UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"EVALUACIÓN DE RIESGOS EN LA INFRAESTRUCTURA CRÍTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO MERCEDES CADENA LTDA PARA LA MITIGACIÓN DE AMENAZAS APOYADO EN LA METODOLOGÍA DE LA NIST SP 800 – 30."

Trabajo de titulación previo a la obtención del título de Ingeniero en Telecomunicaciones

Línea de investigación: Innovación Tecnológica y de productos, Netwoking

AUTOR:

Marlon Emanuel Ipiales Jingo

DIRECTOR:

Ing. Fabián Geovanny Cuzme Rodríguez Msc.

Ibarra, 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

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			
CÉDULA DE IDENTIDAD:	100438269 – 1		
APELLIDOS Y NOMBRES:	Ipiales Jingo Marlon Emanuel		
DIRECCIÓN:	Profesor Secundino Peñafiel 622 y Carlos Proaño		
EMAIL:	meipialesj@utn.edu.ec / marlonipiales551@gmail.com		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0983557392

DATOS DE LA OBRA	
TÍTULO:	Evaluación de riesgos en la infraestructura crítica de la Cooperativa de ahorro y crédito Mercedes Cadena LTDA para la mitigación de amenazas apoyado en la metodología de la NIST SP 800 – 30.
AUTOR (ES):	Ipiales Jingo Marlon Emanuel
FECHA: DD/MM/AAAA	29 de julio del 2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Telecomunicaciones
DIRECTOR:	Ing. Fabián Geovanny Cuzme Rodríguez Msc.
ASESOR:	Ing. Carlos Alberto Vásquez Ayala Msc.

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 29 días del mes de julio de 2025

EL AUTOR:

(Firma).....
Nombre: Ipiales Jingo Marlon Emanuel

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 29 de julio de 2025

Ing. Fabián Geovanny Cuzme Rodríguez Msc.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) .....

Ing. Fabián Geovanny Cuzme Rodríguez Msc.

C.C.: 1311527012

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular "EVALUACIÓN DE RIESGOS EN LA INFRAESTRUCTURA CRÍTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO MERCEDES CADENA LTDA PARA LA MITIGACIÓN DE AMENAZAS APOYADO EN LA METODOLOGÍA DE LA NIST SP 800 – 30." elaborado por Marlon Emanuel Ipiales Jingo, previo a la obtención del título de Ingenierio en Telecomunicaciones, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

(f): .....

Ing. Fabián Geovanny Cuzme Rodríguez Msc.

C.C.: 1311527012

(f): .....

Ing. Carlos Alberto Vásquez Ayala Msc.

C.C.: 1002424982

DEDICATORIA

Dedico este proyecto que fue realizado con todo mi corazón a mi familia, por ser un pilar constante en cada paso que he dado. A mis padres, por su amor incondicional, sacrificio y apoyo que ha sido motivación para nunca rendirme. A mis hermanos por su entera compañía.

También quiero dedicar este trabajo a mí mismo, por la perseverancia, las largas noches de estudio, las dudas superadas y el esfuerzo puesto en cada detalle, puesto que es el resultado de la constancia y del deseo de superarme.

Marlon Emanuel Ipiales Jingo

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a Dios, por darme la fortaleza y la claridad necesarias para seguir adelante en este camino. A mi familia, por estar siempre a mi lado con su apoyo incondicional, por sus palabras de aliento, por cada sacrificio realizado y por ser mi mayor fuente de motivación.

A mi querida abuelita Margarita Leonor Ipiales Angamarca por su apoyo cuando más lo necesité, que, aunque ya no está físicamente, su recuerdo aun vive acompañándome silenciosamente en cada paso hasta llegar a esta meta.

A mis amigos, gracias por estar presentes en este proceso, por compartir ideas, preocupaciones y alegrías, y por ayudarme a mantenerme firme en los momentos difíciles, en especial a Jenny, quien ha sido un apoyo constante en todo este trayecto.

También agradezco a mis docentes por cada enseñanza, por su guía paciente y exigente, y por su valioso aporte a mi formación profesional. Finalmente, a todos quienes, de una u otra manera, fueron parte de este logro: gracias de corazón.

Marlon Emanuel Ipiales Jingo

RESUMEN EJECUTIVO

El presente trabajo tuvo como objetivo evaluar mecanismos de seguridad aplicando la metodología de la NIST SP 800 – 30 para la mitigación de vulnerabilidades y amenazas en la infraestructura crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA. Se inició con la identificación y clasificación de los activos tecnológicos, considerando su nivel de criticidad e impacto dentro de los procesos de la institución. A partir de esta información, se elaboró una matriz de riesgos visualizara los niveles de riesgo y determinar así los activos con mayor vulnerabilidad. Con los activos con riesgo igual o superior al 48%, se diseñó un plan integral de ciberseguridad que incluye estrategias de mitigación, políticas de seguridad informática y procedimientos internos para reducir la probabilidad de incidentes y riesgos. Este plan fue validado con la creación de entornos de prueba en donde se implementaron configuraciones que se siguieren en si en las mismas guías que fueron diseñadas en el desarrollo de este trabajo donde parte con temas como la segmentación de red, políticas de acceso y control, servicios web y de base de datos protegidos, y medidas de seguridad que garantizan la continuidad operativa de los sistemas críticos. Se instauraron algunas sugerencias que fortalecerán la estructura de red critica de la cooperativa tomando en cuenta tiempos de gestión de forma inmediata y a largo plazo impulsando así una cultura de seguridad informática y ciberseguridad que sea activa dentro de la institución para evitar a futuro posibles daños o riesgos. En conclusión, la NIST SP 800-30 facilitó una visión del estado actual de la infraestructura crítica y ofreció una base sólida para implementar medidas preventivas y correctivas que resguarden la información y los servicios esenciales de la institución.

Palabras clave: Mitigación, gestión de riesgo, vulnerabilidad, impacto, seguridad informática, endurecimiento de sistemas, controles de acceso, protección de datos, encriptación de datos.

ABSTRACT

The objective of this work was to evaluate security mechanisms by applying the NIST SP 800–30 methodology to mitigate vulnerabilities and threats in the critical infrastructure of the Mercedes Cadena LTDA Savings and Credit Cooperative. The process began with the identification and classification of technological assets, considering their level of criticality and impact within the institution's processes. Based on this information, a risk matrix was developed to visualize risk levels and determine the most vulnerable assets. For assets with a risk level equal to or greater than 48%, a comprehensive cybersecurity plan was designed, including mitigation strategies, information security policies, and internal procedures to reduce the likelihood of incidents and risks. This plan was validated through the creation of test environments where configurations were implemented, as outlined in the guides developed throughout this work. These included topics such as network segmentation, access and control policies, protected web and database services, and security measures to ensure the operational continuity of critical systems. Several suggestions were established to strengthen the cooperative's critical network infrastructure, considering both immediate and long-term management actions. This promotes a proactive culture of information security and cybersecurity within the institution to prevent potential future damage or risks. In conclusion, the NIST SP 800-30 provided a clear view of the current state of the critical infrastructure and offered a solid foundation for implementing preventive and corrective measures to safeguard the institution's essential information and services.

Keywords: Mitigation, risk management, vulnerability, impact, information security, system hardening, access controls, data protection, data encryption.

LISTA DE SIGLAS

COAC. Cooperativa de Ahorro y Credito

NIST. National Institute of Standards and Technology.

SP. Special Publication (publicación especial del NIST).

LOETA. Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos.

LOPDP. Ley Organiza de Protección de Datos Personales.

SEPS. Superintendencia de economía popular y solidaria.

IGS. Intendencia General de Seguimiento.

IGT. Intendencia General Técnica.

IGJ. Intendencia General Jurídica.

IGDO. Intendencia General de Desarrollo Organizacional.

INGINT. Intendencia General de Negocios y Supervisión.

INTIC. Intendencia de Tecnología de la Información y Comunicación.

INSESF. Intendencia de Seguimiento de Entidades del Sector Financiero.

INR. Intendencia Nacional de Riesgos.

SGSI. Sistemas de Gestión de Seguridad Informática.

QoS. Quality of Service.

CID. Confidencialidad, integridad y disponibilidad.

TI. Tecnologías de la Información.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Capítulo I

Antecedentes

En este capítulo se presentan los apartados que brindan una visión general del desarrollo de trabajo de integración curricular, donde se abordarán los siguientes puntos tales como el tema principal, los objetivos establecidos, el alcance de la investigación y la justificación de la misma.

1.1 Problema de investigación.

Hoy en día el rol que cumplen las tecnologías de información en las organizaciones y empresas es muy importante, esto debido a que esta logra mantener control sobre su información y servicios que ofrecen a la sociedad. No obstante, cuando se considera este tema en el desarrollo dentro de los mercados financieros o la bancarización esta ha obtenido un crecimiento acelerado en los últimos años. De acuerdo con Alfonso Gimeno (2010):

> A lo largo de los años entre los 60's hasta el año presente y los futuros periodos, el sistema bancario se ha visto inmiscuido en un proceso acelerado de cambios y transiciones en cuanto a su respuesta con la adaptación de los negocios bancarios con el uso de aplicaciones TIC en sus funciones remotas. (p. 44)

Es por ello que, las tecnologías de la información han causado una mayor dependencia, por tanto, los riegos asociados se transfieren a los procesos de información que se manejan diariamente en el campo financiero.

Tal es el caso en Ecuador en donde las anomalías, conflictos y ataques cibernéticos no pasan desapercibidos puesto que pueden ser muy dañinos y potencialmente catastróficos en el área financiera. De acuerdo con la Superintendencia de Bancos (2021) en su página oficial evidencio que en las fechas del 8 y 9 de octubre del año 2021 el Banco Pichincha llevó a cabo pruebas de inspección en su data center alterno de uno de sus servidores activos, en donde lo más relevante que fue encontrado es que se detectó una anomalía que al principio actuaban como intermitencias en los canales, poco después esta anomalía dio paso al despliegue de un equipo de supervisores para realizar pruebas de inspección más profundas, este hecho dio paso para tomar acciones preventivas, ya que ante a este incidente existe la posibilidad de filtraciones de datos personales o robos de información a los ciudadanos que hacen uso de los servicios financieros de la entidad bancaria antes mencionada.

Por ende, es fundamental que las organizaciones y entidades bancarias sin importar rubro o tamaño opten por adecuadas medidas de seguridad cibernéticas y de información, ya que siempre está abierta la posibilidad de estar expuesto a alguna vulnerabilidad. Tal es el caso de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA que es un candidato excelente que figura dentro del contexto mencionado debido a que al ser una institución que proporciona servicios financieros, esta maneja una gran cantidad de información confidencial y valiosa, como datos de clientes, información financiera y transacciones en línea, por lo que también está abierta a sufrir vulnerabilidades como sucesos o anomalías en sus equipos que si no llegan a controlarse a tiempo pueden obtener consecuencias a corto o largo plazo, como la pérdida de datos confidenciales, el robo de identidad, la interrupción del servicio bancario o en el peor de los casos estar abierta a un ataque cibernético donde si esta no se la detecta o controla a tiempo puede

implicar pérdidas significativas tanto en el área económica como administrativa generando así la pérdida de confianza de sus clientes.

Ante este hecho, se plantea realizar un análisis dentro de la institución antes mencionada de su estado situacional en cuanto a su infraestructura para la identificación de vulnerabilidades y amenazas, para así proponer un plan integral de ciberseguridad que dé respuesta y prevención frente a las anomalías detectadas, todo bajo la estandarización organizada del marco metodológico de la NIST SP 800 – 30 ya que principalmente tendrá la función de mitigar los riesgos cibernéticos que lleguen a existir dentro de la institución.

1.2 Objetivos.

1.2.1 Objetivo General.

Evaluar mecanismos de seguridad aplicando la metodología de la NIST SP 800 – 30 para la mitigación de vulnerabilidades y amenazas en la infraestructura crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA.

1.2.2 Objetivos Específicos.

- Realizar el estado del arte acerca de los temas que involucran en el desarrollo del proyecto incluyendo la metodología de la NIST SP 800 – 30.
- Realizar un análisis de riesgos y evaluación a la infraestructura crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA para la identificación de vulnerabilidades y amenazas mediante la metodología NIST SP 800 – 30.

- Implementar un plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800 – 30 que aborde las amenazas y vulnerabilidades identificadas y fortalezca así su infraestructura.
- Establecer pruebas específicas que permitan validar el plan de ciberseguridad para los servicios financieros que proporciona la institución.

1.3 Alcance.

El presente proyecto tiene como objetivo el evaluar mecanismos de seguridad basados en el marco metodológico de ciberseguridad de la NIST SP 800 – 30 para la mitigación de amenazas en la infraestructura crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA, es por ello que la aplicación de esta metodología permitirá fortalecer su infraestructura, por lo que la información a obtener se lo realizara con un proceso de investigación de campo dentro de la institución abriendo paso a la visualización de resultados para detectar problemas, amenazas o riesgos y mediante estos resultados mejorar procesos o políticas, desarrollar o implementar estrategias, tomar decisiones y aplicar recomendaciones.

Para el desarrollo de este trabajo integrador, se ha tomado en cuenta la metodología de estudio de la NIST SP 800-30. De acuerdo con la Comisión Interamericana de Telecomunicaciones - CITEL (2009) esta metodología consta en tres fases: evaluación del riesgo, mitigación del riesgo, y análisis y evaluación. Por consiguiente, se describe cada una de estas fases conforme al trabajo:

La primera fase consiste en la evaluación del riego, proceso determina el nivel de amenaza y los riesgos asociados al sistema TIC; que incluye caracterización del sistema, identificación de amenazas ya sean humana, natural o ambiental dando lugar así a la identificación de vulnerabilidades para luego realizar un análisis de control y de impacto que determinara así una valoración del nivel de riesgo del sistema de información.

La segunda fase, consiste en la mitigación del riesgo, esta es una metodología implícita que consiste en reducir los riesgos identificados, donde su función principal es la de evaluar e implementar los controles apropiados de reducción de riesgos recomendados por la norma NIST SP 800 – 30. En este caso se desarrollará e implementará un plan integral de ciberseguridad en base a las vulnerabilidades y amenazas identificadas. Una vez realizado este proceso, con base a los resultados obtenidos se realizará la aplicación de las medidas de control de riesgos.

La tercera fase, análisis y evaluación, consiste en los cambios que pueden llegar a tener a lo largo del tiempo las políticas empresariales respecto a la seguridad de la información impuesta por el plan integral de ciberseguridad, puesto que dentro de estos cambios también existe la posibilidad de que aparezcan nuevos riesgos diferentes a los ya mitigados. Al evaluar este proceso se ofrece la opción de continuar con el plan actual o invocar otro plan de contingencia que para dar cierre al riesgo definitivamente, todo mientras continúen con las actividades de la institución.

Finalmente, en las pruebas de validación, se pretende realizar las respectivas pruebas que permitan validar el plan de ciberseguridad para los servicios financieros que la institución

proporciona, de esta forma se podrá validar que los planes y estrategias implementados funcionan correctamente permitiendo así corregir las vulnerabilidades y fortalecer su infraestructura tanto critica como tecnológica.

1.4 Justificación.

La implementación de mecanismos de seguridad en la infraestructura de instituciones que proporcionan servicios bancarios, son de vital importancia ya que actualmente las amenazas cibernéticas se encuentran en constante evolución. Es por ello que la protección adecuada de los datos personales de los clientes se ha convertido un tema demasiado dominante desde el punto de vista ético y legal. Así, en este sentido, la Ley General de Instituciones del Sistema Financiero y La Ley Orgánica de Protección de Datos Personales vigentes en el Ecuador indican un marco legal robusto que busca salvaguardar los derechos y la privacidad de los individuos en relación con el tratamiento de sus datos personales.

En concordancia con el Articulo [37] segundo parrado del Reglamento a Ley Orgánica de Protección de Datos Personales - LOPDP (2021) indica lo siguiente:

> Las entidades encargadas de manejar información personal deben establecer procedimientos para verificar, evaluar y mantener de forma constante la eficacia, eficiencia y efectividad de las medidas técnicas, administrativas y de seguridad implementadas. Esto se realiza con el propósito de asegurar la protección adecuada de los datos personales durante su tratamiento. (p. 18)

Por lo que la normativa descrita exige que se implementen medidas técnicas y organizativas con base a protocolos organizacionales que sean acordes con el estado de la técnica y que permitan prevenir, mitigar y responder de manera efectiva a las amenazas y riesgos que puedan afectar la seguridad de los datos personales.

Una de las cuestiones más importantes a considerar también es la dependencia que se ha generado hacia la tecnología en los últimos años.

> Como menciona Ruth Arregui Solano titular de la Superintendencia de Bancos quien fue en el año 2021 indica que en los últimos años entre el 2019 y el 2020 que corresponde a la pandemia del Covid – 19, las intrusiones interactivas se multiplicaron por cuatro mediante el incremento de los servicios digitales con una tasa del 33% en tan solo transacciones virtuales. (Superintendencia de Bancos, 2021)

En este sentido se ha generado una dependencia de las tecnologías en los sectores financieros para los procesos y servicios que ofrecen, lo que refuerza el contexto antes mencionado que es muy importante la implementación de medidas y protocolos que permitan detectar y prevenir amenazas a sus diferentes estructuras organizacionales y elementales.

En adición, conforme con otros reglamentos internacionales y estandarizaciones, en el Articulo [49] del Diario Oficial de la Unión Europea el Reglamento - 2016/679 - EN - GDPR - EUR-Lex (2016) indica que el encargado que "Constituye un interés legítimo del responsable del

tratamiento de datos personales debe mantener la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, siendo único responsable de salvaguardar su información" (p. 9).

Esta sección indica que las regulaciones con la seguridad de las redes de comunicaciones se aplican de manera general a nivel internacional. Se valida que los responsables de gestionar dichas redes deben prevenir el acceso no autorizado y evitar la difusión intencionada de claves, lo que impide el paso negativo de servicios y daños a los sistemas informáticos y de comunicaciones bajo su mando.

En base a las normas establecidas dentro del marco metodológico de ciberseguridad de la NIST SP 800 – 30, se propone una guía de mecanismos de seguridad en la infraestructura tecnológica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA, para así seguir un mejor enfoque apoyado en la Ley Orgánica de Protección de Datos Personales (LOPDP) entre otras normas vigentes en el Ecuador basados en protección de datos o endurecimiento de infraestructuras críticas.

Esta adopción permitirá a la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA fortalecer su postura en cuanto a la confidencialidad, integridad y disponibilidad de los datos personales de sus clientes. Además de proponer los mecanismos de seguridad basados en el marco de ciberseguridad de NIST, esta asegurará el cumplimiento de las disposiciones legales establecidas por las leyes y reglamentos vigentes en el Ecuador que rigen estas instituciones.

Capítulo II

Marco teórico

En este capítulo se fundamentará el estudio bibliográfico que abarcará temas relacionados con el desarrollo del proyecto, como las instituciones financieras, la seguridad de la información, la gestión y manejo de riesgos, la identificación de activos, así como la metodología que se utilizará para el desarrollo del proyecto, además de considerar las normativas y leyes que rigen dentro del ámbito de la seguridad informática para instituciones financieras en el Ecuador, todo con el fin de proporcionar la respectiva fundamentación y validación teórica del trabajo integrador.

2.1 Instituciones financieras.

Según el Banco Internacional (2021) una institución financiera es un ente que actúa de forma pública o privada al servicio de la comunidad que toma parte del sistema financiero de un país, en donde una de sus principales funciones es la de brindar la facilidad de servicios de transacción financiera y administración de los recursos monetarios de las personas asociadas a esta institución.

El propósito principal del Sistema Financiero nacional de un país consiste en dirigir el ahorro individual de las personas hacia el crecimiento económico saludable del país, es por ello que este sistema abarca todas las instituciones bancarias, mutualistas o cooperativas tanto quienes trabajan de forma pública como privada que operan legalmente dentro de un país, vale decir que el papel de estas entidades es convertir el ahorro de las personas en inversiones para otros,

gestionando de manera efectiva los riesgos que también implican a los asociados (Banco Internacional, 2021).

Así en cuanto a las instituciones financieras dentro de un país, estas se dividen dependiendo de su función ya sea que operen de forma pública o privada. Existen varios tipos de instituciones financieras en un país, en las cuales las principales son:

- **Bancos:** Institución financiera que proporciona servicios de depósitos, servicios de inversión, acceso a préstamos, facilitación de transacciones entre otros servicios actuando, así como intermediario entre quienes necesitan financiamiento.
- **Sociedades e intermediarias financieras:** Empresas dedicadas a actividades de financiamiento, como es la compra y venta de activos, acceso a créditos y administración de inversiones, siendo los inversionistas y los mercados financieros sus principales clientes.
- **Mutualistas:** Los miembros de una mutualista son propietarios y beneficiarios de dicha institución puesto que ofrecen servicios de carácter financiero como seguros y prestamos crediticios a sus miembros, esta institución actúa bajo el principio de mutualidad.
- **Cooperativas de ahorro y crédito:** Institución que promueve el bienestar económico de la comunidad donde sus miembros son propietarios de dicha institución con acceso a servicios de ahorro y crédito, así como otros servicios financieros.

Sin embargo, dentro del alcance de este proyecto la institución financiera de interés son las Cooperativas de ahorro y crédito que se darán a conocer a continuación.

2.1.1 Cooperativas de ahorro y crédito (COACs).

Las cooperativas de ahorro y crédito son instituciones financieras que operan bajo el concepto de cooperatividad en el que promueven el bienestar económico de la comunidad de sus miembros y usuarios, esta brinda servicios de tipo financieros tales como cuentas de ahorro, acceso a préstamos crediticios, servicios de remesas e inversión, entre otros.

Según Banco Central del Ecuador (2022), indica que los objetivos esenciales de las COACs son la autorresponsabilidad, autoayuda y autogerencia de todos sus socios y miembros lo que significa que deben hacer sentir a los socios y miembros que pertenecen a la misma organización, impulsando así el bienestar de la organización por medio de los pagos de los prestamos emitidos que se brindan.

Las COACs operan por medio de un orden geográfico estratégico para así elevar sus puntos y estar más cerca de sus miembros y de la situación local de los diferentes sectores productivos en donde estas serán captadas para así invertir en diferentes proyectos de producción dentro de la zona, sin embargo, para el desarrollo de todos estos proyectos y sus respectivos financiamientos también las COACs deben seguir una normativa de acuerdo con al uso de activos financieros.

2.1.1.1 Segmentación de las entidades del sector financiero popular y solidario.

Por otro lado, en cuanto se refiere a las regulaciones que siguen las COACs, estas siguen normativas específicas que deben mantener lineamientos y requisitos para su funcionamiento. Según la Resolución No. 521-2019-F (2019) de La Junta de Política y Regulación Monetaria y Financiera de la Superintendencia de Economía Popular y Solidaria en el Artículo 1, indica la

normativa para la segmentación de las entidades financieras en el sector financiero popular y solidario que va de acuerdo con el tipo y saldo de sus activos según los respectivos segmentos descritos en la Tabla 1.

Tabla 1

Segmentación de las entidades del sector financiero popular y solidario.

Segmento	Activos (USD)
1	Mayor a 80'000.000,00
2	Mayor a 20'000.000,00 hasta 80'000.000,00
3	Mayor a 5'000.000,00 hasta 20'000.000,00
4	Mayor a 1'000.000,00 hasta 5'000.000,00
5	Hasta 1'000.000,00

Nota. Datos tomados de la Resolución No. 521-2019-F (2019).

2.2 Seguridad de la información.

La seguridad de la información consiste en proteger la información sea de clasificación interna o confidencial contra accesos no autorizados, sin embargo, también se protege contra la divulgación, alteración de la integridad de la información y cualquier otra amenaza que comprometa su privacidad. Esto significa que la seguridad de la información abarca temas de implementación prácticas para garantizar que la información esté segura y protegida. Según Díaz (2004), "La seguridad es un proceso que tiene como objetivo intervenir en todas las tecnologías, todos los productos y, especialmente, el sentido común de los seres humanos que los gestionan" (p. 24).

Por otro lado, una de las cuestiones más importantes en lo que respecta al desarrollo de este proyecto, es la implementación de un plan integral de ciberseguridad que aporte al fortalecimiento del sistema de seguridad financiero de una institución, también existen conclusiones donde se afirma que “Un buen sistema de seguridad bancario debe tener en cuenta la prevención, la detección y la respuesta al problema en general” (Díaz, 2004, p. 25). En este sentido, el plan integral de ciberseguridad deberá abarcar las amenazas y vulnerabilidades identificadas y fortalecer así su infraestructura para mantener integro los servicios que se ofrecen al público y sus clientes.

Hoy en la actualidad, el sistema financiero de una institución hace uso de computadoras, sistemas de transacción monetaria, dispositivos digitalizados y aplicaciones móviles entre otros sistemas para el procesamiento de información, puesto que la seguridad de la información es crucial dentro de una institución, esta debe mantenerse al margen con respecto a la triada CIA (Confidencialidad, Integridad, Disponibilidad), ya que es un concepto muy utilizado en el ámbito de seguridad de la información y es la base de estrategias que permiten evaluar y diseñar sistemas de seguridad en diversos entornos ya sea empresariales o institucionales.

La importancia que tienen los estudios y métodos de seguridad de la información para la aplicación en empresas o instituciones financieras que manejan cierta información de naturaleza sensible con clasificación interna o confidencial son de suma importancia hoy en día al igual que para sus futuras generaciones en lo que respecta a sus respectivos campos de trabajo. Ramos Mera (2020) determinó que debido a que si se considera el avance tecnológico y la dependencia que tienen ciertas instituciones hacia la virtualización y automatización de sus servicios, la sociedad

también requiere de la seguridad que proteja y resguarde la información de los clientes y sus intereses, ya que estos avances tecnológicos vienen de la mano del avance en cuanto a ataques y amenazas de robos, problemas en sus servicios o suplantación de información, siendo así vulnerables a ciertas organizaciones delictivas dedicadas a los ciberdelitos.

Según Ramos Mera (2020) debido a la creciente sofisticación tecnológica en las instituciones financieras también incrementan las amenazas y riesgos, los aspectos a tomar en cuenta en el ámbito bancario respecto a la seguridad de la información son los siguientes:

- **Protección de datos sensibles:** Las instituciones financieras almacenan gran cantidad de información de clasificación interna y confidencial para los clientes, por ejemplo, como sus datos personales, números de identificación o cuentas bancarias con detalles en sus transacciones o transferencias, por consiguiente, ante la pérdida o divulgación de esta información podría obtener consecuencias graves tanto para los clientes como la reputación de la institución perdiendo credibilidad.
- **Prevención de fraude financiero:** En este término de prevención de fraude financiero abordan ciertos temas como los ataques financieros, phishing o la ingeniería social que pueden ser utilizados para realizar estos fraudes.
- **Interrupción de servicios:** Uno de los objetivos para los atacantes, son el de interrumpir los servicios ya que la disponibilidad de los servicios es fundamental para la confianza de los clientes, así como su estabilidad financiera con sus respectivos socios.

- **Cumplimiento normativo:** Hoy en día las instituciones financieras deben sujetarse a estrictas regulaciones legales en cuanto a su calidad de servicio y seguridad de la información, para garantizar la privacidad de los clientes y de la institución misma. La reglamentación existente en Ecuador es:
    - Ley para la optimización y eficiencia de trámites administrativos.
    - Ley Orgánica de Protección de Datos Personales.
    - Resolución No. 521-2019-F de La Junta de Política y Regulación Monetaria y Financiera.
- **Protección contra RANSOMWARE:** El ataque ransomware es un tipo de ataque informático donde la atacante cifra los datos del usuario para luego exigir un rescate para su liberación, comprometiendo así la integridad de sus datos. Las instituciones bancarias son blancos para este tipo de ataques por poseer gran cantidad de información crítica y confidencial.
- **Protección de la reputación:** Las violaciones de seguridad pueden perjudicar a la reputación de un banco o una institución financiera y llevar así a una perdida significa de clientes, es por ello por lo que una ciberseguridad adecuada mantendría la confianza con el público y sus clientes.
- **Innovación tecnológica:** A medida que los bancos y las instituciones financieras mantienen un crecimiento constante en cuanto a la adquisición de tecnología también aumentan los ataques dirigidos, es por ello que la ciberseguridad permite la innovación en seguridad protegiendo así su integridad a la vista del público y sus clientes.

2.2.1 Modelo de seguridad CIA.

El modelo de seguridad CIA de la Figura 1, o conocida también como triada CIA contribuye en la seguridad de la información al sistema bancario de una institución financiera. Alshathri et al. (2022) indica que la triada CIA conformada por la confidencialidad, integridad y disponibilidad, conocidas como el triángulo de la seguridad de la información, son los principios fundamentales de la seguridad de los datos y la ciberseguridad en sistemas bancarios, ya que proporcionan el marco de referencia para la seguridad requerida de la información manejada por una institución bancaria.

Figura 1

Relación entre Confidencialidad, integridad y disponibilidad.

Nota. Comparación entre los términos del triángulo CIA con su respectiva relación. Fuente: Thakare & Gore (2014).

2.2.1.1 Objetivos específicos del modelo de seguridad CIA.

Dentro del modelo de seguridad CIA cada componente contiene objetivos específicos en cuanto a su funcionamiento. Aguilera López (2010) propone que el modelo de seguridad CIA forman la base de la seguridad de la información ya que es compatible con diversos entornos donde esta incluye las redes informáticas, los sistemas de almacenamiento, las bases de datos y cualquier otro medio donde se procese, almacene o transmita información. Los componentes de la triada CIA y sus objetivos se detallan a continuación:

- **Confidencialidad:** Se basa en la protección de la información para evitar el acceso no autorizado y comprende los siguientes aspectos:
    - *Control de Acceso:* Limitar el acceso a la información solo a aquellos usuarios autorizados, asegurando que la información sensible no caiga en manos equivocadas.
    - *Cifrado de Datos:* Implementar técnicas de cifrado para proteger la información confidencial, tanto en reposo como durante la transmisión.
    - *Políticas de Seguridad:* Desarrollar y aplicar políticas de seguridad que establezcan claramente quién tiene acceso a qué tipo de información y en qué condiciones.
- **Integridad:** Implica a la protección y resguardo de la información que garantizara que la información no haya sido alterada sin autorización, tomando en cuenta lo siguiente:
    - *Controles de Cambios:* Respaldo de autorización de cambios en la información evitando así alteraciones no autorizadas.
    - *Firmas Digitales:* Estas firmas cuando son aplicadas verifican la autenticidad, origen y el no repudio de la información.

- *Checksums y Hashes:* Verifica la integridad de la información de modo que asegura no haber sido manipulada durante su circulación.

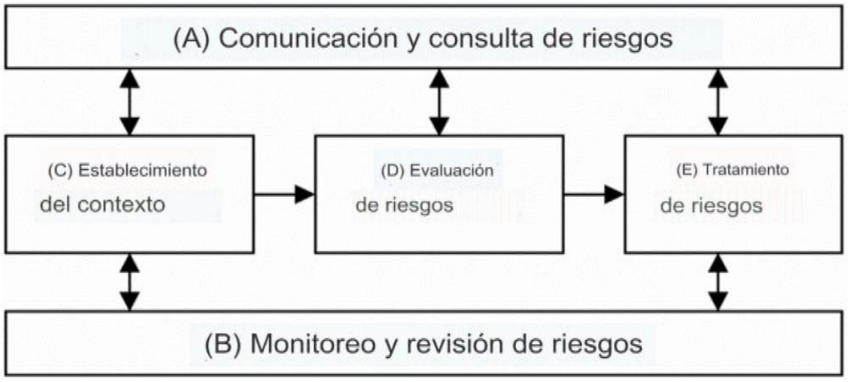
- **Disponibilidad:** La información estará disponible el momento que el usuario con autorización lo necesite, considerando así también los siguientes aspectos:
  - *Respaldo de Datos:* Son hábitos de respaldo que aseguran la disponibilidad de la información en caso de pérdidas o daños en su infraestructura de red interna.
  - *Tolerancia a Fallos:* Implementar medidas que permitan la continuidad del servicio incluso en situaciones de fallos o ataques.
  - *Planificación de la Continuidad del Negocio:* Desarrollar estrategias para mantener operativas las funciones del negocio en situaciones diferentes.

2.3 Gestión y manejo de riesgos.

Según Moreno García (2022) determinó que la gestión y manejo de riesgos en ciberseguridad es un proceso fundamental para identificar, evaluar y mitigar las amenazas y vulnerabilidades que podrían afectar la seguridad de la información y los sistemas tecnológicos. Sin embargo, existen metodologías que mantiene el mismo fundamento general en el ámbito del análisis de la gestión de riesgos de seguridad de la información, entre las cuales está la ISO 27005: 2011.

Figura 2

Metodología general de análisis de la gestión de riegos de la seguridad de la información en un entorno empresarial.



Nota. La figura muestra la metodología general de análisis de la gestión de riesgos de la información basado en la norma ISO 27005: 2011. Fuente: Jaya Putra et al. (2020).

Este diseño permite a las organizaciones tomar acciones sobre cómo proteger sus activos de información y minimizar los riesgos, por lo que a continuación se detallan algunos aspectos conforme en la gestión de riesgos:

- **Identificación de Activos:** Identifica y cataloga todos los activos de información, tales como datos, sistemas, redes, hardware y software dentro de su infraestructura.
- **Evaluación de Riesgos:** Se analizan todas las amenazas y vulnerabilidades asociadas a cada activo lo cual permite determinar la probabilidad de riesgo podría generar un impacto sobre cada activo analizado.
- **Análisis de Riesgos:** Se aplica un estudio más detallado de los riesgos identificados con forme a cada activo dado que este análisis puede ser cuantitativo, esta asigna valores a los

riesgos mediante una clasificación subjetiva basada en niveles como alto, medio o bajo dependiendo de la clasificación que se desea aplicar.

- **Tratamiento de Riesgos:** El tratamiento de riesgos se divide en tres acciones escenciales los cuales son:
    - *Mitigación:* Implementación de medidas que reducen la probabilidad del impacto de los riesgos, lo cual puede incluir controles de seguridad de red interna y externa, actualizaciones, capacitación del personal, entre otros.
    - *Transferencia:* Se comparte el riesgo con terceros lo cual es mediante con la contratación de seguros contra ciberataques y amenazas.
    - *Aceptación:* Se decide aceptar determinados riesgos cuando el costo de mitigarlos supera los beneficios que se tenían esperados.
- **Implementación de Controles:** Con forme en la evaluación de riesgos se aplican controles y medidas de seguridad para proteger los activos más críticos dentro de la institucion. Entre ellos se encuentran equipos de Networking, sistemas internos, políticas de seguridad, entre otros.
- **Monitoreo y Evaluación Continua:** La gestión de riesgos es un proceso constante puesto que las amenazas y la tecnología avancen constantemente, entonces es fundamental monitorear de forma continua los controles implementados y realizar evaluaciones periódicas en un determinado tiempo.
- **Plan de Respuesta:** Al contar con un plan detallado que permita actuar ante posibles incidentes de seguridad, esta debe incluir la asignación de roles y responsabilidades, procedimiento y pasos necesarios para contener y remediar los problemas detectados.

- **Cultura de Seguridad:** El generar una cultura de seguridad en toda la organización es muy importante, ya que esto implica concientizar a los colaboradores sobre las mejores prácticas en seguridad con una responsabilidad individual creando asi un entorno seguro para toda la institución.

La gestión de riesgos en ciberseguridad no solo es importante para proteger los activos de información, sino que también para cumplir con requisitos normativos legales y garantizar la continuidad operativa de la organización frente a amenazas y riesgos.

2.3.1 Riesgo Tecnológico.

En cuanto a ciberseguridad dentro de la institución esta se refiere a la posibilidad de que los activos tecnológicos, así como sistemas informáticos, redes, software y datos, enfrenten amenazas o vulnerabilidades que podrían resultar perjudiciales para la organización.

Jaya Putra et al. (2020) indica que este tipo de riesgo se asocia con el entorno tecnológico tanto físico como digital en el que opera una organización y los posibles eventos adversos que podrían afectar la triada CIA de la información. Jaya Putra et al. (2020) indica que algunos elementos clave asociados con el riesgo tecnológico en ciberseguridad incluyen lo siguiente:

- **Amenazas Cibernéticas:** Conformadas como malware, ransomware, ataques de denegación de servicio (DDoS), phishing y otros, representan riesgos tecnológicos significativos a la institución.

- **Vulnerabilidades del Software y Hardware:** Estas pueden ser explotadas por atacantes para comprometer la seguridad, ya que estas vulnerabilidades pueden incluir errores en la programación, falta de actualizaciones o configuraciones inseguras en su estructura interna o física.
- **Fallas en la Seguridad de la Red:** Esto hace referencia a problemas en la seguridad de la red tales como brechas de seguridad, configuraciones incorrectas de firewalls y falta de segmentación de red que pueden dar lugar a riesgos tecnológicos.
- **Fallas en la Infraestructura de TI**: Toma a consideración problemas en la infraestructura de tecnologías de la información, fallas en servidores, almacenamiento y equipos de red que pueden tener un impacto directo en la disponibilidad de servicios y datos.
- **Problemas de Gestión de Identidades y Accesos:** La gestión inadecuada de identidades y accesos, como contraseñas débiles, acceso no autorizado o falta de controles adecuados, puede aumentar el riesgo de compromisos de seguridad ya que esto permitiría el acceso no autorizado a los servicios o datos.
- **Fallas en la Gestión de Parches:** La falta de aplicación o actualización de parches de seguridad puede dejar sistemas vulnerables a exploits conocidos ya que recomendable mantener actualizado el software para mitigar riesgos tecnológicos.
- **Fallas en la Protección de Datos:** La falta de controles de protección de datos como la encriptación insuficiente pueden exponer información muy importante a usuarios no autorizados o atacantes.

El control efectivo del riesgo tecnológico en cuanto a seguridad implica con la identificación y evaluación de los riesgos, seguida de la implementación de sugerencias, medidas

y controles para mitigarlos. Además de la concientización y capacitación del personal ya que son componentes clave para reducir el riesgo asociado con factores humanos como el phishing. La seguridad informática es un campo en constante evolución dado que la gestión de riesgos debe ser un proceso continuo.

2.3.2 Identificación de activos y evaluación de riesgos.

Según en la página oficial de Infórmate de riesgos - Pirani (2024) menciona que la identificación de activos y la evaluación de riesgos son dos etapas clave en el proceso de gestión de riesgos en ciberseguridad. Estas etapas proporcionan una base sólida para comprender la infraestructura de tecnología de la información de la organización, identificando así los activos críticos y evaluando así las amenazas y vulnerabilidades asociadas dentro de cada elemento. A continuación, se presenta más detalles sobre cada una:

2.3.2.1 Identificación de Activos.

Esta etapa en Infórmate de riesgos - Pirani (2024) indica que se realizara un seguimiento de los recursos físicos y digitales que conforman la estructura de red de la organización, en las cuales se clasifican como:

- **Activos de Información:** Es la identificación de todos los activos de información de la organización tanto físico como digital, en estos puede incluir bases de datos, aplicaciones, sistemas operativos, hardware, software, redes, y cualquier otro elemento que almacene, procese o transmita información dentro y fuera de su entorno.

- **Inventario de Activos:** Este inventario debe incluir detalles como la ubicación física de cada elemento donde esta indique los propietarios, las dependencias y cualquier información relevante para entender el valor y función de cada activo.
- **Clasificación de Activos:** Clasificación de los activos según su importancia. Esto ayuda a priorizar la protección y asignar recursos de manera eficiente. Los activos pueden clasificarse en función de la confidencialidad, integridad y disponibilidad.
- **Propietarios de Activos:** Asignar responsabilidades asignando propietarios a cada activo. Los propietarios son responsables de la protección y la gestión de los riesgos asociados con sus activos asignados.

2.3.2.2 Identificación y evaluación de Riesgos.

Esta etapa en Infórmate de riesgos - Pirani (2024) con el inventario de activos ya realizado se debe identificar y evaluar los riesgos mediante técnicas de investigación o metodologías de análisis de campo para luego realizar su debido tratamiento, esta fase se clasifica de la siguiente forma:

- **Identificación de Amenazas:** Identificar las posibles amenazas y escenarios de riesgo que podrían afectar a los activos de información. Las amenazas pueden incluir ciberataques, desastres naturales, errores humanos, entre otros.
- **Identificación de Vulnerabilidades:** Identificar las vulnerabilidades en los activos que podrían ser explotadas por las amenazas identificadas.

- **Análisis de Riesgos:** Evaluar la probabilidad de que ocurran las amenazas identificadas y el impacto potencial de esas amenazas en los activos. Esto implica asignar valores a la probabilidad e impacto para calcular el riesgo.
- **Calificación de Riesgos:** Al clasificar los riesgos esto puede ser detallando en una escala como baja, media y alta o incluso una clasificación numérica, esto es más dependiente del modo que se desee interpretar estos datos.
- **Documentación de Riesgos:** Al documentar los riesgos esto debe incluir detalles sobre las amenazas, vulnerabilidades, niveles de riesgo de cada activo, puesto que esta documentación será útil para la implementación de controles y políticas de mitigación.
- **Desarrollo de Estrategias de Mitigación:** Estas estrategias son la gestión de controles de seguridad, actualizaciones de software, capacitación, entre otras medidas controlando así los riesgos detectados.
- **Monitoreo constante:** El periodo de revisión continua es un proceso muy importante dentro de un tiempo determinado que permite el control de las estrategias implementadas.

La identificación de activos y la evaluación de riesgos son procesos continuos en el ciclo de vida de gestión de riesgos, ya que proceso ayuda a las organizaciones a entender los riesgos de manera proactiva para proteger y fortalecer sus activos más críticos.

2.3.3 Herramientas específicas para la identificación y evaluación de riesgos.

Existen varias herramientas hoy en día que son específicamente diseñadas para la identificación y evaluación de riesgos en el ámbito de la ciberseguridad y la gestión de la información tales como:

- **Microsoft Threat Modeling Tool:** Ayuda en la identificación y gestión de riesgos de seguridad durante el desarrollo de software mediante el modelado de amenazas.
- **NIST Risk Management Framework (RMF):** El Marco de Gestión de Riesgos del Instituto Nacional de Estándares y Tecnología (NIST), es una guía detallada para gestionar riesgos en sistemas de información.
- **CIS Critical Security Controls (CSC):** Conjunto de mejores prácticas de seguridad desarrollado por el Centro de Internet Segura (CIS) para ayudar a organizaciones a prevenir y responder a ciberataques.

Sin embargo, la principal herramienta a utilizar en el desarrollo de este proyecto es la del Marco Metodológico de la NIST en la versión SP 800 – 30 que es excelente para la evaluación y mitigación de riesgos.

2.3.3.1 NIST Marco de Gestión de Riesgos SP 800 - 30

El Marco de Gestión de Riesgos del Instituto Nacional de Estándares y Tecnología (NIST) es una guía detallada para gestionar riesgos en sistemas de información. ESGinnova Group (2021) plantea que el aumento de ataques cibernéticos se debe al incremento progresivo de los servicios y modelos de comunicación, como es al aumento de Tecnologías de la Información IT. Este hecho ha llevado a las empresas a buscar métodos para realizar análisis preventivos, control y reducción de riesgos de seguridad de la información.

Para ello, una de metodologías implementadas en numerosas empresas es: el análisis y mitigación de riesgos según la metodología NIST SP800-30. Este método nació en el Instituto

Nacional de Estándares y Tecnología que fue establecido con el propósito de analizar y mitigar los riesgos pueda presentar la seguridad de la información, con la meta de brindar respaldo a las organizaciones en todo lo concerniente a la Tecnología (ESGinnova Group, 2021). Para un informe detallado, se requiere evaluar la probabilidad de riesgos de cada activo critico de la organización, discutir el proceso de control y su relación con las evaluaciones de riesgos, comunicar la realización de estas evaluaciones en sistemas de información y listar los pasos del proceso de evaluación de riesgos los cuales son:

- Preparación de la evaluación
- La realización de la evaluación
- Comunicar los resultados de la evaluación, y el mantenimiento de la evaluación
- Proceso de gestión de riesgo

Para los procesos de gestión del riesgo se tienen los siguientes pasos:

- Estructura del riesgo
- Evaluación del riesgo
- Responder a los riesgos
- Seguimiento de los riesgos
- Procesos de análisis de riesgos

La metodología NIST SP800-30 para el análisis de los riesgos de seguridad de la información está compuesta por nueve fases:

- **Caracterización del sistema:** Permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa.
- **Identificación de amenazas:** Se identifican los diversos motivos que fomentan a ataques, riesgos y problemas de red.
- **Identificación de vulnerabilidades:** Se realiza una lista de puntos débiles que detectan posibles intrusiones de riegos y amenazas dentro de cada activo critico de la organización.
- **Análisis de controles:** Examinar los controles existentes dentro de la organización y elaborar una lista correspondiente de por sí que permita un mejor control.
- **Determinación de probabilidades:** Entender las razones detrás de los ataques dado que la capacidad de las amenazas y la naturaleza de las vulnerabilidades detectadas nos permite clasificar la probabilidad de que la amenaza se materialice dentro de la institución.
- **Análisis del impacto:** El análisis busca determinar el riesgo de impacto de la institución y sugerir así controles para mitigar el riesgo identificado hasta alcanzar un nivel aceptable que este mejor controlado.
- **Determinación del riesgo:** Implica en elaborar un plan integral donde es necesario comprender la probabilidad de riesgos, el alcance de los impactos y la eficacia de los controles existentes proporcionando así un control a estos riesgos evaluados.
- **Recomendación de controles:** Se necesita revisar regularmente las políticas de seguridad, actualización, cambio de contraseñas periódicamente, instalar firewalls y aplicar sanciones por incumplimiento de normativas en caso de ser necesario.

- **Documentación de resultados:** Conforme a los riesgos de la organización que han sido evaluados se debe proceder a la elaboración de un informe de valoración de los riesgos que detalle cada activo.

Ya desarrollado el análisis de los riegos se procede a realizar la parte de gestión de riesgos que está compuesta por seis fases que son:

- **Priorización de acciones:** Basándose en los niveles de riesgo previamente analizados y en su respectivo informe de evaluación de riesgos, se establecerá una tabla de acciones a implementar en la empresa.
- **Evaluación de operaciones de control recomendados:** Esta sección da paso a la evaluación de la viabilidad, eficacia y compatibilidad de los controles para hacer frente a los riesgos detectados.
- **Seleccionar los controles que nos ayudarían a eliminar los riesgos:** Para prevenir intrusiones en la red, debemos considerar qué controles implementar, como firewalls, cambio periódico de contraseñas o actualizaciones de los firewalls.
- **Asignación de responsabilidades:** Elegir quién o quiénes supervisan los controles seleccionados.
- **Desarrollo del plan de implementación de salvaguardas:** Desarrollar un plan integral de seguridad que corrija y mitiga ciertos riesgos en base a la evaluación realizada.

2.3.4 Rol de la ciberseguridad en la gestión de riesgos.

Según Linares Lizarazo (2018) la ciberseguridad no es simplemente un complemento en la gestión de riesgos; es un componente crítico que determina la capacidad de una organización para prosperar en un entorno digital y hacer frente a futuras amenazas. Ya que la colaboración entre la ciberseguridad y el control de riesgos es esencial para una estrategia puesto que la evaluación y cuantificación de riesgos se integran con la evaluación general de riesgos en todos sus activos, permitiendo a las organizaciones tomar decisiones basadas sobre la inversión en tecnologías de seguridad, así como su implementación.

2.4 Metodologías, normativas y leyes en el ámbito de la seguridad.

En esta sección se abordarán temas de relación legal conforme a lo establecido en los artículos y reglamentos que rigen en Ecuador en cuanto a seguridad de la información y ciberseguridad, los cuales son fundamentales para mantener el orden dentro de las empresas, entidades bancarias o instituciones financieras que manejan datos de carácter confidencial.

2.4.1 Normativas y leyes que rigen a las instituciones financieras a nivel nacional.

Entre las normativas y leyes existentes que afectan a las instituciones financieras en materia de ciberseguridad y protección de datos en el Ecuador son:

- **Ley para la optimización y eficiencia de trámites administrativos:** Tal como indica el Articulo 11, párrafo 6 del Reglamento General a la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos (2018):

> Las personas naturales o jurídicas del sector privado que sean concesionarias de un servicio público, es de su obligación implementar controles de seguridad informática y de la información ya que es de conformidad con lo que establezca el órgano que preside el Sistema Nacional de Registro de Datos Públicos. (p. 9)

Esta sección tiene como objetivo el regular su simplificación en cuanto administración informática con el fin de facilitar la relación entre las y los administrados y la Administración Pública y entre las entidades que la componen.

- **Ley Orgánica de Protección de Datos Personales:** La ley deja toda la responsabilidad en manos de las organizaciones, quienes, con base en el principio de protección proactiva de los datos, no solo deben modificar los contratos con los proveedores o clientes, sino que deben implicar a la totalidad de la organización: desde los altos directivos hasta el recepcionista, pasando por el técnico de sistemas y de recursos humanos. Además, hay que tener en cuenta terceras partes interesadas, como proveedores, accionistas de las cuales se rigen a los reglamentos existentes tales como:

  - Reglamento de la Ley Orgánica de Protección de Datos Personales.
  - El acuerdo Ministerial Número 006-2021 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
  - Superintendencia de Economía Popular y Solidaria (SEPS) de la resolución No. EPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR

- **SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR:** La Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002, emitida por la Superintendencia de Economía Popular y Solidaria, comprende aspectos relacionados con la ciberseguridad en entidades bancarias. Esta resolución establece directrices y medidas específicas para fortalecer la seguridad de la información en el sector financiero, con el objetivo de proteger los datos sensibles de los clientes, prevenir fraudes cibernéticos y garantizar la integridad de las operaciones financieras. Como indica en su reforma en el Artículo 10 de las Resoluciones de Entidades del Sector Financiero Popular y Solidario - Superintendencia de Economía Popular y Solidaria - SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 (2022) indica lo siguiente:

> Las entidades y empresas que conforman este régimen deberán implementar y mantener un SGSI que se encuentre orientado a garantizar la adecuada gestión de seguridad de la información acorde a la normativa legal vigente. (p.9)

La Superintendencia, a través de esta resolución, busca promover prácticas seguras en el manejo de la información y fomentar la adopción de estándares de seguridad cibernética en las entidades financieras bajo su supervisión.

- **Acuerdo Ministerial Número 006-2021:** Según el Acuerdo-No.-006-2021-Politica-de-Ciberseguridad (2022) del Ministerio de Telecomunicaciones y de la Sociedad de la Información indica que con esta resolución se permite el fortalecimiento de las capacidades nacionales para garantizar los derechos y libertades de la población para proteger los bienes

jurídicos del Estado en el ciberespacio, tal como indica que en el marco de la prevención de incidentes cibernéticos se ha priorizado la protección de infraestructuras digitales y servicios esenciales dentro de una organización.

Capitulo III

Análisis de la situación actual

En este capítulo se hace un estudio de la estructura física, distribución de departamentos, servicios prestados por la cooperativa, activos de información, red de datos y espacio físico del cuarto de telecomunicaciones para el establecimiento de las fortalezas, amenazas, oportunidades y debilidades de la COACs.

3.1 Diagnostico de la situación actual.

La estructura de red de la COAC Mercedes Cadena LTDA involucra el manejo y funcionamiento de varios elementos relacionados con base de datos financieras. Cabe recalcar que la institución misma proporciono los permisos correspondientes para el análisis y estudio de su infraestructura, esto se encuentra en documentos formales que puede ser visualizados en el **ANEXO A** y **ANEXO B**. Durante el horario de atención de la institución, se llevan a cabo distintos tipos de transacciones, lo que implica que las bases de datos experimenten cambios significativos en un solo día y que los servidores se encuentren en constante actividad dentro de la organización. Esta situación genera la necesidad de monitorear todos los activos de la red e implementar controles de seguridad, gestiones de red y políticas de mitigación de riesgos, ya que son aspectos en los cuales la organización antes mencionada carece actualmente.

La institución se encuentra en un proceso integral de mejora de su Plan de Negocios ya que, bajo este contexto, la documentación desempeña un papel fundamental al igual que la

necesidad de realizar evaluaciones periódicas de riesgos, amenazas y vulnerabilidades dentro de su estructura interna de red.

Implementar un plan integral de ciberseguridad prepara a la institución para enfrentar diversas amenazas y responder eficientemente a cualquier incidente que se genere dentro de la organización. Este enfoque busca garantizar la continuidad del negocio y mantener un alto nivel de disponibilidad, beneficiando tanto a los clientes como a la propia cooperativa.

3.1.1 Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda.

La Cooperativa de Ahorro y Crédito Mercedes Cadena CACME LTDA.es una institución legalmente establecida y controlada por la Superintendencia de Economía Popular y Solidaria, con el respaldo del Banco Central del Ecuador y la Corporación de Seguros de Depósitos Fondo de Liquidez y Fondos de Seguros Privados, que tiene un trayecto de más de 15 años al servicio de la comunidad. (COAC Mercedes Cadena LTDA., 2007b)

CACME LTDA., inicia con la idea de facilitar el servicio de prestación de dinero entre los miembros de la comunidad Mercedes Cadena, ya que las entidades financieras en ese entonces no daban acogida a la gente indígena, la situación y el tiempo no era favorable para adquirir un crédito en dichas entidades. (COAC Mercedes Cadena LTDA., 2007b)

Con el acogimiento que tuvo la asociación entre los comuneros, en el año 2000 se la denomina Caja de Ahorro y Crédito Mercedes Cadena, con el alto crecimiento y rentabilidad de

fondos que está mantuvo y las exigencias de la ley en el año 2007 se llega a constituir como una Cooperativa de Ahorro y Crédito. (COAC Mercedes Cadena LTDA., 2007b)

Actualmente CACME LTDA. trabaja con personal altamente calificado para desempeñar sus labores y brindar una atención personalizada de calidad, ofreciendo productos y servicios con la capacidad de satisfacer las necesidades de nuestros socios y clientes. (COAC Mercedes Cadena LTDA., 2007b)

CACME LTDA. fomenta el desarrollo entre los emprendedores y microempresarios que tienen la visión de crecer junto a sus negocios. (COAC Mercedes Cadena LTDA., 2007b)

3.1.1.1 Misión Institucional.

"Promover la inclusión financiera de calidad y oportuna, apoyando el desarrollo integral de sus asociados, bajo principios de transparencia, responsabilidad social, fortaleciendo el desarrollo e integración de la economía popular y solidaria."

3.1.1.2 Visión Institucional.

"Ser una institución líder en la prestación de productos y servicios financieros accesibles, confiables e innovadores; con una estructura financiera sólida y un capital humano altamente capacitado y comprometido, enmarcados en la economía popular y solidaria. Promover el desarrollo y bienestar tanto de nuestros socios como del país."

3.1.2 Servicios prestados por la COAC Mercedes Cadena Ltda.

La Cooperativa Mercedes Cadena Ltda., como entidad financiera privada, brinda una amplia gama de servicios diseñados para impulsar el desarrollo económico de sus socios y comunidades emprendedoras. Esto se logra gracias a un equipo altamente capacitado y eficiente. Para obtener más información sobre los servicios disponibles, consulta la Tabla 2.

Tabla 2

Servicios prestados por la COAC Mercedes Cadena Ltda.

SERVICIOS PRESTADOS POR LA COAC CACME LTDA.	
Ahorros	**Créditos**
• Ahorro a la vista	• Crédito de consumo
• Ahorro futuro	• Microcréditos
• Ahorro programado	
• Ahorro infantil	

Nota. Datos tomados de la carta cooperativa de la (COAC Mercedes Cadena LTDA., 2007).

3.1.3 Servicios consumidos por la COAC Mercedes Cadena Ltda.

Para que la COAC pueda realizar sus actividades de manera efectiva, es fundamental que tenga acceso a los servicios detallados en la Tabla 3. Estos servicios incluyen tanto las necesidades básicas, como el suministro de agua potable, electricidad y telefonía, así como aquellos servicios utilizados regularmente por la cooperativa, provenientes de proveedores, contratistas y terceros esenciales para su operación.

Tabla 3

Servicios consumidos por la COAC Mercedes Cadena Ltda.

SERVICIOS CONSUMIDOS POR LA COAC CACME LTDA.		
Contacto	**Servicio**	**Número Telefónico**
Emelnorte	Electricidad	062-997100
EMAPA	Agua potable	062-906 823
Telconet	Internet	+593 4 39 22 000
ECU911	Emergencias	911
SITETRIOR	Provisión del sistema Administración financiera Asistencia técnica del sistema	099 764 1477
Banco Central del Ecuador	Servicios Bancarios	Call Center: 1700 153 -153 / 02-3938-600

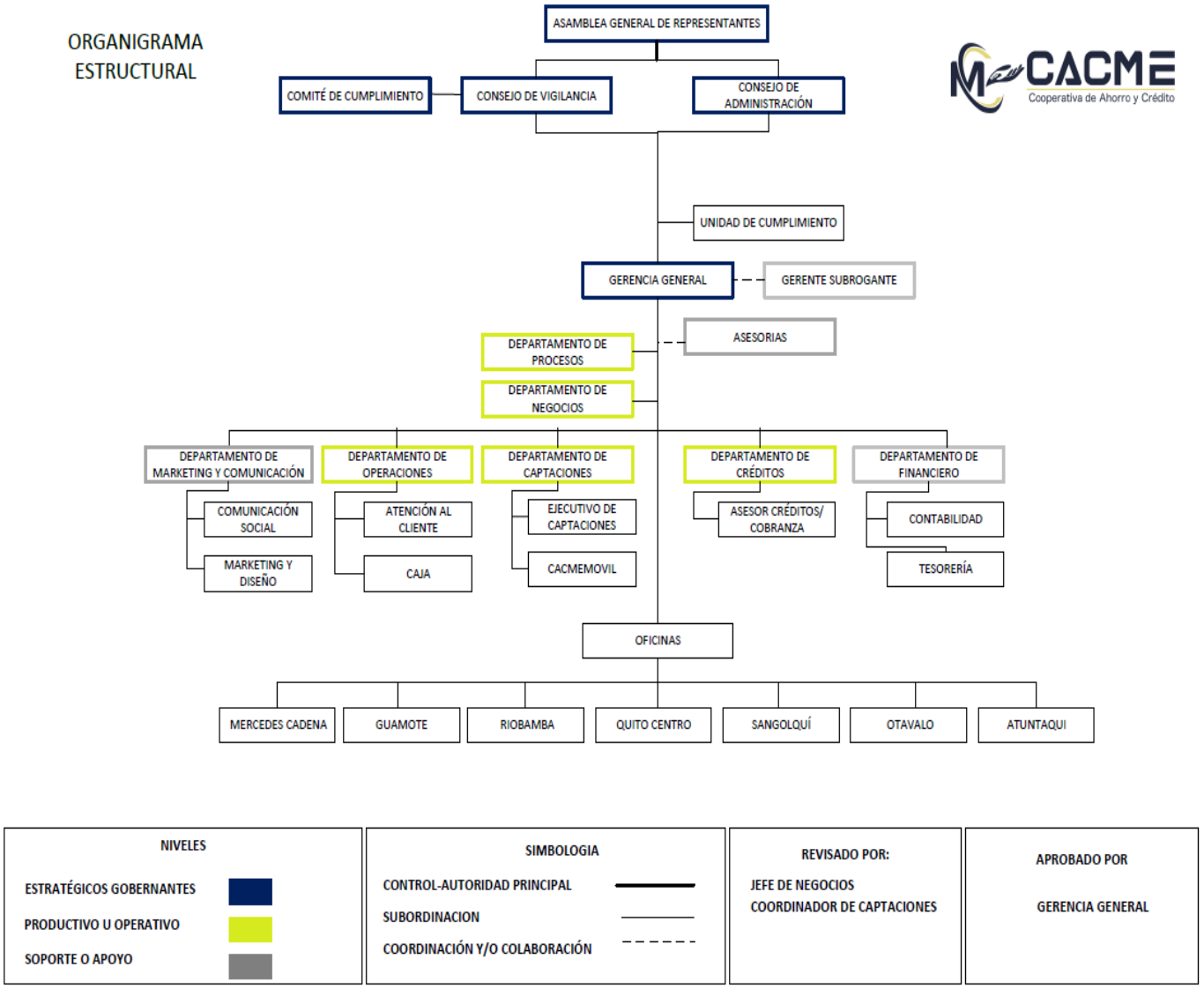
Nota. Datos tomados del departamento de procesos de la COAC Mercedes Cadena LTDA.

3.1.4 Estructura organizativa de la COAC Mercedes Cadena Ltda.

En la Figura 3 y 4 muestran el organigrama estructural y funcional de la COAC Mercedes Cadena Ltda., respectivamente. Es esencial comprender esta estructura para elaborar el Plan de Ciberseguridad propuesto en este trabajo, ya que nos permite identificar a las personas responsables en cada área y asignar responsabilidades de manera que se asegure la protección de la información:

Figura 3

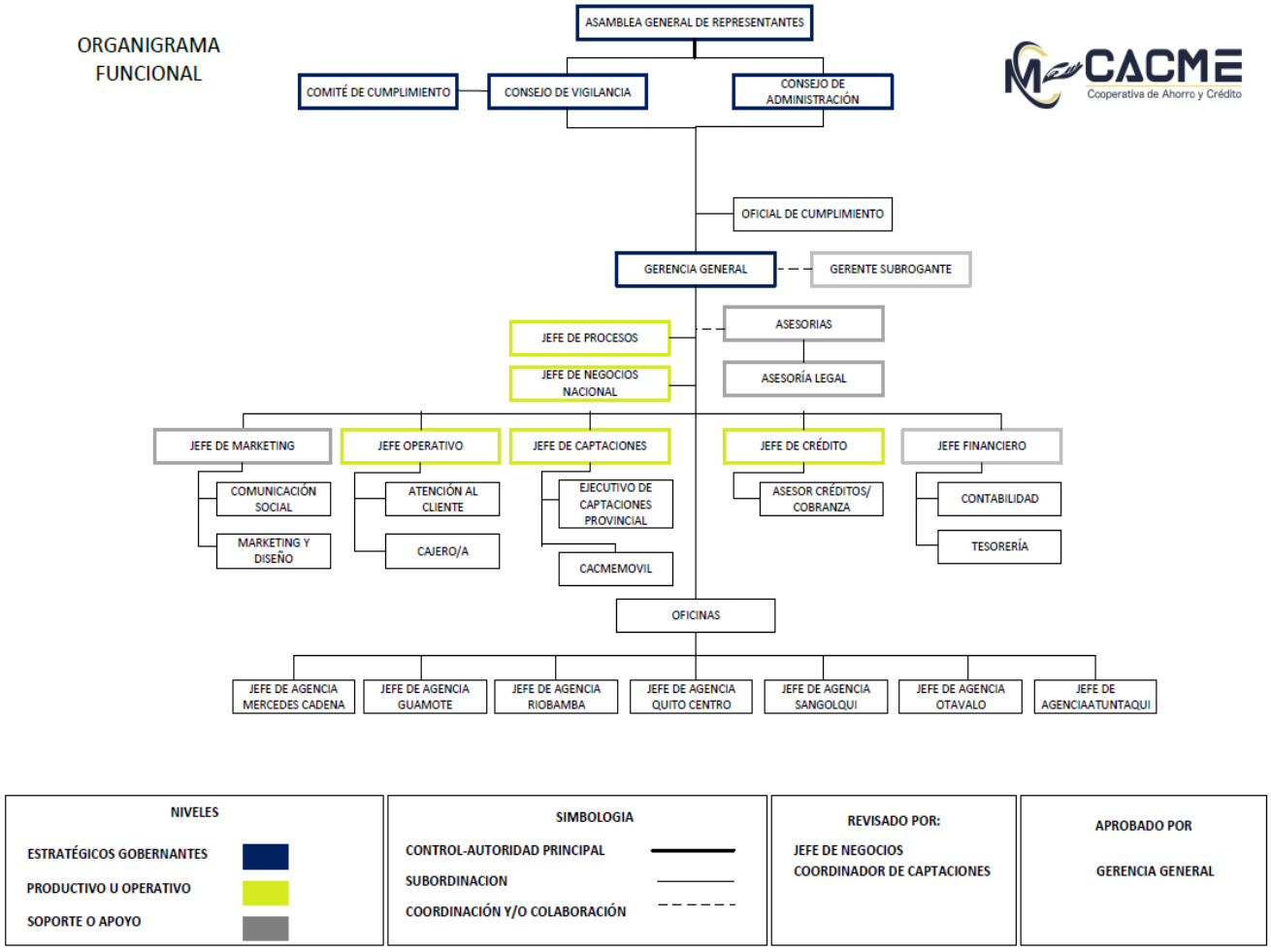
Organigrama estructural de la COAC Mercedes Cadena.



Nota. Organigrama estructural de la COAC Mercedes Cadena Ltda. Fuente: COAC Mercedes Cadena LTDA. (2007)

Figura 4

Organigrama funcional de la COAC Mercedes Cadena.



Nota. Organigrama funcional de la COAC Mercedes Cadena Ltda. Fuente: COAC Mercedes Cadena LTDA. (2007)

3.1.5 Infraestructura de red.

En la actualidad, la información se ha convertido en el activo más valioso para cualquier institución, lo que requiere la implementación de diversas metodologías para su adecuado almacenamiento y protección. Los datos de una organización pueden encontrarse en diversos formatos, como documentos físicos, dispositivos de almacenamiento digital, discos extraíbles y bases de datos en servidores, entre otros. Para prevenir posibles pérdidas, es esencial contar con controles de seguridad que aseguren los principios fundamentales de la información, como la confiabilidad, integridad y disponibilidad. Sin embargo, la COAC Mercedes Cadena LTDA. Así como carece de algunos de estos controles necesarios para garantizar la seguridad de la información, también cuenta con algunas especificaciones que protegen y cubren sus activos, como se evidencia a continuación en la Figura 5 donde se observa la presencia de gabinetes para los equipos de conexión intermedia.

Figura 5

Equipos de conexión intermedia con protección.

Nota. Imagen adquirida de departamento de procesos de la COAC Mercedes Cadena LTDA.

3.1.5.1 Topología de la red.

La COAC Mercedes Cadena LTDA tiene establecido una red interna cableada que conecta los diferentes departamentos de la institución, además de una red inalámbrica exclusivamente disponible para dispositivos autorizados por el Departamento de Telecomunicación o área de Tecnología como la suelen mencionar. Para más detalles sobre estas redes de comunicación, consulta la Tabla 4.

Tabla 4

Redes de comunicación de la COAC Mercedes Cadena LTDA.

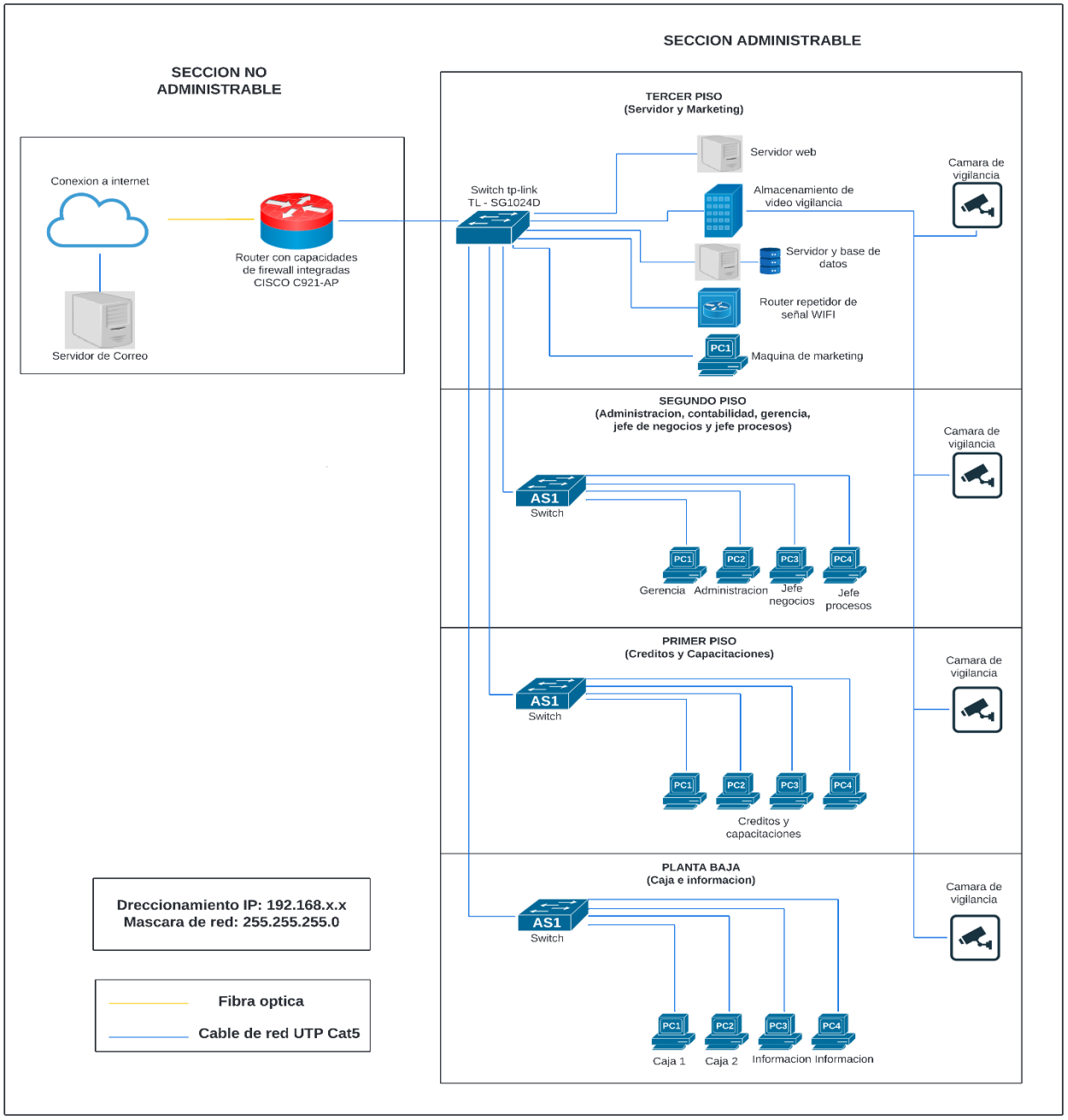
RED	DESCRIPCION
Red Local	Conformado por red cableada categoría 5e y categoría 6.
Red Wireless	Conformada por la red inalámbrica distribuida exclusivamente para la 3ra planta y la 2da planta.

Nota. Adquirida del departamento de procesos de la COAC Mercedes Cadena LTDA.

La topología de red de la cooperativa está establecida mediante la implementación de un switch en cada piso del edificio, que cuenta con cuatro plantas: planta baja, primer piso, segundo piso y tercer piso. Cada uno de estos switches está configurado con un etiquetado implícito, lo que le permite conmutar la red a los diferentes puntos de acceso distribuidos en cada nivel. Cabe mencionar que los dispositivos conectados a esta red cuentan con una dirección IP estática asignada, lo que garantiza una conectividad adecuada, incluso con el servidor de datos de la cooperativa. Además, el proveedor de servicios de internet de la organización es Telconet, quien les suministra una conexión de fibra óptica monomodo de 6 hilos, brindando así un servicio de internet de alta velocidad y calidad.

Figura 6

Topología física de red de la COAC Mercedes Cadena LTDA.



Nota. Imagen realizada por el autor e ilustrando la idea del departamento de procesos de la COAC Mercedes Cadena LTDA.

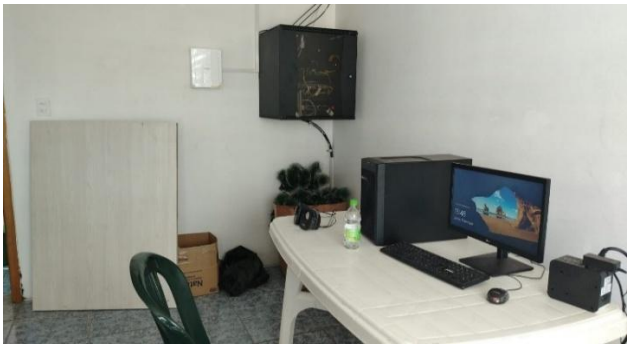
La estructura de red y el cableado han estado en funcionamiento por un breve período, desde su reciente reubicación el domingo 5 de mayo de 2024. Este nuevo diseño de red se implementó con el objetivo de adaptarse a las nuevas instalaciones de la cooperativa y asegurar una conectividad óptima para todos los dispositivos y sistemas que forman parte de su infraestructura tecnológica.

3.1.5.2 Cuarto de telecomunicaciones.

El cuarto de telecomunicaciones se encuentra ubicado en el tercer piso del edificio, el cual alberga las áreas de Marketing y Servidores. En este espacio, el servidor principal, que es una máquina Dell PowerEdge T150, está instalado directamente en el cuarto. Sin embargo, sus complementos como el firewall, el switch principal de conmutación y el almacenamiento de video, se encuentran en un gabinete separado con su respectivo sistema de refrigeración y medidas de seguridad adecuadas.

Figura 7

Cuarto de telecomunicaciones.



Nota. Imagen adquirida del departamento de procesos de la COAC Mercedes Cadena LTDA.

Es importante señalar que el cuarto de telecomunicaciones tiene una ventana que da hacia la calle, lo cual no es una práctica recomendada en salas de servidores o centros de procesamiento de datos. Esta ventana permite la visibilidad desde el exterior hacia el interior del cuarto, lo que podría comprometer la seguridad y privacidad de la información y los equipos allí resguardados. Se recomienda que las salas de datos no tengan ventanas o, en su defecto, que estas sean opacas y selladas herméticamente para evitar cualquier tipo de acceso no autorizado o visual al interior del recinto.

Figura 8

Cuarto de telecomunicaciones con vista la ventana.

Nota. Imagen adquirida del departamento de procesos de la COAC Mercedes Cadena LTDA.

3.1.5.3 Direccionamiento.

Para el direccionamiento IP del edificio, se valida que tiene implementado una subred de clase C, específicamente la 192.168.x.x, con una máscara de red 255.255.255.0. Esta red se distribuye a todas las máquinas y dispositivos conectados en las instalaciones. Cada computadora utilizada por los empleados recibe una dirección IP estática dentro de esta subred, lo que permite

su conexión a través de los puntos de red ubicados en los diferentes pisos del edificio. Esto garantiza una identificación y acceso individualizados para cada equipo, facilitando la administración y el control de la red interna de la organización.

3.1.5.4 Activos de hardware en la COAC Mercedes Cadena.

A continuación, se detalla la distribución de hardware del edificio de la COAC Mercedes Cadena, que incluye equipos clave como estaciones de trabajo, conexiones de red y dispositivos de seguridad entre otros. Estos activos han sido seleccionados para optimizar la eficiencia operativa y asegurar una conectividad fiable, apoyando así las operaciones diarias de la cooperativa.

Tabla 5

Elementos activos de hardware en la estructura tecnología de la COAC Mercedes Cadena.

Elemento	Cantidad	Imagen	Gestión sobre el equipo
Maquinas personales	13		Si
Switch de conmutación no administrable	3		Si
Router CISCO C921-AP con capacidades de firewall integradas	1		No

Almacenamiento de video vigilancia	1		Si
Cámaras de vigilancia	4		Si
Seridor powershell Dell PowerEdge T150	1		Si
Switch tp-link TL-SG1024D no administrable	1		Si
Router tp-link inalámbrico	1		Si

Nota. Adquirido por el departamento de procesos de la COAC Mercedes Cadena LTDA.

De esta manera, la cooperativa ha distribuido estratégicamente los recursos de hardware en cada uno de los pisos como se observa en la Figura 5, asignando las máquinas de uso personal necesarias para cubrir las necesidades de las diferentes áreas y departamentos que conforman su estructura organizacional.

3.1.5.5 Activos de software en la COAC Mercedes Cadena.

A continuación, se describen los sistemas operativos, softwares y aplicaciones financieras empleados por la COAC Mercedes Cadena, junto con un breve comentario sobre su uso y funcionalidad. Esta explicación abarca tanto las plataformas tecnológicas de base como las herramientas específicas utilizadas para gestionar diversas operaciones financieras, administrativas y de atención al cliente.

Tabla 6

Elementos activos de software en la estructura tecnología de la COAC Mercedes Cadena.

Software	Imagen	Descripción	Tipo de licencia	Gestión sobre el software
Sistema operativo Windows 10		El sistema operativo de Windows 10, tiene una buena acogida por medio de los empleados debido a su amigable y fácil uso, además de ser compatible con todos los Softwares administrativos que utiliza la institución.	Licencia por Volumen	Si
WinSPC		Es un software estadístico de control de procesos (SPC) diseñado para el análisis y monitoreo de la calidad en procesos de manufactura y producción.	Licencia Comercial	Si
LogMein HAMACHI		Dentro de la institución la aplicación de servidor de base de datos LogMein HAMACHI se utiliza para establecer una conexión segura y remota a una base	Licencia Freemium (con opción a premium)	Si

		de datos desde cualquier ubicación por medio de una red privada virtual (VPN).		
Putty		Es un cliente de terminal remoto gratuito y de código abierto que permite establecer conexiones seguras (SSH y Telnet) a sistemas remotos desde una computadora local.	Licencia Open Source	Si
AFC.2023		Este software permite realizar las transacciones bancarias dentro de la COAC Mercedes Cadena. Es proporcionado por una empresa exterior llamada SITETRIOR, que ofrece el sistema de administración financiera para la institución.	Licencia Comercial	Si
MySQL		Es un sistema de gestión de bases de datos relacionales (RDBMS) de código abierto y multiplataforma. MySQL se lo utiliza para almacenar, organizar y recuperar datos de manera eficiente en la institución.	Licencia Dual (GPL y Comercial)	Si

Nota. Adquirido por el departamento de procesos de la COAC Mercedes Cadena LTDA.

Estos softwares complementarios brindan a la empresa herramientas adicionales para el control de calidad, la creación de redes privadas virtuales, la gestión remota de sistemas, el manejo de bases de datos y la administración financiera de la empresa, respectivamente. Cada uno de ellos desempeña un papel importante en áreas específicas de las operaciones de la empresa.

3.1.5.6 Conectividad a internet.

La conectividad a Internet en el edificio de la cooperativa es proporcionada por el proveedor de servicios TELCONET. Su proveedor les proporciona un router CORE con características de firewall integrado de la marca CISCO modelo C921-4P, cuya gestión del dispositivo es realizada únicamente por parte de su proveedor de servicios de internet (ISP). Este dispositivo es conocido por su alto rendimiento y seguridad ya que es ideal para entornos empresariales que requieren una conectividad confiable y protección contra amenazas externas claro que su gestión no está dado por parte de la organización.

El router CORE CISCO C921-4P actúa como puerta de enlace entre la red interna del edificio y la conexión de salida a Internet de la misma, ya que, además, gracias a su firewall incorporado, da una capa adicional de seguridad que monitorea y filtra el tráfico de entrada y de salida protegiendo así la red y los dispositivos conectados contra posibles ataques y amenazas futuras.

Figura 9

Router CORE CISCO C921-4P.

Nota. Imagen adquirida del departamento de procesos de la COAC Mercedes Cadena LTDA.

Todo este servicio de conectividad a Internet está respaldado por un enlace de fibra óptica de alta velocidad, con una capacidad de 1000 Mbps (aproximadamente 1 Gbps). Este ancho de banda robusto garantiza una conexión a Internet rápida y confiable, capaz de soportar las demandas de toda la infraestructura tecnológica del edificio, incluyendo aplicaciones, servidores y el tráfico de datos generado por los usuarios.

3.1.5.7 Tipo de información que maneja la COAC Mercedes Cadena.

La cooperativa maneja diferentes tipos de información, cada una con un nivel de clasificación específico, esto se determinó de acuerdo con el **ANEXO C** que conforma el levantamiento de información. Sin embargo, tomando en cuenta que no consta inicialmente con un modelo referencial de organización o categorización de información, se aplica a continuación un modelo de clasificación de información adaptado a las necesidades de la organización.

Tabla 7

Modelo de clasificación de datos de la COAC Mercedes Cadena.

Característica	Descripción
Público	• Información general sobre los servicios y productos ofrecidos por la cooperativa. • Materiales de marketing y publicidad. • Comunicados de prensa y noticias relacionadas con la organización. • Información de contacto básica de la cooperativa.
Sensible	• Información interna principalmente del departamento de procesos y negocios. • Datos personales de clientes/socios. • Registros de auditorías y cumplimientos.
Privada	• Datos personales de empleados. • Documentos internos de planificación estratégicas enfocadas a futuro.

	• Información financiera interna (Transacciones bancarias internas).
Confidencial	• Información de clientes (Detalles transaccional de los clientes/socios). • Contraseñas y credenciales de acceso. • Acuerdos y contratos legales con empleados y clientes/socios.

Nota. Adquirido por el departamento de procesos de la COAC Mercedes Cadena LTDA.

Esta información es de carácter personal y está protegida por las leyes de privacidad correspondientes. Su manejo y acceso están restringidos únicamente al personal autorizado y se implementan medidas de seguridad adicionales para salvaguardar la privacidad de los empleados. Es fundamental que la Cooperativa implemente políticas y procedimientos claros para el manejo adecuado de cada tipo de información que esta controla, asegurando la protección de los datos confidenciales, privados y sensibles al igual que el cumplimiento de las regulaciones aplicables.

3.2 Análisis de riesgos de la COAC Mercedes Cadena.

Esta sección presenta una evaluación detallada de los riesgos asociados de los activos de software y hardware de la Cooperativa de Ahorro y Crédito Mercedes Cadena, este análisis sigue la guía metodológica de la NIST SP 800-30 y aplicando conceptos de MAGERIT. Este análisis permite en la identificación de amenazas y vulnerabilidades que evalúan su impacto, probabilidad y nivel de riesgo que permitirán priorizar acciones de mitigación dentro de la institución.

3.2.1 Identificación y justificación de amenazas y vulnerabilidades.

Identificar y comprender las amenazas y vulnerabilidades es crucial para proteger los activos de información de la red interna de la COAC Mercedes Cadena. En este análisis, se han

considerado las siguientes fuentes de amenazas y vulnerabilidades que han sido extraídas del levantamiento de información del **ANEXO C**.

Tabla 8

Modelo de clasificación de amenazas/vulnerabilidades de la COAC Mercedes Cadena.

Amenazas/Vulnerabilidades	Descripción	Justificación
Ciberataques	Incluyen malware, ransomware y ataques de denegación de servicio (DDoS).	Basados en tendencias globales y reportes de la industria financiera el departamento de procesos indica que los ciberataques son una amenaza constante para la integridad y disponibilidad de los sistemas de información.
Errores humanos	Configuraciones incorrectas, eliminación accidental de datos, desactualización, falta de mantenimiento de equipos o contraseñas debiles.	Según el departamento de procesos los errores humanos son inevitables y pueden conducir a incidentes de seguridad, especialmente cuando las medidas de control no son adecuadas.
Fallas técnicas	Fallos de hardware/software y cortes de energía.	El departamento de procesos indica que las fallas técnicas, que son más frecuentes, pueden causar interrupciones significativas en las operaciones críticas.
Desastres naturales	Incendios, inundaciones, terremotos.	Aunque son menos probables, los desastres naturales deben considerarse en la planificación de continuidad de negocio.

Nota. Adquirido y evaluado por el departamento de procesos de la COAC Mercedes Cadena LTDA.

3.2.2 Evaluación cuantitativa de riesgos.

El nivel de riesgo se calcula aplicando una fórmula sencilla que combina el impacto y la probabilidad, lo que ayuda a obtener un valor claro que muestra qué tan crítico es cada activo frente a posibles amenazas. Este enfoque, que se utiliza en metodologías conocidas como la guía NIST SP 800-30 y el marco MAGERIT, ofrece una forma organizada de evaluar los riesgos. Ambas metodologías tienen el mismo propósito: identificar, priorizar y reducir riesgos, ajustándose a las necesidades y realidades de cada organización.

3.2.2.1 Explicación matemática del Nivel de Riesgo.

La ecuación para calcular el nivel de riesgo se fundamenta en dos valores clave que son el impacto y la probabilidad del riesgo. Estos dos elementos se combinan para generar un resultado que permite clasificar el nivel de riesgo de manera clara y cuantitativa. A continuación, se explicará qué significa cada término y cómo se relacionan de acuerdo con la siguiente ecuación:

$$NR = Impacto \times Probabilidad \qquad (I)$$

- ***Nivel de Riesgo (NR):*** Este es el producto entre el impacto y la probabilidad de que ocurrencia. Si el resultado de un NR es alto, esta indica una mayor amenaza para la organización.
- ***Impacto:*** Evaluado en una escala de 1 a 5, donde 5 es un impacto severo en las operaciones de la cooperativa.
- ***Probabilidad:*** Evaluado en una escala de 1 a 5, donde 5 es una alta probabilidad de ocurrencia dentro de un sistema.

El producto entre estas dos variables genera un valor cuantitativo que varía entre 1 y 25, lo cual esto permite clasificar el riesgo de cada activo o amenaza según su criticidad, siendo 25 el nivel más alto.

3.2.2.2 Explicación matemática del Porcentaje del Nivel de Riesgo.

El Porcentaje del Nivel de Riesgo facilita una mejor comprensión de forma clara y uniforme al nivel de riesgo de cada activo dentro de la institución. Esta medida permite visualizar a cada activo como se posiciona en términos de riesgo en una escala estándar. Para calcularlo, se divide el nivel de riesgo obtenido entre el valor máximo posible (25) y luego se multiplica por 100, lo que ayuda a comparar el nivel de riesgo de diferentes amenazas de manera sencilla y consistente. La ecuación que lo representa es:

$$PNR = \left(\frac{Nivel\ de\ riesgo}{25}\right) \times 100 \qquad (II)$$

- **Porcentaje de nivel de riesgo (PNR):** Resultado que indica qué tan alto es un riesgo en comparación con el máximo posible. Se calcula dividiendo el NR entre 25 y multiplicando por 100, facilitando su comparación.
- **Nivel de riesgo (NR):** Resultado obtenido de la ecuación (I) anterior.
- **25:** Es el valor máximo posible del nivel de riesgo, que corresponde al caso extremo en el que tanto el impacto como la probabilidad tienen un valor de 5.
- **100:** Factor de conversión para expresar el resultado como un porcentaje.

La ecuación (II) priorizar los riesgos al identificar aquellos que requieren atención inmediata en contraste con los que pueden ser gestionados con controles menos intensivos.

3.2.2.3 Descripción de niveles de probabilidad e impacto para el análisis de riesgos.

En cambio, para el análisis y familiarizarlo con el nivel de riesgo de cada activo, es crucial determinar tanto la probabilidad de que una amenaza se materialice como el impacto que dicha amenaza podría tener sobre los activos de la organización. A continuación, se presentan las tablas utilizadas para evaluar la probabilidad y el impacto de las amenazas identificadas en el análisis de riesgos.

Tabla 9

Descripción de los niveles de probabilidad en el análisis de riesgos.

Cualitativo	Cuantitativo	Descripción
Muy probable	1	Ocurre en casos excepcionales
Improbable	2	Poco probable, pero podría ocurrir en algún momento
Posible	3	Moderadamente probable, podría ocurrir de vez en cuando
Probable	4	Probable, ocurrirá en varias ocasiones
Muy probable	5	Muy probable, ocurrirá en la mayoría de las ocasiones.

Nota. Los valores en la tabla representan los niveles de probabilidad que se utilizan para calcular el riesgo.

Tabla 10

Descripción de los niveles de impacto en el análisis de riesgos.

Cualitativo	Cuantitativo	Descripción
Insignificante	1	Consecuencias mínimas, sin impacto significativo.
Menor	2	Consecuencias menores, poco impacto en la operación.
Moderado	3	Impacto notable, pero manejable sin intervención externa.
Mayor	4	Impacto severo, requiere intervención significativa.
Catastrófico	5	Impacto crítico, amenaza la continuidad de la operación.

Nota. Los valores en la tabla representan los niveles de impacto que se utilizan para calcular el riesgo.

Las tablas anteriores presentan las escalas utilizadas para medir la probabilidad y el impacto de las amenazas, donde la Tabla 9 abarca cinco niveles de probabilidad, desde "Muy Improbable" hasta "Muy Probable", permitiendo cuantificar la frecuencia esperada de ocurrencia, adicional que la Tabla 10 categoriza el impacto en niveles que van desde "Insignificante" hasta "Catastrófico", lo que es esencial para evaluar el daño que una amenaza podría causar a la COAC Mercedes Cadena.

3.2.2.4 Matriz de evaluación de riesgos en función del impacto y la probabilidad.

La siguiente matriz fue utilizada para calcular los niveles de riesgo en función de las evaluaciones de impacto y probabilidad que será utilizada para dar un valor de nivel de riesgo a cada activo de la COAC Mercedes Cadena:

Tabla 11

Matriz de Evaluación de Riesgos en Función del Impacto y la Probabilidad con su porcentaje de nivel de riesgo.

Impacto / **Probabilidad**	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Muy improbable (1)	(4%) 1	(8%) 2	(12%) 3	(16%) 4	(20%) 5
Improbable (2)	(8%) 2	(16%) 4	(24%) 6	(32%) 8	(40%) 10
Posible (3)	(12%) 3	(24%) 6	(36%) 9	(48%) 12	(60%) 15
Probable (4)	(16%) 4	(32%) 8	(48%) 12	(64%) 16	(80%) 20
Muy probable (5)	(20%) 5	(40%) 10	(60%) 15	(80%) 20	(100%) 25

Nota. Los valores de la tabla representan el nivel de riesgo calculado al multiplicar la probabilidad por el impacto y en adicional su porcentaje del nivel del riesgo.

Esta matriz fue aplicada para evaluar los riesgos de cada activo, proporcionando una base clara y estructurada para la priorización y mitigación de los riesgos identificados en los activos identificados de la COAC Mercedes Cadena.

En donde de una forma más sencilla se puede expresar como su nivel de riesgo está relacionado con su porcentaje en la siguiente tabla.

Tabla 12

Clasificación del Nivel de Riesgo Según Impacto y Porcentaje de Probabilidad.

Impacto	Clasificación del Riesgo	Rango de porcentaje
1 – 5	Muy bajo	1% a 20%
6 – 10	Bajo	21% a 40%
11 – 15	Moderado	41% a 60%
16 – 20	Alto	61% a 80%
21 – 25	Muy alto	81% a 100%

Nota. Los valores de la tabla representan el nivel de riesgo calculado al multiplicar la probabilidad por el impacto y en adicional su porcentaje del nivel del riesgo con su respectiva clasificación.

3.2.2.5 Evaluación de riesgos de la COAC Mercedes Cadena en función del impacto y la probabilidad.

La Tabla 13 presenta la evaluación cuantitativa de riesgos de los activos de la COAC Mercedes Cadena, detallando su nivel de valor y el porcentaje de riesgo asociado, calculados según la metodología descrita en el subtema 3.2.2. Además, este análisis se complementa con la valoración de impacto y probabilidad realizada en el **ANEXO D**, donde se evaluaron los riesgos de cada activo de la institución, donde en conjunto, se destacan como activos críticos el Servidor Dell PowerEdge T150, el Switch TP-Link TL-SG1024D, PuTTY y MySQL. Estos resultados resaltan la urgencia de priorizar la implementación de medidas de mitigación, especialmente en las áreas con vulnerabilidades más significativas.

Tabla 13

Tabla de amenazas y vulnerabilidades y evaluación cuantitativa de riegos de cada activo de la COAC Mercedes Cadena.

Activo	Tipo de activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
Maquinas personales	Hardware	Malware	Sin antivirus	4	3	12 (48%)
Switch de Conmutación no administrable	Hardware	Fallo de hardware	Falta de inspecciones	3	4	12 (48%)
Almacenamiento de Video Vigilancia	Hardware	Pérdida de datos	Mala configuración de respaldos	3	3	9 (36%)
Cámaras de Vigilancia	Hardware	Fallo del equipo	Falta de mantenimiento	4	1	4 (16%)
Servidor Dell PowerEdge T150	Hardware	Fallo de hardware	Falta de redundancia	5	4	20 (80%)
Switch TP-Link TL-SG1024D	Hardware	Fallo de hardware	Sin configuración redundante	4	4	16 (64%)
Router TP-Link Inalámbrico	Hardware	Interrupción de red	Firmware desactualizado	3	1	3 (12%)
S.O. Windows 10	Software	Vulnerabilidades de seguridad	Software desactualizado	4	3	12 (48%)
WinSPC	Software	Interrupción del Sistema	Falta de monitoreo de rendimiento	4	4	16 (64%)
LogMeIn Hamachi	Software	Acceso no autorizado	Configuración VPN insegura	5	4	20 (80%)
PuTTY	Software	Acceso no autorizado	Contraseñas débiles	5	4	20 (80%)

AFC.2023	Software	Acceso no autorizado	Contraseñas débiles	5	5	25 (100%)
MySQL	Software	Pérdida de datos	Sin respaldos	5	5	25 (100%)

Nota. Esta tabla fue creada por el autor para ilustrar la evaluación cuantitativa de los activos que son administrables por la COAC Mercedes Cadena y su respectivo nivel de riesgo.

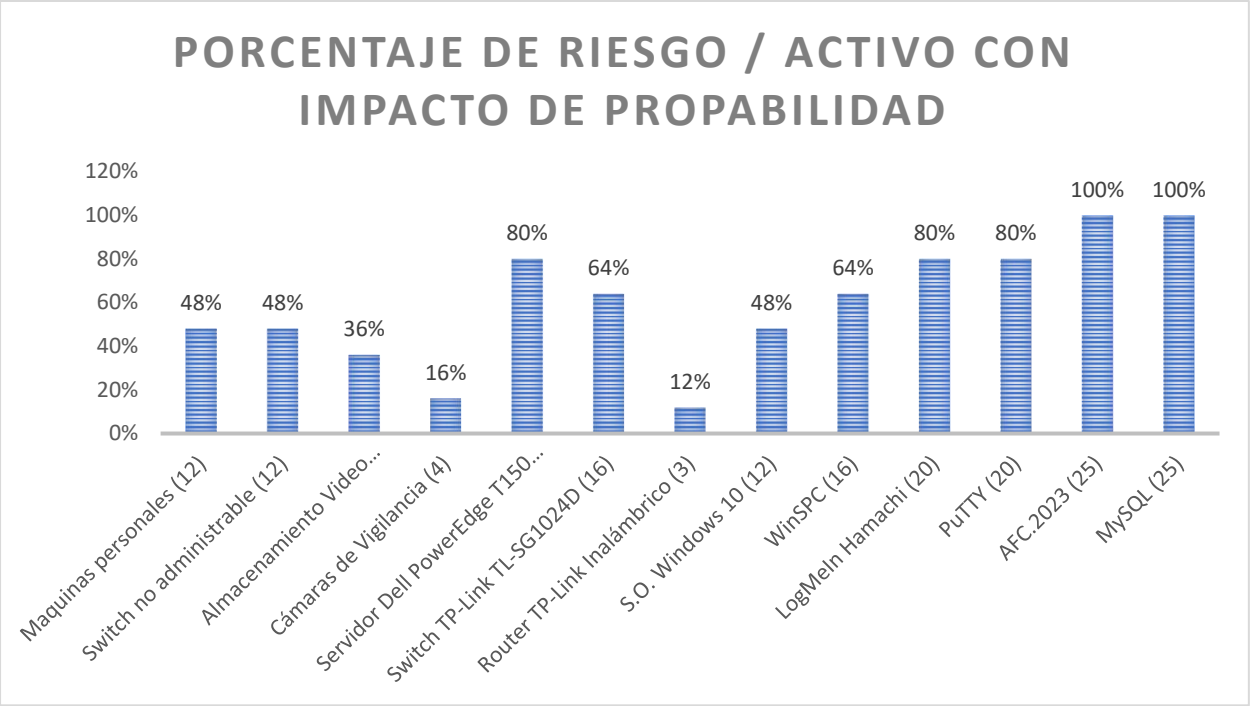
Además, la Tabla 13 sobre amenazas y vulnerabilidades refleja un nivel y porcentaje de riesgo muy significativo para cada activo de la COAC Mercedes Cadena, estos resultados proporciona una visión que resalta las áreas clave que requieren atención, justificando prioridades en la gestión de riesgos dentro de la cooperativa. Cada valor mostrado está directamente relacionado con las tablas anteriores, que son la Tabla 11 y la Tabla 12, las cuales complementan los datos del **ANEXO D** y la Tabla 13 al detallar los riesgos específicos y sus respectivas valoraciones de cada activo de la institución.

3.2.3 Análisis de riesgo.

El análisis detalla que cada activo está evaluando las amenazas específicas asociadas con ellos, tal como se documenta en el **ANEXO D**. Se ha analizado tanto el impacto como la probabilidad de ocurrencia de cada amenaza, siguiendo así un enfoque coherente con la guía metodológica de la NIST SP 800-30 y la metodología MAGERIT. Dado que este enfoque respalda que cada activo sea gestionado de manera adecuada tomando en cuenta su nivel de criticidad y vulnerabilidad puesto que la gráfica que sigue a continuación indica el nivel de riesgo asociado con cada activo de acuerdo con un rango de porcentaje.

Tabla 14

Grafica de nivel y porcentaje de riesgo asociado a cada activo de la COAC Mercedes Cadena.



Nota. Esta grafica fue creada por el autor para ilustrar el nivel y porcentaje de riesgo asociado a cada activo que es administrable por la COAC Mercedes Cadena.

Los activos con nivel de riesgo alto y muy alto (25) tal como se indica en la Tabla 14, incluyen al servidor Dell, el software de gestión financiera AFC.2023 y MySQL. Estos requieren medidas de seguridad adicionales y monitoreo constante. Por lo que se recomienda realizar evaluaciones de riesgos periódicas y actualizar las medidas de seguridad para mantener los riesgos en un nivel aceptable, acorde con los principios de MAGERIT.

Capítulo IV

Desarrollo del plan integral de ciberseguridad para la COAC Mercedes Cadena.

Este capítulo desarrolla un plan integral de ciberseguridad diseñado para mitigar los riesgos identificados en los activos con niveles de riesgo mayor o igual al 48%, según el análisis del capítulo anterior (Capitulo III). Dicho plan se fundamenta en la metodología NIST SP 800-30 y busca implementar medidas de mitigación efectivas, adaptadas a las necesidades específicas de cada activo crítico en función de la institución.

4.1 Identificación de activos críticos.

Como resultado del análisis de riesgos realizado en el Capítulo III, se identificaron los activos críticos de la Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda. con un nivel de riesgo igual o superior al 48%. Estos activos representan elementos esenciales en la infraestructura tecnológica de la organización, cuya afectación podría comprometer la disponibilidad, integridad o confidencialidad de los sistemas según el triángulo CIA de la seguridad informática. A continuación, se presentan los activos priorizados (≥ 48%) basados en la Tabla 15:

Tabla 15

Tabla de identificación de activos con una probabilidad (≥ 48%) de riesgo de la COAC Mercedes Cadena.

Activo	Riesgo
Maquinas personales	12 (48%)
Switch de Conmutación no administrable	12 (48%)

S.O. Windows 10	12 (48%)
Switch TP-Link TL-SG1024D	16 (64%)
WinSPC	16 (64%)
Servidor Dell PowerEdge T150	20 (80%)
LogMeIn Hamachi	20 (80%)
PuTTY	20 (80%)
AFC.2023	25 (100%)
MySQL	25 (100%)

Nota. Esta tabla fue creada por el autor para ilustrar los activos con alto porcentaje de riesgo de COAC Mercedes Cadena.

Todos estos activos serán considerados prioridad para el desarrollo del plan integral de ciberseguridad de la COAC Mercedes Cadena, debido a su nivel de impacto en las operaciones mismas dentro de la institución, así como también la necesidad de establecer medidas correctivas para minimizar los niveles riesgos identificados dentro de la institución.

4.2 Desarrollo del plan integral de ciberseguridad para la COAC Mercedes Cadena

En esta sección el plan propuesto se fundamenta en la metodología NIST SP 800-30, que proporciona un marco de mitigación en contra de las amenazas y vulnerabilidades para la gestión de riesgos de ciberseguridad. En este contexto, se plantean controles técnicos, administrativos y operativos dirigidos a fortalecer la seguridad de los activos más vulnerables. Además, se presentan reportes de cumplimiento con la metodología NIST SP 800-30, estrategias de mitigación específicas, y una guía de políticas y procedimientos que aseguren la implementación efectiva del mismo, dato que este enfoque integral busca garantizar la protección de los sistemas de información y la continuidad operativa de la cooperativa frente a amenazas actuales y futuras dentro de la institución.

4.2.1 Reporte de cumplimiento de la NIST SP 800-30.

En la Sección 3.2.2.5 del proyecto se presenta un análisis detallado del grado de cumplimiento de la COAC Mercedes Cadena con respecto a los lineamientos establecidos en la metodología NIST SP 800-30. A partir de la evaluación realizada en el capítulo anterior (Capitulo III), se identificaron activos con un riesgo elevado (≥ 48%), como el Servidor Dell PowerEdge T150, MySQL, y LogMeIn Hamachi que son la base de los elementos que tienen un nivel riesgo a considerar, entre otros. Este reporte no solo evidencia los riesgos y vulnerabilidades asociadas a estos activos, sino que también establece los principales vacíos de cumplimiento en las áreas de evaluación de riesgos, gestión de vulnerabilidades y respuesta a incidentes, proporcionando una base para priorizar las medidas correctivas necesarias además de la sección más importante de la institución al no contar con un departamento dedicado a la tecnología de la información,

4.2.2 Plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.

El plan integral de ciberseguridad propuesto se basa en la metodología NIST SP 800-30 y tiene como objetivo mitigar los riesgos identificados en los activos críticos con un nivel de riesgo mayor o igual al 48%. Este plan prioriza la implementación de controles específicos, como la instalación de antivirus en las máquinas personales, la configuración adecuada de contraseñas en PuTTY y AFC.2023, y la mejora de la redundancia en el Servidor Dell PowerEdge T150. Además, se establecen medidas técnicas, como la actualización periódica de software en Windows 10 y MySQL, y controles administrativos, como políticas de acceso restringido para LogMeIn Hamachi, para garantizar la seguridad integral de la infraestructura, tal como se muestra a continuación.

PLAN INTEGRAL DE CIBERSEGURIDAD EN BASE A LA APLICACIÓN DE LA METODOLOGÍA DE LA NIST SP 800-30.

CACME
Cooperativa de Ahorro y Crédito

MARLON EMANUEL IPIALES JINGO

MITIGACIÓN DE RIESGOS Y VULNERABILIDADES

PLAN INTEGRAL DE CIBERSEGURIDAD EN BASE A LA APLICACIÓN DE LA METODOLOGÍA DE LA NIST SP 800-30.

Control de documentación.

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Sr. Marlon Ipiales	Ing. Anderson Bonilla	Ing. Marcelo Guamán
Cargo:	Tesista	Jefe de procesos	Gerente
Firma:			
Fecha:	6 de junio del 2025	12 de julio del 2025	

Ficha de edición del documento:

Nombre del documento	Plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.	
Código del documento	Código: PIC-NIST-01	
Edición	01	
Fecha de edición	6 de junio del 2025	
Responsable de Edición	Marlon Emanuel Ipiales Jingo	
Cargo	Tesista	
Cambios realizados	**Autor de Edición**	**Fechas de Ediciones**

Contenido.

1. Gestión de Plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.

La Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda enfrenta retos significativos en la protección de su infraestructura crítica conforme a cada uno de sus activos mas importantes esto debido al incremento de amenazas cibernéticas y vulnerabilidades tecnológicas. Este plan tiene como objetivo mitigar los riesgos identificados en activos críticos con un nivel de riesgo ≥ 48%, garantizando la continuidad operativa, la protección de la información y el cumplimiento normativo. Siendo este documento del dominio público que está disponible para cualquier persona interesada en conocer los estándares de control propuestos el procedimiento del plan integral de ciberseguridad.

1.1. Objetivo.

Implementar un plan integral de ciberseguridad basado en la metodología NIST SP 800-30, enfocado a reducir los niveles de riesgos de los activos críticos más importantes de la infraestructura critica mejorando así la fortaleza de la infraestructura tecnológica de la institución.

1.2. Alcance.

Este plan se centra en 10 activos críticos con un nivel de riesgo igual o superior al 48% dado que esto incluye elementos de hardware, software junto con sus sistemas esenciales que sustentan las operaciones de la institución, tomando en cuenta que su protección es clave para garantizar la continuidad operativa frente a amenazas y ataques cibernéticos.

1.3. Metodología.

Basado en la metodología NIST SP 800-30, este plan identifica y evalúa cada activo crítico, analizando amenazas y detectando vulnerabilidades para calcular los niveles de riesgo, tomando en cuenta que finalmente, se priorizan las acciones de mitigación mediante controles específicos, asegurando una gestión eficiente de los riesgos identificados.

2. Referencias normativas.

- NIST SP 800-30: Guía para la gestión de riesgos.
- ISO/IEC 27001: Sistema de gestión de seguridad de la información.
- Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador.

3. Términos y definiciones.

- Activo: Recursos técnicos o humanos necesarios para la operación.
- Amenaza: Evento potencial que puede dañar un activo.
- Vulnerabilidad: Debilidad que puede ser explotada por una amenaza.
- Riesgo: Combinación de la probabilidad de ocurrencia de un evento y su impacto.
- Control: Medida implementada para mitigar un riesgo.

4. Estructura del plan integral de ciberseguridad.

La estructura del presente plan integral de ciberseguridad considera de manera sistemática la identificación de activos críticos, las estrategias de mitigación para reducir los riesgos asociados y un cronograma detallado de implementación, dado que este enfoque garantiza que las medidas propuestas estén alineadas con las prioridades de la cooperativa y las mejores prácticas en ciberseguridad.

4.1. Identificación de activos críticos

Como se detalla en el proceso de identificación de activos e identificación de amenazas y vulnerabilidades calculado, se toma a consideración los activos que tiene un alto nivel de porcentaje de riesgo mayor o igual al 48% esto debido a la influencia que

tienen los activos dentro de la estructura critica de la topología interna de red que tienen la institución.

Tabla 1

Tabla de identificación de activos con una probabilidad (≥ 48%) de riesgo de la COAC Mercedes Cadena.

Activo	Riesgo
Maquinas personales	12 (48%)
Switch de Conmutación no administrable	12 (48%)
S.O. Windows 10	12 (48%)
Switch TP-Link TL-SG1024D	16 (64%)
WinSPC	16 (64%)
Servidor Dell PowerEdge T150	20 (80%)
LogMeIn Hamachi	20 (80%)
PuTTY	20 (80%)
AFC.2023	25 (100%)
MySQL	25 (100%)

Nota. Esta tabla fue creada por el autor para ilustrar los activos de alta prioridad.

4.2. Estrategias de mitigación de amenazas y vulnerabilidades.

CACME		
	Activo:	Maquinas personales
	Amenaza identificada:	Malware
	Vulnerabilidad identificada:	Sin antivirus
Descripción:	Nivel de riesgo:	12 – 48%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0001
	Versión:	1.0

Pol. 1. Todas las máquinas personales deben tener instalado un software antivirus actualizado, ya que este software debe ser capaz de detectar, bloquear y eliminar amenazas en tiempo real, con esta medida se reduce de manera significativa el riesgo de infecciones por malware, protegiendo así la integridad de los datos y garantizando la seguridad de los equipos contra virus.

Pol. 2. El antivirus debe configurarse para realizar escaneos periódicos de los equipos y actualizarse automáticamente su escaneo de base de datos de virus, asegurando que las máquinas estén protegidas contra las amenazas más recientes, manteniendo un nivel óptimo de seguridad en todo momento.

Pol. 3. Brindar sesiones de capacitación a los colaboradores para evitar el acceso a sitios web maliciosos y phishing infiltrados por correos, reforzando así la protección de sus equipos.

Pol. 4. El acceso a documentos críticos debe estar limitado mediante la asignación de permisos basados en roles. Esta medida garantiza la confidencialidad de la información y previene accesos no autorizados, protegiendo así los datos sensibles de la organización.

Pol. 5. Utilizar herramientas de monitoreo que detecten comportamientos inusuales en los equipos para responder rápidamente a incidentes.

Pol. 6. Implementar una aplicación de código abierto, para gestionar y proteger las contraseñas de la institución. Esta herramienta permitirá almacenarlas de forma segura, generar claves fuertes y limitar el acceso solo a usuarios autorizados, reduciendo así los riesgos de seguridad.

Pol. 7. Se debe implementar un departamento de TI encargado de brindar soporte técnico ante cualquier anomalía o problema que surja en los equipos además del departamento de seguridad de la información ya que ambos departamentos trabajan en conjunto, ya sea a nivel físico o lógico, dentro de la estructura de red. Este departamento garantizará una respuesta eficiente y oportuna para mantener la operatividad y la seguridad de los sistemas.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	Switch de Conmutación no administrable
	Amenaza identificada:	Fallo de hardware
	Vulnerabilidad identificada:	Falta de inspecciones
Descripción:	Nivel de riesgo:	12 – 48%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0002
	Versión:	1.0

Pol. 1. Realizar revisiones de forma periódica que permita validar el estado físico y funcional del equipo, dado que esto ayudará a identificar posibles fallos antes de que afecten las operaciones dentro de la institución tomando a consideración si es factible un cambio o mantenimiento.

Pol. 2. Capacitar a los colaboradores en las mejores prácticas de configuración y uso de los equipos en forma básica, ya que este entrenamiento garantiza un funcionamiento adecuado del equipo y reducirá los riesgos operativos asociados a un uso inadecuado.

Pol. 3. Aplicar la implementación de softwares de monitoreo para detectar problemas en tiempo real mejorando así el tiempo de respuesta ante incidentes brindando una estabilidad en la red interna de la organización.

Pol. 4. Es importante la disposición de switches adicionales como respaldo en caso de avería o fallo dentro de los equipos principales minimizando así interrupciones del proceso continuo evitando problemas a futuro.

Pol. 5. Considerar la adquisición de un switch administrable en Capa 3 que permita gestionar configuraciones avanzadas como políticas de QoS y mejoras en la seguridad de la red interna con distribución equilibrada.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	S.O. Windows 10
	Amenaza identificada:	Vulnerabilidades de seguridad
	Vulnerabilidad identificada:	Software desactualizado
Descripción:	Nivel de riesgo:	12 – 48%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0003
	Versión:	1.0

Pol. 1. Configurar el sistema operativo para recibir parches de seguridad y actualizaciones automáticamente de manera periódica, ya que de esta manera ayuda a mitigar vulnerabilidades que sean conocidas antes de que puedan ser explotadas por atacantes.

Pol. 2. Realizar evaluaciones regulares del sistema operativo para verificar que las configuraciones cumplan con las mejores prácticas de seguridad. Esto garantiza un entorno más protegido y confiable.

Pol. 3. Identificar y desactivar servicios o funcionalidades que no se utilicen. Esto previene que elementos innecesarios sean aprovechados como puntos de entrada por posibles atacantes.

Pol. 4. Habilitar y configurar los firewalls integrados del sistema operativo. Esto limita las conexiones no autorizadas entrantes y salientes, protegiendo al sistema de ataques externos.

Pol. 5. Establecer controles que restrinjan la instalación de software no autorizado. Con esta medida, se protege el entorno del sistema operativo contra aplicaciones malintencionadas o indeseadas.

Pol. 6. Tomar a consideración la migración y uso de sistemas operativos diferentes como los basados en Linux para el aprovechamiento de recursos en las maquinas, sobre todo para las maquinas más importantes como los servidores.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	Switch TP-Link TL-SG1024D
	Amenaza identificada:	Fallo de hardware
	Vulnerabilidad identificada:	Sin configuración redundante
Descripción:	Nivel de riesgo:	16 – 64%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0004
	Versión:	1.0

Pol. 1. Asegurar que el dispositivo esté optimizado y cumpla con las políticas de seguridad establecidas. Esto garantiza su correcto funcionamiento y protege contra posibles amenazas.

Pol. 2. Verificar que las configuraciones actuales del dispositivo sean consistentes con las necesidades operativas y de seguridad, ajustándolas si es necesario para mantener un entorno eficiente y seguro.

Pol. 3. Registrar todos los ajustes realizados en el dispositivo. Esto facilita la recuperación de configuraciones anteriores en caso de fallas o incidentes inesperados.

Pol. 4. Llevar un registro de los ajustes permite volver a configuraciones anteriores si ocurre algún problema.

Pol. 5.Dar uso al equipo para la aplicación de VLANs (Redes Locales Virtuales) ya que es una práctica esencial para mejorar la gestión, seguridad y rendimiento de una red. Las VLANs permiten segmentar una red física en múltiples redes lógicas, facilitando el control del tráfico de datos y mejorando la eficiencia en la comunicación interna.

Pol. 6. Planificar la sustitución del hardware antes de que alcance el final de su vida útil considerando uno de mejor capacidad, ya que esta acción garantizara la continuidad operativa y un buen rendimiento dentro su red evita interrupciones en los servicios.

Pol. 7. Al considerar la posibilidad de seguir utilizando los mismos equipos en lugar de optar por dispositivos mejorados con mayor capacidad de procesamiento y puertos de mejor rendimiento como los Gigabit Ethernet en lugar de Fast Ethernet, es importante tener en cuenta que los actuales presentan limitaciones tanto en desempeño como en tiempo de vida útil, es por ello que se recomienda la renovación progresiva de estos equipos por versiones más robustas, que garanticen la continuidad operativa y el crecimiento tecnológico de la institución.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	WinSPC
	Amenaza identificada:	Interrupción del Sistema
	Vulnerabilidad identificada:	Falta de monitoreo de rendimiento
Descripción:	Nivel de riesgo:	16 – 64%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0005
	Versión:	1.0

Pol. 1. El software debe estar actualizado con los ultimos parches para mantener la estabilidad del software ya que esta práctica es esencial para proteger el sistema contra vulnerabilidades y garantizar un rendimiento óptimo en sus funciones.

Pol. 2. Asignar permisos a los usuarios únicamente según sus funciones específicas, dado que esta medida minimiza los riesgos de accesos no autorizados y protege los recursos del sistema.

Pol. 3. Revisar de manera continua los registros de actividad del sistema permitiendo identificar comportamientos inusuales evitando asi problemas de seguridad y actuar a tiempo para mitigarlos.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	Servidor Dell PowerEdge T150
	Amenaza identificada:	Fallo de hardware
	Vulnerabilidad identificada:	Falta de redundancia
Descripción:	Nivel de riesgo:	20 – 80%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0006
	Versión:	1.0

Pol. 1. Proteger los datos utilizando sistemas de almacenamiento redundante que garantizara su disponibilidad incluso en caso de fallos del hardware.

Pol. 2. Emplear herramientas de monitoreo proactivo para detectar posibles problemas antes de que afecten la operación, permitiendo una gestión preventiva y efectiva de los equipos establecidos en la red de la organizacion.

Pol. 3. Seguir las recomendaciones del fabricante para el mantenimiento y uso del servidor, así como también el considerar el mejorar la sección de hardware del mismo, ya que esto asegura un rendimiento óptimo y prolonga la vida útil del equipo.

Pol. 4. Proveer energía constante al servidor mediante sistemas de respaldo, como UPS o generadores, para evitar interrupciones durante fallas eléctricas y garantizar la continuidad operativa.

Pol. 5. Tomar a consideración el cambio del sistema operativo a uno basado en Linux, con el objetivo de optimizar el rendimiento del equipo y aprovechar al máximo sus recursos. Los sistemas Linux ofrecen una mayor eficiencia y mejor seguridad, lo que puede traducirse en un funcionamiento más estable y confiable.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	LogMeIn Hamachi
	Amenaza identificada:	Acceso no autorizado
	Vulnerabilidad identificada:	Configuración VPN insegura
Descripción:	Nivel de riesgo:	20 – 80%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0007
	Versión:	1.0

Pol. 1. Exigir el uso de contraseñas complejas que sean difíciles de adivinar o descifrar, combinando letras, números y caracteres especiales para aumentar la seguridad.

Pol. 2. Monitorear continuamente el uso del servicio VPN para identificar accesos sospechosos o no autorizados y actuar de inmediato en caso de detectar irregularidades.

Pol. 3. Registrar y validar los dispositivos autorizados para conectarse a la VPN. Esto garantiza que solo equipos confiables puedan acceder al sistema.

Pol. 4. Reducir la superficie de ataque eliminando usuarios innecesarios o inactivos del sistema VPN. Esto limita los puntos de entrada potenciales para atacantes.

Pol. 5. Establecer un área gestión para seguridad de la información donde además que se informe al personal de TI sobre posibles ataques o intentos fallidos de autenticación, también esta área puede apoyar una respuesta rápida y efectiva.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	PuTTY
	Amenaza identificada:	Acceso no autorizado
	Vulnerabilidad identificada:	Contraseñas débiles
Descripción:	Nivel de riesgo:	20 – 80%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0008
	Versión:	1.0

Pol. 1. Limitar el uso de PuTTY exclusivamente a usuarios autorizados mediante la implementación de políticas claras que regulen su acceso y utilización.

Pol. 2. Utilizar claves criptográficas robustas para autenticar a los usuarios. Esto refuerza la seguridad y previene accesos no autorizados al sistema.

Pol. 3. Establecer y aplicar estándares de complejidad para las contraseñas asociadas al uso de PuTTY, garantizando que sean lo suficientemente seguras para resistir intentos de ataque.

Pol. 4. Restringir las conexiones remotas realizadas con PuTTY únicamente al personal autorizado. Esto minimiza el riesgo de accesos no deseados o potencialmente dañinos.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	AFC.2023
	Amenaza identificada:	Acceso no autorizado
	Vulnerabilidad identificada:	Contraseñas débiles
Descripción:	Nivel de riesgo:	25 – 100%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0009
	Versión:	1.0

Pol. 1. Configurar contraseñas robustas que cumplan con estándares de complejidad, incluyan caracteres variados y se renueven de forma periódica. Esto refuerza la seguridad de las credenciales y dificulta su vulneración.

Pol. 2. Realizar auditorías regulares del uso del sistema. Monitorear las acciones realizadas en la plataforma ayuda a identificar usos indebidos y a mantener un control adecuado de las actividades.

Pol. 3. Implementar políticas de actualización y mantenimiento del software, ya que mantener el sistema actualizado con las últimas versiones reduce vulnerabilidades.

Pol. 4. Monitorear los registros del sistema para detectar actividades sospechosas ya que esto es una práctica que permite identificar patrones y actuar anticipadamente ante posibles amenazas y riesgos.

Pol. 5. Establecer controles de acceso basados en roles asegurara que cada usuario solo tenga permisos para las funciones necesarias según su perfil ya que esto limita el riesgo de accesos no autorizados.

Pol. 6. Instalar aplicaciones de código abierto a cada colaborador para gestionar y proteger las contraseñas de acceso a la institución, permitiendo así almacenar las contraseñas de forma segura y generar claves fuertes.

CACME		
CACME Cooperativa de Ahorro y Crédito	Activo:	MySQL
	Amenaza identificada:	Pérdida de datos
	Vulnerabilidad identificada:	Sin respaldos
Descripción:	Nivel de riesgo:	25 – 100%
	Elaborado por: Fecha:	Ing. Fabián Cuzme y Sr. Marlon Ipiales Junio/2025
	Revisado por: Fecha:	Jefe de procesos Julio/2025
	Aprobado por:	
	Código:	POL-0010
	Versión:	1.0

Pol. 1. Configurar backups automáticos mediante programación de copias de seguridad regulares. Esto garantiza la disponibilidad y recuperación de los datos en caso de pérdida o incidente.

Pol. 2. Aplicar la limitación los accesos de los usuarios para que únicamente tengan permisos estrictamente necesarios según sus funciones, ya que esto minimiza riesgos de accesos indebidos.

Pol. 3. Al utiliza un servidor web para visualizar transacciones con datos privados o brindar servicios, es importante implementar medidas de seguridad adecuadas, como el uso de puertos seguros, así como el puerto 443 junto con el uso de certificados SSL y protocolos como HTTPS, ya que esto ayuda a proteger la información y garantiza una navegación más segura para los usuarios.

Pol. 4. Implementar cifrado robusto para proteger los datos sensibles almacenados en la base de datos. Esto asegura la confidencialidad de la información crítica frente a accesos no autorizados.

Pol. 5. Realizar auditorías de seguridad periódicas en los esquemas y configuraciones de la base de datos. Esto permite validar su integridad, identificar posibles fallos y fortalecer la protección de los datos.

4.3. Priorización y cronograma de implementación.

La priorización y el cronograma de implementación son esenciales para garantizar que las estrategias de mitigación se lleven a cabo de manera estructurada y eficiente. Este apartado organiza las actividades en etapas progresivas, asignando tiempos y recursos específicos a cada acción con base en la criticidad de los activos y la facilidad de implementación. De esta forma, se asegura un uso óptimo de los recursos y una reducción efectiva de los riesgos prioritarios.

4.3.1. Criterios de priorización.

La priorización se basa en los siguientes termino debido a que cada nivel de riesgo de los activos identificados influye en su tiempo de implementación y esta no debe afectar su estatus de operación, por consiguiente, su priorización se basa en:

Tabla 2

Tabla de criterios de priorización.

Criterio	Descripción
Nivel de riesgo	Mayor porcentaje de riesgo, como en el caso de MySQL (100%), PuTTY (80%) y el Servidor Dell PowerEdge T150 (80%), que son los activos más vulnerables.
Impacto operacional	Activos esenciales para garantizar la continuidad de los servicios de la cooperativa, como el Switch de Comunicación no administrable y el S.O.

	Windows 10, que soportan la infraestructura de red y los sistemas operativos.
Facilidad de implementación	Acciones que pueden realizarse rápidamente y con recursos mínimos, como la configuración de antivirus en Máquinas personales (48%) y las auditorías de seguridad iniciales en WinSPC (64%).

Nota. Esta tabla fue creada por el autor para ilustrar los criterios de priorización para su respectivo cronograma de implementación.

Estos criterios permiten un enfoque estratégico y eficiente para mitigar los riesgos más críticos y gestionarlos para la implementación dentro de un tiempo respectivamente prudente.

4.3.2. Cronograma.

Este cronograma asegura que los recursos sean utilizados eficientemente, comenzando por los activos más críticos y finalizando con una evaluación completa de las medidas aplicadas.

Tabla 3

Cronograma de implementación.

Fase	Objetivo principal	Activos afectados	Detalle de implementación
Inmediata (1 - 2 Mes)	Acciones críticas y urgentes	- Máquinas personales - S.O. Windows 10 - AFC.2023 - MySQL	- Configuración de antivirus. - Activación de actualizaciones automáticas. - Implementación de software de gestión de contraseñas de código abierto. - Restricción de instalación de software no autorizado.
Corto plazo (2 - 3 Mes)	Mitigación de riesgos intermedio	- Switch TP-Link TL - SG1024D, LogMeIn - Hamachi, Servidor Dell - PowerEdge T150 - PuTTY	- Auditorías de configuración. - Configuración de autenticación basadas en claves seguras. - Configuración de redundancia de UPS
Mediano plazo (3 - 4 Mes)	Mitigación de riesgos bajos	- Switch TP-Link TL-SG1024D - LogMeIn Hamachi - Servidor Dell PowerEdge T150 - WinSPC - AFC.2023	- Auditorías de configuración. - Auditoría se seguridad periódica en softwares administrativos (WinSPC, AFC.2023). - Configuración de redundancia de UPS.
Largo plazo (4 - 5 Mes)	Consolidación y pruebas	- WinSPC - PuTTY - AFC.2023 - MySQL	- Configuración de políticas de acceso. - Pruebas de restauración de datos.
Evaluación (6 Mes)	Monitoreo y mejora continua	- Todos los activos	- Monitoreo continuo de medidas implementadas. - Capacitación y auditorías integrales.

Nota. Esta tabla fue creada por el autor para ilustrar los tiempos de implementación de acuerdo con su criterio de priorización.

El presente cronograma establece en el plan una estrategia integral para abordar las vulnerabilidades y amenazas de los activos críticos de la cooperativa junto con su respectiva implementación que garantizará la seguridad de los sistemas de información de la institución, promoviendo una cultura de ciberseguridad alineada con las mejores prácticas y normativas internacionales que en este caso es la NIST SP 800-30.

5. Recomendaciones.

- Es fundamental aplicar políticas de acceso basado en roles (RBAC), donde cada usuario acceda únicamente a la información y funciones que necesita para cumplir su trabajo. Esto reduce el riesgo de exposición de datos sensibles y ayuda a prevenir accesos indebidos, especialmente en sistemas financieros, servidores, bases de datos y archivos críticos.
- Todo sistema debe contar con una estrategia de respaldos periódicos, automáticos y almacenados en diferentes ubicaciones (local y en la nube), además, se debe probar de forma periódica la restauración de estos respaldos para garantizar que los datos realmente puedan recuperarse ante fallas, ataques de ransomware o errores humanos.
- Utilizar una herramienta de monitoreo como Zabbix, SIEM u otra solución de vigilancia permite recolectar, correlacionar y analizar registros de eventos provenientes de diferentes equipos. Esto permite actuar rápidamente en caso de comportamientos sospechosos o accesos no autorizados, reduciendo el impacto de los incidentes.

- La información institucional debe ser categorizada según su sensibilidad, estableciendo niveles como: pública, interna, confidencial y crítica. Esta clasificación permite definir medidas de protección proporcionales, como cifrado, control de accesos, restricciones de copia o eliminación segura.
- El plan debe contemplar el cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador, así como alinearse con estándares reconocidos como la ISO 27001, NIST SP 800-30 y buenas prácticas bancarias del sector cooperativo. Esto respalda la legalidad de las acciones y eleva el nivel de confianza en la institución.
- Se recomienda revisar el contenido del plan al menos una vez al año, o de forma inmediata si se produce un cambio importante en la infraestructura tecnológica, aparición de nuevas amenazas, incorporación de nuevos sistemas o cambios regulatorios. Esta revisión debe ser liderada por el área de TI con participación del Comité de Seguridad.

4.2.3 Guía de políticas y procedimientos del plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.

La guía de políticas y procedimientos se constituye al ser un documento fundamental para aplicar las políticas del plan integral de ciberseguridad en la COAC Mercedes Cadena, dentro de esta guía, se proponen procedimiento de guía para su respectiva implementación y la definición de procedimientos claros para para su respectiva implementación.

Además, se establece un protocolo para realizar auditorías periódicas y pruebas de seguridad en activos clave con respecto a sus activos asegurando así la continuidad y mejora del nivel de ciberseguridad de la institución.

MANUAL DE PROCESOS PARA EL PLAN INTEGRAL DE CIBERSEGURIDAD EN BASE A LA APLICACIÓN DE LA METODOLOGÍA DE LA NIST SP 800-30.

CACME
Cooperativa de Ahorro y Crédito

MARLON EMANUEL IPIALES JINGO

MANUAL DE PROCESOS DE MITIGACIÓN DE RIESGOS Y VULNERABILIDADES

MANUAL DE PROCESOS PARA EL PLAN INTEGRAL DE CIBERSEGURIDAD EN BASE A LA APLICACIÓN DE LA METODOLOGÍA DE LA NIST SP 800-30.

Control de documentación.

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre:	Sr. Marlon Ipiales	Ing. Anderson Bonilla	Ing. Marcelo Guamán
Cargo:	Tesista	Jefe de procesos	Gerente
Firma:			
Fecha:	6 de junio del 2025	12 de julio del 2025	

Ficha de edición del documento:

Nombre del documento	Manual de procesos para el plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.	
Código del documento	Código: MPPIC-NIST-01	
Edición	01	
Fecha de edición	6 de junio del 2025	
Responsable de Edición	Marlon Emanuel Ipiales Jingo	
Cargo	Tesista	
Cambios realizados	**Autor de Edición**	**Fechas de Ediciones**

Contenido.

1. Manual de procesos de plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30.

El presente documento establece un conjunto de procesos esenciales para la implementación del Plan Integral de Ciberseguridad en la Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda., basados en la metodología NIST SP 800-30.

Este plan busca mitigar riesgos en la infraestructura crítica y establecer estrategias para la prevención, detección y respuesta a incidentes de seguridad informática. Además, define lineamientos y responsabilidades clave dentro de la organización para garantizar la protección de la información y la continuidad del negocio.

1.1. Objetivo.

El objetivo principal del Plan de Procesos es proporcionar un marco estructurado para la gestión de riesgos identificados en la institución, mediante la evaluación y mitigación de amenazas que puedan afectar la infraestructura tecnológica de la cooperativa, a esto se busca garantizar la disponibilidad, confidencialidad e integridad de la información mediante controles efectivos y estrategias de seguridad.

1.2. Alcance.

Este manual aplica a los activos con un nivel de riesgo mayor o igual al 48%, garantizando la protección de los sistemas críticos de la institución mediante estrategias de mitigación, monitoreo y respuesta ante incidentes siguiendo un respectivo proceso.

1.3. Metodología.

La metodología de evaluación de riesgos es un proceso fundamental para la identificación, análisis y tratamiento de las amenazas que pueden afectar la infraestructura crítica de la institucion, ya que esta se basa en un enfoque sistemático que permite evaluar el impacto potencial y definir estrategias de mitigación eficaces. Esta evaluación debe realizarse periódicamente para garantizar la seguridad de la información y minimizar vulnerabilidades.

1.3.1. Metodología de evaluación de riesgos según NIST SP 800-30.

La evaluación de riesgos seguirá las directrices establecidas en la metodología de la NIST SP 800-30, considerando la identificación de activos críticos, el análisis de amenazas y vulnerabilidades, la evaluación del impacto y determinación del nivel de riesgo, la implementación de estrategias de mitigación y el monitoreo continuo para la mejora del plan. Estos procedimientos permiten establecer un proceso estructurado que garantiza un orden de seguimiento en cuento a la seguridad de la información y minimiza las vulnerabilidades en la

cooperativa. A continuación, se presenta un diagrama de flujo que ilustra el proceso de evaluación de riesgos:

Imagen 1

Diagrama de flujo de evaluación de riesgos y procedimiento.

Nota. Este diagrama fue creado por el autor para ilustrar el procedimiento de evaluación de riesgo basado en la NIST SP 800-30.

2. Identificación y Clasificación de Activos Críticos.

Los activos críticos de la cooperativa han sido identificados con base en su importancia dentro de la infraestructura tecnológica y el impacto con un posible nivel de riesgo que podría generarse en la operatividad, considerando a la clasificación de estos activos permite priorizar acciones de seguridad y aplicar controles específicos según su nivel de riesgo. El análisis de activos debe considerar no solo los sistemas físicos, sino también los servicios y aplicaciones que son esenciales para la continuidad del negocio.

3. Términos y definiciones.

- Activo: Recursos técnicos o humanos necesarios para la operación.
- Amenaza: Evento potencial que puede dañar un activo.
- Vulnerabilidad: Debilidad que puede ser explotada por una amenaza.
- Riesgo: Combinación de la probabilidad de ocurrencia de un evento y su impacto.
- Control: Medida implementada para mitigar un riesgo.
- Mitigación: Medidas que se toman para reducir un riesgo o minimizar los daños si algo llega a suceder.
- Impacto: Efectos negativos que puede generar un evento no deseado encima los activos de la organización.

4. Referencias normativas.

- NIST SP 800-30: Guía para la gestión de riesgos.
- ISO/IEC 27001: Sistema de gestión de seguridad de la información.

5. Procedimientos específicos.

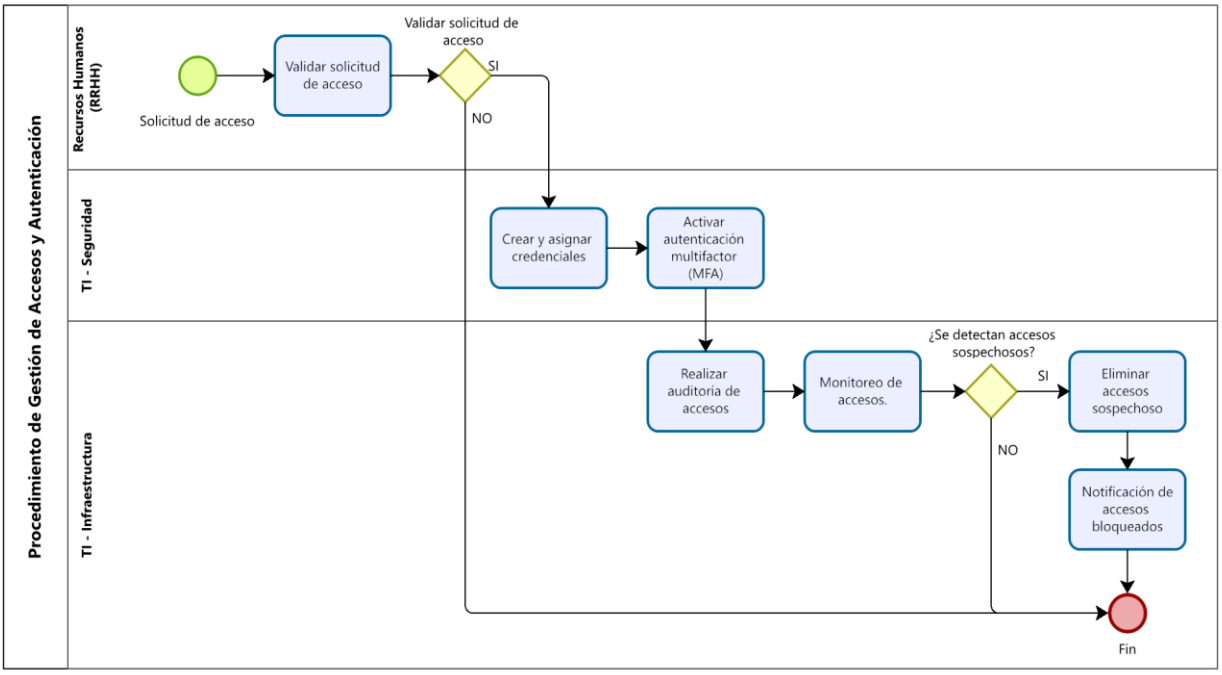
Los procedimientos especificados a continuación detallan las acciones concretas que deben realizarse para garantizar la seguridad de la información y la fortaleza de los sistemas críticos, ya que estos procedimientos deben ser seguidos por todos los responsables de la seguridad de TI en la cooperativa y actualizados conforme a las amenazas emergentes y las mejores prácticas de la industria.

5.1. Procedimiento de Gestión de Accesos y Autenticación

Para garantizar la seguridad de los sistemas críticos, se aplican controles estrictos sobre quién puede acceder a ellos, ya que cada usuario recibe permisos específicos de acuerdo con su roles y funciones asegurando que solo tenga acceso a lo que realmente necesita, además de que es obligatorio seguir políticas de autenticación seguras para proteger la información y evitar accesos no autorizados.

Imagen 2

Diagrama de procedimiento de Gestión de Accesos y Autenticación.



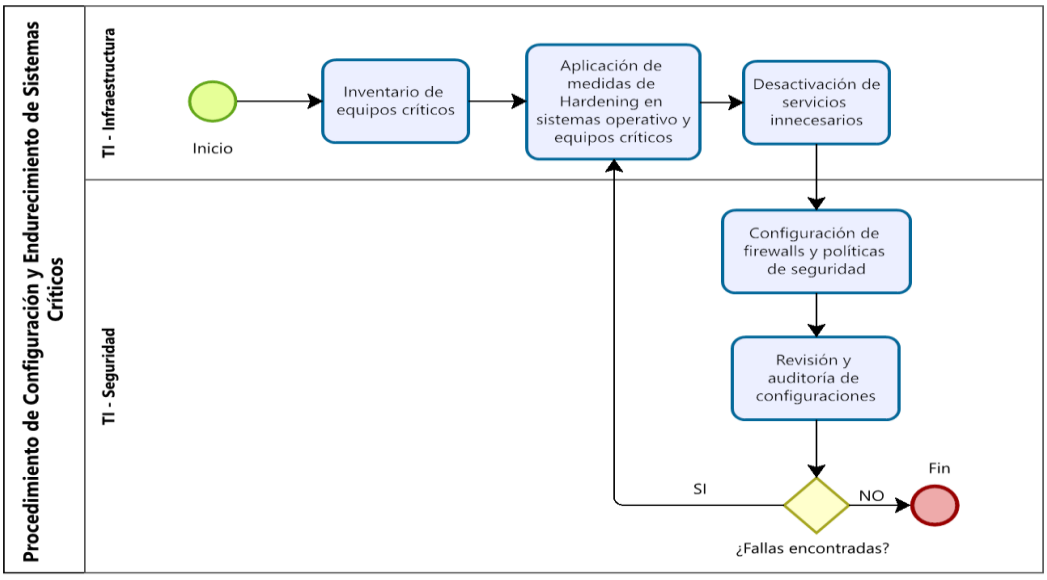
Nota. Este diagrama fue creado por el autor para ilustrar los procedimientos de Gestión de Accesos y Autenticación.

5.2. Procedimiento de Configuración y Endurecimiento de Sistemas Críticos

El proceso para reducir los riesgos y fortalecer la protección de la red interna de la institución, se aplican diversas configuraciones de seguridad en sus servidores, redes y equipos de trabajo, con base a estos procesos se busca minimizar los riesgos de ciberataques y garantizar un entorno más seguro para la operación de la organización.

Imagen 3

Diagrama procedimiento de Configuración y Endurecimiento de Sistemas Críticos.



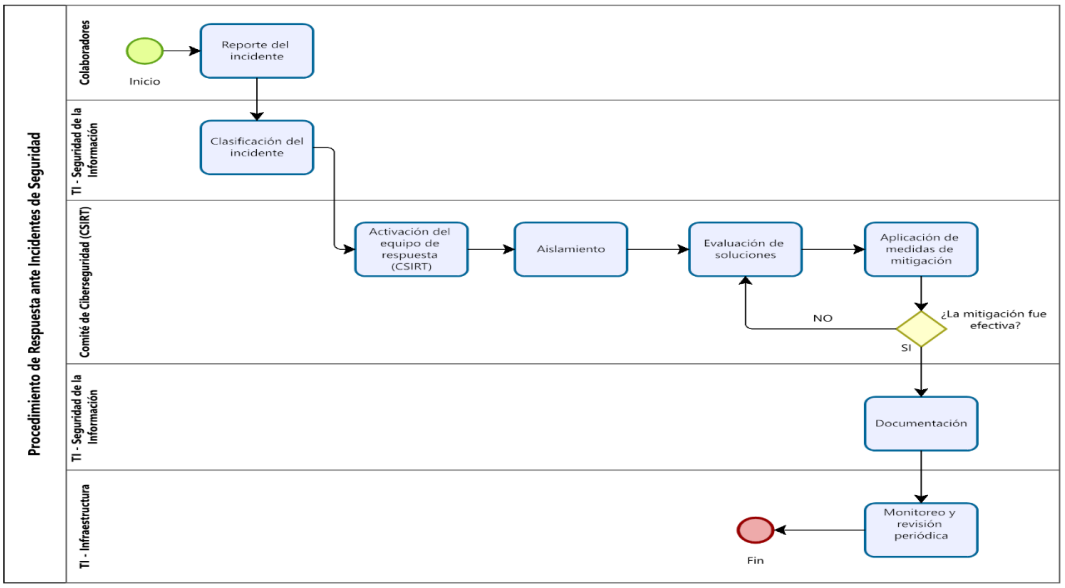
Nota. Este diagrama fue creado por el autor para ilustrar los procedimientos de Configuración y Endurecimiento de Sistemas Críticos.

5.3. Procedimiento de Respuesta ante Incidentes de Seguridad

Se definen claramente los pasos a seguir cuando ocurre un incidente de seguridad interna, tomando en cuenta desde el momento en que se detecta la amenaza hasta la completa recuperación del equipo o sistema, incluyendo la identificación del problema, la evaluación de su impacto, la implementación de medidas correctivas y, finalmente, un monitoreo, asegurando que se minimicen los riesgos y se refuercen las defensas para prevenir futuros incidentes.

Imagen 4

Diagrama de Procedimiento de Respuesta ante Incidentes de Seguridad.



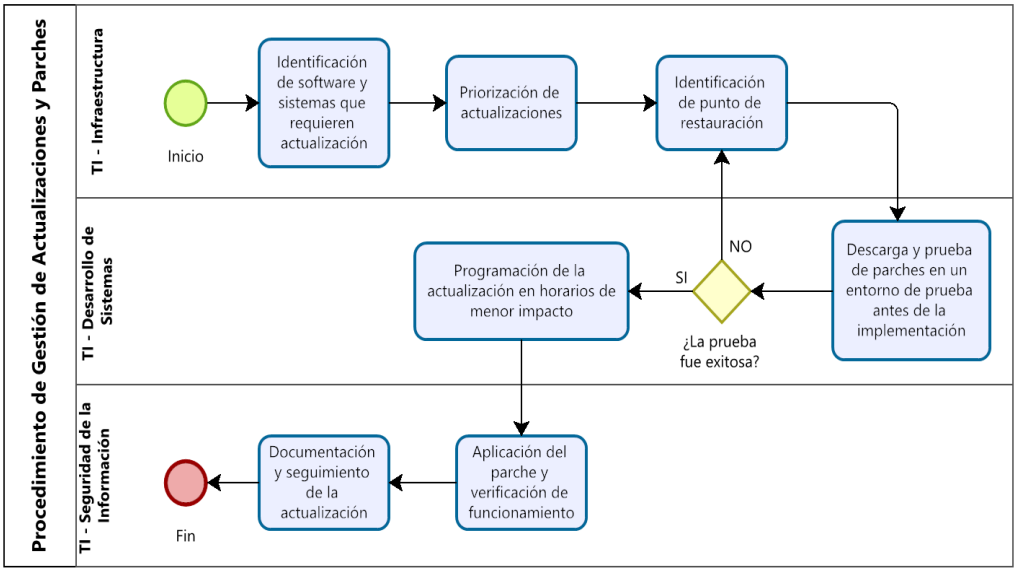
Nota. Este diagrama fue creado por el autor para ilustrar los procedimientos de respuesta ante Incidentes de Seguridad.

5.4. Procedimiento de Gestión de Actualizaciones y Parches

Se asegura que el software y los sistemas siempre estén actualizados para minimizar riesgos y cerrar posibles brechas de seguridad que los ciberdelincuentes podrían aprovechar. Mantener estas actualizaciones al día no solo mejora el rendimiento y la estabilidad, sino que también refuerza la protección contra amenazas emergentes, reduciendo la posibilidad de ataques que se aprovechen de estas vulnerabilidades conocidas.

Imagen 5

Diagrama de Procedimiento de Gestión de Actualizaciones y Parches.



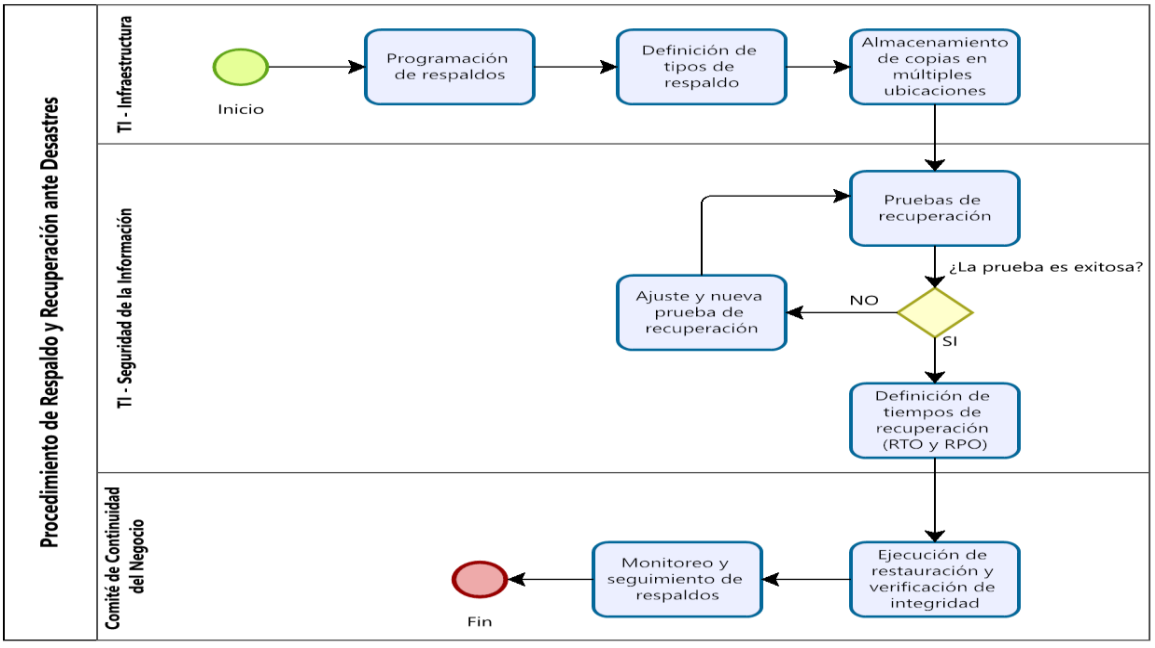
Nota. Este diagrama fue creado por el autor para ilustrar los procedimientos de Gestión de Actualizaciones y Parches.

5.5. Procedimiento de Respaldo y Recuperación ante Desastres

Para asegurar que la información esté siempre protegida y disponible cuando se necesite, se implementan medidas de evaluación periódica con copias de seguridad y la preparación de planes de recuperación ante incidentes, ya que estas acciones permiten minimizar el impacto de posibles fallos, ataques o errores humanos, garantizando que los datos puedan ser restaurados de manera rápida y segura en caso de cualquier eventualidad.

Imagen 6

Diagrama de Procedimiento de Respaldo y Recuperación ante Desastres.



Nota. Este diagrama fue creado por el autor para ilustrar los procedimientos de Procedimiento de Respaldo y Recuperación ante Desastres.

El RTO es el tiempo máximo para restaurar un sistema sin afectar el negocio, y el RPO es la cantidad de datos que se pueden perder desde el último respaldo sin generar impacto.

6. Indicadores y Métricas de Cumplimiento

El seguimiento y la evaluación del desempeño de las medidas de seguridad implementadas son fundamentales para mejorar continuamente el Plan Integral de Ciberseguridad de la institución, dado que se establecen indicadores clave que permiten medir la efectividad de los controles de seguridad, el tiempo de respuesta ante incidentes y el nivel de cumplimiento de las políticas establecidas, ya que cabe recalcar que estos indicadores deben ser revisados periódicamente para detectar oportunidades de mejora y optimizar la gestión de riesgos.

6.1. Indicadores Claves

Se han definido métricas específicas para evaluar la efectividad del plan de ciberseguridad, garantizando así que los controles y medidas implementados realmente contribuyan a la protección de la información y la mitigación de riesgos, tomando en cuenta que entre los principales indicadores clave se encuentran:

- **Número de incidentes detectados:** Permite evaluar la frecuencia con la que se presentan amenazas o vulnerabilidades en el entorno tecnológico. Un número elevado puede indicar la necesidad de reforzar las estrategias de prevención.
- **Tiempo promedio de respuesta a incidentes:** Mide la rapidez con la que se atienden y mitigan los incidentes de seguridad, asegurando una reacción oportuna ante posibles amenazas.
- **Cumplimiento de parches de seguridad (%):** Representa el porcentaje de sistemas actualizados con las últimas correcciones de seguridad. Un alto cumplimiento reduce la exposición a vulnerabilidades conocidas.
- **Eficiencia en respaldo y recuperación (%):** Evalúa la capacidad del sistema para realizar copias de seguridad efectivas y recuperar datos de manera rápida y fiable en caso de un incidente.
- **Número de accesos no autorizados detectados:** Indica la cantidad de intentos o accesos indebidos a los sistemas, reflejando la efectividad de los controles de acceso y autenticación.

6.2 Evaluación Periódica del Plan

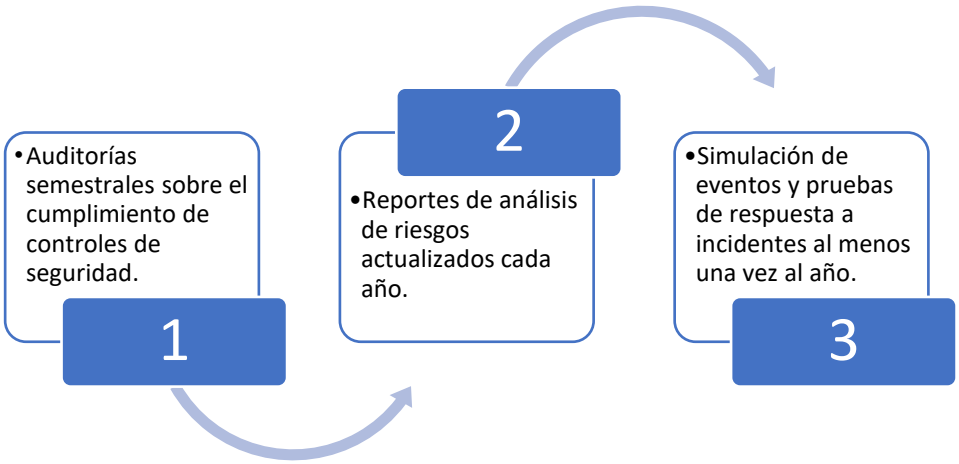
Es clave realizar un seguimiento constante del plan de ciberseguridad para asegurarse de que realmente cumpla con su propósito, ya que, a través de auditorías,

reportes y pruebas de seguridad, se pueden identificar oportunidades de mejora y reforzar las defensas frente a nuevas amenazas, permitiendo mantener una protección más efectiva y actualizada.

Por ello, a continuación, se presenta un diagrama que explica el proceso de seguimiento y evaluación periódica del plan asegurando asi su correcta implementación y mejora continua.

Imagen 7

Diagrama de Evaluación periódica del plan.



Nota. Este diagrama fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

7. Recomendaciones.

- Cada proceso descrito dentro del manual debe especificar a qué colaborador le corresponde su ejecución o aprobación, ya que esto ayuda a evitar ambigüedades permitiendo así auditar responsabilidades en caso de errores y facilitando la introducción de nuevos colaboradores.
- Los diagramas deben seguir una simbología reconocida y estar acompañados de una breve descripción, ya que estos deben ser fáciles de entender para la secuencia lógica de pasos, decisiones, entradas y salidas del proceso, lo que favorece su implementación práctica.
- El manual debe contemplar una sección donde los usuarios puedan registrar sugerencias o incidentes que evidencien deficiencias en la ejecución de los procesos, ya que estas observaciones pueden ser evaluadas periódicamente por el área de seguridad para proponer mejoras a futuro.
- Cada procedimiento debe especificar qué se necesita para iniciarse (documentos, accesos, software), cómo se ejecuta (paso a paso), y cuál es el producto final esperado (por ejemplo, informe generado, respaldo realizado, etc.). Esto permite que el personal actúe con mayor autonomía y precisión frente a una toma de decisiones.
- Se recomienda establecer métricas cuantificables, como tiempo promedio de respuesta a incidentes, porcentaje de procesos ejecutados correctamente o cantidad de auditorías aprobadas. Estos indicadores pueden ser revisados en informes trimestrales o semestrales, fomentando la mejora continua y el cumplimiento organizacional.

4.2 Entrega de documentos.

Al culminar el desarrollo del “Plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30” y del “Manual de procesos para el plan integral de ciberseguridad en base a la aplicación de la metodología de la NIST SP 800-30”, estos documentos fueron entregados al actual encargado general de las áreas dentro de la institución que es el Ing. Anderson Bonilla. Con respaldo de dicha entrega, se generó un documento que valida la entrega de los mismo, el cual el documento se encuentra disponible y visible en el **ANEXO F**.

Capítulo V

Desarrollo de pruebas en base al plan integral de ciberseguridad propuesto para la COAC Mercedes Cadena.

Para asegurar que el plan de ciberseguridad desarrollado en el Capítulo IV funcione correctamente, en este capítulo se ponen a prueba las acciones y medidas previamente establecidas, ya que el objetivo es comprobar que los procedimientos y controles realmente protegen los activos más importantes de la cooperativa junto con los servicios financieros que ofrece la institución, es por ello que se aplicará una revisión, listas de verificación y pruebas prácticas que permitirán identificar qué está funcionando bien y qué es lo que necesita mejoras, ya que todo este proceso se llevó a cabo siguiendo la guía implementada en el desarrollo de este trabajo que ayuda a manejar los riesgos tecnológicos de manera organizada y efectiva.

5.1 Metodología de prueba.

Para realizar las pruebas de validación, se dio uso de una metodología estructurada que se organizada en varias fases: inmediata, corto plazo, mediano plazo, largo plazo y evaluación continua. Este cronograma de fases está detallado en la Tabla 3 del Plan Integral de Ciberseguridad del Capítulo IV. En cada una de estas fases, se aplican checklists específicos que facilitan la validación de los controles establecidos para los activos más críticos de la cooperativa y sus funciones.

5.2 Checklists de verificación por fase.

Los checklists de verificación de cada fase del proceso de pruebas están diseñados para evaluar de manera detallada y sistemática los controles de seguridad implementados en los activos más críticos de la organización. Cada fase, desde la inmediata hasta la de evaluación, se estructuró con un conjunto específico de pruebas adaptadas a los objetivos de mitigación de riesgos establecidos. La aplicación de estos checklists brinda una revisión de los controles de seguridad, asegurando que se cumplan los estándares definidos y facilitando así la identificación de áreas que requerían mejoras o ajustes.

5.2.1 Diseño de Checklist de fase inmediato.

Durante las primeras semanas, lo más urgente es asegurar que las medidas básicas se encuentren correctamente implementadas en los activos más importantes. Esta fase se enfoca en aspectos esenciales como la protección contra virus, gestión de contraseñas y la restricción de softwares no autorizados.

Tabla 16

Checklist propuesta para la fase 1 de pruebas de la COAC Mercedes Cadena.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 1 Inmediata (1 - 2 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	Máquinas personales (Windows 10)	Configuración de antivirus	Verificar que el antivirus está actualizado y funcionando			
2	AFC.2023	Configuración de software de gestión de contraseñas	Verificar que el software de contraseñas está instalado y funcionando			
3	MySQL	Restricción de instalación de software no autorizado	Intento de instalación de software no autorizado			

Firma Estudiante

Firma Jefe de Procesos

Firma Tutor

Nota. Este checklist fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

5.2.2 Diseño de Checklist de fase a corto plazo.

El enfoque en esta fase está en mejorar la seguridad de las redes y la gestión de accesos, ya que aquí comienza a asegurar que la red estuviera correctamente segmentada y que el acceso a los sistemas sensibles se encuentre controlados adecuadamente.

Tabla 17

Checklist propuesta para la fase 2 de pruebas de la COAC Mercedes Cadena.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 2 Corto Plazo (2 - 3 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	Switch TP-Link TL-SG1024D	Auditorías de configuración	Verificar la configuración de la red y el control de acceso			
2	LogMeIn Hamachi	Configuración de autenticación basada en claves seguras	Intento de conexión con credenciales no autorizadas			
3	Servidor Dell PowerEdge T150	Configuración de redundancia de UPS	Verificación de que el sistema UPS está correctamente configurado			

Firma Estudiante Firma Jefe de Procesos Firma Tutor

Nota. Este checklist fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

5.2.3 Diseño de Checklist de fase a mediano plazo.

En esta fase se encuentra dedicada la implementación de medidas de seguridad más avanzadas, ya que aquí se introduce la revisión de los accesos a los servidores más importantes Además de un análisis más profundo de los accesos a los sistemas más críticos para asegurar que

todo se encuentre bajo control junto con la verificación de redundancia de UPS para la continuidad de sus procesos.

Tabla 18

Checklist propuesta para la fase 3 de pruebas de la COAC Mercedes Cadena.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 3 Mediano Plazo (3 - 4 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N °	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	WinSPC	Auditorías de configuración	Revisión de accesos y configuración de políticas de acceso			
2	AFC.2023	Auditorías de seguridad periódicas	Realización de auditoría de seguridad periódica			
3	Servidor Dell PowerEdge T150	Configuración de redundancia UPS	Verificación de redundancia de UPS			

Firma Estudiante **Firma Jefe de Procesos** **Firma Tutor**

Nota. Este checklist fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

5.2.4 Diseño de Checklist de fase a largo plazo.

En esta etapa, se pone a prueba la capacidad de recuperación ante incidentes o fallos del sistema, como la restauración de datos. También que en esta parte se encuentra la parte de realizar la verificación de las políticas de acceso a sistemas y datos.

Tabla 19

Checklist propuesta para la fase 4 de pruebas de la COAC Mercedes Cadena.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 4 Largo Plazo (4 - 5 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	WinSPC	Configuración de políticas de acceso	Verificación de las políticas de acceso a sistemas y datos			
2	PuTTY	Pruebas de restauración de datos	Realizar pruebas de restauración en caso de fallo del sistema			

Firma Estudiante | Firma Jefe de Procesos | Firma Tutor

Nota. Este checklist fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

5.2.5 Diseño de Checklist de fase de evaluación.

Finalmente, se llega a la fase de evaluación, donde se analiza el desempeño general del sistema de ciberseguridad después de varias pruebas a todos los activos. Aquí se realiza la revisión completa a todos los elementos de la institución de forma continua y se evalúa si todo el personal se encuentra apto para responder adecuadamente ante cualquier situación.

Tabla 20

Checklist propuesta para la fase 5 de pruebas de la COAC Mercedes Cadena.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 5 Evaluacion (6 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	Todos los activos	Monitoreo continuo de medidas implementadas	Revisar que todos los activos están siendo monitoreados de forma continua			
2	Todos los activos	Capacitación y auditorías integrales	Realizar auditoría final y verificar la capacitación del personal			

Firma Estudiante | Firma Jefe de Procesos | Firma Tutor

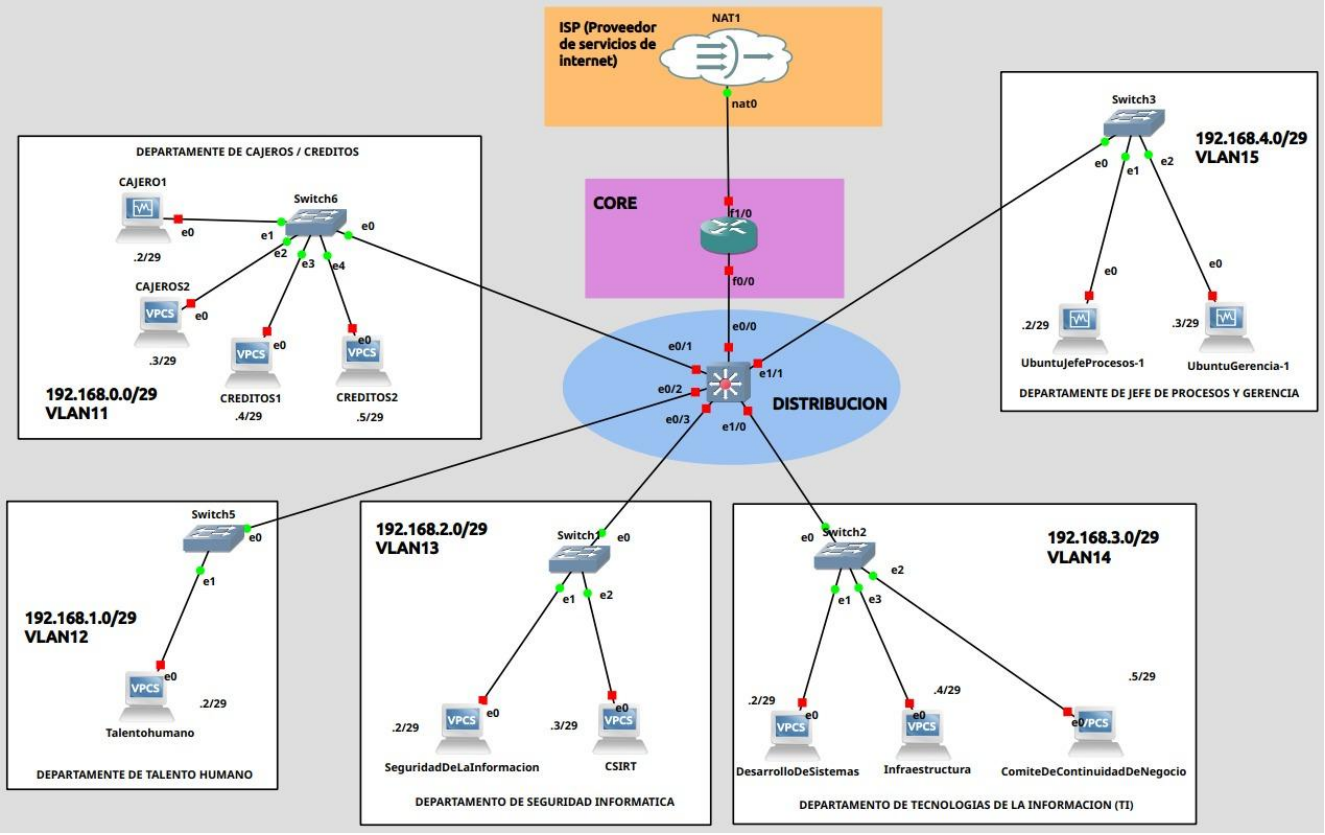
Nota. Este checklist fue creado por el autor para ilustrar el procedimiento para una evaluación periódica del plan.

5.3 Simulación de mecanismos de mitigación a implementar.

A continuación, se presenta una propuesta de topología simulada que refleja la estructura de la red empresarial de la cooperativa tomando a consideración que los equipos utilizados en esta simulación son similares en cuanto a la capacidad y rendimiento a los que poseen actualmente la institución, así mismo diseñada según los departamentos sugeridos por el Plan Integral de Ciberseguridad y su plan de procesos. La red se encuentra segmentada en áreas críticas, lo que facilita un flujo de información de manera ordenada y eficiente. Claro que a partir de este diseño, se realizarán las pruebas correspondientes para evaluar la efectividad de los controles y estrategias del plan integral de ciberseguridad diseñado, asegurando que la infraestructura sea capaz de enfrentar posibles saturaciones y amenazas cumpliendo así con los estándares de seguridad sugeridos en el plan, tomando en cuenta los equipos han sido simulados dentro de la topología.

Figura 10

Topología de infraestructura critica propuesta simulada de la COAC Mercedes Cadena.



Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.1 Estructura de diseño de la red interna.

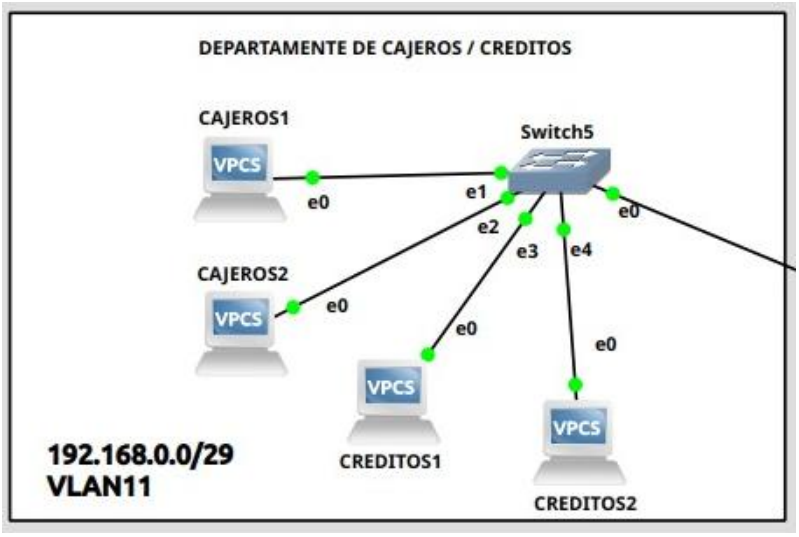
La topología de red se organiza en VLANs (Virtual Local Area Networks), que son redes virtuales separadas dentro de la misma infraestructura física, lo que mejora tanto la seguridad como el rendimiento de la red. Cada VLAN está asignada a un departamento o grupo de trabajo específico tal como se está propuesto en el desarrollo de este Plan Integral de Ciberseguridad permitiendo que las comunicaciones dentro de cada segmento sean más eficientes y seguras.

5.3.1.1 VLAN11 – Departamento de Cajeros / Créditos (192.168.0.0/29)

Este segmento alberga los sistemas de transacciones financieras, representados por estaciones como CAJEROS1, CAJEROS2, CREDITOS1 y CREDITOS2. Estos servidores están conectados a un Switch, el cual permite gestionar el tráfico dentro de este departamento tan crítico para la cooperativa. Este diseño asegura que la información relacionada con las transacciones esté aislada de otras áreas, protegiéndola de accesos no autorizados.

Figura 11

Topología de infraestructura propuesta simulada con respecto a la VLAN11.



Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.1.2 VLAN12 – Departamento de Talento Humano (192.168.1.0/29)

En esta subred se encuentra el sistema de gestión de personal, representado por el equipo de Talento humano. Este equipo está conectado a un Switch, con el objetivo de gestionar los datos de los empleados, permisos de acceso y otras funciones administrativas, todo dentro de un entorno controlado y seguro.

Figura 12

Topología de infraestructura propuesta simulada con respecto a la VLAN12.

Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

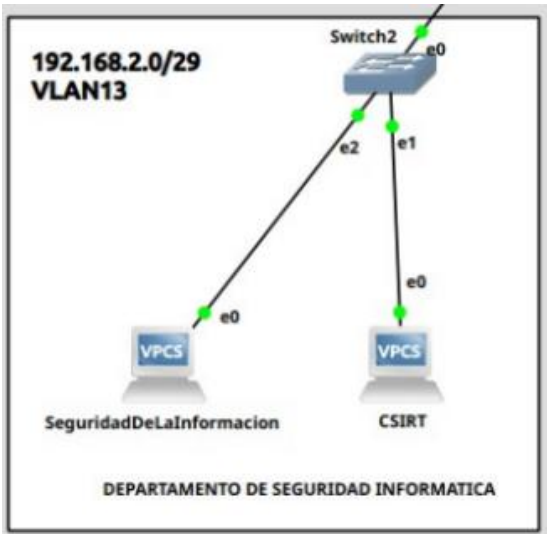
5.3.1.3 VLAN13 – Departamento de Seguridad Informática (192.168.2.0/29)

Aquí se encuentran los equipos de Seguridad De La Información y CSIRT, que son fundamentales para el monitoreo, prevención y respuesta ante incidentes de seguridad. Este

segmento está aislado para evitar interferencias externas y proteger los datos sensibles. Los equipos de seguridad utilizan este entorno para gestionar las amenazas en tiempo real y aplicar las estrategias de defensa cibernética necesarias.

Figura 13

Topología de infraestructura propuesta simulada con respecto a la VLAN13.



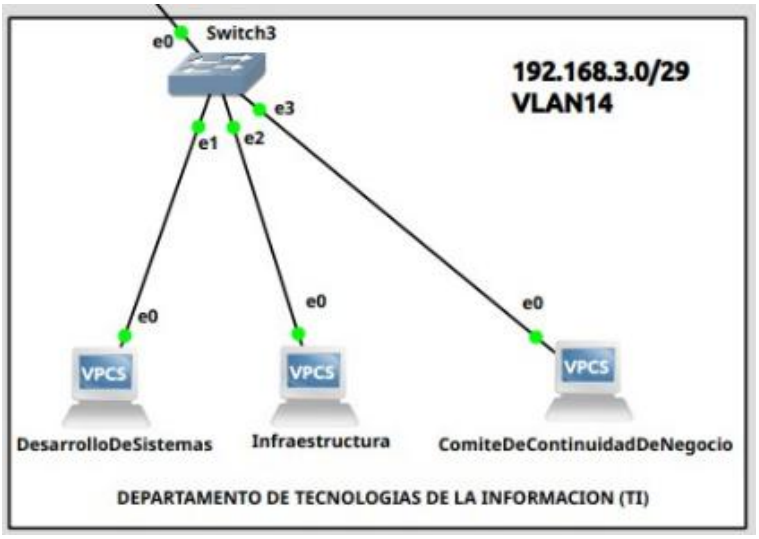
Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.1.4 VLAN14 – Departamento de Tecnologías de la Información (192.168.3.0/29)

Esta subred alberga los equipos como Desarrollo De Sistemas, Infraestructura y Comité De Continuidad De Negocio, que son esenciales para el mantenimiento de la infraestructura tecnológica de la cooperativa. Estos equipos están conectados a un Switch, que gestiona la comunicación interna de sistemas que soportan la operación diaria y los servicios tecnológicos.

Figura 14

Topología de infraestructura propuesta simulada con respecto a la VLAN14.



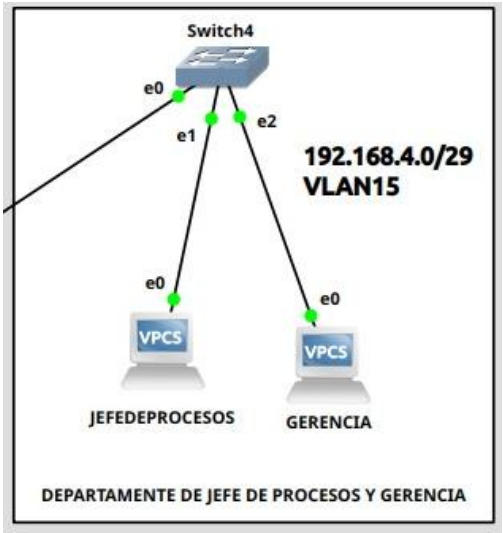
Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.1.5 VLAN15 – Departamento de jefe de Procesos y Gerencia (192.168.4.0/29)

En esta red se encuentran los equipos principales tanto para jefe Procesos y Gerencia, los cuales son clave para las decisiones estratégicas y operativas de la cooperativa. El acceso a estos servidores es estrictamente controlado, dado que contienen información sensible y de alto nivel.

Figura 15

Topología de infraestructura propuesta simulada con respecto a la VLAN15.



Nota. Esta topología fue creada por el autor para ilustrar la idea de la infraestructura basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

Este diseño de topología no solo permite la segmentación lógica de la red para facilitar el manejo del tráfico, sino que también reduce los riesgos de intrusión al limitar el acceso no autorizado entre las diferentes áreas puesto que su direccionamiento IP tan solo está permitido para un cierto número de equipos con proyección a crecimiento de un nuevo integrante en cada área. Cada subred tiene configuraciones específicas que favorecen tanto el rendimiento como la resiliencia ante fallos, un aspecto clave para garantizar que las operaciones no se vean afectadas ante posibles incidentes.

5.3.2 Configuración de equipos CORE y Distribución

Con el objetivo de evaluar el comportamiento de la red en un entorno seguro y controlado, sin comprometer los sistemas reales de la cooperativa, se llevó a cabo la simulación de los equipos CORE y DISTRIBUCIÓN. Esta simulación permitió reproducir de forma precisa una infraestructura de red que incluye segmentación por VLAN, enrutamiento y control de tráfico, tomando a consideración que los equipos simulados son básicamente similares a los que posee actualmente la institución. Es importante destacar que la configuración de estos equipos se basó en las políticas y lineamientos definidos en el plan integral de ciberseguridad desarrollado previamente, lo cual aseguró que la arquitectura simulada cumpliera con los estándares establecidos en materia de protección, control de acceso y priorización del tráfico crítico.

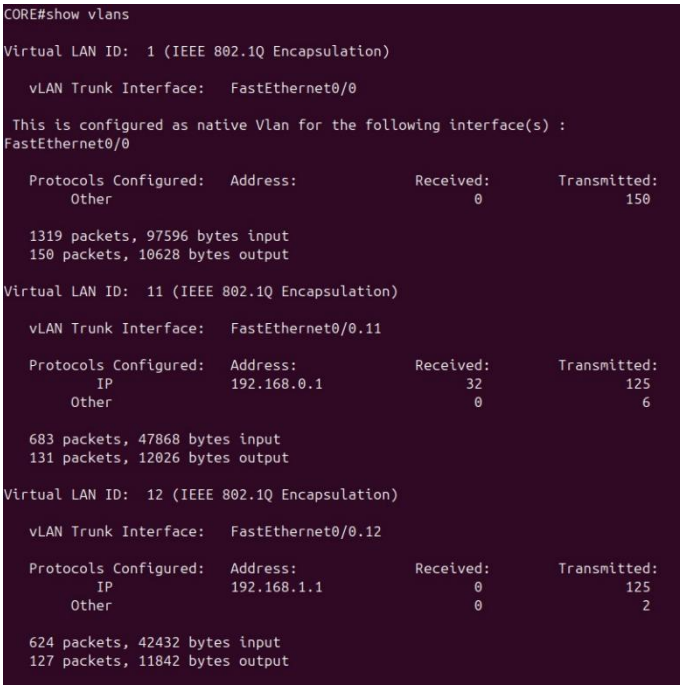
5.3.2.1 Configuración de equipo CORE en cuanto a VLANs y Políticas de Calidad de servicio.

Tanto en el equipo DISTRIBUCIÓN como en el equipo CORE se llevó a cabo la configuración de múltiples VLANs con el objetivo de segmentar la red de la organización según sus distintos departamentos que han sido sugeridos en el manual de procesos a los cuales se habilitaron VLANs del 11 al 15 asignadas respectivamente a las áreas de Cajeros/Créditos, Talento Humano, Seguridad Informática, Tecnologías de la Información y Jefatura de Procesos con Gerencia. En el equipo DISTRIBUCIÓN, cada VLAN fue asociada a una interfaz Ethernet específica para asegurar una separación eficiente del tráfico entre los distintos segmentos de red. Paralelamente, en el equipo CORE se configuraron subinterfaces sobre la interfaz FastEthernet 0/0, correspondientes a cada VLAN, permitiendo así el enrutamiento entre ellas y facilitando la comunicación interdepartamental. Para todas las áreas se utilizó un esquema de direccionamiento /29, lo que garantiza una asignación adecuada de direcciones IP y deja espacio disponible para

incluir, si es necesario, un equipo adicional por área, proyectando así un crecimiento ordenado de la infraestructura sin necesidad de modificaciones estructurales futuras.

Figura 16

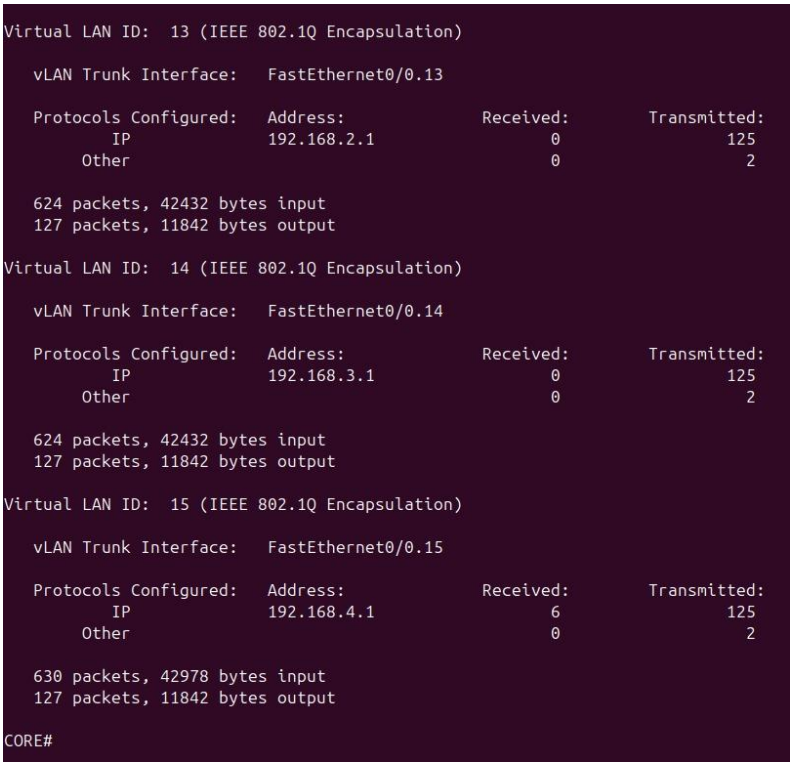
Visualización de VLANs simuladas con respecto al equipo CORE.



Nota. Esta configuración fue creada por el autor para ilustrar la idea de administración VLAN basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

Figura 17

Visualización de VLANs propuestas simulada con respecto al equipo CORE.



```
Virtual LAN ID:  13 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.13

   Protocols Configured:   Address:             Received:       Transmitted:
           IP              192.168.2.1                 0               125
        Other                                          0                 2

   624 packets, 42432 bytes input
   127 packets, 11842 bytes output

Virtual LAN ID:  14 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.14

   Protocols Configured:   Address:             Received:       Transmitted:
           IP              192.168.3.1                 0               125
        Other                                          0                 2

   624 packets, 42432 bytes input
   127 packets, 11842 bytes output

Virtual LAN ID:  15 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   FastEthernet0/0.15

   Protocols Configured:   Address:             Received:       Transmitted:
           IP              192.168.4.1                 6               125
        Other                                          0                 2

   630 packets, 42978 bytes input
   127 packets, 11842 bytes output

CORE#
```

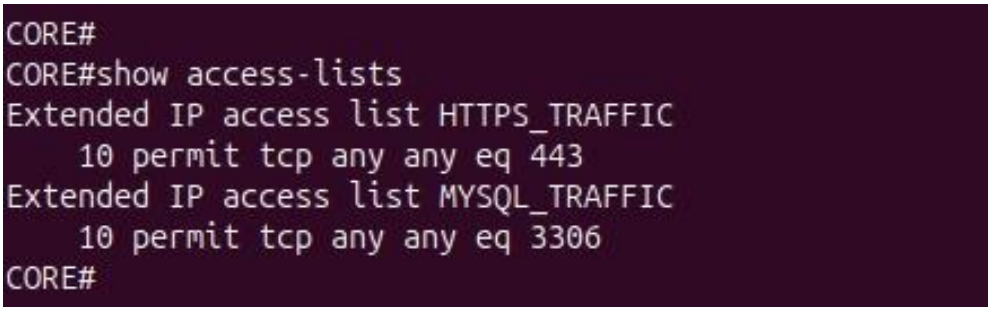
Nota. Esta configuración fue creada por el autor para ilustrar la idea de administración VLAN basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

Con respecto al equipo CORE se crearon listas de control de acceso extendidas (ACL) con el fin de identificar y clasificar el tráfico crítico que debía ser priorizado dentro de la red al igual que restringir el tráfico de red y filtrar los paquetes antes de que lleguen a los servidores establecidos. Se configuraron dos listas específicas: la primera denominada HTTPS_TRAFFIC, que permite el tráfico TCP por el puerto 443, correspondiente a servicios web seguros; y la segunda, MYSQL_TRAFFIC, que autoriza el tráfico TCP por el puerto 3306, utilizado para la comunicación con bases de datos MySQL. Estas listas permiten filtrar y diferenciar el tráfico

sensible del resto, estableciendo la base para su posterior priorización dentro de las políticas de calidad de servicio.

Figura 18

Visualización de ACLs simuladas con respecto al equipo CORE.

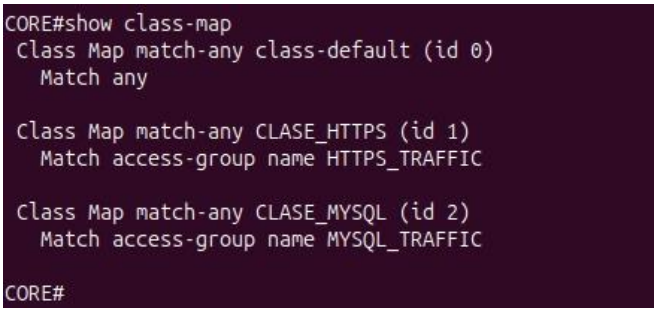


Nota. Esta configuración fue creada por el autor para ilustrar la idea de administración basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

En la siguiente etapa, estas listas de acceso fueron asociadas a clases específicas a través de la creación de mapas de clase. En este caso, se definieron CLASE_HTTPS y CLASE_MYSQL, las cuales hacen referencia directa a los grupos de acceso anteriormente mencionados. De esta forma, se estructuró una forma ordenada de aplicar las políticas diferenciadas a cada tipo de tráfico, asegurando que tanto las consultas a la base de datos como el acceso a servicios web protegidos tengan un tratamiento especial dentro del manejo del tráfico general, tomando en cuenta que los class-map si no se llegan a usar en una policy-map no tendrían efecto pero se puede dejar a la opción de conservarlos puesto que si se considera aplicar políticas de calidad de servicio (QoS) en un futuro estas ayudarían a su respectiva configuración con firewalls o equipos basados en capa 3.

Figura 19

Visualización de clases simuladas con respecto al equipo CORE.



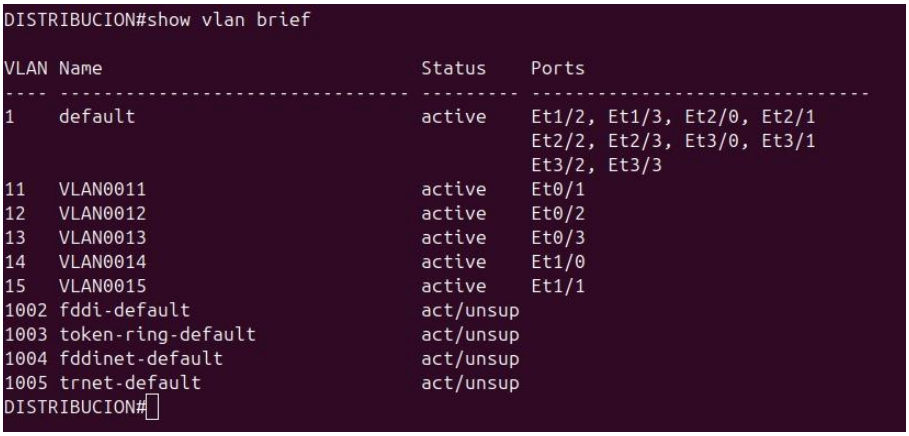
Nota. Esta configuración fue creada por el autor para ilustrar la idea de administración class – map basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.2.2 Configuración de equipo de distribución.

En el equipo DISTRIBUCIÓN, que corresponde a un switch administrable de capa 2, se llevó a cabo la configuración de las VLANs necesarias para la segmentación lógica de la red de la cooperativa. Este switch, al operar en la segunda capa del modelo OSI (capa de enlace de datos), permite dividir el dominio de broadcast sin requerir funciones de enrutamiento. Mediante el comando show vlan brief se puede verificar que se crearon y activaron las VLANs 11, 12, 13, 14 y 15, las cuales fueron asignadas a puertos específicos del switch de acuerdo con la distribución departamental definida previamente. Esta configuración facilita la organización del tráfico por área y mejora el control de la red, asegurando que cada departamento opere dentro de su propio segmento, reduciendo así la posibilidad de colisiones y aumentando la eficiencia del entorno de red simulado.

Figura 20

Visualización de VLANs simuladas y configuradas respecto al equipo DISTRIBUCION.



Nota. Esta configuración fue creada por el autor para ilustrar la idea de administración VLAN basada en el plan de integral de ciberseguridad para la COAC Mercedes Cadena.

5.3.3 Simulación de servicios financieros

Con el fin de realizar pruebas sin comprometer la operatividad real de la cooperativa, se optó por implementar una simulación de servidores en un entorno controlado en un sistema operativo basado en Linux tal como sugiere el plan integral de ciberseguridad. Esta simulación permitió replicar las funciones de los servidores críticos, sin intervenir directamente en el sistema financiero ni en la gestión real de datos de la institución, evitando así posibles riesgos de pérdida de información o interrupciones en los servicios. En este entorno simulado se configuraron tanto la página web institucional como el sistema financiero, ambos basados en un servidor web alojado en Nginx y operando sobre el puerto 443 con certificados SSL, garantizando conexiones cifradas y seguras. Cabe destacar que para el desarrollo de esta simulación se aplicaron las dos primeras fases de evaluación establecidas las cuales son la fase inmediata (checklist 5.2.1) y la fase a corto

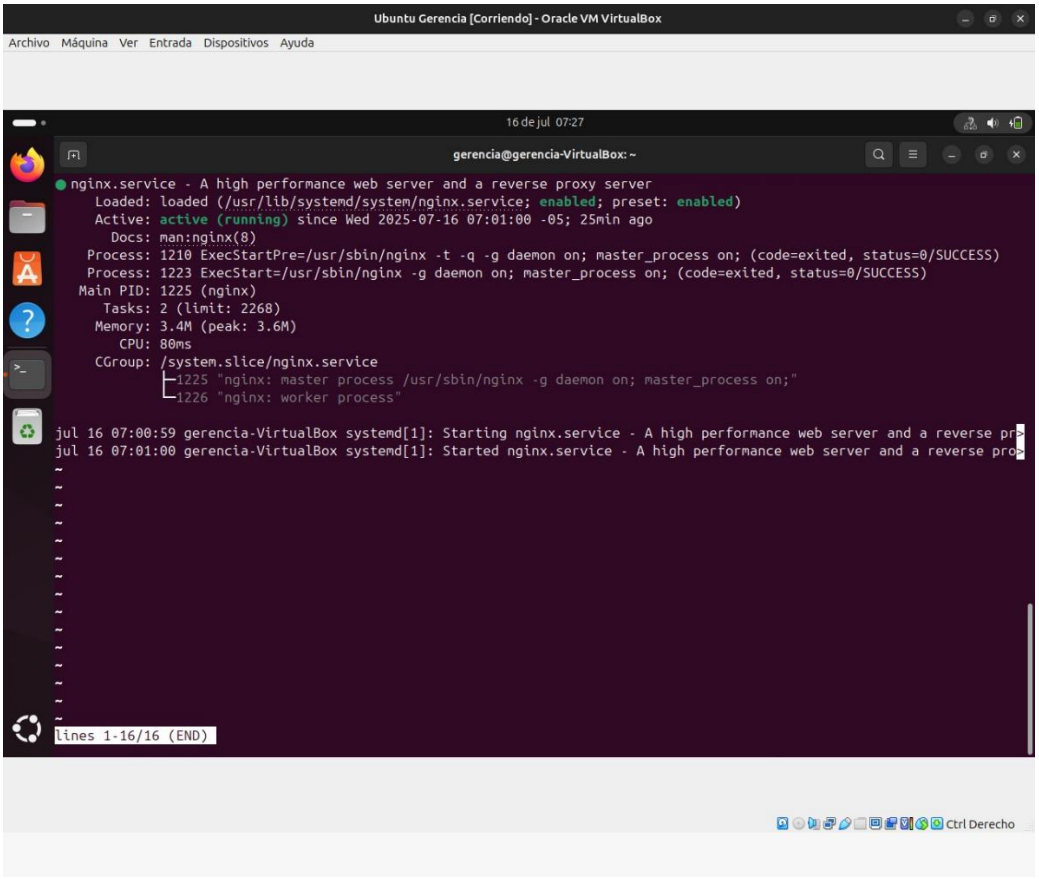
plazo (checklist 5.2.2), ya que las pruebas se enfocaron exclusivamente en los activos más importantes y vulnerables.

5.3.3.1 Simulación de servidor WEB.

Para la simulación del servidor web, se configuró un servidor NGINX con el objetivo de hospedar diversas aplicaciones internas de la cooperativa CACME así como sus servicios financieros, como las áreas correspondientes al departamento de talento humano, seguridad de la información y tecnologías de la información. Para garantizar la seguridad de las comunicaciones entre los clientes y el servidor, se implementaron certificados SSL autofirmados localmente, lo que asegura que los datos transmitidos a través de la red interna no se enviarán en texto claro sino de forma cifrada, evitando posibles vulnerabilidades en la transmisión de información a través de la red. Este enfoque de cifrado se llevó a cabo utilizando el puerto 443, el cual es utilizado para establecer conexiones seguras a través del protocolo web HTTPS, tomando en cuenta que esta práctica es ampliamente recomendada, ya que el puerto 443 proporciona una capa de seguridad adicional mediante la encriptación SSL/TLS, lo que protege la confidencialidad de los datos.

Figura 21

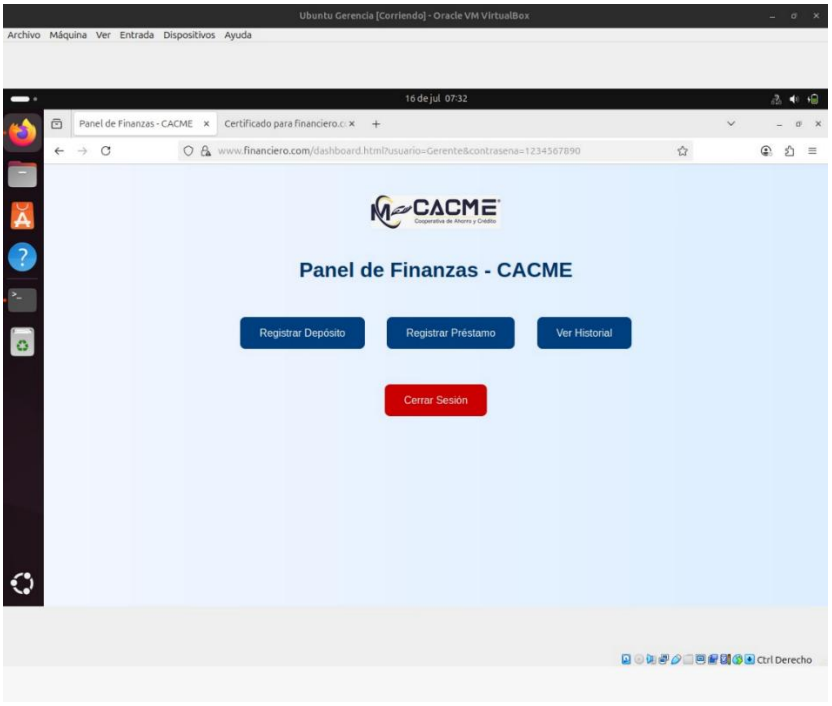
Simulación del servidor web de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para la sección del servidor WEB de la COAC Mercedes Cadena.

Figura 22

Simulación del servidor web de la Cooperativa en un entorno controlado.

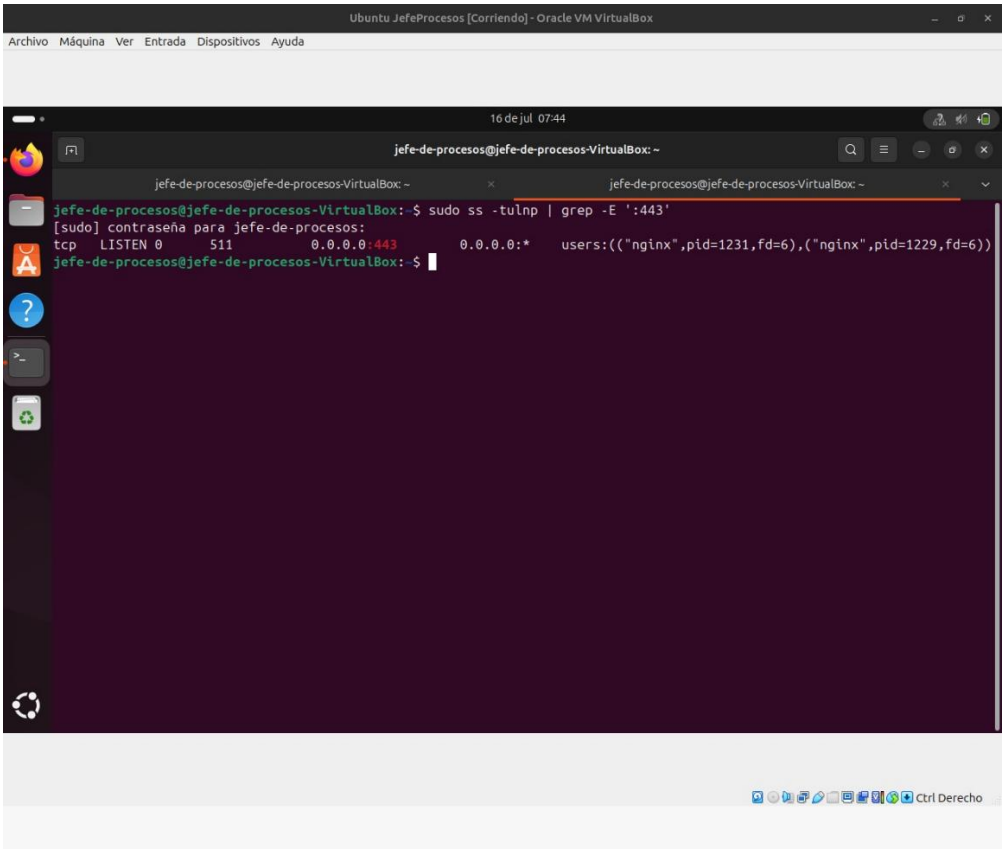


Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para la sección del servidor WEB de la COAC Mercedes Cadena.

De acuerdo con las políticas establecidas en el Plan Integral de Ciberseguridad, se infiere el refuerzo del uso al puerto 443, como una medida esencial para garantizar comunicaciones seguras dentro de la red, alineándose con las mejores prácticas de seguridad informática y mitigación de riesgos, ya que adicional de uso del puerto esta contribuye a mejorar la eficiencia del tráfico de la red al asegurar que las comunicaciones sean manejadas de manera más segura y protegida, especialmente en un entorno corporativo donde la confidencialidad es crucial.

Figura 23

Uso de puerto 443 en la simulación al servidor web de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de uso de puertos en un entorno controlado para la sección del servidor WEB de la COAC Mercedes Cadena.

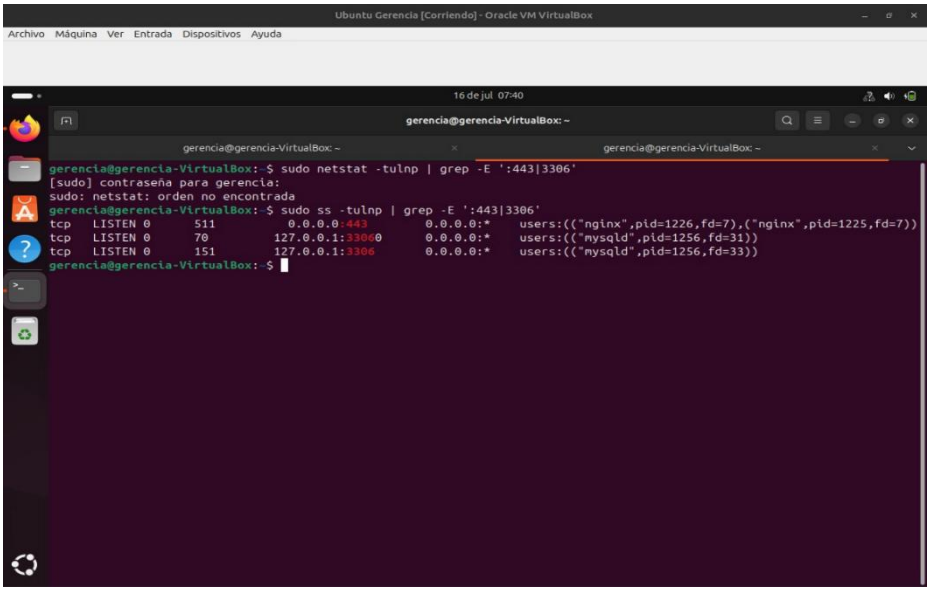
Sin embargo, cabe señalar que, debido a que este entorno es simulado, la verificación de los UPS (Uninterruptible Power Supply) se presenta como circunstancial, y aunque no se ha implementado un sistema de respaldo eléctrico en esta simulación, se recomienda su consideración para garantizar la disponibilidad continua de los servicios en entornos reales, especialmente cuando se manejan aplicaciones críticas para el negocio.

5.3.3.2 Simulación de servidor de Base de Datos.

Para la simulación del servidor de base de datos se estableció la comunicación entre el servidor web NGINX y el servidor MySQL, utilizando el puerto 3306, reservado específicamente para el servicio de bases de datos MySQL. A través de este canal se almacenan y consultan los datos de los usuarios, tales como registros de depósitos y préstamos. El servidor web, por su parte, accede a esta información mediante consultas desarrolladas en PHP, presentando los resultados en las páginas del sistema. Todo el proceso de visualización se realiza de forma segura mediante el protocolo HTTPS, alojado en el servidor web que opera bajo el puerto 443.

Figura 24

Uso de puerto 443 y 3306 en la simulación al servidor de base de datos con acceso WEB de la Cooperativa en un entorno controlado.

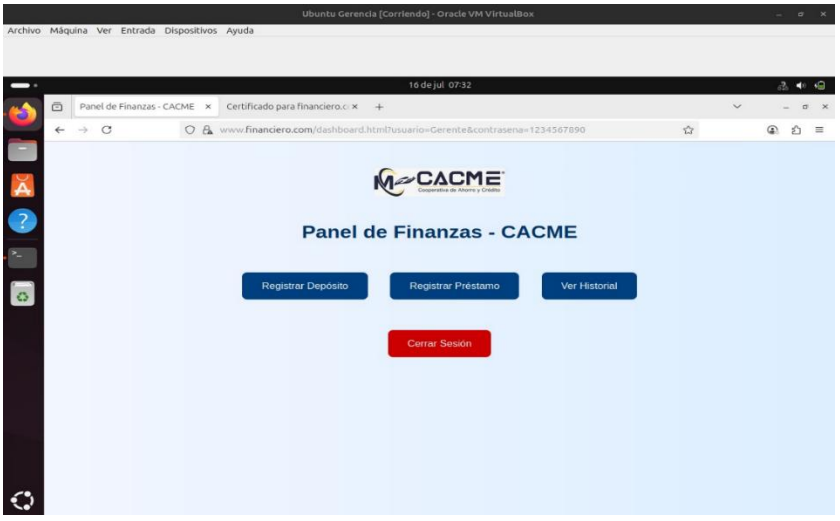


Nota. Esta figura fue creada por el autor para ilustrar la idea de uso de puertos en un entorno controlado para la sección del servidor de Base de Datos de la COAC Mercedes Cadena.

Para la simulación del servidor de base de datos, se configuró un servidor MySQL destinado a alojar las bases de datos utilizadas por las aplicaciones internas de la cooperativa CACME. Como parte de las medidas de seguridad implementadas, se restringió el acceso únicamente a través de puertos seguros, destacando el uso del puerto 3306 para la comunicación con el servicio de MySQL. Adicionalmente, se habilitó el puerto 443 para permitir conexiones web seguras mediante el protocolo HTTPS. Para facilitar la interacción con el sistema, se desarrolló una interfaz web que permite la visualización e ingreso de registros a la base de datos, asegurando en todo momento una transmisión cifrada y un acceso restringido solo a usuarios autorizados.

Figura 25

Simulación de interfaz WEB al servidor de base de datos con acceso WEB de la Cooperativa en un entorno controlado.

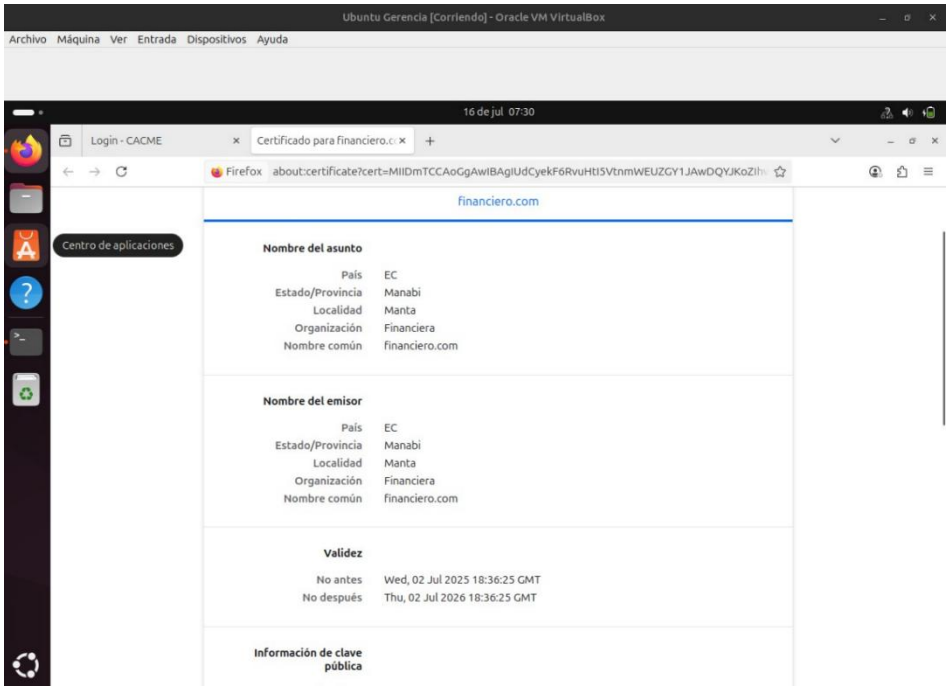


Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para la sección del servidor de Base de Datos de la COAC Mercedes Cadena.

Además, se emplearon certificados SSL autofirmados y conexiones cifradas SSL/TLS, lo que permite asegurar que los datos enviados entre los clientes y el servidor de base de datos no sean interceptados ni modificados durante su transmisión. Esto se implementó configurando el servidor para aceptar solo conexiones seguras y forzando la utilización de certificados SSL válidos para autenticar la identidad del servidor y cifrar los datos.

Figura 26

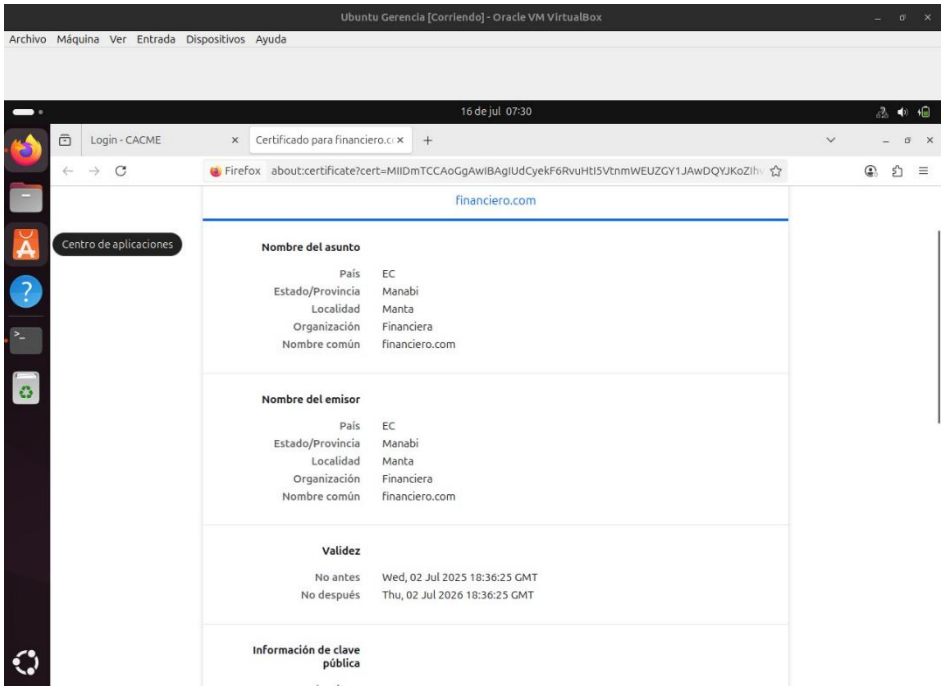
Uso de certificados SSL autofirmado en la simulación al servidor web de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación de certificados SSL en un entorno controlado para la visualización web de la COAC Mercedes Cadena.

Figura 27

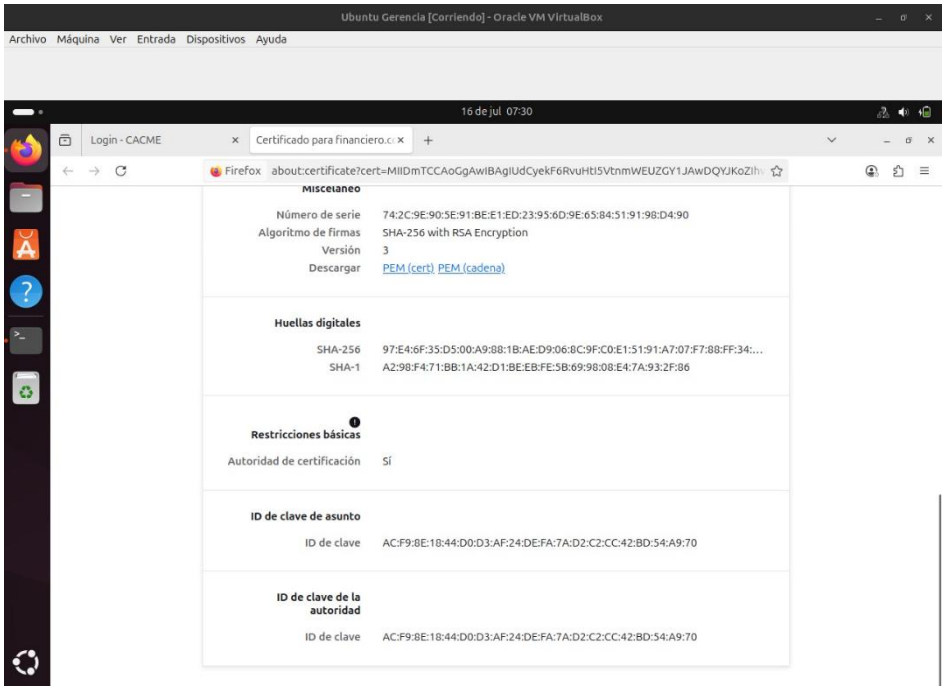
Uso de certificados SSL autofirmado en la simulación al servidor web de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación de certificados SSL en un entorno controlado para la visualización web de la COAC Mercedes Cadena.

Figura 28

Uso de certificados SSL autofirmado en la simulación al servidor web de la Cooperativa en un entorno controlado.



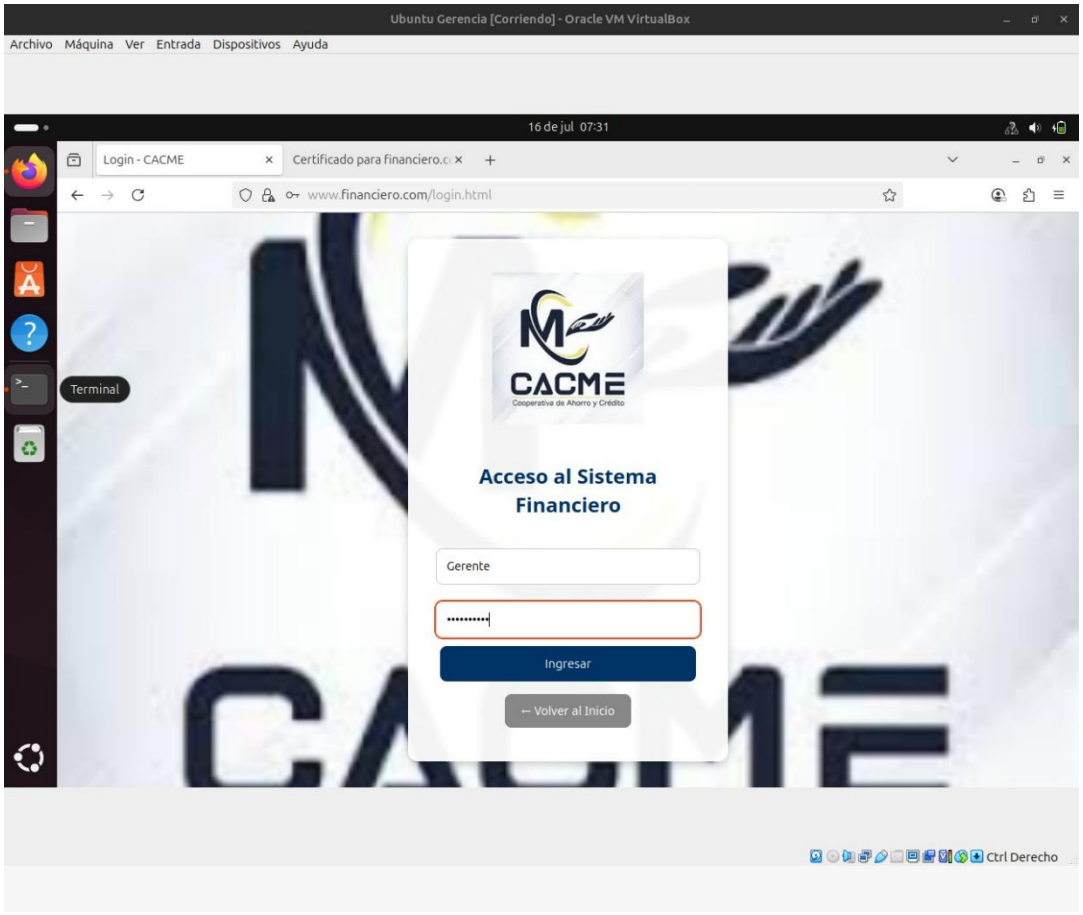
Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación de certificados SSL en un entorno controlado para la visualización web de la COAC Mercedes Cadena.

Una de las acciones clave implementadas fue la habilitación de un mecanismo de autenticación segura mediante contraseñas robustas para todas las cuentas con acceso a la base de datos. Se evitó por completo el uso de credenciales predeterminadas o débiles, lo cual permitió disminuir significativamente el riesgo de accesos no autorizados al sistema. Además, se estableció que la visualización de las tablas y registros de la base de datos solo puede realizarse previa autenticación, ya sea a través de las interfaces gráficas o directamente desde la terminal virtual,

utilizando comandos específicos. Este acceso controlado garantiza que únicamente el personal autorizado, con credenciales válidas, pueda consultar o gestionar la información almacenada.

Figura 29

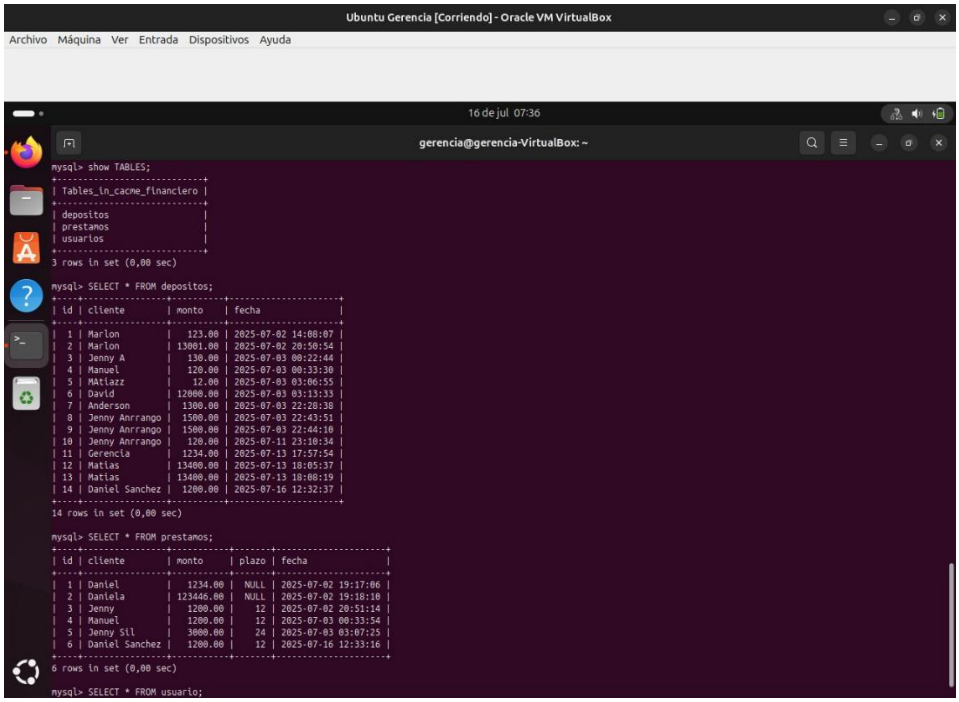
Acceso al servidor simulado de Base de Datos de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación de accesos en un entorno controlado para la sección del servidor de Base de Datos de la COAC Mercedes Cadena.

Figura 30

Visualización de datos registrados en el servidor simulado de Base de Datos de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para la visualización del servidor de Base de Datos de la COAC Mercedes Cadena.

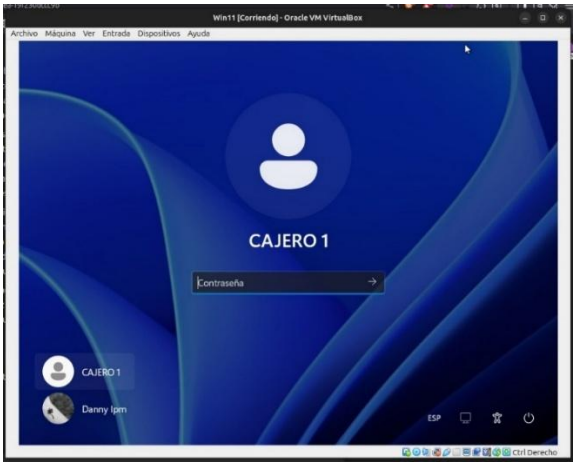
Se implementaron diversas prácticas para garantizar la seguridad en la conexión, transmisión y almacenamiento de la información en la base de datos, protegiendo los datos sensibles de accesos no autorizados y asegurando una navegación segura y fiable entre las aplicaciones y la base de datos, acorde con las mejores prácticas de seguridad informática establecidas en el Plan Integral de Ciberseguridad

5.3.3.2 Simulación de pruebas en equipo final (CAJERO).

En la simulación del equipo final asignado al cajero, se configuró un entorno que reúne todas las aplicaciones y procesos necesarios para llevar a cabo funciones clave como depósitos, préstamos y consulta de historiales al igual que actividades esenciales para el funcionamiento operativo de la institución. Este equipo en si fue diseñado específicamente para alojar todos los servicios simulados, incluyendo la visualización de acceso a los servidores financieros y el acceso a sus respectivas páginas web desarrolladas para la gestión de dichas operaciones ya que adicional, la máquina fue creada bajo el perfil de "Cajero 1", lo que permite restringir la instalación de aplicaciones no autorizadas y prevenir el uso indebido del sistema, reforzando así la seguridad del entorno simulado.

Figura 31

Visualización de equipo final para la simulación de los servicios configurados dentro de la Cooperativa en un entorno controlado.

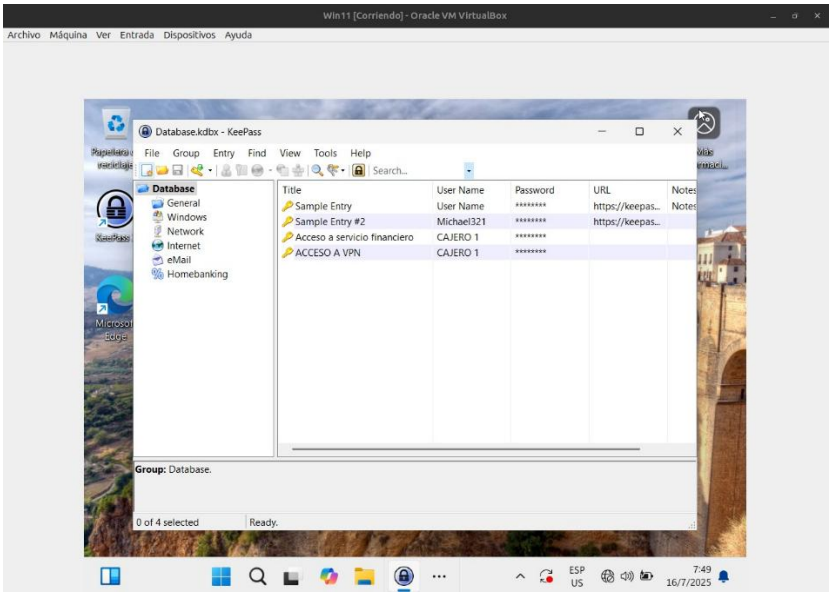


Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para un usuario final dentro de la COAC Mercedes Cadena.

El acceso con las aplicaciones web fueron protegidas mediante autenticación segura mediante roles, dado en este caso, se implementó el uso del gestor de contraseñas Keepass, el cual permitió al equipo de CAJERO 1 almacenar y acceder a las credenciales necesarias de manera segura, tomando en cuenta que Keepass se configuró para generar contraseñas robustas, que se almacenaron de forma cifrada, evitando así el uso de contraseñas débiles que pudieran poner en riesgo la seguridad de las aplicaciones críticas para la institución, el gestor de contraseñas ayudó al equipo a ingresar sus credenciales de forma correcta, minimizando los riesgos asociados a errores humanos o intentos de acceso no autorizado.

Figura 32

Aplicativo de gestor de contraseñas dentro del equipo final CAJERO 1.



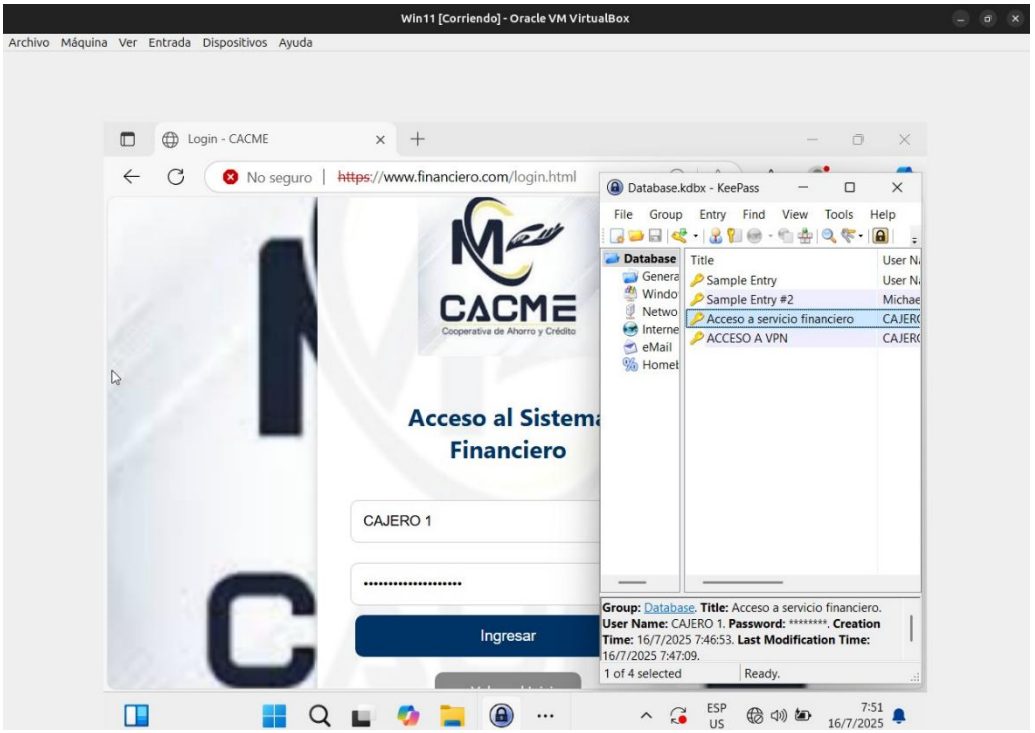
Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para el uso de gestor de contraseñas de la COAC Mercedes Cadena.

Por otro lado, para garantizar que los cajeros solo pudieran realizar las operaciones necesarias dentro del sistema, se creó un usuario exclusivo para el cajero, que fue configurado con permisos limitados. Este usuario no tiene la capacidad de instalar aplicaciones sin el permiso explícito del administrador del sistema, esta restricción es parte del Plan Integral de Ciberseguridad, el cual establece políticas de control de acceso para prevenir la instalación de softwares no autorizados que pudieran comprometer la integridad y seguridad del sistema en cuanto a su continuidad, a esto cabe mencionar que solo el área de TI tiene la autoridad para realizar modificaciones en el equipo, asegurando que las configuraciones del sistema y las aplicaciones instaladas estén debidamente verificadas y controladas para cada colaborador.

En lo referente a las operaciones que realiza el equipo del CAJERO 1 aquí los procesos de depósitos y préstamos fueron configurados siguiendo un flujo de tráfico riguroso y seguro, dado que estas funciones se gestionan a través de visualizaciones web protegidas mediante cifrado SSL/TLS y HTTPS por parte del puerto 443, lo que garantiza que todas las transacciones realizadas en la red sean realizadas de forma cifrada y segura, para reforzar aún más la seguridad en el acceso al sistema financiero, se incorporó el uso de la herramienta KeePass, la cual permite almacenar y gestionar de forma segura las credenciales, minimizando el riesgo de accesos no autorizados y malas prácticas en el manejo de contraseñas. Además, el sistema permite consultar de manera eficiente el historial de transacciones de depósitos y préstamos, manteniendo un registro detallado de todas las actividades realizadas, lo que facilita tanto la auditoría como el monitoreo continuo de las operaciones.

Figura 33

Uso de aplicativo de gestor de contraseñas dentro del equipo final CAJERO 1 para el ingreso al sistema financiero que fue configurado.



Nota. Esta figura fue creada por el autor para ilustrar la idea de la simulación en un entorno controlado para el uso de gestor de contraseñas de la COAC Mercedes Cadena.

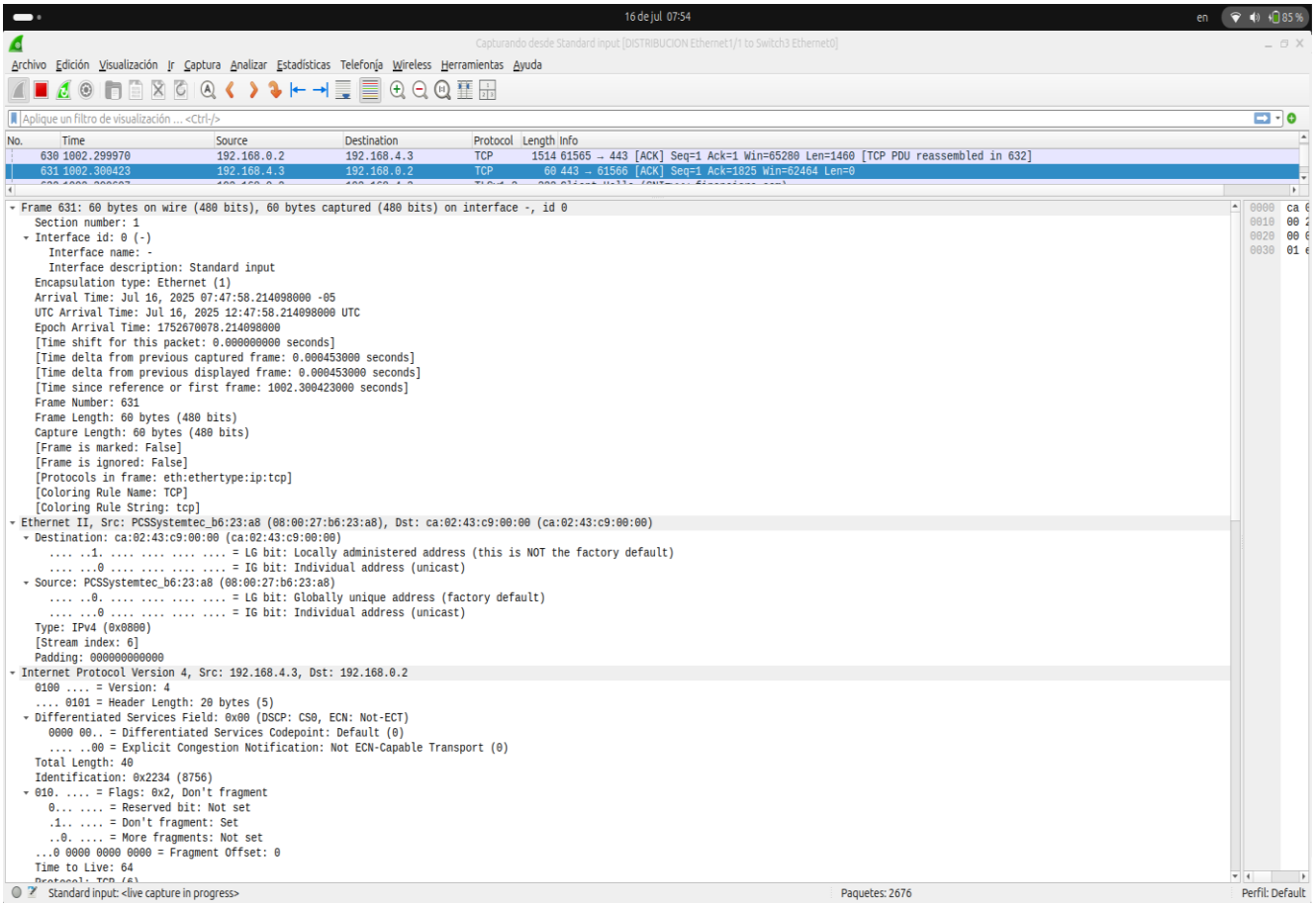
En general, la simulación del equipo final para el cajero se estructuró para garantizar una navegación segura, la integridad de los procesos de depósito y préstamo, y el control estricto de las operaciones. El uso de Keepass para gestionar contraseñas y la creación de un usuario exclusivo con permisos limitados refuerzan la seguridad en el acceso y la ejecución de las tareas, cumpliendo con las políticas de ciberseguridad establecidas en el Plan Integral de Ciberseguridad.

5.4 Análisis de cumplimiento.

Como parte fundamental de la fase de evaluación, se llevó a cabo una captura y análisis del tráfico de red utilizando la herramienta Wireshark, con el propósito de verificar el cumplimiento de las políticas definidas en el plan integral de ciberseguridad y el manual de procesos. Esta actividad se realizó en base a las fases establecidas en los checklists 5.2.1 (fase inmediata) y 5.2.2 (fase a corto plazo), Lo cual estas checklist que fueron realizadas se encuentran documentados en el **ANEXO E**. Las capturas obtenidas demuestran comunicaciones cifradas a través del protocolo HTTPS (puerto 443), lo que confirma que el acceso a los servicios web internos se está realizando de manera segura, en concordancia con la política que prohíbe el uso de protocolos sin cifrado o vulnerables.

Figura 34

Captura de paquetes de los servicios financieros de la Cooperativa en un entorno controlado.

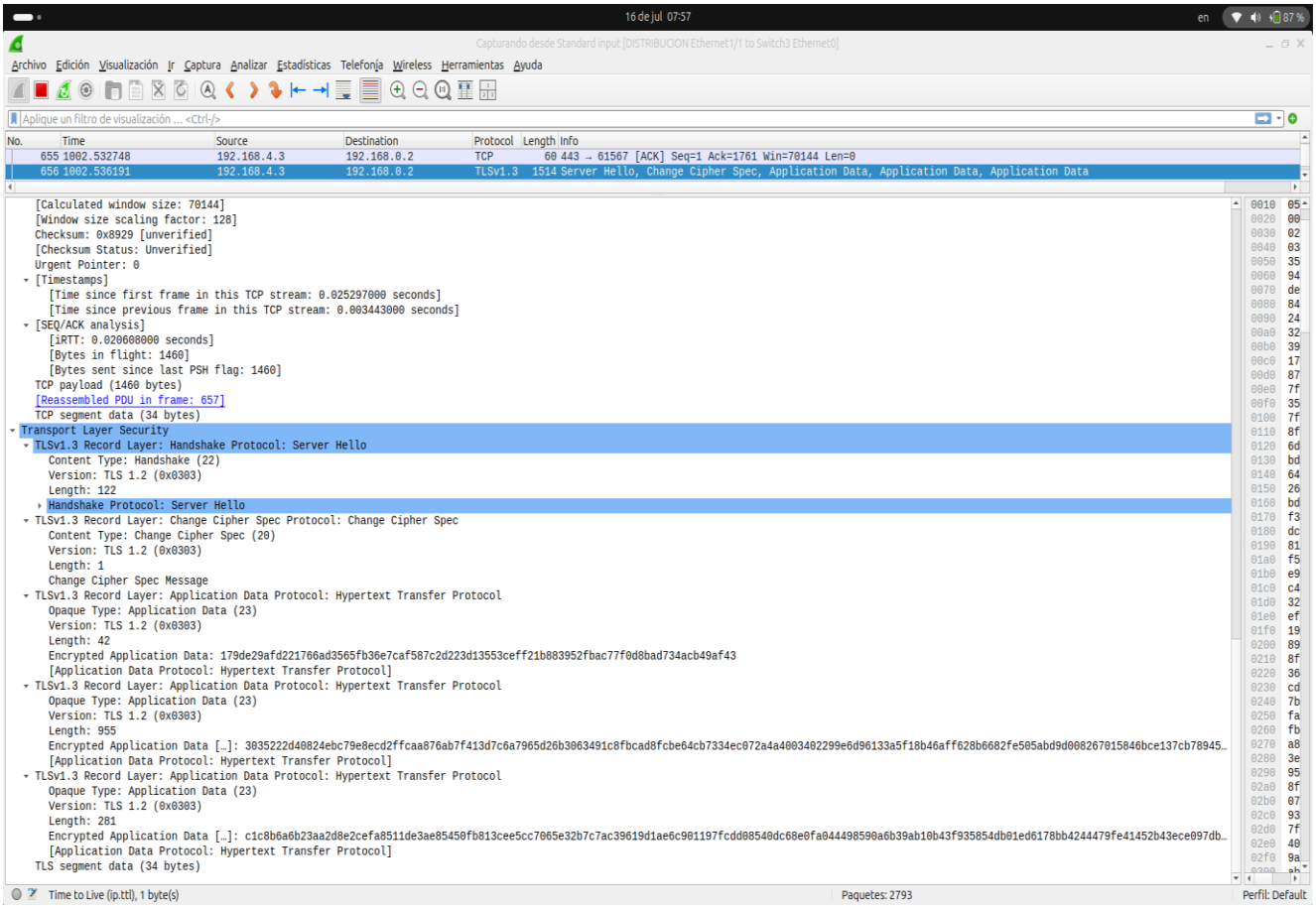


Nota. Esta figura fue creada por el autor para ilustrar los resultados de la simulación en un entorno controlado para la COAC Mercedes Cadena.

Asimismo, se pudo observar el establecimiento del protocolo TLS en su versión 1.3 lo cual demuestra que la transmisión de datos entre el cliente y el servidor se encuentra protegida con estándares actuales de seguridad. Este detalle valida la correcta aplicación de las políticas que exigen el uso obligatorio de conexiones cifradas para el ingreso, visualización y gestión de información sensible a través de la red interna de la cooperativa.

Figura 35

Captura de paquetes de los servicios financieros en cuanto al tráfico SSL/TLS de la Cooperativa en un entorno controlado.



Nota. Esta figura fue creada por el autor para ilustrar los resultados de la simulación en un entorno controlado para la COAC Mercedes Cadena.

Adicional, se observan intercambios TCP relacionados exclusivamente con el puerto 443, correspondiente al servicio HTTPS. No obstante, la presencia y funcionamiento del tráfico HTTPS confirma que las listas de control de acceso (ACL) y las políticas de calidad de servicio aplicadas en el equipo CORE están funcionando correctamente para los servicios web.

Conclusiones y recomendaciones

Conclusiones

- Durante las primeras fases de prueba se valida que la infraestructura de red como la implementación de VLANs mostró un rendimiento adecuado en cuanto a aislamiento y seguridad, ya que las configuraciones implementadas proporcionaron resultados positivos, lo que refuerza la validez de la metodología NIST SP 800-30 para la evaluación de riesgos.

- El uso de Keepass como herramienta para gestionar contraseñas mejoró la seguridad organizacional al evitar la creación de contraseñas débiles o repetidas, protegiendo las credenciales de acceso a sistemas críticos. La implementación de esta herramienta es una práctica recomendada para proteger las credenciales administrativas.

- La medida de restringir la instalación de aplicaciones a usuarios no autorizados por parte del departamento de TI en un área de entorno controlado demuestra ser efectiva para evitar que aplicaciones maliciosas o no autorizadas afectaran el sistema, puesto que esta medida debe ser mantenida y evaluada regularmente.

- Los resultados en las fases de evaluación inmediata y de corto plazo obtuvieron resultados satisfactorios, considerando que entonces las pruebas de evaluación a mediano, largo plazo y demás requieren la necesidad de revisar y ajustar algunas configuraciones con más tiempos de pruebas, validando así que la infraestructura debe seguir siendo evaluada y adaptada ante nuevas amenazas que surjan a medida que el entorno tecnológico evoluciona.

- La configuración de VLAN se comportó correctamente al segmentar eficazmente las redes internas y mejorar la seguridad general de la infraestructura, esto permitió un control más

eficiente sobre el tráfico de la red y contribuyó a la mitigación de riesgos asociados a posibles accesos no autorizados.

- Las restricciones impuestas para evitar la instalación no autorizada de aplicaciones y el control de acceso físico y lógico fueron elementos cruciales en la prevención de incidentes de seguridad. Estas medidas contribuyeron significativamente a minimizar el riesgo de vulnerabilidades internas.

- El manual de procesos y el plan integral de ciberseguridad fueron esenciales para estructurar y guiar las acciones de ciberseguridad en la institución, dado que ambos documentos proporcionaron una base sólida sobre la cual se pudieron aplicar los controles y procedimientos, demostrando que la implementación de un enfoque sistemático para la gestión de riesgos cibernéticos es fundamental para la protección de la infraestructura crítica.

- Al realizar las pruebas generales en los activos críticos más importantes con el nivel de riesgo mayor o igual al 48% calculado, se llegó a la conclusión que el proceso de simulación funciono correctamente, sin embargo, al aplicar las configuraciones en el equipo CORE como en el equipo de DISTRIBUCIÓN, se evidenció que si a futuro se implementara configuraciones más avanzadas, como por ejemplo las políticas de calidad de servicio (QoS), supera las capacidades actuales del equipo CORE, por lo que se concluye que es necesario fortalecer las capacidades de los equipos de DISTRIBUCIÓN en capa 3, con el fin de lograr una distribución más equilibrada de las configuraciones y evitar que toda la carga recaiga en un solo equipo que en este caso es el CORE.

Recomendaciones

- Si bien el plan integral de ciberseguridad funcionó correctamente en las fases de evaluación inmediata y de corto plazo, se debe reforzar la validación de controles y medidas de seguridad para las fases que siguen a continuación como las de mediano plazo, largo plazo y evaluación, ya que esto incluye revisar todas las configuraciones y protocolos de seguridad, para asegurar que la infraestructura pueda soportar amenazas emergentes a medida que evoluciona el entorno cibernético.

- La capacitación en el uso de herramientas de seguridad a todo el personal activo y en la correcta implementación de políticas de seguridad debe ser una prioridad, ya que el equipo de TI debe estar actualizado constantemente sobre nuevas las vulnerabilidades y de por si saber cómo mitigarlas, además de conocer a fondo las políticas de seguridad internas, como la configuración de su red y la función correcta de cada una de ellas.

- Aunque el bloqueo de instalación de aplicaciones funcionó correctamente bajo la supervisión del área de TI en un entorno contralado, es recomendable establecer una revisión periódica de los accesos físicos y lógicos a los sistemas más importantes, ya que esto debe incluir un control más exhaustivo sobre los dispositivos conectados a la red interna, asegurando que no se omitan medidas de seguridad en el proceso o instalaciones indebidas.

- La fase inmediata y de corto plazo en cuanto a la evaluación de acceso a sistemas críticos a través de redes externas debe ser rigurosamente controlado, ya que es necesario validar más a profundidad las políticas de acceso que se tiene de modo local y remoto, dado que estos accesos deben estar alineadas con las mejores prácticas de seguridad, puesto que el uso de redes privadas virtuales (VPN) y la encriptación de datos, evitan ataques externos.

- A medida que se vayan implementando nuevas tecnologías, se debe garantizar que sean totalmente compatibles con la infraestructura existente, ya que por ejemplo las VLANs y otras configuraciones de red como la implementación de políticas de calidad de servicio (QoS), deben integrarse sin comprometer la seguridad ni la eficiencia operativa, dado que se recomienda realizar pruebas exhaustivas de integración antes de cada implementación para asegurar un funcionamiento adecuado.

- Es recomendable realizar una actualización anual de las políticas de ciberseguridad propuestas, con el fin de mantenerlas alineadas a los cambios tecnológicos, nuevos riesgos emergentes y necesidades internas de la organización, dado que esta revisión periódica permitirá ajustar las medidas implementadas reforzando así los controles existentes y garantizando que las acciones de protección continúen siendo efectivas y beneficiosas para la infraestructura crítica de la cooperativa junto con su procesos continuos sin interrupción alguna.

- Aunque las pruebas iniciales mostraron buenos resultados, un plan de respuesta ante incidentes debe ser detallado y probado en escenarios más complejos, ya que esto debe incluir simulacros de crisis de diferentes magnitudes, como ataques de ransomware o pérdida de datos, para garantizar que todos los involucrados sepan cómo proceder de manera eficiente y coordinada, tomando en cuenta los tiempos o fases de verificación.

- Se recomienda que, en futuras implementaciones o configuraciones, la institución considere la aplicación de políticas de Calidad de Servicio (QoS) a través de dispositivos que integren funciones de firewall. Esto permitirá no solo gestionar de manera eficiente el uso del ancho de banda, priorizando servicios críticos como el acceso a sus sistemas financieros, sino también controlar y filtrar el tráfico con base en criterios de seguridad informática, ya que un firewall

con capacidades de QoS permitirá establecer reglas por usuario y la optimización de la red y fortaleciendo así la protección ante accesos no autorizados o consumo excesivo de recursos.

GLOSARIO

- **SSL (Secure Socket Layer):** Protocolo de seguridad utilizado para encriptar la comunicación entre servidores y navegadores, garantizando la protección de datos transmitidos en línea.
- **HTTPS (Hypertext Transfer Protocol Secure):** Versión segura del protocolo HTTP, utilizado para asegurar que las comunicaciones en la web estén cifradas mediante SSL/TLS.
- **VLAN (Virtual Local Area Network):** Red local virtual que permite segmentar redes físicas en subredes lógicas para mejorar el rendimiento y la seguridad dentro de una infraestructura de red.
- **Firewall:** Sistema de seguridad que controla el tráfico de red entrante y saliente, filtrando posibles accesos no autorizados.
- **Backup:** Proceso de hacer copias de seguridad de los datos almacenados en un sistema para protegerlos contra pérdidas debido a fallos de hardware o errores humanos.
- **Cifrado:** Proceso de convertir información en un formato ilegible para personas no autorizadas, asegurando que solo las personas con la clave adecuada puedan acceder a los datos.
- **Monitoreo de logs:** Revisión y análisis de los registros (logs) generados por los sistemas para detectar comportamientos sospechosos o actividades no autorizadas.
- **CSIRT (Computer Security Incident Response Team):** Equipo encargado de gestionar y responder a incidentes de seguridad informática, como ciberataques o vulnerabilidades detectadas.
- **Redundancia:** Diseño de sistemas que incluye componentes duplicados para asegurar que, en caso de fallo de uno de ellos, el sistema continúe funcionando sin interrupciones.

- **Man-in-the-Middle (MITM):** Tipo de ataque donde el atacante intercepta y posiblemente modifica la comunicación entre dos partes sin que estas lo sepan.
- **Seguridad perimetral:** Conjunto de medidas de seguridad implementadas en los puntos de entrada de una red para protegerla de accesos no autorizados.

Referencias Bibliográficas

Acuerdo-No.-006-2021-Politica-de-Ciberseguridad (2022).

Aguilera López, P. (2010). *Seguridad informática - Purificación Aguilera López - Google Libros* (Editex). https://books.google.es/books?id=Mgvm3AYIT64C&printsec=frontcover&hl=es#v=twopage&q&f=false

Alfonso Gimeno, V. (2010). La influencia de las nuevas tecnologías de la información y las comunicaciones y su repercusión en las estrategias empresariales: La banca online y su aplicación en las cooperativas de crédito. In *TDX (Tesis Doctorals en Xarxa)*. https://www.tdx.cat/handle/10803/52170

Alshathri, S., Alrashidi, E., Albawardi, N., Almojel, H., & Jamail, N. S. M. (2022). Improvement Of The CIA Triad For Al-Rajhi Online Banking System. *Proceedings - 2022 5th International Conference of Women in Data Science at Prince Sultan University, WiDS-PSU 2022*, 67–69. https://doi.org/10.1109/WIDS-PSU54548.2022.00025

Banco Central del Ecuador. (2022, August 25). *Todo lo que no sabías sobre las cooperativas en Ecuador*. https://www.bce.fin.ec/educacion-financiera/articulos/todo-lo-que-no-sabias-sobre-las-cooperativas-en-ecuador

Banco Internacional. (2021, February 5). *¿Qué es y cómo funciona el sistema financiero ecuatoriano?* https://www.bancointernacional.com.ec/que-es-y-como-funciona-el-sistema-financiero-ecuatoriano/

COAC Mercedes Cadena LTDA. (2007a). *ASAMBLEA GENERAL DE REPRESENTANTES CONSEJO DE VIGILANCIA CONSEJO DE ADMINISTRACIÓN GERENCIA GENERAL ORGANIGRAMA ESTRUCTURAL*.

COAC Mercedes Cadena LTDA. (2007b). CARTA CORPORATIVA. *Cooperativa de Ahorro y Credito Mercedes Cadena LTDA.*

Comisión Interamericana de Telecomunicaciones - CITEL. (2009, September). *Gestión de riesgos de seguridad*. https://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp

Díaz, G. D. O. (2004). *Seguridad en las comunicaciones y en la información*. UNED.

ESGinnova Group. (2021, August 26). *Metodología NIST SP 800 – 30 para el análisis de Riesgos en SGSI*. https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/

Infórmate de riesgos - Pirani. (2024, February 20). *Etapas para la gestión de riesgos de ciberseguridad*. LinkedIn. https://www.linkedin.com/pulse/etapas-para-la-gesti%C3%B3n-de-riesgos-ciberseguridad-pirani-8qkcc/?originalSubdomain=es

Jaya Putra, S., Nur Gunawan, M., Falach Sobri, A., Muslimin, J. M., Amilin, & Saepudin, D. (2020). Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. https://doi.org/10.1109/CITSM50537.2020.9268845

Linares Lizarazo, Y. (2018). *¿Cómo estamos en ciberseguridad nacional e internacional, su gestión de riesgos y tendencias?* http://repository.unipiloto.edu.co/handle/20.500.12277/4653

Moreno García, M. (2022). *Gestión de incidentes de ciberseguridad*. RA-MA Editorial. https://www.digitaliapublishing.com/a/116384

Ramos Mera, J. M. (2020). Delitos contra la seguridad de los activos de los sistemas de información y comunicación en el Ecuador. *Corporación de Estudios y Publicaciones.*, 18–33. https://elibro.net/es/lc/uta/titulos/171995

Reglamento - 2016/679 - EN - GDPR - EUR-Lex (2016). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Reglamento a Ley Orgánica de Protección de Datos Personales - LOPDP, 33 (2021). https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

Reglamento General a La Ley Orgánica Para La Optimización y Eficiencia de Trámites Administrativos (2018). https://www.gob.ec/regulaciones/reglamento-general-ley-organica-optimizacion-eficiencia-tramites-administrativos

Resolución No. 521-2019-F (2019). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.seps.gob.ec/wp-content/uploads/521-2019-F.pdf

Resoluciones de Entidades Del Sector Financiero Popular y Solidario - Superintendencia de Economía Popular y Solidaria - SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 (2022). https://www.seps.gob.ec/resoluciones-de-entidades-del-sector-financiero-popular-y-solidario/

Superintendencia de Bancos. (2021, October 21). *Acciones de la Super de Bancos frente a Ciberataque de entidad controlada - Superintendencia de Bancos*. https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada/

Thakare, S. V., & Gore, D. V. (2014). Comparative study of CIA and revised-CIA algorithm. *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, 713–718. https://doi.org/10.1109/CSNT.2014.150

ANEXOS

ANEXO A

CACME AGENCIA MATRIZ ATUNTAQUI | Cooperativa de Ahorro y Crédito

Msc. Marcelo Guamán

GERENTE GENERAL

Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA

Calle Pérez Muñoz y Rio Amazonas

Atuntaqui, Imbabura

0991238953

Coac.mercedescadena@gmail.com

16 de octubre de 2023

Sr. Marlon Ipiales

Estudiante de Ingeniería en Telecomunicaciones

Universidad Técnica del Norte

Ibarra, Imbabura

Estimado Sr. Ipiales,

Es un placer dirigirme a usted en respuesta a su solicitud para llevar a cabo su investigación de trabajo de grado en la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA. Estamos entusiasmados por la oportunidad de colaborar en su proyecto de investigación titulado "Evaluación de Riesgos en la Infraestructura Crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA para la Mitigación de Amenazas Apoyado en la Metodología de la NIST SP 800 – 30".

Hemos revisado con atención su propuesta de trabajo de grado y reconocemos la importancia y relevancia de su investigación. La seguridad y la continuidad de nuestras operaciones son fundamentales para nuestra cooperativa, y entendemos que su trabajo podría aportar conocimientos valiosos en este ámbito.

Por lo tanto, nos complace brindarle la autorización para realizar su investigación en nuestras instalaciones. Le proporcionaremos acceso a la infraestructura crítica, los recursos necesarios y el apoyo que pueda requerir durante su proceso de investigación. Estaremos encantados de asignar un punto de contacto en nuestra cooperativa para ayudarlo en cualquier consulta o solicitud que pueda tener.

Le pedimos que se comunique con su respectivo director de trabajo de grado para coordinar los detalles específicos de su proyecto, incluyendo fechas de inicio y finalización, así como cualquier requisito adicional que debamos tener en cuenta.

CACME
AGENCIA MATRIZ ATUNTAQUI
Cooperativa de Ahorro y Crédito

Esperamos que esta colaboración sea beneficiosa tanto para usted como para la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA. Le deseamos mucho éxito en su investigación y estamos seguros de que sus hallazgos serán valiosos.

Si tiene alguna pregunta o necesita más información, no dude en ponerse en contacto con nosotros. Esperamos con interés trabajar juntos en este proyecto.

Atentamente,

Msc. Marcelo Guamán
GERENTE GENERAL
Coac Mercedes Cadena LTDA
Ecuador-Chimborazo-Guamote
0991238953
coac.mercedescadena@gmail.com

Cooperativa de Ahorro y Crédito Mercedes Cadena
CACME
MATRIZ ATUNTAQUI

ANEXO B

CACME | Cooperativa de Ahorro y Crédito

Estimado

Ipiales Jingo Marlon Emanuel

Nos complace expresar nuestro interés en permitir el desarrollo de su trabajo de integración curricular en nuestra empresa. Reconocemos la importancia de la investigación académica y nos complace brindarle la oportunidad de llevar a cabo su trabajo de integración curricular en un entorno empresarial.

Por medio de la presente, me complace otorgarle el permiso para llevar a cabo su trabajo de interacción curricular en referencia a la aplicación de metodologías de ciberseguridad para la mitigación de vulnerabilidades y amenazas en la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA. Reconocemos y apoyamos la importancia de la investigación académica, y nos complace brindarle la oportunidad de realizar su trabajo dentro de nuestras instalaciones.

Entendemos que, en este momento, aún no ha definido completamente el tema de su trabajo. No obstante, le permitimos utilizar nuestros recursos y llevar a cabo su investigación en nuestra institución hasta que logre determinar y establecer de manera definitiva el tema de su trabajo.

Quedamos a su disposición para cualquier consulta adicional.

Atentamente,

Firmado electrónicamente por:
SEGUNDO MARCELO
GUAMAN TENE

Marcelo Guamán
GERENTE GENERAL
Coac Mercedes Cadena
Ecuador-Chimborazo-Guamote
0991238953
coac.mercedescadena@gmail.com

ANEXO C

CACME
Cooperativa de Ahorro y Crédito

Control:	Protección de datos y privacidad		
Descripción:	La protección de datos y privacidad son componentes críticos de la seguridad de la información.		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X	X	X	
Observaciones:	La institución cuenta con estrategias básicas de protección de datos y privacidad, al igual que el tipo de información que maneja que es confidencial correspondiente a datos internos como socios y clientes, la cual cada una contiene diferentes procesos y transacciones, Sin embargo en mejor concepto esta maneja información Pública, Sensible, Privada y Confidencial.		

Responsable a cargo:

Rango: Jefe de Procesos

Nombre: Andrea Mota Bonilla Velasquez

Firma: Bonilla

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Aspectos organizativos de la Seguridad de la Información		
Descripción: Este control tiene la finalidad de incluir dentro de los procesos de servicios de la institucion, la seguridad de la informacion. Uno de estos aspectos es el establecer responsabilidades y funciones que ayuden a manejar el servicio basado en la seguridad de la informacion.			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
	X		
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X		X	
Observaciones: Datos del contrato de los empleados existen funciones establecidad, pero pocas estan referidas a colaborar con la seguridad de la informacion; por lo que no existe un departamento a cargo de la seguridad o de tecnologia de la informacion, este trabajo por lo general lo respalda su jefe de procesos.			

Responsable a cargo:

Rango: Sefe de Process

Nombre: Andersa Mateo Banila Velasquez

Firma: Banilla

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Políticas de seguridad		
Descripción:	Las políticas de seguridad son documentos en los que se publican de manera formal por parte del comité administrativo de la institución con instrucciones globales, para su respectivo cumplimiento en todas las áreas que se crea necesario.		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
	X		
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X	X		
Observaciones:	Existen características de la seguridad de la información que no se encuentran respaldadas por una política de seguridad y en otros casos la información no se encuentra actualizada.		

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Jadersen Mateo Bonilla Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Contacto con las autoridades		
Descripción: Se debe establecer contactos apropiados con las autoridades correspondientes a la zona donde se encuentra la institucion, en esta lista se incluyen las números de emergencia, servicios de GADS y proveedores de internet, asi como ayuda de asistencia técnica.			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
	X		
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
		X	
Observaciones: La institucion cuenta con los números de contactos con autoridades y servicios, pero no se encuentran en una lista de acceso rapido.			

Responsable a cargo:

Rango: Sefe de procesos

Nombre: Andrea Nataly Bonilla Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Contactos con grupos de interes personal		
Descripción:	Se debe contemplar una lista de contactos con grupos, foros, empresas o instituciones especializadas en la seguridad informatica.		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
	X		
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
		X	
Observaciones:	La institucion cuenta con contactos de grupos de interés especial pero no se encuentran en una lista de acceso rapido, por lo que requiere igualmente un departamento de TI y para problemas de seguridad de la informacion un departamento que administre el mismo o aparte.		

Responsable a cargo:

Rango: Sefe de process

Nombre: Anderson Mateo Baulla Delasgar

Firma: Baullex

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Uso de dispositivos para movilidad		
Descripción: Se debe tener cuidado al usar dispositivos móviles en lugares públicos, salas y otras áreas de reuniones no protegidas.			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
	X		
Observaciones: La institucion tiene una politica simple para el uso de dispositivos para movilidad, junto con un plan de actualizacion de claves y administracion de las mismas.			

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Andersa Maria Bonilla Velasquez

Firma: Bonillas

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Teletrabajo		
Descripción: Se refiere al uso de dispositivos de la institución fuera de la infraestructura. Estos dispositivos no deben contener información importante para la organización, solo lo escencial para cumplir su trabajo. Claro que tambien se puede cumplir con el trabajo por medio de redes privadas virtuales (VPN)			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
	X		
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X	X	X	
Observaciones: La institucion tiene restringido la salida de dispositivos de la institucion, debido al tipo de actividades que realiza. Sin embargo, se realizan algunas actividades por medio de VPNs para realizar ciertas actividades, pero estas actividades la realizan solo personal seleccionado como el jefe de procesos, negocios o gerencia, sin embargo el jefe de procesos menciona problemas de navegacion incluso dentro de la institucion debido a no tener una jerarquia de uso de ancho de banda.			

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Anderson Mateo Bonilla Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Investigacion de antecedentes		
Descripción: Se debe realizar controles de verificación a fondo sobre todos los candidatos para el empleo y contratistas; pero esto se debe llevar a cabo de acuerdo con las leyes, regulaciones y ética pertinente. Esto ayuda a mitigar y detectar posibles riesgos internos con el departamento de Talento Humano.			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
	X		
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X	X		
Observaciones: Como parte de la institucion esta cuenta con un plan de contratación adecuado y una prueba para calificar la capacidad del personal, claro que tienen departamento de talento humano pero no tienen o piden experiencia en sistemas de informacion puesto que no tienen departamento alguno al cual dirigirse.			

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Andrea Mateo Bonilla Velasquez

Firma: Bonilla

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Terminos y Condiciones de Contratación		
Descripción: Como parte de sus obligaciones de contratación a empleados debe estar de acuerdo a los terminos y obligaciones de la institucion.			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
	X		
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X	X		
Observaciones: La institucion cuenta con un plan de terminos y condiciones de contratación que incluye tambien terminos en seguridad de la informacion para proteger a la institucion.			

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Andrea Vele Banulo Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Responsabilidades de gestión		
Descripción:	La administracion debe exigir a los empleados y contratistas la aplicacion de politicas y procedimientos de seguridad.		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
	X		
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X			
Observaciones:	La organización cuenta con un departamento de cumplimiento que se encarga de la gestión basado en su reglamento interno, este departamento es el comité de cumplimiento, pero se valida que si requiere de un departamento de TI para una mejor gestion es su infraestructura.		

Responsable a cargo:

Rango: Sefe de procesos

Nombre: Anderson Mote Benitez Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Concientizacion y Capacitacion de Seguridad de la Informacion		
Descripción:	Todos los empleados de la institucion y en su caso contratista y usuarios pertinentes, deben recibir una formación adecuada sobre la informacion sensible y actualizacion en las politicas y procedimientos de la institucion en materia de la seguridad de la informacion		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
			X
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
			Refuerzos
Observaciones:	La institucion carece de capacitaciones sobre la importancia de la seguridad de la información		

Responsable a cargo:

Rango: Jefe de Procesos

Nombre: Andersan Mateo Bonilla Velasquez

Firma: Bonilla

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Auditorias y Control de Cumplimientos		
Descripción:	Las auditorias internas y revisiones de cumplimientos son esenciales para asegurar la efectividad de los controles en cuanto a seguridad de la información		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
			X
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
			Control de auditorias
Observaciones:	La institucion no cuenta con un programa de additorias o revisión de cumplimiento en cuanto a seguridad de la informacion.		

Responsable a cargo:

Rango: Jefe de Procesos

Nombre: Andersan Mateo Bonilla Velasquez

Firma: Bonilla

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Levantamiento de información sobre activos		
Descripción: Hace referencia a un inventario detallado y la clasificación de activos que son fundamentales para la gestión de riesgos			
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
		X	
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
X			
Observaciones: La empresa no cuenta con un levantamiento de información sobre activos, lo que representa un riesgo a la seguridad de la información. Dicha actividad toma mas lugar la institución que proporciona servicios de tecnología a la cooperativa.			

Responsable a cargo:

Rango: Jefe de Procesos

Nombre: Antesan Mateo Bonilla Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

CACME
Cooperativa de Ahorro y Crédito

Control:	Gestión de incidentes y continuidad del negocio		
Descripción:	La capacidad de responder a incidentes y asegurar la continuidad del negocio es crucial para la resilencia organizacional.		
Estado:	**Aplicado**	**Se puede mejorar**	**No aplicado**
			X
Clasificado como:			
Fortaleza	**Oportunidad**	**Debilidad**	**Amenaza**
X			
Requerimientos de seguridad implicados			
Integridad	**Confidencialidad**	**Disponibilidad**	**Otros**
			Soporte ante incidentes
Observaciones:	La institucion no cuenta con un plan que actue ante las incidentes que detengan la continuidad del negocio o los servicios, en el cual puede verse afacto por ciberataques, errores humanos, fallas tecnicas o desastres naturales.		

Responsable a cargo:

Rango: Jefe de Procesos

Nombre: Anderson Mateo Benitez Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

ANEXO D

CACME
Cooperativa de Ahorro y Crédito

Control:	**Anexo de valoraciones de impacto y probabilidad de riesgo de activos de la COAC Mercedes Cadena LTDA.**

Descripción: Con base en la descripción de las siguientes tablas (Tabla 1 y Tabla 2) de los niveles de probabilidad e impacto presentados en el análisis de riesgos, se lleva a cabo la identificación de los activos, asignándoles su correspondiente valor en términos de impacto y probabilidad.

Tabla 1
Descripción de los niveles de probabilidad en el análisis de riesgos.

Cualitativo	Cuantitativo	Descripción
Muy probable	1	Ocurre en casos excepcionales
Improbable	2	Poco probable, pero podría ocurrir en algún momento
Posible	3	Moderadamente probable, podría ocurrir de vez en cuando
Probable	4	Probable, ocurrirá en varias ocasiones
Muy probable	5	Muy probable, ocurrirá en la mayoría de las ocasiones.

Nota. Los valores en la tabla representan los niveles de probabilidad que se utilizan para calcular el riesgo.

Tabla 2
Descripción de los niveles de impacto en el análisis de riesgos.

Cualitativo	Cuantitativo	Descripción
Insignificante	1	Consecuencias mínimas, sin impacto significativo.
Menor	2	Consecuencias menores, poco impacto en la operación.
Moderado	3	Impacto notable, pero manejable sin intervención externa.
Mayor	4	Impacto severo, requiere intervención significativa.
Catastrófico	5	Impacto crítico, amenaza la continuidad de la operación.

Nota. Los valores en la tabla representan los niveles de impacto que se utilizan para calcular el riesgo.

Activo	Impacto	Probabilidad
Maquinas personales	3	3
Switch de Conmutación no administrable	3	4
Almacenamiento de Video Vigilancia	3	3
Cámaras de Vigilancia	4	1
Servidor Dell PowerEdge T150	5	4
Switch TP-Link TL-SG1024D	4	4
Router TP-Link Inalámbrico	3	1
S.O. Windows 10	4	3
WinSPC	4	4
LogMeIn Hamachi	5	4
PuTTY	5	4
AFC.2023	5	5
MySQL	5	5

Observaciones: Se valida que los activos con mayor grado de criticidad son el Servidor Dell PowerEdge T150, el Switch TP-Link TL-SG1024D, PuTTY y MySQL.

Responsable a cargo:

Rango: Jefe de procesos

Nombre: Anderson Mateo Bonilla Velasquez

Firma:

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

ANEXO E

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 1 Inmediata (1 - 2 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	Máquinas personales (Windows 10)	Configuración de antivirus	Verificar que el antivirus está actualizado y funcionando	NO	-Simulacion -Documentacion	Se valida que no poseen un antivirus certificado, se recomienda el uso de antivirus confiables
2	AFC.2023	Configuración de software de gestión de contraseñas	Verificar que el software de contraseñas está instalado y funcionando	SI	-Simulacion -Documentación	El gestor de contraseñas es eficiente para el resguardo de varias contraseñas
3	MySQL	Restricción de instalación de software no autorizado	Intento de instalación de software no autorizado	SI	-Simulacion -Documentación	Se valida que una buena administracion de PCs y usuarios tiene mejor gestion para la instalacion de apps no deseadas

Firma Estudiante

Firma Jefe de Procesos

Firma Tutor

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Checklist Fase 2 Corto Plazo (2 - 3 Meses)

Atuntaqui, 6 de junio del 2025

Unidad/empresa/beneficiarios: Cooperativa de Ahorro y Credito Mercedes Cadena LTDA
Estudiante: Ipiales Jingo Marlon Emanuel
Validacion de Jefe de procesos: Ing. Anderson Bonilla MSc.
Tutor: Ing. Fabián Cuzme MSc.

N°	ACTIVO	CONTROL IMPLEMENTADO	PRUEBA VERIFICACION	CUMPLE (SI / NO)	MEDIO DE VERIFICACIÓN	OBSERVACIONES
1	Switch TP-Link TL-SG1024D	Auditorías de configuración	Verificar la configuración de la red y el control de acceso	SI	-Simulacion -Documentacion	Se valida que la aplicacion de VLANs y Politicas de Qos existe eficiencia en el trafico
2	LogMeIn Hamachi	Configuración de autenticación basada en claves seguras	Intento de conexión con credenciales no autorizadas	SI	-Simulacion -Documetacion	El gestor de contraseñas de codigo abierto resulta ser eficiente
3	Servidor Dell PowerEdge T150	Configuración de redundancia de UPS	Verificación de que el sistema UPS está correctamente configurado	NO	-Simulacion -Documentacion	Se valida que su servidor tiene su UPS para una funcion continua pero se recomienda uno de mejor capacidad

Firma Estudiante

Firma Jefe de Procesos

CACME
Cooperativa de Ahorro y Crédito
DEPARTAMENTO DE PROCESOS

Firma Tutor

ANEXO F

Atuntaqui, 12 de julio de 2025

Ingeniero Anderson Bonilla

Jefe de Procesos

Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda.

Presente. -

Asunto: Entrega formal del Plan Integral de Ciberseguridad y Manual de Procesos basado en la metodología NIST SP 800-30

Estimado Ingeniero Bonilla:

Mediante la presente, una vez concluido el trabajo titulado "Evaluación de riesgos en la infraestructura crítica de la Cooperativa de Ahorro y Crédito Mercedes Cadena LTDA para la mitigación de amenazas apoyado en la metodología de la NIST SP 800 – 30." me permito hacer entrega formal de los siguientes documentos desarrollados como parte de mi trabajo académico en la carrera de Ingeniería en Telecomunicaciones:

- Plan Integral de Ciberseguridad basado en la metodología NIST SP 800-30
- Manual de Procesos para el Plan Integral de Ciberseguridad

Ambos documentos tienen como propósito aportar herramientas técnicas que contribuyan al fortalecimiento de la gestión de riesgos tecnológicos y a la protección de los activos críticos de la Cooperativa de Ahorro y Crédito Mercedes Cadena Ltda.

Quedo atento a cualquier observación que estime pertinente y agradezco de antemano la atención brindada. brindada.

Atentamente,

Marlon Ipiales

Firma: _____

Estudiante de la Carrera en de Ingeniería en Telecomunicaciones.

Recibí conforme:

Firma: _____

Nombre: Ing. Anderson Bonilla

Cargo: Jefe de procesos

Fecha: 12 de julio del 2025

CACME Cooperativa de Ahorro y Crédito

DEPARTAMENTO DE PROCESOS