS del Data Center como primera línea, y adicional el UPS Centralizado.
- Errores de Administrador / Mala Administración en los Parámetros: la amenaza se ha considerado en un nivel Medio (2) y la vulnerabilidad está considerada con un valor de Bajo (1), el riesgo se establece en un nivel Medio y el control implementado para disminuir las probabilidades de ocurrencia, es respaldo realizado antes de ejecutar los cambios, con el fin de realizar rollback, si es que la parametrización es errónea y garantizar la continuidad de operación.
- Caída de Enlace / Cableado de mala calidad o mal instalado: la probabilidad de ocurrencia de estos está considerada como Bajo (12) y su riesgo está considerado en nivel Alto, se mantiene un control en cuánto a la instalación de puntos certificados por parte del proveedor contratado.

El Firewall como activo de red presenta las siguientes amenazas y vulnerabilidades:

- Errores de Administrador / Mala Administración en los Parámetros: la amenaza se considera en nivel Medio (2) y la vulnerabilidad con un valor de Medio (2), dando como resultado al riesgo Alto; para mantener un control en cuanto al nivel de ocurrencia se realizan copias de configuración previo a cambios a realizar, para en caso indirecto se falle en la parametrización, se pueda retornar a su último funcionamiento correcto.
- Errores de Mantenimiento y/o Actualización de equipos / Actualizaciones incompletas debido a error en conectividad: el nivel de amenaza es de Bajo (1) y el nivel de vulnerabilidad es Bajo (1), dando como resultado un riesgo Bajo, el control existente es el respaldo periódico de copias de configuración controladas para usarlas en caso de estos incidentes.
- Denegación de servicio / Ataques Externos: el nivel de amenaza y vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, para mantener el control ante estas probabilidades de ocurrencia se cuenta con el monitoreo de un SOC, quien nos levanta las alertas en caso de ataques.

A continuación, el análisis realizado a los activos de soporte de tipo Personas, los mismos que se ha considerado con un valor de activo Alto (3):

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad			
Jefe de tecnologia	Abuso de autoridad	Modificar datos en BDD	3,00	1	1	Acceso autorizado, mediante control de Administrador de BDD	3,00	BAJO
Jefe de tecnologia	Indisponiblidad del personal	Enfermedad y/o accidente emergente	3,00	2	2	Empleado backup	12,00	ALTO
Jefe de tecnologia	Error humano en tareas críticas	Cambios directos en entorno de producción	3,00	2	1	Se ha definido entornos de pruebas	6,00	MEDIO
Asistente de Soporte Técnico	Robo de soportes o documentos	Mecanismos de seguimiento insuficientes o faltantes	2,67	1	2	Requerimiento a través de una mesa de ayuda	5,33	MEDIO
Asistente de Soporte Técnico	Mal uso de control de acceso	Ingreso de personal no autorizado a áreas restringidas	2,67	2	2	Entrega de credencial única e instransferible para ingreso en puertas	10,67	ALTO
Asistente de Soporte Técnico	Error humano en tareas críticas	Cierre de dia del Core Financiero incompleto no terminado	2,67	1	1	Persona de turno encargada del monitoreo de actividades fuera de horario.	2,67	BAJO

El Jefe de Tecnología como activo de Personas presenta las siguientes amenazas y

vulnerabilidades:

- Abuso de Autoridad / Modificar Datos en la Base de Datos: la amenaza se considera en nivel Bajo (1) y la vulnerabilidad con un valor Bajo (1), dando como resultado al riesgo Bajo; para mantener un control en cuanto al nivel de ocurrencia se mantiene un control de acceso con restricción de IP, cuando alguien intenta conectarse a la base de datos de producción.
- Indisponibilidad del Personal / Enfermedad, Inasistencia o Emergencia: el nivel de amenaza es de Medio (2) y el nivel de vulnerabilidad es Medio (2), dando como resultado un riesgo Alto, el control existente es la existencia de una política del empleado backup en caso de ausencia del titular, previo a esta designación, la persona como tal debe ser capacitada en las actividades acordes al encargo.
- Error Humano en tareas Críticas / Cambios en la BDD de Producción: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Bajo (1), obteniendo un riesgo de nivel Medio, para realizar este tipo de cambios en la base de datos, se debe tener una autorización previa del Jefe de Seguridad y la ejecución la realiza el Jefe de Base de Datos, para el resto del personal de TI existen ambientes de pruebas, que no afectan a la operatividad real de la cooperativa.

El Asistente de Soporte de Tecnología como activo de Personas presenta las siguientes amenazas y vulnerabilidades:

- Robo de soportes o documentos / Mecanismos de seguimiento insuficientes o faltantes: el nivel de amenaza es de nivel Bajo (1) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Medio, cuando se refiere a respaldos de equipos se manejan a través de una mesa de ayuda con previa asignación del Jefe de Tecnología, en el caso de los dispositivos que almacenan estos respaldos se encuentran bajo seguridad física y de control de acceso en el data center.
- Mal uso de control de acceso / Ingreso de personal no autorizado a áreas restringidas: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, en la actualidad

se tiene un control mediante tarjetas electrónicas para el control de acceso a las diferentes áreas de la institución considerando también áreas de acceso restringido como Gerencia, Cajas, Piso Administrativo y Tecnología de la Información, adicionalmente se inició a mejorar este control por registros biométricos para evitar que las tarjetas electrónicas sean prestadas a quien no corresponde.

- Error humano en tareas críticas / Procesos de cierre de día incompleto: el nivel de amenaza representa un valor de Bajo (1), al igual que la vulnerabilidad Bajo (1), obteniendo así un valor de Bajo en el nivel de riesgo, para controlar la probabilidad de ocurrencia de estos factores, se mantiene un turno de Soporte 24/7 para solventar inconvenientes en el cierre de operaciones diarias, monitoreando hasta la culminación de este proceso.

A continuación, el análisis realizado a los activos de soporte de tipo Sitio/Ubicación, los mismos que se ha considerado con un valor de activo Medio (2):

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad				
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Sistema Eléctrico	Fallo de los proveedores de servicios	Esquemas de reemplazo periódico insuficientes de equipos	2,33	2	2	Ninguno	9,33	ALTO
Sistema Eléctrico	Sobrecarga o pico eléctrico	Daño en equipos tecnológicos	2,33	2	2	Central UPS	9,33	ALTO
Sistema Eléctrico	Cortocircuito	Falta de cuidado a disposición	2,33	1	2	Ninguno	4,67	MEDIO
Sistema de Climatización	Polvo, corrosión, congelación	Trabajo no supervisado por personal externo o de limpieza	2,33	2	2	Disposición de Talento Humano	9,33	ALTO
Sistema de Climatización	Fallo del sistema de refrigeración o ventilación	Poca conciencia de seguridad	2,33	2	2	Registro de bitácora con guardias de seguridad	9,33	ALTO
Sistema de Climatización	Pérdida de suministro eléctrico	Red eléctrica inestable	2,33	2	2	UPS de Data Center	9,33	ALTO
Sistema de Climatización	Fallo de los proveedores de servicios	Falta de profesionales en la ciudad y provincia, para mantenimiento del activo	2,33	2	2	Monitoreo diario de la capacidad de funcionamiento del aire acondicionado	9,33	ALTO

Análisis de Riesgos			Evaluación de Riesgos					
			Impacto	Probabilidad				
Nombre Activo	Amenaza	Vulnerabilidad	VA (CID)	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Generador de energía	Deficiencias en la organización	Asignación inexistente o inadecuada de responsabilidades	2,33	3	3	Ninguno	21,00	ALTO
Generador de energía	Errores de mantenimiento	Control insuficiente de los activos fuera de las instalaciones	2,33	3	3	Ninguno	21,00	ALTO
Generador de energía	Leyes o regulaciones gubernamentales en frontera	Falta de suministro de combustible ACPM	2,33	2	2	Permiso especial para adquirir el combustible como entidad financiera	9,33	ALTO
Sistema de UPS	Agua	Ubicación en zona susceptible a inundaciones	2,33	1	1	Ubicación estratégica en el edificio Matriz	2,33	BAJO
Sistema de UPS	Entrada no autorizada a las instalaciones	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	2,33	2	2	Registro de bitácora con guardias de seguridad	9,33	ALTO
Sistema de UPS	Falta de mantenimiento al sistema UPS	Equipos sin respaldo de energía	2,33	2	2	Ninguno	9,33	ALTO

El Sistema Eléctrico como activo de Sitio / Ubicación presenta las siguientes amenazas y vulnerabilidades:

- Fallo de los Proveedores de Servicios / Esquemas de reemplazo periódico insuficientes de equipos: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, en lo que a controles se refiere en este caso solo se contaba con un transformador eléctrico que venía desde la empresa pública de energía EMELNORTE, ya contaba con su tiempo de vida y era compartido, por lo que un control a implementar se trasladó a la adquisición de un transformador eléctrico nuevo, dedicado solamente a la red eléctrica de la Cooperativa de Ahorro y Crédito.

- Sobrecarga o pico eléctrico / Daño en equipos tecnológicos: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, para mitigar en algo la sobrecarga de energía se cuenta con UPS del data center, como segunda línea se mantiene un UPS Centralizado con el cual se trabaja en la implementación de tomas reguladas iniciando en estaciones estratégicas, con el fin de poder cubrir todas las áreas.

- Cortocircuito / Falta de cuidado a disposición: el nivel de amenaza es de nivel Bajo (1) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Medio, al tratarse de un edificio que tiene un tiempo considerable desde su construcción, y con el crecimiento operativo de la cooperativa, se considera que el cableado eléctrico se ha ido adecuando a la institución, como controles a implementar se encuentra el mantenimiento preventivo y correctivo del cableado del sistema eléctrico.

El Sistema de Climatización como activo de Sitio / Ubicación, presenta las siguientes amenazas y vulnerabilidades:

- Polvo, corrosión, congelación / Trabajo no supervisado por personal externo o de limpieza: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, para evitar la

ocurrencia de estas probabilidades se mantiene una disposición de la Subgerencia Administrativa y de Talento Humano, sobre el aseo en áreas restringidas para el personal de limpieza, adicional se implementa un control en la adecuación de horarios del aseo en la unidad de Tecnología, el mismo que sugiere la supervisión acompañada del Jefe de Infraestructura durante el aseo correspondiente.

- Fallo del sistema de refrigeración o ventilación / Poca conciencia de seguridad: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), los agentes de seguridad física realizan un registro del personal externo que realiza trabajos en la edificación así como también los equipos que ingresan, adicional se propone mejorar este registro con una solicitud previa a la unidad de Seguridad Física, indicando la fecha, hora, número de personas y una breve descripción del trabajo a realizar y donde se lo realizará, esto permite estar alerta ante algún daño involuntario o por desconocimiento.

- Pérdida de suministro eléctrico / Red eléctrica inestable: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), la primera línea de respuesta ante estas probabilidades de ocurrencia viene a ser UPS del Data Center. Y como controles adicionales están el UPS Centralizado y el Generador de Energía.

- Fallo de los proveedores de servicios / Incorrecto mantenimiento del activo: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2) dando un nivel de riesgo de Alto, como control del activo se realiza un monitoreo periódico durante del día sobre la capacidad de funcionamiento del activo, como control a implementar se encuentra la adquisición e instalación de un aire acondicionado empresarial que sirva de backup.

El Generador de Energía como activo de Sitio / Ubicación, presenta las siguientes amenazas y vulnerabilidades:

- Deficiencias en la organización / Asignación inexistente o inadecuada de responsabilidades: el nivel de amenaza es de nivel Alto (3) y el de vulnerabilidad

tiene una probabilidad de Medio (3), obteniendo un riesgo de nivel Alto, al no tener un antecedente de emergencia eléctrica nacional de manera extendida, se pasó por alto el mantenimiento y correcto tratamiento del generador de energía, además que el responsable de este activo no se encontraba definido, para mitigar este tema se asignan las responsabilidades del mismo a la Sugerencia Administrativa.

- Errores de mantenimiento / Control insuficiente de los activos fuera de las instalaciones: el nivel de amenaza es de nivel Alto (3) y el de vulnerabilidad tiene una probabilidad de Medio (3), obteniendo un riesgo de nivel Alto, al no tener un antecedente de emergencia eléctrica nacional de manera extendida, los controles a implementar para bajar el nivel de probabilidad de ocurrencia es el establecimiento de un convenio de mantenimiento trimestral con un profesional de la rama.

- Leyes o regulaciones gubernamentales en frontera / Falta de suministro de combustible ACPM: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, la institución accede a un permiso especial para adquirir el combustible como entidad financiera para el funcionamiento del generador de energía, adicional se implementarán tanques de reserva de ACPM.

El Sistema de UPS como activo de Sitio / Ubicación, presenta las siguientes amenazas y vulnerabilidades:

- Agua / Ubicación en zona susceptible a inundaciones: el nivel de amenaza es de nivel Bajo (1) y el de vulnerabilidad tiene una probabilidad de Bajo (1), obteniendo un riesgo de nivel Bajo, la ubicación del sistema central de UPS se encuentra libre de inundaciones de acuerdo con su ubicación estratégica dentro del edificio Matriz de la Cooperativa.

- Entrada no autorizada a las instalaciones / Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, se realiza un registro físico y en bitácora de las personas que ingresan

al sitio, adicional se implementará un control de acceso con biometría ya que solo existe una cerradura mecánica.

- Falta de mantenimiento al sistema UPS / Equipos sin respaldo de energía: el nivel de amenaza es de nivel Medio (2) y el de vulnerabilidad tiene una probabilidad de Medio (2), obteniendo un riesgo de nivel Alto, no se mantiene un control permanente para este activo, sin embargo se procede a realizar un convenio de mantenimiento trimestral con un profesional eléctrico.