

Área de Conocimiento de Tecnología de la
Información y Comunicación

“Propuesta de plan de contingencia para garantizar la continuidad del servicio de internet antes posibles fallas en COOPACRESMHA sucursal San Juan de la Concepción”

Trabajo Monográfico para optar al título de
Ingeniero de Sistemas

Elaborado por:

Br. Bryan Alonso
Canales Levy
Carnet: 2011-37279

Br. Martha Jeanette
Mercado Calero
Carnet: 2002-14751

Br. Claudia Patricia
Romero Carrión
Carnet: 2003-12151

Tutor:

MSc. Mario José
Selva Mendoza

06 de mayo de 2026
Managua, Nicaragua

Managua 09 de Marzo del 2026

Msc. Claudia Lucia Benavidez Rugama
Directora Área de Conocimiento de Tecnología
De la Información y Comunicación
UNI
Su despacho

Estimada Msc. Claudia Benavidez:

Reciba un cordial Saludo, por medio de la presente le comunico que en mi calidad de tutor de trabajo monográfico hago constar que he acompañado y asesorado en el proceso de investigación realizado por los Bachilleres de la carrera de Ing. De Sistemas

Br. Martha Jeanette Mercado Calero **carnet** (2002-14751)

Br. Brayan Alonso Canales Levy **carnet** (2011-37279)

Br. Claudia Patricia Romero Carrión **carnet** (2003-12151)

El presente trabajo titulado: **“Propuesta de plan de contingencia tecnológico para la continuidad del servicio de Internet ante fallas de conectividad en Cooperativa COOPACRESMHA Sucursal San Juan de la Concepción”**. ha sido desarrollado conforme a los lineamientos metodológicos establecidos, cumpliendo con los requisitos académicos exigidos por la institución.

En virtud de lo anterior, considero que el trabajo reúne las condiciones necesarias para ser presentado, evaluado y defendido ante el jurado correspondiente.
Se extiende la presente para los fines que se estimen convenientes.

Atentamente

Mcs. Mario José Selva Mendoza
Docente Tutor



Dirección de Área de
Conocimiento de Tecnología
de la Información y Comunicación

Managua, 26 de enero 2026

Br. Bryan Alonso Canales Levy 2011-37279
Br. Martha Jeanette Mercado Calero 2002-14751
Br. Claudia Patricia Romero Carrión 2003-12151

Egresados Programa académico Ingeniería de Sistemas
Sus manos.-

Estimados Egresados:

Reciban cordiales saludos y éxito en sus actividades.

Por medio de la presente, les comunico la aprobación del trabajo monográfico titulado: **"Propuesta de plan de contingencia para garantizar la continuidad del servicio de internet antes posibles fallas en COOPACRESMHA sucursal San Juan de la Concepción"**, el cual cumple con los requisitos establecidos en el capítulo II de la normativa de trabajos monográficos de la UNI como forma de culminación de estudios, por lo que queda oficialmente aprobado por esta Dirección.

El docente responsable de acompañarle en el proceso de desarrollo de su tema monográfico es el MSc. Mario José Selva Mendoza.

A partir de la fecha de aprobación, tienen como máximo seis meses para realizar el trabajo monográfico incluyendo la defensa.

Atentamente,


MSc. Claudia Lucía Benavidez Rugama
Directora Área de Conocimiento de
Tecnología de la Información y Comunicación



Cc. MSc. Mario José Selva Mendoza – Tutor
MSc. Luisa Massiel Mercado Gutiérrez - Secretaria Académica.
Archivo DACTIC.

Móvil: (505) 8889 0903

Recinto Universitario Simón Bolívar
Avenida Universitaria,
Managua, Nicaragua,
Apdo. 5595

claudia.benavidez@dactic.uni.edu.ni
www.uni.edu.ni

DEDICATORIA

A Dios, por brindarme la vida, la salud y la fortaleza necesaria para culminar esta etapa tan importante de mi formación profesional.

A mi madre, por su apoyo incondicional, por motivarme constantemente y enseñarme que nunca es tarde para alcanzar nuestras metas.

A mi esposo, por su comprensión, paciencia y respaldo durante este proceso, siendo un pilar fundamental en esta etapa de mi vida.

A mis hijos, quienes son mi mayor motivación e inspiración para seguir adelante. Este logro es también para ustedes, como ejemplo de que con esfuerzo, perseverancia y determinación se pueden superar los obstáculos, por difíciles que parezcan, y alcanzar los sueños propuestos.

Ing. Martha Jeanette Mercado Calero

DEDICATORIA

Gracias a Dios porque su luz me guio cada paso de este camino, es la fuerza y el sentido para no rendirme. A ti señor por enseñarme a confiar, por abrirme camino cuando todo parecía cerrado.

A mi hijo por ser el motor de mi vida y fuente de inspiración de mi día a día, a mi esposo que estuvo cada momento conmigo motivándome a superarme y no rendirme este trabajo es también suyo, porque sin su apoyo, paciencia y confianza, nada de esto habría sido posible.

Papa, mama gracias por su amor incondicional, por las palabras de aliento en los momentos difíciles y por celebrar conmigo cada logro.

A mis docentes, por su guía y paciencia; a mis compañeros, por el apoyo mutuo; y a todas las personas que, de una u otra forma, contribuyeron a que este proyecto se hiciera realidad.

A quienes creen que los sueños se alcanzan con esfuerzo y dedicación. Este trabajo es prueba de que cada paso, por pequeño que parezca, nos acerca a nuestras metas."

Ing. Claudia Patricia Romero Carrion.

DEDICATORIA

Este trabajo se lo dedico primeramente a Dios padre por haberme permitido llegar hasta este punto, proveerme salud y las fuerzas necesarias para lograr los objetivos además de su infinito amor,

A mi familia quienes son mi apoyo, sustento y mayor ejemplo de esfuerzo y entrega total,

A los maestros que durante mi estadía en esta alma mater me han formado no solo profesional sino también como ser humano.

Dedico y agradezco a nuestro tutor Ing. Mario José Selva Mendoza por su paciencia ante nuestras inconsistencias por su valiosa dirección y apoyo en la realización de esta investigación y proyecto finalmente terminado.

Ing. Bryan Alonso Canales Levy

AGRADECIMIENTOS

A la universidad, por brindarnos la oportunidad y formarnos profesionalmente y abrirnos las puertas para culminar esta importante etapa académica, contribuyendo significativamente a nuestro crecimiento personal y profesional.

A la Cooperativa de Ahorro, Crédito y Servicios Múltiples Humberto Aguilar (COOPACRESMHA), por su valiosa colaboración en el desarrollo de este estudio, al permitirnos conocer su historia, trayectoria y funcionamiento, así como por la disposición y apertura brindada para la realización de la investigación.

A los docentes, por compartir sus conocimientos, experiencias y orientaciones a lo largo de mi formación académica, contribuyendo al fortalecimiento de mis capacidades profesionales.

Al tutor o instructor de este trabajo, por su acompañamiento, asesoría y guía durante el desarrollo de la investigación, aportando significativamente a la culminación de este proceso.

Al jurado evaluador, por sus observaciones, recomendaciones y aportes, los cuales permitieron mejorar la calidad del presente estudio.

RESUMEN

El presente estudio tiene como objetivo elaborar una propuesta de plan de contingencia para garantizar la continuidad del servicio de Internet ante fallas de conectividad en la Sucursal San Juan de la Concepción de COOPACRESMHA. La investigación surge a partir de la identificación de una alta dependencia del servicio de Internet en los procesos administrativos, financieros y de atención al cliente, así como de la ausencia de un plan de contingencia formal que permita gestionar de manera oportuna las interrupciones del servicio.

La metodología empleada corresponde a un enfoque descriptivo, basado en el análisis de la situación actual, la identificación de vulnerabilidades y la evaluación de los riesgos asociados a la conectividad.

Como resultado, se elabora una propuesta de plan de contingencia que incluye estrategias, procedimientos y alternativas de respuesta ante fallas de conectividad, tales como mecanismos de respaldo, protocolos de actuación y medidas de recuperación orientadas a minimizar el impacto operativo.

El estudio aporta una solución estructurada que fortalece la capacidad de respuesta de la institución, contribuyendo a la continuidad de sus operaciones y a la gestión eficiente de riesgos tecnológicos.

Palabra clave: Plan de contingencia, continuidad del servicio, conectividad, Internet, gestión de riesgos.

CONTENIDO

I.	INTRODUCCION	1
1.1.	Planteamiento del problema	2
II.	ANTECEDENTES	3
III.	OBJETIVOS	5
3.1.	Objetivo General	5
3.2.	Objetivos Específicos:.....	5
IV.	MARCO TEORICO.....	6
4.1.	Cooperativas.....	6
4.2.	Infraestructura de Red	6
4.3.	Conectividad a Internet.....	7
4.4.	Importancia estratégica de la conectividad a Internet	7
4.5.	Transacciones y Operaciones	7
4.6.	Gestión de Riesgo Tecnológico	8
4.7.	Plan de Contingencia.....	8
4.8.	Continuidad Operativa y del Negocio	9
V.	METODOLOGIA DEL PROYECTO	10
5.1.	Tipo de Estudio.....	10
5.2.	Enfoque y Diseño de la Investigación:.....	10
5.3.	Unidad de Análisis:	12
5.4.	Población:.....	12
5.5.	Muestra:	13
5.6.	Procesamiento y Análisis de la Información	13
5.6.1.	Análisis cualitativo:.....	13
5.6.2.	Análisis cuantitativo:	13
5.7.	Fases de la Metodología de la Investigación.....	14
5.7.1.	Diagnóstico de la Situación Actual	14
5.7.2.	Identificación y análisis de riesgos	14
5.7.3.	Elaboración de la propuesta de plan de contingencia	14
5.8.	Análisis de Resultados	15
VI.	DESARROLLO DEL PROYECTO	17
6.1.	Infraestructura Tecnológica actual:	17

6.1.1.	Enlace de Datos:.....	18
6.1.2.	Computadoras, dispositivos Móviles, Dvr y Control de Asistencia	19
6.1.3.	Equipos de red (routers, switch y cableado estructurado)	21
6.1.4.	Sistemas Eléctricos de soporte.....	23
6.1.5.	El servicio de Internet.....	24
6.2.	Sistemas de Información:.....	25
6.3.	Datos Críticos	26
6.4.	Personal y Roles de Tecnologías de la Información (TI).....	28
6.5.	Proveedores Tecnológicos	29
	Fuente: entrevista al responsable de TI	29
6.6.	Identificación de Activos Informáticos críticos	30
6.7.	Identificación de Amenazas	32
6.8.	Análisis de Vulnerabilidades.....	34
6.9.	Vulnerabilidades en la conectividad a Internet	35
6.10.	Vulnerabilidades operativas y de sistemas	35
6.11.	Vulnerabilidades en la gestión de datos	35
6.12.	Vulnerabilidades organizacionales y de proveedores.....	35
6.13.	Evaluación de Riesgos	37
6.13.1.	 Nivel de Riesgo Crítico	37
6.13.2.	 Nivel de Riesgo Alto	38
6.13.3.	 Nivel de Riesgo Medio	38
6.13.4.	 Nivel de Riesgo Bajo.....	38
6.14.	Análisis de Impacto al Negocio (BIA).....	41
6.15.	Evaluación de Medidas Actuales.....	42
6.15.1.	Existencia y Frecuencia de respaldos (Backups)	43
6.15.2.	Almacenamiento Externo.....	45
6.15.3.	Procedimientos Documentados:.....	46
6.15.4.	Responsabilidades Asignadas.....	47
6.15.5.	Planes de Emergencia Previos.....	48
6.16.	Resultado del Diagnóstico.....	49
6.16.1.	Resultados del Componente Cualitativo	49
6.16.2.	Categorías emergentes	49
6.16.3.	Interpretación cualitativa de hallazgos	50

6.16.4.	Síntesis narrativa por áreas.....	50
6.17.	Resultados del Componente Cuantitativo	51
6.17.1.	Matriz de Riesgo.....	51
6.17.2.	Niveles de impacto y criticidad	51
6.17.3.	Probabilidad de interrupciones.....	52
6.18.	Diagnóstico de Infraestructura Tecnológica	52
6.18.1.	Arquitectura de red actual	52
6.18.2.	Equipos y conectividad.....	53
6.18.3.	Dependencias tecnológicas críticas.....	53
6.18.4.	Riesgos técnicos identificados.....	53
6.18.5.	Capacidad contratada - demanda Real	54
6.19.	Integración e interpretación de Resultados (Diagnostico Final)	55
6.20.	Evaluación Técnica del Servicio de Internet.....	58
6.20.1.	Indicadores Técnicos de Conectividad	58
6.20.2.	Prueba de Conectividad Interna (Latencia LAN/ E. CENTRAL)	59
6.21.	Formulación de Propuesta de plan de Contingencia Sucursal San Juan	60
6.21.1.	Propósito del plan	60
6.21.2.	Alcance del Plan de Contingencia	61
6.22.	Objetivo del Plan de Contingencia	63
6.22.1.	Objetivo General	63
6.22.2.	Objetivos Específicos	63
6.23.	Modelo General de Gestión de Contingencias (BCM)*	64
6.24.	Escenarios de Activación del plan	66
6.25.	Prioridad de Procesos Críticos (BIA Integrado)	68
6.26.	Estrategias de Continuidad del Servicio en COOPACRESMHA	70
6.27.	Procedimientos Operativos del Plan	73
6.27.1.	Protocolo de Activación del plan de Contingencia.....	74
6.27.2.	Protocolo de Comunicación de un plan de contingencia.....	75
6.27.3.	Protocolo de Recuperación del Plan de Contingencia.	76
6.27.4.	Protocolo de Restablecimiento	78
6.28.	Roles Y Responsabilidades (RACI)	79
6.29.	Niveles de Activación del Plan de Contingencia TI.....	81
6.30.	Plan de Comunicación durante Incidentes.....	81

6.31.	Plan de Pruebas y Simulacros del Plan de Contingencia TI	83
6.32.	Plan de Mantenimiento y Actualización del Plan de Contingencia TI	84
6.33.	Indicadores de Desempeño (KPIs) del Plan de Contingencia TI	86
6.34.	Análisis de Costo Beneficio del Plan de Contingencia Informático	87
6.34.1.	Cálculo de Costos Estimados	89
6.34.2.	Cálculo de Mano de Obra	90
6.35.	Plan de Implementación	90
6.35.1.	Presupuesto del Plan de Contingencia	92
6.35.2.	Cronograma de Ejecución	93
VII.	CONCLUSIONES	94
VIII.	RECOMENDACIONES	95
IX.	REFERENCIAS BIBLIOGRAFICAS	96
X.	ANEXOS	98
10.1.	Punto de Estudio	98
10.2.	Infraestructura Tecnológica Actual de COOPACRESMHA	100
10.3.	Propuestas de mejoras en Infraestructura y Aumento de Internet.....	107

I. INTRODUCCION

En la actualidad, el acceso a Internet se ha consolidado como un recurso esencial para el funcionamiento de las organizaciones, especialmente en el sector financiero, donde permite la ejecución de transacciones en tiempo real, el acceso a sistemas centralizados y la atención oportuna a los usuarios.

En un entorno cada vez más dependiente de la tecnología, las organizaciones requieren implementar estrategias que les permitan garantizar la continuidad de sus operaciones ante posibles interrupciones. En este contexto, la gestión de contingencias adquiere un papel fundamental al permitir anticipar y responder ante fallas en los servicios tecnológicos.

COOPACRESMHA (Es una Cooperativa de Ahorro, Crédito y Servicios Múltiples Humberto Aguilar), fundada el 12 de septiembre de 1964, es una institución de carácter cooperativo orientada a promover el desarrollo económico y social de sus asociados mediante la prestación de servicios financieros.

A lo largo de su trayectoria, esta cooperativa ha consolidado su presencia en distintas localidades, tales como San Marcos, Masaya, Ticuantepe y Masatepe, entre otras. Para efectos del presente estudio, la investigación se delimita a la Sucursal San Juan de la Concepción. ubicada del estado Harold Rosales 1 cuadra al sur y 30 varas al oeste. Durante el diagnóstico preliminar, se identificó una alta dependencia del servicio de Internet para el desarrollo de sus procesos administrativos, financieros y comerciales.

Asimismo, se evidenció la ausencia de un plan de contingencia formal que permita responder de manera oportuna ante fallas de conectividad, lo que genera retrasos en las operaciones, afectaciones en la atención al cliente y riesgos económicos. Ante esta situación, surge la necesidad de diseñar una propuesta de plan de contingencia orientada a garantizar la continuidad del servicio de Internet, minimizando el impacto de posibles interrupciones y fortaleciendo la capacidad de respuesta de la institución.

La Relevancia del presente estudio radica en la necesidad de fortalecer la resiliencia tecnológica de la cooperativa, permitiendo garantizar la continuidad de sus operaciones ante interrupciones del servicio de Internet, lo cual impacta directamente en la satisfacción de los asociados y la estabilidad financiera institucional.

1.1. Planteamiento del problema

En la Sucursal San Juan de la Concepción de COOPACRESMHA, el servicio de Internet es esencial para el desarrollo de las operaciones administrativas, financieras y de atención al cliente. Sin embargo, se ha identificado una alta dependencia de este servicio sin contar con un plan de contingencia que permita gestionar adecuadamente las fallas de conectividad.

Las interrupciones del servicio generan retrasos en las transacciones, afectaciones en la atención a los usuarios y acumulación de procesos, evidenciando una limitada capacidad de respuesta ante incidentes tecnológicos. A esto se suma la ausencia de mecanismos alternos de conexión y procedimientos definidos, lo que incrementa la vulnerabilidad operativa de la sucursal.

Ante esta situación, el problema central radica en la inexistencia de un plan de contingencia que permita gestionar de manera oportuna y efectiva las fallas de conectividad en la Sucursal San Juan de la Concepción de COOPACRESMHA.

A partir de lo anterior, se plantea la siguiente interrogante de investigación:

¿De qué manera una propuesta de plan de contingencia puede contribuir a la continuidad del servicio de Internet ante fallas de conectividad en la Sucursal San Juan de la Concepción de COOPACRESMHA?

II. ANTECEDENTES

Las Tecnologías de la Información y la Comunicación (TIC) han adquirido un papel fundamental en el funcionamiento de las organizaciones, particularmente en el sector financiero, donde el servicio de Internet constituye un recurso esencial para la ejecución de procesos operativos, administrativos y de atención al cliente. Esta dependencia tecnológica ha generado la necesidad de implementar mecanismos que garanticen la continuidad de los servicios ante posibles interrupciones.

A nivel internacional la **(ISO 22301:2019)**, establece lineamientos para la gestión de la continuidad del negocio, orientados a la implementación de planes de contingencia que permitan a las organizaciones responder de manera oportuna ante eventos que interrumpan sus operaciones. Esta norma promueve la definición de procedimientos, asignación de responsabilidades y el establecimiento de estrategias de recuperación, lo que constituye una base metodológica relevante para el desarrollo de la presente investigación.

En el contexto nacional, durante los eventos sociopolíticos ocurridos en Nicaragua en el año 2018, se registraron interrupciones del servicio de Internet en diversos departamentos, entre ellos Jinotega, Matagalpa, León y Masaya, ocasionadas por daños a la infraestructura de telecomunicaciones.

Ante esta situación, el ente regulador TELCOR implementó un plan de contingencia enfocado en la restauración de los servicios mediante la reparación de infraestructura afectada, la coordinación con proveedores de telecomunicaciones y la activación de mecanismos de respuesta ante emergencias.

Estas acciones evidencian que, a nivel nacional, la interrupción del servicio de Internet es considerada un riesgo crítico que requiere de planificación y estrategias estructuradas para su gestión. Asimismo, demuestran la importancia de contar con medidas anticipadas que permitan reducir el impacto operativo ante fallas en la conectividad.

Por otra parte, en diversas regiones del país se presentan limitaciones en la infraestructura tecnológica, lo que provoca interrupciones frecuentes del servicio debido a factores como fallas en el suministro eléctrico, condiciones climáticas adversas y dependencia de enlaces únicos. Frente a estas situaciones, algunas organizaciones han implementado soluciones como el uso de enlaces alternos, respaldo mediante datos móviles y la aplicación de procedimientos operativos temporales, con el objetivo de mantener la continuidad de sus actividades. Sin embargo, en muchas instituciones estos mecanismos no se encuentran formalmente estructurados dentro de un plan de contingencia, lo que limita la capacidad de respuesta ante fallas del servicio de Internet y aumenta el riesgo de interrupciones prolongadas. En este sentido, se evidencia la necesidad de desarrollar propuestas que permitan gestionar de manera eficiente estas eventualidades y fortalecer la continuidad operativa en organizaciones con alta dependencia tecnológica, como es el caso de COOPACRESMHA, Sucursal San Juan de la Concepción.

III. OBJETIVOS

3.1. Objetivo General

- ✓ Elaborar una propuesta de plan de contingencia para garantizar la continuidad del servicio de Internet ante fallas de conectividad en la Sucursal San Juan de la Concepción de COOPACRESMHA.

3.2. Objetivos Específicos:

- ✓ Analizar la situación actual del servicio de Internet en la sucursal, identificando su nivel de dependencia en los procesos operativos.
- ✓ Identificar las principales vulnerabilidades y causas de fallas de conectividad que afectan la operatividad.
- ✓ Evaluar los riesgos asociados a las interrupciones del servicio de Internet y su impacto en la continuidad de las operaciones.
- ✓ Determinar los recursos, mecanismos y prácticas actuales utilizados para la gestión de fallas en la conectividad.
- ✓ Elaborar la propuesta de plan de contingencia que incluya estrategias, procedimientos y alternativas de respuesta ante fallas de conectividad.

IV. MARCO TEORICO

4.1. Cooperativas.

Las cooperativas son organizaciones de carácter social y económico que buscan satisfacer las necesidades comunes de sus asociados mediante la cooperación, la participación democrática y la ayuda mutua. Estas entidades promueven el desarrollo económico y social a través de la prestación de servicios que benefician directamente a sus miembros.

De acuerdo con (García , 1988) Autor de una Cartilla Titulada Clasificación de las Cooperativas indica que las cooperativas pueden clasificarse según su objeto social y las actividades que desarrollan, destacando aquellas orientadas al sector financiero, como las cooperativas de ahorro y crédito, las cuales ofrecen servicios de captación de ahorro y otorgamiento de créditos

En el contexto de la presente investigación, las cooperativas de ahorro y crédito presentan una alta dependencia de los sistemas tecnológicos y de la conectividad a Internet para la ejecución de sus operaciones, lo que hace necesario implementar mecanismos que garanticen la continuidad del servicio ante posibles fallas.

4.2. Infraestructura de Red

La infraestructura de red comprende el conjunto de componentes físicos y lógicos que permiten la conectividad y el intercambio de información dentro de una organización. Incluye equipos como servidores, routers, switches, así como los sistemas y protocolos que facilitan la comunicación de datos. Según (Stallings , 2013), aborda la infraestructura de red como un ecosistema unificado que integra hardware, software y protocolos para permitir la conectividad y las operaciones de datos.

En las instituciones financieras, esta infraestructura es fundamental para garantizar el funcionamiento de los sistemas transaccionales y la comunicación interna, por lo que cualquier interrupción en su operación puede afectar directamente la continuidad de los servicios.

4.3. Conectividad a Internet

La conectividad a Internet se refiere a la capacidad de los dispositivos y redes para comunicarse e intercambiar información a través de plataformas digitales, utilizando tecnologías alámbricas e inalámbricas.

En el entorno organizacional, el acceso a Internet se ha convertido en un recurso crítico que soporta procesos clave como la ejecución de transacciones, la comunicación con usuarios y el acceso a sistemas de información.

En el caso de las cooperativas financieras, la conectividad es esencial para garantizar la eficiencia operativa, por lo que su interrupción representa un riesgo significativo para la continuidad de las actividades institucionales.

4.4. Importancia estratégica de la conectividad a Internet

La conectividad a Internet constituye un elemento estratégico para las organizaciones, ya que permite optimizar procesos, mejorar la comunicación y facilitar la toma de decisiones basada en información en tiempo real.

De acuerdo con **(Weill & Ross, 2004)**, una infraestructura tecnológica confiable actúa como un habilitador del negocio, al permitir la continuidad de las operaciones y la alineación entre la tecnología y los objetivos organizacionales.

En este sentido, la disponibilidad del servicio de Internet es fundamental para mantener la eficiencia y competitividad de las instituciones financieras, especialmente en contextos donde la digitalización es un factor clave para la prestación de servicios.

4.5. Transacciones y Operaciones

Las transacciones y operaciones representan procesos críticos dentro de las instituciones financieras, ya que garantizan el desarrollo continuo de las actividades económicas y la atención a los usuarios.

La interrupción de estos procesos, causada por fallas en la conectividad, puede generar retrasos, errores operativos y afectaciones en la confianza de los clientes, impactando directamente en la estabilidad y sostenibilidad de la organización.

4.6. Gestión de Riesgo Tecnológico

La gestión del riesgo tecnológico consiste en la identificación, análisis y evaluación de amenazas y vulnerabilidades que pueden afectar los sistemas de información de una organización.

Según **(Stoneburner, Goguen, & Feringa, , 2002)**, este proceso permite determinar el impacto potencial de eventos adversos y establecer estrategias para su mitigación.

Por lo antes expuesto, la interrupción del servicio de Internet representa un riesgo tecnológico que puede afectar la operatividad de la institución, por lo que resulta necesario implementar medidas que permitan anticipar y reducir sus efectos.

4.7. Plan de Contingencia

Un plan de contingencia es un conjunto de estrategias, procedimientos y acciones previamente definidas que permiten a una organización responder ante situaciones imprevistas que afectan su funcionamiento.

Comienzan con una evaluación exhaustiva de los riesgos y amenazas específicas que pueden afectar a la organización, o comunidades, identificando y analizando eventos potenciales como terremotos, inundaciones, incendios o caídas de servicios de internet.

De acuerdo con la Norma **(22301:2019, International Organization for Standardization, 2019)** los planes de contingencia forman parte de la gestión de la

continuidad del negocio, ya que establecen mecanismos para prevenir, responder y recuperarse ante interrupciones.

En el ámbito tecnológico, estos planes permiten mantener la operatividad de los sistemas críticos mediante el uso de alternativas como enlaces de respaldo, procedimientos temporales y estrategias de recuperación.

En el caso de COOPACRESMHA, Sucursal San Juan de la Concepción, la elaboración de una propuesta de plan de contingencia orientada al servicio de Internet permitirá analizar las condiciones actuales de conectividad, identificar vulnerabilidades, evaluar los riesgos asociados y establecer estrategias de respuesta ante fallas, con el fin de contribuir a la continuidad de sus operaciones

4.8. Continuidad Operativa y del Negocio

La continuidad operativa se refiere a la capacidad de una organización para mantener sus funciones esenciales en funcionamiento durante y después de un evento adverso, mientras que la continuidad del negocio constituye un enfoque estratégico más amplio que incluye la planificación, gestión de riesgos y recuperación de los procesos críticos.

Ambos conceptos están estrechamente relacionados, ya que la continuidad operativa representa la ejecución práctica de las estrategias definidas en la continuidad del negocio.

De acuerdo con la norma ISO 22301:2019, la continuidad del negocio permite a las organizaciones anticipar, responder y recuperarse ante eventos disruptivos, garantizando la estabilidad y sostenibilidad de sus operaciones.

En este sentido, la implementación de un plan de contingencia tecnológico contribuye directamente al fortalecimiento de la continuidad operativa, al asegurar la disponibilidad de los servicios esenciales ante fallas en la conectividad.

V. METODOLOGIA DEL PROYECTO

5.1. Tipo de Estudio

La presente investigación se desarrolla bajo un enfoque mixto, permitiendo integrar el análisis cualitativo de la realidad organizacional con la evaluación cuantitativa de los riesgos tecnológicos asociados al servicio de Internet.

Según, **(Hernández, R., Fernández, C., y Baptista, P., 2014)**, el diseño no experimental se caracteriza por analizar los fenómenos en su contexto natural, sin manipulación de variables. En este sentido, el estudio adopta un diseño no experimental, ya que se analiza la situación actual de la conectividad en la Sucursal San Juan de la Concepción de COOPACRESMHA.

Asimismo, el estudio es de tipo transversal, debido a que la recolección de datos se realiza en un único momento del tiempo, específicamente durante el período del 20 al 23 de enero, permitiendo obtener una visión actual del estado de la infraestructura tecnológica y su impacto en las operaciones.

El alcance de la investigación es descriptivo, ya que permite caracterizar las condiciones del servicio de Internet, identificar vulnerabilidades y analizar los riesgos asociados a su interrupción.

Este enfoque metodológico permite sustentar la elaboración de la propuesta de plan de contingencia orientada a garantizar la continuidad del servicio de Internet.

5.2. Enfoque y Diseño de la Investigación:

La presente investigación se desarrolla bajo un enfoque metodológico mixto, el cual permite integrar el análisis cualitativo de la realidad organizacional con la evaluación cuantitativa de los riesgos tecnológicos asociados al servicio de Internet.

La integración de ambos enfoques facilita la comparación de información proveniente de fuentes humanas, técnicas y documentales, fortaleciendo la

confiabilidad del diagnóstico y asegurando que las estrategias propuestas respondan tanto a la realidad operativa de la sucursal como a criterios técnicos de continuidad del negocio.

Según (Roberto Hernández Sampieri, 2014) el diseño no experimental transversal consiste en la recolección de datos en un único momento del tiempo, sin manipulación de variables, con el propósito de describir y analizar los fenómenos en su contexto natural.

El presente estudio adopta un diseño:

- ✓ **No experimental**, ya que no se manipulan variables y se analiza la situación tal como ocurre en la realidad.
- ✓ **Transversal**, debido a que la información se recolecta en un único período de tiempo.
- ✓ **Descriptivo**, porque permite caracterizar las condiciones del servicio de Internet, identificar vulnerabilidades y analizar los riesgos asociados a su interrupción.

La recolección de información se llevó a cabo durante el período comprendido entre el 20 y 23 de enero, etapa en la que se realizó el diagnóstico situacional en la Sucursal San Juan de la Concepción de COOPACRESMHA. Este proceso permitió obtener una visión actual del estado de la infraestructura tecnológica, las prácticas operativas y los mecanismos de gestión del servicio de Internet, constituyendo una “fotografía” del contexto organizacional.

Los registros de eventos ocurridos en períodos anteriores, como interrupciones del servicio o incidentes tecnológicos, fueron utilizados únicamente como antecedentes documentales para el análisis de riesgos, sin formar parte de mediciones longitudinales. Este enfoque metodológico permite sustentar la elaboración de la propuesta de plan de contingencia orientada a garantizar la continuidad del servicio de Internet.

5.3. Unidad de Análisis:

La unidad de análisis está constituida por los procesos tecnológicos, operativos y administrativos que dependen directamente del servicio de Internet en la Sucursal San Juan de la Concepción, incluyendo:

- ✓ Infraestructura de red
- ✓ Equipos de comunicación
- ✓ Proveedores de conectividad
- ✓ Procedimientos operativos ante fallas
- ✓ Gestión del servicio desde el área de TI

La investigación se desarrolló en la Cooperativa de Ahorro, Crédito y Servicios Múltiples Humberto Aguilar (COOPACRESMHA), Sucursal San Juan de la Concepción, la cual constituye el contexto específico de estudio.

5.4. Población:

La población de estudio está conformada por los actores que participan en los procesos relacionados con el uso y gestión del servicio de Internet, incluyendo:

- ✓ Personal del área de informática
- ✓ Personal administrativo
- ✓ Colaboradores operativos
- ✓ Asociados que utilizan servicios digitales

Para la recolección de información se emplearon las siguientes técnicas:

- ✓ Entrevistas semiestructuradas
- ✓ Encuestas estructuradas
- ✓ Observación directa.

5.5. Muestra:

Se empleó un muestreo no probabilístico de tipo intencional, seleccionando a los participantes con base en su conocimiento y relación directa con el objeto de estudio.

La muestra estuvo conformada por:

12 trabajadores (11 encuestados y 1 entrevista al responsable de TI)

50 asociados

5.6. Procesamiento y Análisis de la Información

5.6.1. Análisis cualitativo:

- ✓ Transcripción de entrevistas
- ✓ Codificación temática
- ✓ Categorización de la información
- ✓ Identificación de patrones y problemáticas
- ✓ Triangulación con observación y registros

5.6.2. Análisis cuantitativo:

- ✓ Matriz de riesgos
- ✓ Evaluación de probabilidad e impacto
- ✓ Análisis de criticidad de activos
- ✓ BIA – Análisis de impacto en el negocio

5.7. Fases de la Metodología de la Investigación

5.7.1. Diagnóstico de la Situación Actual

Objetivo

- ✓ Analizar el estado actual del servicio de Internet en la sucursal.

Actividades a Desarrollar

- ✓ Evaluación de infraestructura de red
- ✓ Identificación de procesos dependientes del Internet
- ✓ Observación de prácticas operativas

5.7.2. Identificación y análisis de riesgos

Objetivo:

- ✓ Identificar y evaluar los riesgos que afectan la continuidad del servicio.

Actividades:

- ✓ Identificación de amenazas (fallas técnicas, proveedor, etc.)
- ✓ Evaluación del impacto en las operaciones
- ✓ Aplicación de matriz de riesgos
- ✓ Análisis de criticidad (BIA)

5.7.3. Elaboración de la propuesta de plan de contingencia

✓ Objetivo:

Elaborar una propuesta de plan de contingencia para garantizar la continuidad del servicio de Internet.

Actividades:

- ✓ Definición de estrategias de respuesta
- ✓ Propuesta de mecanismos alternos de conectividad
- ✓ Establecimiento de procedimientos ante fallas
- ✓ Diseño de protocolos de comunicación
- ✓ Recomendaciones técnicas y operativas

5.8. Análisis de Resultados

El análisis de resultados se realizó mediante la integración de la información obtenida a través de entrevistas, encuestas, observación directa y análisis técnico, aplicando un proceso de triangulación metodológica que permitió validar los hallazgos y sustentar la propuesta planteada.

Con el propósito de integrar la información obtenida mediante diferentes técnicas e instrumentos de investigación, se aplicará un proceso de triangulación metodológica que permitirá contrastar datos cualitativos y cuantitativos provenientes de entrevistas, encuestas, observación directa, revisión documental y análisis técnico. A continuación, se presenta la tabla de triangulación utilizada para validar los hallazgos del estudio.

Tabla 1

Triangulación de Datos de la Investigación

Técnica / Método	Fuente de Información	Qué se analizará	Qué permitirá validar	Área relacionada
Observación directa	Procesos diarios en la sucursal	Tiempos de respuesta, interrupciones,	Evidencia operativa de afectación	Cajas y atención al cliente
Encuestas estructuradas	Colaboradores y asociados	Frecuencia de interrupciones percibidas	Tendencias y patrones de impacto	Atención al cliente / asociados
Revisión documental	Registros de incidentes, reportes TI,	Historial de fallas, tiempos de recuperación,	Consistencia entre prácticas documentación formal	TI y gerencia
Matriz de riesgos	Análisis técnico del servicio de internet	Probabilidad e impacto de amenazas tecnológicas	Priorización objetiva de riesgos críticos	Infraestructura TI
BIA (Análisis de Impacto al Negocio)	Procesos operativos dependientes de internet	Nivel de afectación por área, tiempos de tolerancia a la interrupción	Determinación de criticidad de procesos y necesidades	Cajas, crédito, gerencia
Análisis de criticidad de activos	Inventario tecnológico	Dependencia de equipos, sistemas y conectividad	Identificación de activos críticos plan de contingencia	Infraestructura TI

Fuente: Elaboración propia, basada en técnicas de recolección de información y análisis de datos

VI. DESARROLLO DEL PROYECTO

La Cooperativa de Ahorro, Crédito y Servicios Múltiples Humberto Aguilar (COOPACRESMHA), Sucursal San Juan de la Concepción, mantiene una alta dependencia del servicio de internet para la ejecución de sus procesos operativos, administrativos y comerciales. Las fallas ocasionales en la conectividad afectaron el normal desarrollo de sus operaciones, generando retrasos y limitaciones en la atención a los asociados.

En respuesta a esta problemática, se elaboró propuesta para la continuidad del servicio de Internet ante fallas de conectividad en COOPACRESMHA Sucursal San Juan de la Concepción.

El alcance del estudio incluyó el análisis de la infraestructura de conectividad a internet de la sucursal, considerando los componentes tecnológicos relacionados con el acceso, la distribución y la disponibilidad del servicio. Asimismo, se identificaron los riesgos tecnológicos, se diagnosticó el estado actual de la conectividad y se analizaron las vulnerabilidades internas y externas que podrían afectar la continuidad de los procesos comerciales.

6.1. Infraestructura Tecnológica actual:

En el Diagnostico presentado se muestran los resultados del COOPACRESMHA, orientado en evaluar las condiciones actuales de la infraestructura tecnológica y su relación con la continuidad del servicio de Internet.

La información fue obtenida mediante la aplicación de técnicas cualitativas y cuantitativas, tales como entrevistas, encuestas, observación directa, revisión documental y análisis de riesgos.

Los resultados se exponen a través de tablas, con el propósito de identificar las principales debilidades, niveles de afectación operativa y riesgos asociados a posibles

interrupciones del servicio, sirviendo como base para la elaboración de la propuesta de plan de contingencia.

La ausencia de un enlace de respaldo incrementa el nivel de vulnerabilidad de la conectividad y representa un riesgo crítico para la continuidad de los procesos comerciales.

Los Elementos de la infraestructura tecnológica de conectividad a internet evaluados en la Sucursal San Juan de la Concepción fueron los siguientes:

6.1.1. Enlace de Datos:

La Sucursal San Juan de la Concepción cuenta con un único enlace de datos que permite la comunicación con la Oficina Central y el acceso a los sistemas corporativos.

Durante el diagnóstico, se identificó la ausencia de registros formales sobre la frecuencia de interrupciones del servicio. No obstante, a través de entrevistas con el responsable del área de Tecnología de la Información, se evidenció la ocurrencia de al menos un evento reciente de interrupción prolongada, lo cual refleja una limitación en el control y monitoreo del servicio.

Con el fin de evidenciar las interrupciones del servicio de Internet identificadas durante el diagnóstico, a continuación, se presenta el registro de eventos recientes reportados por el área de Tecnología de la Información.

Tabla 2

Registro de interrupciones recientes del servicio de internet

Ubicación	Fecha	Duración de la interrupción	Áreas afectadas	Impacto en la operación
Oficina Central	15/12/2025	8 horas	Todas las áreas	Suspensión de operaciones administrativas y de supervisión
Sucursal San Juan de la Concepción	15/12/2025 16/12/2025	20 horas	Todas las áreas	Interrupción total de los procesos comerciales y atención al cliente

Fuente: Información obtenida mediante entrevista al responsable de TI

Como se observa en la tabla anterior, la interrupción registrada afectó tanto a la Oficina Central como a la Sucursal San Juan de la Concepción, evidenciando una alta dependencia del servicio de Internet para la ejecución de las operaciones institucionales.

En particular, la duración prolongada de la interrupción en la sucursal (20 horas) generó una paralización total de los procesos comerciales y de atención al cliente, lo cual pone de manifiesto la ausencia de mecanismos alternos de conectividad y la necesidad de establecer un plan de contingencia que permita garantizar la continuidad operativa.

6.1.2. Computadoras, dispositivos Móviles, Dvr y Control de Asistencia

A continuación, se detalla la infraestructura tecnológica disponible en las áreas operativas de la Sucursal San Juan de la Concepción, considerando la cantidad de equipos y su nivel de dependencia del servicio de Internet para el desarrollo de los procesos institucionales.

Tabla 3

Distribución de equipos tecnológicos - Impacto operativo

Área / Función	Tipo de equipo	Cantidad	Dependencia de Internet	Impacto ante fallas de conectividad
Área de Cajas	Computadoras de escritorio	2	Alta	Suspensión de atención al cliente
Atención al Cliente	Computadoras de escritorio	2	Alta	Limitación de consulta y atención
Gerencia de Sucursal	Laptop Dell	1	Alta	Dificultad para toma de decisiones y monitoreo de GPS
Promotores y Gestores de Cobro	Teléf. móviles Samsung A34	4	Alta	Imposibilidad de registrar y descargar información de créditos, cobros y ahorros en tiempo real
Promotores y Gestores de Cobro	Computadoras de escritorio	3	Media–Alta	Retrasos en la gestión y consolidación de información financiera, actualización de cartera en disp. móviles
Servicios Financieros	Computadora de escritorio	1	Alta	Atrasos en procesos financieros y generación de reportes
Seguridad	DVR (Sistema de videovigilancia) Hikvision	1	Media	Limitación en la visualización y monitoreo remoto de cámaras

Fuente: Información obtenida mediante observaciones en lugar de trabajo

Con el diagnóstico realizado en las computadoras, dispositivos móviles, sistema de videovigilancia y control de asistencia se evidenció una alta dependencia del servicio de internet para el desarrollo de las diarias de la Sucursal San Juan de la Concepción.

Las fallas en la conectividad impactan directamente en la ejecución de transacciones financieras, la atención al cliente, la gestión de cobros y la supervisión operativa, mientras que en los sistemas de seguridad y control administrativo limitan la supervisión remota y la sincronización de registros. Estos hallazgos confirman que la continuidad de los procesos críticos está estrechamente vinculada a la disponibilidad del servicio de internet.

6.1.3. Equipos de red (routers, switch y cableado estructurado)

La Sucursal San Juan de la Concepción cuenta con equipos de red que permiten la conectividad interna y el acceso a los sistemas institucionales de la cooperativa. Estos equipos constituyen la base de la comunicación entre las áreas operativas y la Oficina Central, por lo que su disponibilidad es crítica para la continuidad del servicio.

Tabla 4

Equipos de red vs impacto operativo

Equipo s	Marca / Modelo	Función	Cantidad	Dependenc ia del servicio	Impacto ante fallas
Router	Huawei / AR611 W	Gestiona el acceso a internet y la comunicación con la Oficina Central y los sistemas corporativos	1	Alta	La falla del router provoca la interrupción total del servicio de internet, operativas.
Switch	CISCO/ S-100- 24	Distribuye la conectividad de red	1 (24 puertos)	Alta	Una falla en el switch genera la pérdida de conectividad interna,
Cableado estructu rado	Cable CAT 5	Interconexión física de los equipos de red y estaciones de trabajo	N/A	Alta	Cualquier falla, en el cableado estructurado puede provocar interrupciones
Punto de acceso (Wi-Fi)	Meraki / MR44	Proporciona conectividad inalámbrica	1	Media–Alta	La indisponibilidad del punto de acceso limita el uso de dispositivos tra

Fuente: Información obtenida mediante observaciones en lugar de trabajo

6.1.4. Sistemas Eléctricos de soporte

Según información obtenida durante la entrevista al responsable de Área de TI, ante eventos de interrupción del suministro eléctrico, la planta eléctrica se orienta a priorizar áreas críticas específicamente Caja y Atención al Cliente, con el objetivo de mantener una operatividad mínima.

Este hallazgo evidencia que el sistema de respaldo eléctrico es limitado y no garantiza la continuidad total de las operaciones durante cortes de energía.

Tabla 5

Evaluación de sistemas eléctricos

Equipos Eléctrico	Marca / Modelo	Tipo de respaldo	Cantidad de equipos	Cobertura operativa	Equipos / Áreas cubiertas	Limitaciones identificadas
Planta eléctrica	Honda / EM 11000	Respaldo central	1	Parcial	Áreas de Caja y Atención al Cliente	No cubre la totalidad de las áreas operativas
UPS	Forza / FDC-RT1000VA	Respaldo por equipo	11	Temporal	Computadoras de escritorio, DVR, reloj biométrico y equipos red	No sostiene la operación durante cortes prolongados
Batería interna de Laptop	DELL / Inspiron 15	Respaldo individual	1	Muy limitada	Laptop de Gerencia Sucursal	Autonomía reducida
Reguladores de voltaje	Tripp Lite	Protección eléctrica	1	Preventiva	Impresora Canon ir1643	No generan energía

Fuente: Información obtenida mediante entrevista al responsable de TI

6.1.5. El servicio de Internet.

Tabla 6

Diagnóstico del servicio de internet y su impacto en los procesos comerciales

Área / Proceso	Uso del Servicio de Internet	Nivel de Dependencia	Impacto ante Interrupción	Frecuencia Estimada	Vulnerabilidad Identificada
Cajas	Acceso a sistemas financieros y transacciones en línea	Alta	Suspensión de operaciones y retrasos en pagos	Media	Dependencia de un único enlace de internet
Atención al cliente	Consultas de cuentas y actualización de datos	Alta	Interrupción de trámites y atención	Media	Falta de enlace de respaldo
Crédito	Evaluación y aprobación de créditos	Alta	Retrasos en análisis y decisiones	Media	Acceso limitado a sistemas en línea
Gestión administrativa	Generación de reportes y registros	Media	Retrasos operativos y administrativos	Media	Monitoreo limitado del servicio
Promotores y gestores de cobro	Descarga y sincronización de información	Alta	Retraso en actualización de datos	Media	Dependencia total de conectividad

Fuente: Información obtenida mediante entrevista al responsable de TI

La matriz evidencia que los procesos comerciales clave presentan un nivel alto de criticidad, debido a su elevada dependencia del servicio de internet y al impacto directo que genera su interrupción. Asimismo, se identificó la ausencia de enlaces alternos y mecanismos de monitoreo, lo que incrementa la exposición al riesgo operativo.

6.2. Sistemas de Información:

En la Investigación se analizaron los principales sistemas de Información utilizados por la cooperativa a continuación se muestra los resultados obtenidos

Tabla 7

Sistema de Información

Sistema de Información	Función Principal	Procesos que Apoya	Dependencia del Internet	Impacto ante caída del servicio
Cartera (Siscomif)	Administración de créditos, pagos, mora y cartera activa	Gestión de créditos, pagos en cajas, reportes financieros	Alta	Retrasos en la actualización de pagos, generación de reportes
Módulo de Ahorros	Gestión de cuentas de ahorro, depósitos y retiros	Atención al cliente, transacciones financieras	Alta	Imposibilidad de realizar operaciones en tiempo real,
Aplicación Tecnomóvil	Gestión de depósitos y recuperación de cartera en campo	Trabajo de promotores y gestores	Alta	Limitación del trabajo en campo y retraso en la sincronización y actualización

Siscomifpic	Administración	Evaluación	Alta	Retrasos en
(Perfil	de información	crediticia, análisis		análisis
Integral del	personal y	financiero,		crediticios,
Asociado)	financiera de	actualización de		
	los asociados	datos		
Tecnocaja	Registro y	Gestión	Media–Alta	Retrasos en el
	control de	administrativa y		registro de
	movimientos	financiera interna		gestiones
	de Caja Chica			aprobación de
				solicitudes
				administrativas

Fuente: Información obtenida mediante entrevista al responsable de TI

De acuerdo a la entrevista realizada con el responsable del área de Tecnologías de la Información, se concluye que los sistemas de información de la cooperativa son esenciales para la continuidad de los procesos operativos, financieros y administrativos. Asimismo, se evidenció que estos sistemas presentan una alta dependencia del servicio de internet, por lo que las interrupciones en la conectividad afectan directamente áreas críticas como cajas, atención al cliente, crédito y gestión administrativa. Esta situación resalta la necesidad de establecer un plan de contingencia que priorice la disponibilidad y recuperación de los sistemas, con el fin de minimizar el impacto de futuras caídas del servicio.

6.3. Datos Críticos

El diagnóstico evidenció que los datos críticos de la cooperativa presentan una alta dependencia de los sistemas tecnológicos y del servicio de internet para su correcta gestión y disponibilidad. Si bien existen mecanismos de respaldo que permiten la recuperación de la información, se identifican vulnerabilidades asociadas a la ejecución manual de los respaldos, la ausencia de ubicaciones alternas y la ocurrencia de inconsistencias en los datos ante caídas de conectividad, lo que incrementa el riesgo para la continuidad operativa.

Tabla 8

Evaluación diagnóstica de los datos críticos y mecanismo de respaldo

Aspecto evaluado	Descripción actual	Frecuencia	Riesgo identificado	Observación diagnóstica
Tipo de datos críticos	Bases de datos financieras, información de asociados, transacciones y reportes	Permanente	Alta dependencia operativa	Información esencial para la continuidad institucional
Políticas de respaldo	Procedimientos definidos y ejecutados por área de TI	Diaria	Dependencia del factor humano	Respaldos realizados de forma manual
Frecuencia de respaldos	Respaldos al cierre de la jornada laboral	Diaria	Pérdida de información reciente	No se realizan respaldos en tiempo real
Almacenamiento de respaldos	Servidores institucionales y discos externos	Permanente	Exposición ante fallas simultáneas	No se identifican ubicaciones alternas, disco guardados en Bóvedas
Recuperación de información	Restauración desde respaldos disponibles	Eventual	Retrasos en la recuperación	Caídas de internet prolongan el restablecimiento

Esta tabla no es de solución, es diagnóstica; muestra cómo están los datos críticos hoy, qué riesgos existen y por qué el servicio de internet es un factor clave en la continuidad.

6.4. Personal y Roles de Tecnologías de la Información (TI)

Tabla 9

Diagnóstico del recurso humano TI

Aspecto evaluado	Descripción actual	Hallazgo del diagnóstico	Impacto en la continuidad operativa
Cantidad de personal TI	2 personas (1 responsable del área y 1 soporte técnico)	Recursos humanos limitados	Riesgo de retrasos en la atención de fallas y sobrecarga operativa
Roles y responsabilidades	Administración de infraestructura,	Roles definidos de forma general	Dependencia de la experiencia individual para la resolución de incidentes tecnológicos.
Nivel de capacitación técnica	Experiencia laboral acumulada y capacitaciones	Capacitación técnica existente, concentrada en personal clave	Capacidad de respuesta condicionada a la disponibilidad del personal capacitado
Procedimientos de respuesta ante incidentes	No existen procedimientos formales ni documentados	Atención de incidentes de forma reactiva	Falta de respuesta estandarizada ante caídas del servicio de internet
Dependencia de personal clave	Alto nivel de dependencia	Conocimiento no documentado ni transferido	Vulnerabilidad ante ausencias imprevistas o contingencias mayores

Fuente: Información obtenida mediante entrevista realizadas TI

Con la presente tabla se evidenció que, aunque la cooperativa cuenta con personal de TI con experiencia y capacitación técnica, la limitada cantidad de recursos humanos, la ausencia de procedimientos formalizados y la alta dependencia del

personal clave representan vulnerabilidades significativas para la continuidad operativa. Estas condiciones afectan directamente la capacidad de respuesta ante interrupciones del servicio de internet y otros incidentes tecnológicos.

6.5. Proveedores Tecnológicos

En el diagnóstico realizado se contactó que la cooperativa cuenta con un único proveedor tecnológico encargado de la prestación del servicio de Internet y del acceso a los sistemas institucionales, lo cual evidencia un alto nivel de dependencia externa.

Esta condición representa un riesgo significativo para la continuidad operativa, ya que ante una interrupción del servicio no se dispone de mecanismos alternos que permitan mantener las operaciones. Asimismo, la capacidad de respuesta ante incidentes depende directamente del proveedor, lo que limita la autonomía institucional para gestionar fallas de conectividad.

Tabla 10

Evaluación de proveedores tecnológicos y gestión de incidentes

Proveedor / Servicio	Elemento evaluado	Situación identificada	atención actual	Evidencia diagnóstica	Impacto en continuidad operativa
Proveedor de internet (ISP)	Servicio de conectividad	Dependencia de un único proveedor de internet	Atención reactiva mediante llamada telefónica	No existen enlaces alternos ni redundancia	Alta afectación a procesos críticos ante caídas prolongadas

Fuente: entrevista al responsable de TI

6.6. Identificación de Activos Informáticos críticos

Con base en los hallazgos del diagnóstico, se procedió a identificar los activos informáticos críticos, entendidos como aquellos cuya falla, indisponibilidad o deterioro afectaría de manera grave la continuidad de las operaciones de la cooperativa.

Tabla 11

Activos informáticos críticos

Tipo de activo	Activo identificado	Función principal	Dependencia tecnológica	Impacto ante falla	Nivel de criticidad
Hardware	Servidor principal	Alojar sistemas institucionales y bases de datos	Alta	Paralización de los sistemas informáticos	Crítico
Hardware	Router de internet	Proveer conectividad a sistemas	Alta	Interrupción total de las operaciones en línea	Crítico
Hardware	Switch principal	Interconexión de equipos dentro de la red local	Media–Alta	Interrupción parcial o total de la red interna	Alto
Hardware	Computadoras de escritorio	Registro de transacciones,	Alta	Detención de procesos financieros y administrativos	Crítico

Fuente: Información obtenida mediante entrevista realizadas TI

Tabla 11

Activos informáticos críticos

Tipo de activo	Activo identificado	Función principal	Dependencia tecnológica	Impacto ante falla	Nivel de criticidad
Dispositivos móviles	Teléfonos móviles corporativos	Registro y sincronización de información en campo	Alta	Retrasos en la actualización de datos y gestión de cartera	Alto
Software	Sistema financiero institucional	Gestión de cuentas, créditos, pagos y reportes	Alta	Interrupción total de las operaciones financieras	Crítico
Software	Sistemas administrativos	Generación de reportes y control operativo	Media–Alta	Retrasos en procesos administrativos	Alto
Base de datos	Base de datos financiera	Almacenamiento de información de Asociado	Alta	Pérdida, corrupción o inconsistencia de la información crítica	Crítico
Infraestructura eléctrica	UPS por equipo	Respaldo eléctrico temporal	Media	Continuidad limitada ante cortes de energía	Alto

Fuente: Información obtenida mediante entrevista realizadas TI

El análisis de la matriz de activos informáticos críticos permitió identificar que la continuidad operativa de la Sucursal San Juan de la Concepción depende del funcionamiento integrado de diversos componentes tecnológicos, tales como la infraestructura de red, los sistemas de información, los equipos de cómputo y los mecanismos de respaldo eléctrico.

El servicio de internet constituye un elemento esencial para la interconexión con la Oficina Central y el acceso a los sistemas corporativos, la operación institucional no depende exclusivamente de este, sino del desempeño coordinado de todos los activos tecnológicos críticos.

6.7. Identificación de Amenazas

En esta fase se identificaron las principales amenazas que podrían interrumpir los servicios informáticos de la Sucursal San Juan de la Concepción, considerando su impacto sobre los activos críticos y, particularmente, sobre la continuidad del servicio de internet.

En la presente la matriz se evidenció que las principales amenazas identificadas en la Sucursal San Juan de la Concepción tienen un impacto directo sobre la continuidad del servicio de internet y, por ende, sobre los procesos críticos de la cooperativa. Las fallas de conectividad y las interrupciones eléctricas destacan como las amenazas de mayor impacto y probabilidad, debido a la alta dependencia de la sucursal de la conectividad con la Oficina Central y de la infraestructura tecnológica local. Asimismo, otras amenazas como el daño de hardware, los errores humanos y los ataques informáticos actúan como factores que incrementan la vulnerabilidad del servicio

Tabla 12

Identificación de amenazas a los servicios informáticos

Amenaza Identificada	Descripción de la Amenaza	Activo / Servicio Afectado	Impacto Operativo	Probabilidad	Relación con el Servicio de Internet
Fallas eléctricas	Interrupciones del suministro eléctrico	Equipos de cómputo, red, sistemas financieros	Interrupción parcial o total de operaciones	Media	La falta de energía impide el funcionamiento de los equipos
Daño de hardware	Fallas en routers, switches o equipos de cómputo	Infraestructura de red y equipos terminales	Pérdida de conectividad interna y externa,	Media	La falla de equipos de red interrumpe el acceso a los sistemas en línea
Ataques informáticos	Riesgo de infección por virus o malware	Red y Sistemas Informáticos	Riesgo de indisponibilidad o alteración de información	Baja	El servicio de internet es el principal vector de ingreso de amenazas informáticas
Errores humanos	Uso incorrecto de los sistemas por parte del personal	Sistemas Informáticos equipos y datos institucionales	Caídas parciales o totales	Media	La indisponibilidad del sistema o internet agrava el impacto de los errores
Robo de equipos	Sustracción de equipos	Equipos de cómputo y dispositivos	Interrupción operativa y riesgo de	Baja	La pérdida de equipos limita el acceso a los

	informáticos o de red	de conectividad	pérdida de información		sistemas que operan vía internet
Fallas de conectividad	Interrupciones del enlace de Internet y del enlace de datos con la Oficina Central	Servicio de Internet y sistemas centrales	Pérdida de acceso a sistemas institucionales	Alta	Afecta directamente la continuidad del servicio de internet
Incendios u otros eventos físicos	Daños a la infraestructura tecnológica por eventos mayores	Infraestructura tecnológica y datos	Interrupción total de operaciones	Baja	Provoca la indisponibilidad completa de los servicios que dependen Internet

Fuente: Elaboración propia, basada en el diagnóstico realizado mediante entrevistas, observación directa y análisis de riesgos.

6.8. Análisis de Vulnerabilidades

El análisis de vulnerabilidades permitió evaluar el nivel de exposición de la Sucursal San Juan de la Concepción ante eventos que puedan afectar la disponibilidad del servicio de Internet, considerando debilidades identificadas en la infraestructura tecnológica, los sistemas de información, la gestión de datos, los recursos humanos y la relación con proveedores.

6.9. Vulnerabilidades en la conectividad a Internet

Se identificó como principal vulnerabilidad la dependencia de un único enlace de Internet, sin mecanismos de redundancia. Esta condición expone a la sucursal a interrupciones totales de sus operaciones ante fallas del proveedor, como se evidenció en el evento de interrupción prolongada ocurrido en diciembre de 2025.

Asimismo, la ausencia de registros históricos y de herramientas de monitoreo limita la capacidad para anticipar fallas, evaluar el desempeño del servicio y reducir los tiempos de recuperación.

6.10. Vulnerabilidades operativas y de sistemas

Los sistemas de información críticos presentan una alta dependencia de la conectividad, sin alternativas de operación en escenarios de falla. Como consecuencia, procesos clave como cajas, atención al cliente y gestión administrativa se ven interrumpidos, generando retrasos y suspensión de servicios.

6.11. Vulnerabilidades en la gestión de datos

Se evidenció que los respaldos de información se realizan de forma manual al cierre de la jornada, lo que incrementa la dependencia del factor humano y el riesgo de pérdida de información reciente.

Adicionalmente, se identificaron inconsistencias en los datos durante interrupciones del servicio, lo que afecta la integridad de la información y aumenta el riesgo operativo.

6.12. Vulnerabilidades organizacionales y de proveedores

La limitada disponibilidad de personal de TI, la ausencia de procedimientos documentados y la dependencia de un único proveedor sin acuerdos formales de nivel de servicio incrementan la exposición ante fallas prolongadas, dificultando una respuesta oportuna y estructurada.

A partir de las vulnerabilidades identificadas, a continuación, se presenta la sistematización de los principales factores de exposición que afectan la continuidad del servicio de Internet en la sucursal:

Tabla 13

Identificación de riesgo derivados de amenazas y vulnerabilidades

Amenaza	Vulnerabilidad identificada	Activo afectado	Impacto operativo	Nivel de riesgo
Caída del servicio de internet	Dependencia de un único proveedor sin enlace de respaldo	Sistemas de gestión operativa	Suspensión total de operaciones en cajas y atención al cliente	Alto
Falla del proveedor de internet	Ausencia de SLA y tiempos de respuesta garantizados	Conectividad institucional	Prolongación del tiempo de recuperación del servicio	Alto
Fallas eléctricas prolongadas	Respaldo eléctrico parcial para equipos de red	Infraestructura de red	Interrupción de la conectividad y pérdida de continuidad operativa	Medio
Error humano	Respaldos manuales dependientes del personal de TI	Información crítica	Pérdida o inconsistencia de datos recientes	Medio
Incidencias técnicas en red	Infraestructura sin redundancia (router/switch únicos)	Red interna	Interrupción simultánea de todos los servicios	Alto

La matriz de riesgos permite evidenciar que los principales riesgos tecnológicos de la Sucursal San Juan de la Concepción se concentran en la dependencia del servicio de internet y en la falta de mecanismos de redundancia y formalización de procesos críticos. Los riesgos clasificados como altos representan una amenaza directa para la continuidad operativa de la sucursal.

6.13. Evaluación de Riesgos

La evaluación de riesgos en Cooperativa COOPACRESMHA Sucursal San Juan se fundamenta en el análisis integral de las amenazas identificadas, las vulnerabilidades existentes y el impacto operativo que dichos eventos pueden generar sobre los procesos institucionales, especialmente aquellos que dependen de los sistemas informáticos y del servicio de internet.

Este análisis permitió determinar el nivel de exposición de la sucursal, establecer prioridades de atención y orientar la toma de decisiones para la definición de controles preventivos, correctivos y medidas de contingencia tecnológica. La evaluación se realizó mediante el cruce entre la probabilidad de ocurrencia y el impacto operativo, dando como resultado la clasificación de los riesgos en cuatro niveles: crítico, alto, medio y bajo.

6.13.1. Nivel de Riesgo Crítico

El nivel de riesgo crítico corresponde a eventos con alta probabilidad de ocurrencia y alto impacto operativo, los cuales tienen la capacidad de generar la interrupción total o parcial de los servicios financieros, afectando directamente las áreas de caja, atención al cliente y servicios financieros. En la Sucursal San Juan, los riesgos críticos se encuentran estrechamente vinculados a la alta dependencia del servicio de internet, a la conectividad con la Oficina Central y a fallas que comprometan la disponibilidad de los sistemas transaccionales y administrativos, lo que convierte a estos eventos en detonantes inmediatos de la activación del Plan de Contingencia de TI.

6.13.2. Nivel de Riesgo Alto

El nivel de riesgo alto agrupa eventos cuya probabilidad o impacto es significativo, generando afectaciones relevantes en los procesos críticos, aunque sin provocar necesariamente la paralización total de la sucursal. Estos riesgos pueden ocasionar retrasos operativos, reprocesos administrativos y disminución en la calidad del servicio brindado a los asociados.

Para este nivel de riesgo, COOPACRESMHA debe implementar medidas preventivas y correctivas prioritarias, así como mantener un seguimiento continuo por parte del área de TI y las jefaturas involucradas, con el fin de evitar su escalamiento a un nivel crítico.

6.13.3. Nivel de Riesgo Medio

El nivel de riesgo medio corresponde a eventos con probabilidad e impacto moderados, cuyos efectos pueden ser gestionados mediante los controles tecnológicos y procedimientos operativos existentes. Si bien estos riesgos no representan una amenaza inmediata para la continuidad del negocio, su acumulación o falta de seguimiento puede generar ineficiencias operativas.

En este contexto, la sucursal San Juan debe mantener un monitoreo constante, reforzar la capacitación del personal y avanzar en la documentación de procedimientos, con el objetivo de reducir progresivamente su exposición a este nivel de riesgo.

6.13.4. Nivel de Riesgo Bajo

El nivel de riesgo bajo agrupa aquellos eventos con baja probabilidad de ocurrencia y bajo impacto operativo, cuyos efectos no comprometen la continuidad del negocio ni la seguridad de la información institucional. Estos riesgos se consideran aceptables, siempre que se mantengan los controles administrativos y tecnológicos existentes, así como las prácticas de supervisión periódica.

Escala Utilizada para la matriz de Probabilidad + impacto

Valor	Probabilidad	Impacto
1	Baja	Bajo
2	Media	Medio
3	Alta	Alto

El análisis de la matriz de evaluación del riesgo y el mapa de calor evidencia que los riesgos con mayor nivel de criticidad para COOPACRESMHA Sucursal San Juan se concentran en la dependencia del servicio de internet y en las fallas eléctricas prolongadas, debido a su alta probabilidad de ocurrencia y elevado impacto sobre los procesos institucionales.

Estos resultados justifican la necesidad de fortalecer el Plan de Contingencia Tecnológica, priorizando estrategias orientadas a garantizar la continuidad del servicio de internet, la disponibilidad de los sistemas informáticos y la reducción de los tiempos de recuperación ante incidentes.

Tabla 14

Matriz de evaluación de riesgo

Amenaza	Vulnerabilidad asociada	Probabilidad	Impacto	Nivel Riesgo	Procesos afectados
Fallas eléctricas prolongadas	Planta eléctrica sin capacidad total	Alta (3)	Alto (3)	 Crítico	Cajas, Atención al Cliente, y Sistemas finan
Falla del servicio de internet	Dependencia de enlace con oficina central	Alta (3)	Alto (3)	 Crítico	Sistemas transaccionales, administrativos
Daño de equipos de red	Falta de mantenimiento preventivo	Media (2)	Alto (3)	 Alto	Acceso a sistemas, conecta interna
Errores humanos en caja	Falta de procedimientos documentados	Alta (3)	Medio (2)	 Alto	Operaciones de cobro y pago
Ataques informáticos	Capacitación no formalizada	Media (2)	Alto (3)	 Alto	Seguridad de la información
Fallas menores de hardware	Equipos en uso continuo	Media (2)	Medio (2)	 Medio	Atención al cliente
Rotación de personal	Falta de plan de inducción formal	Media (2)	Medio (2)	 Medio	Procesos administrativos
Robo de equipos	Controles físicos existentes	Baja (1)	Medio (2)	 Bajo	Infraestructura TI
Interrupciones breves de energía	UPS instalados	Baja (1)	Bajo (1)	 Bajo	Operación general

Fuente: Elaboración propia con base en el diagnóstico y análisis de riesgos.

Mapa de Calor de Riesgos

		PROBABILIDAD		
		BAJA	MEDIA	ALTA
IMPACTO		1	2	3
ALTA	3	M	A	C
MEDIO	2	B	M	A
BAJA	1	B	B	M

El mapa de calor de riesgos permite visualizar de manera gráfica el nivel de exposición de la Cooperativa Coopacresmha – Sucursal San Juan, a partir del cruce entre la probabilidad de ocurrencia y el impacto operativo de los eventos identificados. Esta herramienta facilita la priorización de riesgos y la toma de decisiones para la implementación de medidas de contingencia.

6.14. Análisis de Impacto al Negocio (BIA)

Con el propósito de identificar los procesos críticos de la Sucursal San Juan de la Concepción y evaluar el impacto que generaría una interrupción del servicio de Internet, se realizó un Análisis de Impacto en el Negocio (BIA), considerando las áreas operativas, los sistemas utilizados y los tipos de pérdida asociados.

A continuación, se presentan los resultados del análisis:

Tabla 15
Matriz BIA

Proceso	Área	Sistema	Impacto	Tipo de Pérdida	Prioridad
Operaciones de Caja	Cajas	SISCOMIF / Ahorros / Remesas	Muy Alto	Financiera / Reputacional	1
Atención al Cliente	Servicio	SISCOMIF / SISCOMIFPIC	Alto	Operativa / Comercial	1
Servicios Financieros	Crédito	SISCOMIF / TransUnion	Alto	Comercial	2

Fuente: Elaboración propia con base en el diagnóstico y análisis de impacto en el negocio.

El Análisis de Impacto al Negocio permitió identificar que los procesos de Operaciones de Caja y Atención al Cliente presentan el menor tiempo máximo tolerable de interrupción, siendo altamente dependientes de los sistemas de información y del servicio de internet. En consecuencia, estos procesos deben ser priorizados dentro del Plan de Contingencia de TI, ya que su indisponibilidad prolongada compromete la continuidad operativa, el desempeño financiero y la confianza de los asociados.

6.15. Evaluación de Medidas Actuales

La evaluación de las medidas actuales permitió determinar el nivel real de preparación de COOPACRESMHA, Sucursal San Juan de la Concepción, frente a interrupciones tecnológicas, particularmente aquellas relacionadas con fallas del servicio de internet y del suministro eléctrico.

Este análisis se orientó a identificar las fortalezas existentes, así como las debilidades que limitaban la continuidad operativa, con el propósito de establecer una base objetiva para la formulación del Plan de Contingencia Tecnológica.

6.15.1. Existencia y Frecuencia de respaldos (Backups)

COOPACRESMHA sucursal San Juan cuenta con un modelo de respaldos de la información que se realiza de forma diaria al finalizar la jornada laboral, lo cual constituye una medida básica de protección de los datos institucionales.

La ausencia de respaldos automáticos o en tiempo real durante la operación diaria genera una vulnerabilidad significativa, ya que, ante interrupciones del sistema, fallas eléctricas, daños de hardware o caídas del servicio de internet, la información generada durante el día podría perderse, afectando directamente los procesos operativos y administrativos.

Tabla 16

Evaluación de la existencia y frecuencia de respaldo de la información

Aspecto evaluado	Situación actual	Frecuencia	Impacto ante incidentes	Riesgo identificado
Existencia de respaldos	Respaldos de la información al finalizar la jornada laboral	Diaria	recuperación de información generada hasta el cierre del día	Protección limitada durante la jornada operativa
Tipo de respaldo	Respaldos ejecutados de forma manual por el área de informática	Diaria	Dependencia del factor humano para la ejecución correcta del respaldo	Riesgo de omisión o error en la ejecución
Automatización de respaldos	No se cuenta con respaldos automáticos ni en tiempo real	No aplica	La información generada durante el día no queda protegida	Alta vulnerabilidad ante incidentes
Protección ante fallas durante la jornada	No existen respaldos intermedios durante el horario laboral	No aplica	Pérdida de registros de cajas, atención	Reprocesos manuales y posibles errores operativos
Recuperación de información	Restauración último respaldo diario disponible	Eventual	Retrasos en la normalización de operaciones	Impacto operativo y administrativo

6.15.2. Almacenamiento Externo

La cooperativa cuenta con almacenamiento externo de los respaldos de la información mediante el uso de discos duros externos, los cuales complementan el servidor institucional y permiten disponer de copias de seguridad alternas.

Tabla 17

Evaluación del almacenamiento externo de los respaldos

Aspecto evaluado	Situación actual	Ubicación	Medida de seguridad
Tipo de almacenamiento	Discos duros externos	Servidor institucional	Control de acceso físico
Respaldo alterno	Discos externos fuera del servidor	Área de tesorería	Resguardo en caja fuerte
Seguridad física	Protección contra robo y acceso no autorizado	Tesorería	Caja fuerte
Accesibilidad de respaldos	Recuperación manual de la información	Local	Dependencia del personal de TI
Redundancia geográfica	No existe almacenamiento externo fuera de la sucursal	No aplica	No aplica

Fuente: Elaboración propia con base en el diagnóstico y entrevista al responsable de TI

6.15.3. Procedimientos Documentados:

La cooperativa cuenta con almacenamiento externo de los respaldos de la información mediante el uso de discos duros externos, los cuales complementan el servidor institucional y permiten disponer de copias de seguridad alternas.

Tabla 18

Evaluación de los procedimientos documentados

Aspecto evaluado	Situación actual	Forma de atención	Riesgo identificado
Existencia de procedimientos documentados	No existen manuales, instructivos ni protocolos formales	Atención basada en la experiencia del personal	Alta dependencia del recurso humano
Gestión de incidentes tecnológicos	Actuación ante caídas de internet, fallas del sistema financiero y	Decisiones reactivas en el momento del evento	Incremento del tiempo de recuperación
Respaldo y restauración de información	Procesos ejecutados sin documentación formal	Conocimiento empírico del personal de TI	Riesgo de errores en la restauración
Capacitación del personal	No existen guías formales para entrenamiento	Aprendizaje informal	Interrupciones prolongadas del servicio

Fuente: entrevista al responsable de TI

6.15.4. Responsabilidades Asignadas

La asignación de responsabilidades permitió identificar los actores encargados de ejecutar y supervisar los controles asociados a los principales riesgos tecnológicos, contribuyendo a fortalecer la gestión de la continuidad operativa en COOPACRESMHA – Sucursal San Juan.

Tabla 19

Responsabilidades asignadas a los riesgos tecnológicos

Riesgo identificado	Control existente / propuesto	Responsable
Fallas eléctricas	Planta eléctrica, UPS en equipos críticos y procedimientos de apagado	TI / Gerencia
Caída del servicio de internet	Enlace principal, monitoreo de conectividad y propuesta de enlace de respaldo	TI
Errores humanos	Capacitación operativa y validaciones del sistema	Jefe de Caja / TI
Dependencia del proveedor del sistema	Acuerdos de soporte y escalamiento de incidencias	Gerencia / TI
Ataques informáticos	Firewall Fortinet y antivirus actualizado	TI
Respaldos no automáticos	Respaldos manuales diarios y pruebas periódicas	Responsable de TI
Robo de equipos	Cámaras de seguridad y control de acceso	Gerencia Administrativa

Fuente: Elaboración propia a partir del diagnóstico de riesgos tecnológicos

6.15.5. Planes de Emergencia Previos

La evaluación de los planes de emergencia previos en Coopacresmha Sucursal San Juan evidencia que la institución no cuenta con un Plan de Contingencia Informático formalmente documentado. Las acciones que se ejecutan ante incidentes tecnológicos corresponden, en su mayoría, a prácticas operativas informales basadas en la experiencia del personal del área de Tecnologías de la Información.

Ante eventos como la caída del servicio de internet, fallas de sistemas o daños en equipos críticos, la respuesta se limita a la notificación al responsable de TI y al contacto reactivo con el proveedor correspondiente, sin que exista un procedimiento estandarizado que defina tiempos de respuesta, responsables alternos o mecanismos de continuidad operativa.

Esta situación evidencia la necesidad de diseñar e implementar un Plan de Contingencia formal que permita fortalecer la continuidad operativa de la sucursal.

Tabla 20

Evaluación de planes de emergencia previos

Tipo de evento	Plan de emergencia previo	Nivel de formalización	Responsable	Evaluación
Caída del servicio de internet	Procedimiento operativo informal (aviso a TI y contacto con ISP)	No documentado	Responsable de TI	Insuficiente
Fallas eléctricas	Uso de planta eléctrica	Parcialmente documentado	Administración / TI	Parcial

Fallas de sistemas	Atención basada en errores con proveedor	No documentado	Área de TI	Insuficiente
Pérdida de información	RespalDOS diarios manuales	No documentado	Responsable de TI	Parcial
Incidentes de seguridad	Uso de firewall y antivirus	Implementado técnicamente	Área de TI	Adecuado
Ausencia de personal clave	No existe plan de sustitución	Inexistente	Recursos Humanos	Insuficiente

Fuente: Elaboración propia con base en el diagnóstico institucional

6.16. Resultado del Diagnóstico

6.16.1. Resultados del Componente Cualitativo

✓ El componente cualitativo permitió comprender las dinámicas operativas, percepciones del personal y prácticas actuales ante interrupciones del servicio de internet en la sucursal San Juan de la Concepción. La información se obtuvo mediante entrevistas al responsable de TI, observación directa de las operaciones.

✓ El análisis de la información permitió identificar patrones recurrentes relacionados con la dependencia tecnológica, las dificultades operativas durante las caídas del servicio y las estrategias informales utilizadas por los colaboradores para continuar las operaciones.

6.16.2. Categorías emergentes

A partir del análisis de la información recopilada se identificaron las siguientes categorías principales:

- ✓ **Dependencia operativa del internet:** interrupción inmediata de operaciones en cajas y atención al cliente cuando se pierde la conectividad.

- ✓ **Limitaciones en procedimientos alternos:** ausencia de protocolos estandarizados para trabajar sin conexión.
- ✓ **Comunicación interna limitada:** dificultades para coordinar acciones durante contingencias tecnológicas.
- ✓ **Impacto en la atención al asociado:** retrasos en procesos, tiempos de espera prolongados y reducción de la productividad.
- ✓ **Gestión reactiva ante incidentes:** respuesta basada en experiencia empírica más que en procedimientos formales.

6.16.3. Interpretación cualitativa de hallazgos

✓ Los resultados evidencian una alta dependencia de los sistemas informáticos conectados a internet para el desarrollo de las actividades críticas de la sucursal. Las áreas operativas presentan limitaciones para continuar sus funciones cuando ocurre una interrupción del servicio, lo que genera impactos directos en la atención al cliente y en la toma de decisiones.

✓ Se identificó que las acciones de respuesta ante fallas tecnológicas son mayormente reactivas y no se encuentran formalmente documentadas, lo cual incrementa el nivel de riesgo operativo.

✓

6.16.4. Síntesis narrativa por áreas

En las entrevistas realizadas al responsable de TI se le consultó ¿Qué sucede operativamente en la sucursal cuando ocurre una caída del servicio de internet? A lo que se logró evidenciar lo siguiente:

 Área de Cajas:

Las caídas del servicio impiden realizar transacciones financieras, provocando retrasos en pagos, depósitos y consultas de saldo.

Atención al Cliente:

Se evidencian dificultades para consultar información del asociado y gestionar solicitudes en tiempo real.

Gerencia y servicios Financieros:

La toma de decisiones operativas se ve limitada por la falta de acceso a reportes e información actualizada.

Promotores y Gestores de cobro:

Se presentan retrasos en el descargue de datos y sincronización de información de campo

6.17. Resultados del Componente Cuantitativo

✓ El análisis cuantitativo permitió evaluar los riesgos asociados a la interrupción del servicio de internet mediante matrices de riesgo, niveles de criticidad y evaluación de probabilidad e impacto.

6.17.1. Matriz de Riesgo

Se identificaron riesgos relacionados con:

- ✓ Interrupciones del proveedor de internet
- ✓ Fallas de equipos de red
- ✓ Problemas eléctricos
- ✓ Saturación de la conectividad

✓ Estos riesgos fueron clasificados según su nivel de probabilidad e impacto operativo.

6.17.2. Niveles de impacto y criticidad

Los procesos con mayor criticidad fueron:

- ✓ Operaciones en cajas
- ✓ Atención al asociado
- ✓ Gestión financiera y reportes

6.17.3. Probabilidad de interrupciones

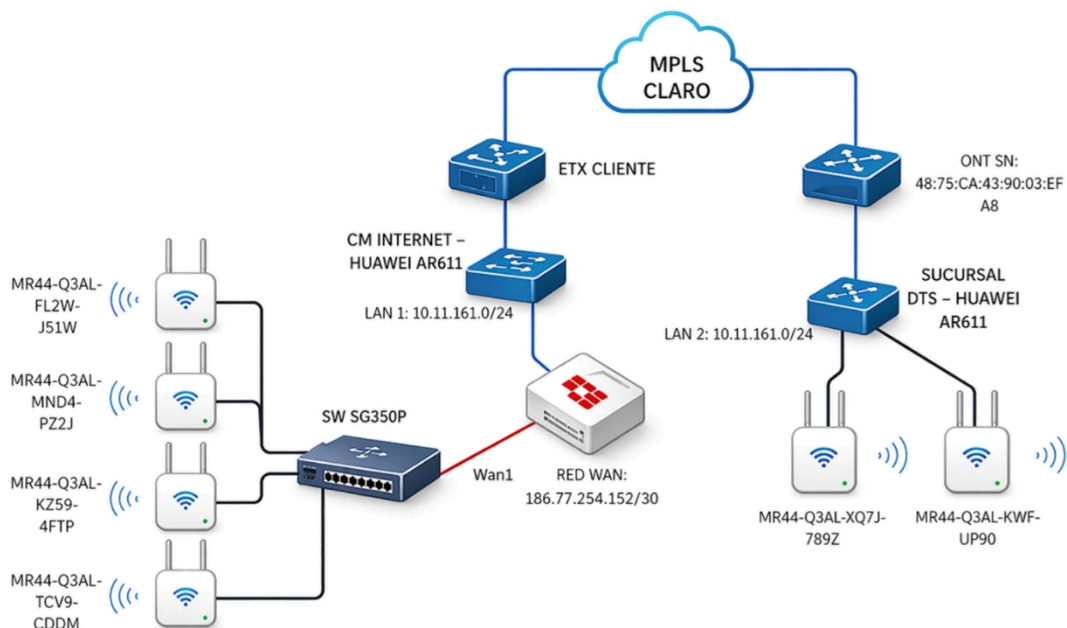
✓ El análisis identificó que las interrupciones del servicio presentan una probabilidad moderada alta debido a factores externos del proveedor y limitaciones internas de infraestructura tecnológica.

6.18. Diagnóstico de Infraestructura Tecnológica

6.18.1. Arquitectura de red actual

Como parte del diagnóstico técnico realizado en la Cooperativa COOPACRESMHA, sucursal San Juan de la Concepción, se elaboró el diagrama de la infraestructura de red actual con el propósito de visualizar la estructura de conectividad, los enlaces de comunicación existentes y los activos tecnológicos.

Arquitectura actual de conectividad e infraestructura de red – Sucursal San Juan de la Concepción, COOPACRESMHA.



Fuente: Elaboración propia a partir del diagnóstico técnico (2026).

6.18.2. Equipos y conectividad

Se identificaron equipos críticos como:

- ✓ Routers y switches
- ✓ UPS
- ✓ Equipos de cómputo de áreas operativas
- ✓ Enlace principal de internet

6.18.3. Dependencias tecnológicas críticas

Los sistemas institucionales dependen directamente de la conectividad para:

- ✓ Operaciones financieras
- ✓ Consultas de base de datos
- ✓ Sincronización de información
- ✓ Gestión administrativa

6.18.4. Riesgos técnicos identificados

- ✓ Dependencia de un solo proveedor
- ✓ Ausencia de redundancia
- ✓ Vulnerabilidad ante fallas eléctricas
- ✓ Falta de monitoreo continuo de la conectividad

6.18.5. Capacidad contratada - demanda Real

Se realizó una prueba técnica de velocidad del servicio de internet utilizando la herramienta Speedtest, obteniendo una velocidad de descarga de 9.88 Mbps y una velocidad de subida de 9.63 Mbps, con una latencia promedio de 15 ms. Los resultados evidencian que el enlace contratado de 10 Mbps opera cercano a su capacidad máxima, lo cual confirma una limitada disponibilidad de ancho de banda ante escenarios de alta demanda operativa. Esta condición incrementa el riesgo de saturación del enlace durante horas pico, generando lentitud en el sistema financiero institucional y afectando directamente la continuidad de los procesos críticos de la cooperativa.

Prueba de velocidad del servicio de internet mediante herramienta Speedtest



Elaboración propia a partir de pruebas técnicas de conectividad (2026).

Tabla 21

Matriz técnica del servicio de internet

Indicador técnico	Resultado obtenido	Nivel	Interpretación operativa	Riesgo BCM
Velocidad descarga	9.88 Mbps	Alto uso	Cercano al límite contratado	Saturación
Velocidad subida	9.63 Mbps	Alto uso	Poca capacidad adicional	Lentitud
Latencia externa	15 ms	Aceptable	Respuesta adecuada	Bajo
Capacidad contratada	10 Mbps	Limitada	Sin margen de crecimiento	Crítico
Estimación usuarios simultáneos	15–20	Alto	Demanda elevada	Alto

Fuente: Elaboración propia con base en pruebas técnicas de conectividad y diagnóstico institucional

6.19. Integración e interpretación de Resultados (Diagnostico Final)

El diagnóstico del estado actual de la gestión tecnológica de COOPACRESMHA Sucursal San Juan de la Concepción permitió evidenciar que sus procesos dependían de manera significativa de la disponibilidad de los servicios informáticos, de la conectividad a internet y de la infraestructura tecnológica que soporta los procesos financieros, administrativos y de atención a los asociados.

A partir del análisis de los proveedores tecnológicos, se identificó una alta dependencia de servicios externos, particularmente del proveedor de internet y de los proveedores de hardware y software, cuyos mecanismos de atención se encontraban orientados principalmente a una gestión correctiva posterior a la ocurrencia de incidentes. Asimismo, se evidenció la ausencia de acuerdos formales de nivel de servicio (SLA), registros históricos de incidentes y procedimientos documentados de

contingencia, lo que limitaba la capacidad institucional de respuesta ante interrupciones prolongadas.

La identificación de los activos informáticos críticos permitió determinar que la continuidad operativa de la sucursal no dependía únicamente del servicio de internet, sino del funcionamiento integrado de diversos componentes tecnológicos, entre los que se destacan la infraestructura de red, los sistemas centrales de información, los equipos de cómputo y los mecanismos de respaldo eléctrico. La indisponibilidad de cualquiera de estos activos tendría un impacto directo en la prestación de los servicios financieros y en la atención a los asociados.

El análisis de amenazas y vulnerabilidades evidenció la exposición de la sucursal a eventos como fallas eléctricas, interrupciones de conectividad, daños en equipos críticos, errores humanos y dependencias operativas del proveedor de sistemas. Si bien la cooperativa contaba con ciertos controles tecnológicos, como el uso de antivirus licenciados, dispositivos de seguridad perimetral y sistemas de respaldo energético, se identificaron debilidades relacionadas con la falta de formalización de procedimientos, la dependencia del conocimiento individual del personal de TI y la inexistencia de planes documentados de respuesta ante incidentes.

La evaluación de riesgos permitió clasificar varios escenarios como riesgos críticos y altos, principalmente aquellos asociados a caídas del servicio de internet, fallas eléctricas prolongadas y errores operativos en áreas clave como caja y atención al cliente. Estos riesgos tenían la capacidad de interrumpir total o parcialmente las operaciones de la sucursal, afectando la continuidad del servicio, la satisfacción de los asociados y el control operativo institucional.

En síntesis, el diagnóstico evidenció que COOPACRESMHA Sucursal San Juan de la Concepción operaba con una limitada preparación formal ante contingencias tecnológicas, sustentándose en prácticas operativas no documentadas y en una gestión mayormente correctiva. Esta situación justificó la necesidad de Proponer un plan de Contingencia Informático que permita fortalecer la continuidad operativa, reducir la exposición a riesgos tecnológicos y establecer procedimientos claros de respuesta ante interrupciones del servicio de internet y otros eventos críticos.

Tabla 22

Plan de contingencia

Actividad	Indicador de cumplimiento	Responsable
Implementación de políticas de respaldo	Políticas formalizadas y aprobadas	Área de TI
Automatización de respaldos	Respaldos automáticos operativos	Área de TI
Pruebas de restauración	Registros de pruebas de restauración	Área de TI
Definición de roles y responsables	Documento de responsabilidades	Gerencia / TI
Documentación de procedimientos	Procedimientos documentados	Área de TI
Capacitación del personal	Personal capacitado	Gerencia / TI
Implementación de respaldo en la nube	Backups en la nube disponibles	Gerencia / TI
Fortalecimiento de respaldo energético	Equipos críticos protegidos	Gerencia Administrativa

Con el propósito de fortalecer el diagnóstico técnico de la continuidad operativa, se realizó una evaluación del desempeño del servicio de internet mediante indicadores técnicos clave como latencia, capacidad de ancho de banda, estabilidad operativa, pérdida de paquetes y relación entre capacidad contratada y demanda real. Estos indicadores permitieron identificar vulnerabilidades técnicas que afectan la resiliencia tecnológica de la sucursal ante posibles interrupciones del servicio.

6.20. Evaluación Técnica del Servicio de Internet

Se realizó una prueba de trazado de ruta (tracert) hacia el servidor público 8.8.8.8 con el objetivo de evaluar el comportamiento de la conectividad externa del enlace de datos. Los resultados evidencian una latencia promedio final de 38 ms, considerada dentro de parámetros aceptables para operaciones financieras en línea.

Sin embargo, durante el recorrido se identificaron nodos intermedios con tiempos de espera agotados, lo cual puede estar asociado a restricciones de seguridad o a episodios de congestión en la red del proveedor.

Indicadores Técnicos de Conectividad

Destino: 8.8.8.8 (dns. Google)

Sucursal: San Juan/Caja N°2

Tipo de Prueba: trazado de ruta (Tracert)

Tabla 23

Resultados de prueba de conectividad mediante TRACERT

Indicador técnico	Resultado observado	Interpretación técnica	Impacto en COOPACRESMHA
Latencia final	38 ms	Conexión dentro de rango aceptable	Operación normal del sistema financiero
Salto	14 nodos	Ruta estándar de proveedor ISP	Sin impacto crítico
Tiempo máximo intermedio	45 ms	Variación moderada	Posible congestión en horas pico
Salto con pérdida	4 nodos sin respuesta	Bloqueo ICMP o saturación parcial	Posible inestabilidad temporal

Fuente: Elaboración propia con base en pruebas técnicas de conectividad y diagnóstico institucional

Indicador	Valor evidenciado
Latencia promedio real	38 – 45 ms
Estabilidad del enlace	Moderada
Dependencia del proveedor	Alta
Evidencia de congestión	Sí (timeouts intermedios)
Conectividad final	Funcional

La presencia de saltos sin respuesta durante la traza indica posibles limitaciones en la visibilidad de la red o congestión parcial, lo cual representa un riesgo operativo en escenarios de alta demanda, considerando que COOPACRESMHA Sucursal San Juan de la Concepción depende directamente del servicio de internet para la ejecución de procesos críticos financieros.

6.20.1. Prueba de Conectividad Interna (Latencia LAN/ E. CENTRAL)

```

C:\Us
TrazasobreC:\Users\CajaNo2SnJuan.CAJANO2SNJ>ping 10.11.148.100
1 Haciendo ping a 10.11.148.100 con 32 bytes de datos:
2 Respuesta desde 10.11.148.100: bytes=32 tiempo=2ms TTL=124
3 Respuesta desde 10.11.148.100: bytes=32 tiempo=1ms TTL=124
4 Respuesta desde 10.11.148.100: bytes=32 tiempo=2ms TTL=124
5 Respuesta desde 10.11.148.100: bytes=32 tiempo=2ms TTL=124
6
7 Estadísticas de ping para 10.11.148.100:
8 Paquetes: enviados = 4, recibidos = 4, perdidos = 0
9 (0% perdidos),
10 Tiempos aproximados de ida y vuelta en milisegundos:
11 Mínimo = 1ms, Máximo = 2ms, Media = 1ms
12
13 TrazasobreC:\Users\CajaNo2SnJuan.CAJANO2SNJ>_

```

Fuente: Elaboración propia con base en pruebas técnicas de conectividad

Se realizó una prueba de conectividad interna mediante el comando PING hacia el servidor institucional (10.11.148.100), obteniendo tiempos de respuesta entre 1 ms y 2 ms, sin pérdida de paquetes. Estos resultados evidencian una conectividad estable dentro de la red local y hacia el enlace con la sucursal central, indicando que la infraestructura interna presenta niveles adecuados de desempeño. Por lo tanto, las interrupciones operativas identificadas en la investigación no se asocian a fallas internas de red, sino principalmente a la dependencia del servicio de internet externo.

6.21. Formulación de Propuesta de plan de Contingencia Sucursal San Juan

6.21.1. Propósito del plan

El Plan de Contingencia Informática para la Cooperativa de Ahorro, Crédito y Servicios Múltiples Humberto Aguilar (COOPACRESMHA), Sucursal San Juan de la Concepción, se elabora a partir de los resultados del diagnóstico tecnológico, la evaluación de riesgos y el Análisis de Impacto al Negocio (BIA), los cuales evidenciaron una alta dependencia del servicio de internet para la continuidad de los procesos operativos, administrativos y comerciales de la cooperativa.

El presente plan tiene como propósito establecer un conjunto de estrategias, procedimientos, recursos, responsabilidades y acciones orientadas a garantizar la continuidad operativa del servicio de internet y minimizar los procesos críticos ante eventuales interrupciones (fallas eléctricas, errores humanos, fallas de hardware e interrupciones del servicio de internet), reduciendo los tiempos de recuperación y minimizando el impacto operativo, financiero y reputacional para la institución.

Este plan se ajusta con la principal Norma de la ISO 22301:2019 sobre continuidad del negocio, priorizando la identificación de escenarios de riesgo, la preparación organizacional y la capacidad de respuesta ante incidentes tecnológicos que afecten la conectividad y los sistemas de información

6.21.2. Alcance del Plan de Contingencia

En la matriz de alcance del Plan de Contingencia Tecnológico se identifica los recursos tecnológicos, humanos y operativos que participan en la respuesta ante incidentes que afecten la continuidad de los servicios en la sucursal, especialmente la caída del servicio de internet.

Con el propósito de definir el alcance del plan de contingencia, se identificaron los elementos críticos que intervienen en la continuidad del servicio de internet en la Sucursal San Juan de la Concepción.

La siguiente matriz presenta los componentes tecnológicos, humanos y operativos, así como su nivel de dependencia y criticidad dentro de la organización.

Tabla 24

Matriz alcance del plan de contingencia

Categoría	Elemento Incluido	Función Operativa	Dependencia	N crítico
Infraestructura Tecnológica	Router principal	Gestiona conectividad hacia sistemas centrales	Alta	Crítica
Infraestructura Tecnológica	Switches de red	Distribución interna de la red	Media	Alta
Infraestructura Tecnológica	Enlace de datos hacia oficina central	Comunicación con sistemas financieros	Alta	Crítica
Infraestructura Tecnológica	UPS de soporte eléctrico	Respaldo energético de equipos críticos	Media	Alta

Infraestructura Tecnológica	Equipos de caja y atención	Ejecución de transacciones financieras	Alta	Crítica
Infraestructura Tecnológica	Servidor local	Servicios internos y soporte operativo	Media	Media
Sistemas e Información	SISCOMIF	Sistema financiero principal	Alta	Crítica
Sistemas e Información	Tecnocaja	Operaciones de caja	Alta	Crítica
Sistemas e Información	Tecnomóvil	Operaciones de promotores	Alta	Alta
Sistemas e Información	Base de datos financiera	Almacenamiento de información institucional	Alta	Crítica
Servicios Tecnológicos	Internet ISP principal	Acceso a sistemas centralizados	Alta	Crítica
Recursos Humanos	Responsable TI	Gestión técnica del incidente	Alta	Crítica
Recursos Humanos	Personal de cajas	Operaciones financieras	Alta	Crítica
Recursos Humanos	Atención al cliente	Servicio al asociado	Media	Alta
Recursos Humanos	Gerencia de sucursal	Toma de decisiones	Baja	Crítica

Fuente: Elaboración propia con base en el diagnóstico institucional

Los resultados evidencian que la mayoría de los elementos críticos presentan una alta dependencia del servicio de internet, especialmente los sistemas financieros, la infraestructura tecnológica y los procesos de atención al cliente. Asimismo, se observa que los componentes más críticos están directamente vinculados a la operatividad diaria de la cooperativa, lo que refuerza la necesidad de establecer estrategias de contingencia orientadas a garantizar la disponibilidad del servicio y minimizar el impacto ante posibles fallas de conectividad.

6.22. Objetivo del Plan de Contingencia

6.22.1. Objetivo General

Establecer un conjunto de acciones preventivas y correctivas que permitan garantizar la continuidad del servicio de internet y de los procesos críticos de COOPACRESMHA, Sucursal San Juan de la Concepción, ante eventos que afecten la infraestructura tecnológica, minimizando los tiempos de interrupción y el impacto operativo, financiero y reputacional.

6.22.2. Objetivos Específicos

- ✓ Definir procedimientos de actuación ante fallas TIC que permitan reducir los tiempos de interrupción.
- ✓ Establecer estrategias preventivas y correctivas basadas en riesgos priorizados.
- ✓ Asegurar la recuperación de servicios dentro de los tiempos máximos tolerables (MTD).
- ✓ Determinar roles, responsabilidades y cadena de mando para situaciones de contingencia.
- ✓ Proveer lineamientos para la comunicación interna y externa durante incidentes.
- ✓ Definir los planes de pruebas, auditoría y actualización del plan.

6.23. Modelo General de Gestión de Contingencias (BCM)*

Plan de Contingencia ante la caída del servicio de internet se estructura bajo el Modelo de Gestión de Continuidad del Negocio (Business Continuity Management – BCM), el cual permite a la organización anticiparse, responder y recuperarse de eventos que interrumpen la operatividad normal de los sistemas de información y los procesos críticos.

Este modelo se basa en el ciclo de continuidad del negocio, garantizando la disponibilidad de los servicios esenciales y la reducción del impacto operativo, financiero y reputacional durante una interrupción del servicio de internet.

El plan se estructura según el ciclo de gestión de continuidad de negocio:

- ✓ Prevención
- ✓ Preparación
- ✓ Respuesta
- ✓ Recuperación
- ✓ Revisión y mejor continua

Estos elementos son consistentes con ISO 22301, se integran en las estrategias siguientes.

Con base en los principios de la gestión de continuidad del negocio (BCM) y en concordancia con la norma ISO 22301, se estructuró un modelo general de gestión de contingencia orientado a garantizar la continuidad del servicio de internet en COOPACRESMHA, Sucursal San Juan de la Concepción. Este modelo se organiza en fases que permiten prevenir, preparar, responder, recuperar y mejorar continuamente la gestión ante eventos disruptivos.

Tabla 25

Modelo General de gestión de contingencia (BCM)

Fase BCM	Objetivo	Responsable	Recursos Requerido	Resultados Esperados
Prevención	Reducir riesgos	Administrador TI Soporte Técnico	Router, switches, UPS,	Disminución de fallas operativa
Preparación	Definir estructura	Jefe TI Gerencia Personal Operativo	Manual del plan,	Personal preparado y respuesta estructurada
Respuesta	Mantener operaciones durante la caída del internet	Administrador TI Soporte TI Jefes de Área	Conexión alterna, telefonía móvil,	Continuidad mínima de operaciones críticas
Recuperación	Restablecer la operación normal del servicio	Equipo TI Usuarios de Sistemas Gerencia	Sistemas informáticos, bases de datos,	Retorno seguro a la normalidad
Revisión y Mejora Continua	Fortalecer el plan	Equipo tecnico y operativo.	Informes de incidentes,	Mejora continua del sistema BCM

Fuente: Elaboración propia con base en el enfoque de continuidad del negocio (BCM) e ISO 22301

La implementación de este modelo permite establecer una respuesta estructurada ante fallas del servicio de internet, integrando recursos tecnológicos, humanos y organizacionales. Asimismo, facilita la reducción de riesgos, la continuidad de los procesos críticos y la mejora continua de las capacidades institucionales frente a incidentes tecnológicos.

6.24. Escenarios de Activación del plan

Con el propósito de definir los criterios de activación del plan de contingencia, se identificaron los principales escenarios que pueden afectar la continuidad del servicio de internet en la sucursal. La siguiente tabla presenta los eventos críticos, su impacto en los sistemas institucionales y las acciones iniciales a ejecutar ante cada situación.

Tabla 26

Escenarios de activación del plan

Escenario	Descripción del Evento	Impacto en Sistema Centralizado	Nivel de Activación	Acción Inicial
Caída total del internet en sucursal	Pérdida completa de conectividad externa	Sin acceso a sistemas centrales	Crítico	Activar plan completo y operación manual
Fallo del proveedor ISP	Incidencia externa	Interrupción total	Crítico	Activar enlace alternativo
Intermitencia prolongada del servicio	Conexión inestable	Lentitud o errores en transacciones	Medio	Monitoreo y preparación de contingencia

Corte eléctrico prolongado	Falta de energía en sucursal	Desconexión de red y sistemas	Crítico	Activar UPS y protocolos manuales
Falla de router principal	Daño en equipo de conectividad	Sin acceso a casa matriz	Medio	Sustitución o reconfiguración

Fuente: Elaboración propia con base en el análisis de riesgos y diagnóstico institucional (2026).

La identificación de escenarios de activación permite establecer criterios claros para iniciar el Plan de Contingencia Informático ante eventos que comprometan la conectividad con los sistemas centralizados. Esto facilita la toma de decisiones oportunas, minimiza el impacto en la atención a los asociados y asegura la continuidad de las operaciones críticas de la sucursal.

Con el objetivo de validar la efectividad del Plan de Contingencia Informático y asegurar la preparación del personal ante interrupciones del servicio de internet, se establecen pruebas y simulacros periódicos que permitan evaluar tiempos de respuesta, coordinación operativa y cumplimiento de los procedimientos definidos.

Tabla 27

Matriz prueba y simulacro

Tipo de Prueba	Objetivo	Frecuencia	Participantes	Responsable	Evidencia
Simulacro de caída total de internet	Evaluar activación del plan	Semestral	TI, Caja, Atención	Responsable TI	Acta y bitácora
Prueba de enlace alternativo (4G/ISP secundario)	Validar conmutación y continuidad	Trimestral	Soporte TI	Soporte TI	Registro técnico
Ejercicio de comunicación interna	Medir tiempos y claridad de avisos	Trimestral	Administración, Jefaturas	Administración	Lista de difusión
Prueba de respaldo y restauración		Semestral	Administrador de Sistemas	TI	Informe de prueba

6.25. Prioridad de Procesos Críticos (BIA Integrado)

Con base en el análisis de impacto al negocio (BIA), se identificaron y priorizaron los procesos críticos de la sucursal considerando su dependencia del sistema centralizado, el impacto financiero, el impacto en la atención al asociado y el tiempo máximo tolerable de interrupción.

Tabla 28

Matriz de prioridad de procesos críticos (orden de recuperación)

Proceso Crítico	Dependencia del Sistema Central	Impacto si se detiene	Tiempo Máximo Tolerable	Nivel
Operaciones de Caja depósitos, retiros, pagos	Total	Paralización inmediata de atención	30 – 60 min	Crítico
Consulta de saldos y cuentas	Total	Imposibilidad de validar operaciones	1 hora	Crítico
Registro de transacciones financieras	Total	Riesgo de errores contables	1 – 2 horas	Alto
Atención al asociado	Parcial	Retrasos y acumulación de usuarios	2 horas	Alto
Transferencias y pagos electrónicos	Total	Afectación a compromisos financieros	2 horas	Alto
Reportes operativos diarios	Media	Retraso administrativo	4 horas	Medio
Comunicación institucional (correo)	Media	Coordinación limitada	6 horas	Medio
Procesos administrativos internos	Baja	Impacto operativo menor	8 horas	Bajo

Fuente: Elaboración propia con base en el análisis de impacto en el negocio (BIA) y diagnóstico institucional.

6.26. Estrategias de Continuidad del Servicio en COOPACRESMHA

Considerando los riesgos tecnológicos identificados, el análisis de impacto al negocio (BIA) y la dependencia de la sucursal respecto al sistema centralizado de casa matriz, se establecen las siguientes estrategias de continuidad orientadas a reducir el impacto operativo y garantizar la disponibilidad de los procesos críticos ante incidentes tecnológicos.

Tabla 29

Estrategia de continuidad del servicio

Amenaza / Escenario de Contingencia	Estrategia de Continuidad	Responsable	Tiempo Objetivo (RTO)
Caída del servicio de internet	Redundancia de conectividad	Área de TI	2–10 minutos
Fallas del suministro eléctrico	UPS para equipos críticos	Administración / TI	0–45 minutos
Fallas de hardware crítico	Inventario de repuestos	Área de TI	Preventivo
Fallas de hardware crítico	Sustitución de equipos	Área de TI	10–30 minutos
Fallas de sistemas informáticos	Restauración del sistema	Área de TI / Proveedor	30–120 minutos
Errores humanos	Capacitación y manuales	RRHH / TI	Preventivo

Fuente: Elaboración propia en base a entrevistas

Las estrategias propuestas permiten asegurar la continuidad del servicio de internet mediante redundancia de conectividad, respaldo eléctrico, sustitución de equipos y medidas de seguridad informática, mejorando la disponibilidad y confiabilidad del servicio en COOPACRESMHA.

Con el propósito de evaluar la viabilidad estratégica de las estrategias de continuidad propuestas, se desarrolló una matriz FODA que identifica los factores internos y externos que influyen en la implementación del plan de contingencia.

Tabla 30

Matriz FODA del plan de contingencia del servicio de internet

Fortalezas (F)	Oportunidades (O)
F1. Redundancia de conectividad mediante enlaces alternos.	O1. Disponibilidad de múltiples proveedores de internet en el mercado.
F2. Procedimientos documentados de respuesta a incidentes.	O2. Avances tecnológicos en redes y seguridad informática.
F3. Uso de UPS y planta eléctrica para respaldo energético.	O3. Programas de capacitación en ciberseguridad y continuidad del negocio.
F4. Inventario de hardware crítico para sustitución inmediata.	O4. Normativas internacionales (ISO 22301, NIST) que fortalecen la gestión de continuidad.
F5. Políticas de seguridad informática y firewall implementados.	O5. Disponibilidad de soluciones en la nube para respaldo de información.
F6. Definición de tiempos objetivos de recuperación (RTO).	O6. Apoyo de proveedores tecnológicos y consultoras de TI.

Matriz FODA del plan de contingencia del servicio de internet

Debilidades (D)	Amenazas (A)
D1. Presupuesto limitado para infraestructura tecnológica.	A1. Fallas prolongadas del proveedor de internet principal.
D2. Dependencia de proveedores externos de tecnología.	A2. Cortes prolongados de energía eléctrica.
D3. Personal con limitada formación en continuidad del negocio.	A3. Ciberataques (malware, ransomware, phishing).
D4. Falta de monitoreo automatizado de infraestructura.	A4. Desastres naturales (tormentas, inundaciones).
D5. Ausencia de pruebas periódicas del plan de contingencia.	A5. Fallas críticas del sistema financiero o del servidor.
D6. Documentación limitada de procesos tecnológicos.	A6. Errores humanos en operaciones críticas.

Fuente: Elaboración propia con base en el diagnóstico institucional

El análisis FODA permite identificar estrategias que combinan fortalezas, oportunidades, debilidades y amenazas, facilitando la formulación de planes estratégicos organizacionales

Estrategias FO (Fortalezas–Oportunidades)

- ✓ Implementar soluciones avanzadas de seguridad informática aprovechando los avances tecnológicos del mercado.
- ✓ Fortalecer la continuidad del negocio mediante la adopción de estándares internacionales como ISO 22301.
- ✓ Capacitar al personal utilizando programas de formación ofrecidos por proveedores tecnológicos y universidades.

Estrategias DO (Debilidades–Oportunidades)

- ✓ Gestionar financiamiento institucional para fortalecer la infraestructura tecnológica.

- ✓ Implementar monitoreo automatizado aprovechando herramientas tecnológicas disponibles en el mercado.
- ✓ Documentar procedimientos y manuales técnicos con apoyo de consultores de TI.

Estrategias FA (Fortalezas–Amenazas)

- ✓ Utilizar enlaces redundantes para mitigar fallas del proveedor principal.
- ✓ Implementar políticas de seguridad informática para reducir riesgos de ciberataques.
- ✓ Utilizar UPS y planta eléctrica para garantizar continuidad ante cortes de energía.

Estrategias DA (Debilidades–Amenazas)

- ✓ Realizar pruebas periódicas del plan de contingencia para reducir vulnerabilidades operativas.
- ✓ Capacitar al personal para disminuir errores humanos.
- ✓ Establecer contratos de soporte con proveedores tecnológicos para reducir dependencia externa

6.27. Procedimientos Operativos del Plan

Los procedimientos operativos del Plan de Contingencia de la Cooperativa COOPACRESMHA constituyen el conjunto de acciones estructuradas que permiten responder de manera oportuna y organizada ante incidentes que afecten la disponibilidad del servicio de internet y los procesos tecnológicos críticos de la institución.

Estos procedimientos establecen las responsabilidades, los mecanismos de activación, los canales de comunicación y las acciones de recuperación y restablecimiento del servicio, con el propósito de garantizar la continuidad operativa de las actividades financieras y administrativas de la cooperativa.

6.27.1. Protocolo de Activación del plan de Contingencia

La Tabla de Protocolo de activación presenta el flujo del Protocolo de Activación del Plan de Contingencia, el cual describe las etapas desde la detección del incidente hasta el registro del evento. Este flujo permite estructurar la respuesta organizacional ante incidentes tecnológicos, garantizando una activación oportuna del plan y una adecuada documentación para la mejora continua del proceso.

Tabla 31

Protocolo de activación del plan de contingencia

Etapas	Descripción del Proceso	Responsable	TR Máximo
1. Detección del Incidente	El área de Tecnologías de la Información (TI) detecta una anomalía servicio.	Área de TI / Usuarios	5 minutos
2. Evaluación del Incidente	El responsable de TI evalúa la magnitud del incidente,	Responsable de TI	10 minutos
3. Verificación de Condiciones de Activación	Se verifica si el incidente cumple las condiciones de activación del plan,	Área de TI	5 minutos
4. Notificación y Autorización	El responsable de TI notifica a la Gerencia sobre la situación	Responsable de TI / Gerencia	15 minutos
5. Activación del Plan de Contingencia	Una vez autorizada la activación, se ejecuta	Área de TI	30 minutos

6.27.2. Protocolo de Comunicación de un plan de contingencia.

El protocolo de comunicación del Plan de Contingencia establece los mecanismos formales para la transmisión de información durante la ocurrencia de incidentes que afecten la continuidad del servicio de internet en la cooperativa COOPACRESMHA.

Este protocolo define los canales de comunicación, el flujo de información y los responsables involucrados, con el propósito de garantizar una respuesta coordinada, oportuna y efectiva ante situaciones de emergencia tecnológica. Una comunicación estructurada permite minimizar el impacto de los incidentes, facilitar la toma de decisiones y asegurar la continuidad de las operaciones críticas de la institución.

La Tabla del Protocolo de Comunicación del Plan de Contingencia representa como se definen los canales, el flujo de información y los responsables involucrados en la gestión de incidentes tecnológicos, permitiendo una coordinación eficiente entre el área de Tecnologías de la Información, la Gerencia y el personal operativo.

Tabla 32

Protocolo de comunicación del plan de contingencia

Elemento	Descripción	Responsables
Objetivo del Protocolo	Establecer los mecanismos y canales de comunicación durante la ocurrencia de un incidente para garantizar una respuesta coordinada y oportuna.	Gerencia / Área de TI
Canales de Comunicación	Teléfono institucional; correo electrónico corporativo; mensajería instantánea interna; comunicaciones verbales directas.	Área de TI / Gerencia / Personal Operativo

Flujo de Comunicación	1) El personal afectado reporta el incidente al área de TI. 2) El área de TI informa a la Gerencia sobre el estado del servicio. 3) La Gerencia comunica al personal operativo (Caja, Atención al Cliente,	Área de TI / Gerencia / Oficina Central
Responsable Técnico	Coordinar la gestión técnica del incidente y validar la información antes de comunicarla.	Responsable del Área de TI
Responsable de Decisiones	Tomar decisiones operativas y autorizar acciones durante el incidente.	Gerencia
Responsables Operativos	Ejecutar los procedimientos alternos y brindar atención a los usuarios durante la contingencia.	Personal Operativo (Caja, Atención al Cliente, Promotores)

Fuente: Elaboración propia con base en el plan de contingencia propuesto para COOPACRESMHA, sucursal San Juan de la Concepción.

6.27.3. Protocolo de Recuperación del Plan de Contingencia.

Este protocolo define las actividades de diagnóstico, activación de recursos de respaldo, validación del servicio y documentación del proceso de recuperación, con el fin de garantizar continuidad de las operaciones financieras y administrativas de la cooperativa COOPACRESMHA.

Tabla 33

Protocolo de recuperación del plan de contingencia

Elemento	Descripción	Involucrados
Objetivo del Protocolo	Restaurar el servicio de internet y los sistemas críticos en el menor tiempo posible tras una interrupción, garantizando la continuidad de las operaciones de la cooperativa COOPACRESMHA.	Gerencia, Área de TI, Oficina Central
Procedimiento de Recuperación	1) Diagnóstico del origen de la falla (conectividad, hardware, energía o software). 2) Activación de enlaces alternos o equipos de respaldo. 3) Restauración del sistema desde copias de seguridad, 4) Verificación de conectividad con sistemas críticos (SISCOMIF, Oficina Central, plataformas financieras). 5) Validación del funcionamiento de caja y atención al cliente. 6) Documentación del tiempo de recuperación (RTO).	Área de TI, Personal de Caja, Atención al Cliente, Promotores
Herramientas de Recuperación	Enlace alternativo de internet, UPS, planta eléctrica, equipos de red de respaldo, servidores alternos, copias de seguridad del sistema, software de monitoreo.	Área de TI, Proveedores de tecnología
Responsable	Área de TI: Ejecución técnica del proceso de recuperación. Gerencia: Supervisión y toma de decisiones operativas.	Área de TI, Gerencia

Indicadores de Recuperación	Tiempo de recuperación (RTO), disponibilidad del servicio (%), número de incidentes recuperados, tiempo promedio de respuesta técnica.	Gerencia, Área de TI,
-----------------------------	--	-----------------------

Fuente: Elaboración propia con base en el plan de contingencia propuesto para COOPACRESMHA, sucursal San Juan de la Concepción.

6.27.4. Protocolo de Restablecimiento

El Protocolo de Restablecimiento del Servicio define las actividades necesarias para retornar a las operaciones habituales de la cooperativa COOPACRESMHA una vez superado el incidente que activó el Plan de Contingencia. Este protocolo asegura que los sistemas críticos, la conectividad y los procesos operativos vuelvan a su estado normal de funcionamiento, garantizando la estabilidad del servicio y la continuidad de las operaciones financieras

Tabla 34

Protocolo de restablecimiento del plan de contingencia.

Procedimiento de Restablecimiento	Descripción	Área Responsable
Confirmación de estabilidad del sistema	Verificar que el enlace principal, los servidores y los sistemas críticos operen correctamente sin fallas.	Área de TI
Retorno a la infraestructura primaria	Migrar las operaciones del enlace alternativo o equipos de respaldo al enlace principal o infraestructura primaria.	Área de TI
Desactivación de recursos de contingencia	Desconectar enlaces alternos, apagar equipos de respaldo y desactivar configuraciones temporales.	Área de TI

Evaluación del incidente	Analizar el incidente ocurrido, su impacto operativo y tecnológico, y las acciones ejecutadas durante la contingencia.	Área de TI y Gerencia
Análisis de causa raíz	Identificar las causas técnicas y organizativas del incidente para evitar recurrencias.	Área de TI
Elaboración del informe post-incidente	Documentar el incidente, tiempos de recuperación, impacto y recomendaciones de mejora.	Área de TI y Gerencia

Fuente: Elaboración propia con base en el plan de contingencia propuesto para COOPACRESMHA, sucursal San Juan de la Concepción.

6.28. Roles Y Responsabilidades (RACI)

Con el fin de garantizar una respuesta organizada y oportuna ante la caída del servicio de internet en la Sucursal San Juan de la Concepción, se establece la siguiente matriz de roles y responsabilidades bajo el modelo RACI. Esta herramienta permite definir claramente quién ejecuta las acciones técnicas, quién toma decisiones operativas, quién debe ser consultado durante el incidente y quién debe mantenerse informado, facilitando la coordinación entre el personal interno y los proveedores tecnológicos durante la activación del plan de contingencia TI.

Indicadores de la Matriz

- R Responsable (Ejecuta acción)
- A Aprobador (Autoridad)
- C Consultado
- I Informado

Tabla 35

Matriz RACI plan de contingencia

Actividad / Cargo	Gerente General	Admon / Jefe de Agencia	Admon de TI	Auxiliar de TI	Jefatura de Cajas	Cajeros / Promotores	Proveedores ISP / Soporte Externo
Detección del incidente	I	I	C	R	I	R	I
Evaluación del incidente	C	A	R	C	I	I	C
Activación del Plan de Contingencia	A	R	C	C	I	I	I
Comunicación del incidente	A	R	C	I	I	I	I
Failover (enlace alternativo)	I	I	R	R	I	I	C
Activación UPS / Planta eléctrica	I	I	R	R	I	I	C
Recuperación de sistemas y datos	C	I	R	R	I	I	C
Validación de operaciones de caja	I	I	C	I	R	R	I
Restablecimiento del servicio normal	A	R	C	C	I	I	C
Informe post-incidente	A	R	C	C	I	I	I
Actualización del Plan de Contingencia	A	R	R	C	C	I	I

La matriz RACI permite establecer una distribución clara de responsabilidades durante la activación del plan de contingencia TI ante la caída del servicio de internet en la Sucursal San Juan de la Concepción. Su aplicación facilita la coordinación entre la gerencia, el área tecnológica, el personal operativo de cajas y los proveedores externos, asegurando una respuesta estructurada

que contribuya a reducir tiempos de interrupción y mantener la continuidad de los servicios brindados a los asociados.

6.29. Niveles de Activación del Plan de Contingencia TI

Con el propósito de garantizar una respuesta proporcional a la gravedad de la caída del servicio de internet en la Sucursal San Juan de la Concepción, se establecen niveles de activación del plan de contingencia TI. Estos niveles permiten definir el grado de impacto operativo y asignar acciones específicas a cada rol institucional, facilitando una intervención escalonada que reduzca tiempos de interrupción y mantenga la continuidad en la atención a los asociados.

6.30. Plan de Comunicación durante Incidentes

Con el objetivo de garantizar una comunicación clara, oportuna y organizada durante incidentes relacionados con la caída del servicio de internet en la Sucursal San Juan de la Concepción, se establece el siguiente plan de comunicación. Este plan define los responsables de informar, los canales oficiales y los tiempos de notificación según el nivel de gravedad del incidente, permitiendo coordinar acciones operativas y mantener informados a los colaboradores y autoridades institucionales durante la contingencia.

Tabla 36

Matriz de comunicación durante incidentes

Nivel de Incidente	Quién Comunica	A Quién se Comunica	Información a Transmitir	Canal de Comunicación	Tiempo Máximo
 Bajo	Área de TI	Jefe de Cajas	Estado del servicio y acciones técnicas iniciales	Mensajería interna / Teléfono	10 minutos
 Medio	Área de TI	Gerencia y Jefe de Cajas	Activación de enlace alternativo y estado operativo	Teléfono / Correo institucional	15 minutos
 Crítico	Gerencia + Área de TI	Todo el personal operativo y proveedores	Activación del plan, impacto en operaciones y medidas a aplicar	Reunión rápida / Teléfono / Correo	Inmediato (≤5 min)

El plan de comunicación permite establecer un flujo estructurado de información durante incidentes de conectividad, garantizando que cada nivel organizacional reciba instrucciones claras según el impacto operativo

6.31. Plan de Pruebas y Simulacros del Plan de Contingencia TI

Con el propósito de verificar la efectividad del plan de contingencia TI ante la caída del servicio de internet y otros incidentes tecnológicos que puedan afectar la operación de la Sucursal San Juan de la Concepción, se establece el siguiente plan de pruebas y simulacros.

Estas actividades permiten evaluar la capacidad de respuesta del personal, validar los procedimientos técnicos definidos y detectar oportunidades de mejora continua para garantizar la continuidad de las operaciones financieras y administrativas.

Tabla 37

Matriz del plan de pruebas y simulacros.

Tipo de Prueba / Simulacro	Objetivo	Frecuencia	Responsable Principal	Participantes	Evidencia Generada
Prueba de conmutación de internet (failover)	Verificar activación del enlace alternativo ante caída del servicio	Cada 3 meses	Área de TI	Jefatura de Cajas	Bitácora técnica y resultados de conexión
Simulacro de falla eléctrica	Validar funcionamiento de UPS y continuidad operativa	Cada 6 meses	Área de TI	Personal operativo	Registro de prueba y tiempos de respuesta
Simulacro de caída del sistema SISCOMIF	Evaluar respuesta operativa ante	Cada 6 meses	Área de TI	Cajas y Atención al asociado	Informe del simulacro

	interrupción del sistema				
Restauración de respaldos (backups)	Verificar integridad y recuperación de la información	Semanal	Área de TI	—	Registro de restauración
Auditoría del Plan de contingencia TI	Evaluar cumplimiento y actualización del plan	Anual	Gerencia / TI	Soporte externo	Informe de auditoría

Después de cada prueba o simulacro, el área de TI deberá elaborar un informe que incluya los resultados obtenidos, los tiempos de recuperación observados y las oportunidades de mejora detectadas. Estos resultados serán revisados por la gerencia para actualizar procedimientos, reforzar capacitaciones y fortalecer las estrategias de continuidad operativa ante posibles interrupciones del servicio de internet.

6.32. Plan de Mantenimiento y Actualización del Plan de Contingencia TI

Con el fin de asegurar la vigencia y efectividad del plan de contingencia TI ante la caída del servicio de internet en la Sucursal San Juan de la Concepción, se establece un programa de mantenimiento y actualización continua. Este plan permite revisar periódicamente los procedimientos definidos, incorporar mejoras derivadas de pruebas.

Tabla 38

Matriz de mantenimiento y actualización del plan

Actividad de Mantenimiento	Objetivo	Frecuencia	Responsable	Evidencia
Revisión general del plan de contingencia TI	Verificar vigencia de procedimientos y roles	Semestral	Área de TI	Informe de revisión
Actualización de contactos y proveedores	Mantener información operativa actualizada	Trimestral	Área de TI	Registro actualizado
Actualización de inventario tecnológico	Validar equipos críticos y respaldos	Trimestral	Área de TI	Listado de activos actualizado
Incorporación de mejoras post-simulacros	Ajustar procedimientos según resultados	Después de cada prueba	Área de TI / Gerencia	Acta de mejora
Revisión de políticas de seguridad informática	Fortalecer controles ante amenazas tecnológicas	Anual	Área de TI	Documento actualizado
Validación del plan por Gerencia	Asegurar alineación con operaciones de la sucursal	Anual	Gerencia	Acta de aprobación

El mantenimiento periódico del plan de contingencia TI permite que la sucursal mantenga una preparación constante ante posibles interrupciones del servicio de

internet, asegurando que los procedimientos definidos respondan a las condiciones reales de operación, a los cambios tecnológicos y a las lecciones aprendidas durante pruebas y eventos reales.

6.33. Indicadores de Desempeño (KPIs) del Plan de Contingencia TI

Con el propósito de evaluar la efectividad del plan de contingencia TI ante interrupciones del servicio de internet en la Sucursal San Juan de la Concepción, se establecen indicadores clave de desempeño (KPIs) que permiten medir la capacidad de respuesta técnica, la continuidad operativa y el cumplimiento de las estrategias de recuperación implementadas. Estos indicadores facilitan el monitoreo continuo del desempeño institucional durante incidentes tecnológicos y contribuyen a la mejora permanente del plan.

Tabla 39

Indicadores de plan de contingencia

Indicador (KPI)	Descripción	Fórmula de Cálculo	Frecuencia de Medición	Responsable	Meta Referencial
Tiempo promedio de recuperación (MTTR)	Restablecimiento de conectividad tras una caída	Tiempo total de recuperación	Mensual	Área de TI	≤ 10 minutos
Cantidad de incidentes	Número de caídas totales del operaciones	Total, de incidentes críticos	Mensual	Área de TI	≤ 2 incidentes
Disponibilidad del internet (%)	Porcentaje servicio operativo	(Horas disponibles ÷ horas totales) × 100	Mensual	Área de TI	≥ 98%

Tiempo en modo contingencia	Tiempo total que la sucursal opera bajo procedimientos alternos	Horas totales en contingencia	Mensual	Área de TI / Gerencia	≤ 2% del tiempo operativo
-----------------------------	---	-------------------------------	---------	-----------------------	---------------------------

Los indicadores definidos permiten evaluar de manera objetiva el desempeño del plan de contingencia TI ante la caída del servicio de internet, facilitando el seguimiento de los tiempos de recuperación, la disponibilidad del servicio y la efectividad de las estrategias implementadas. Su análisis periódico contribuye a la toma de decisiones informadas por parte de la gerencia y al fortalecimiento continuo de la capacidad operativa de la sucursal frente a incidentes tecnológicos.

6.34. Análisis de Costo Beneficio del Plan de Contingencia Informático

Con el propósito de garantizar la viabilidad técnica y operativa del Plan de Contingencia Informático propuesto para COOPACRESMHA Sucursal San Juan de la Concepción, se realizó un análisis costo–beneficio orientado a evaluar las posibles inversiones necesarias para fortalecer la continuidad operativa ante interrupciones del servicio de internet y otros eventos tecnológicos críticos. Este análisis se fundamenta en los principios de continuidad del negocio establecidos en la norma ISO 22301:2019, la cual promueve la evaluación de los recursos requeridos para asegurar la disponibilidad de los procesos críticos frente a escenarios de interrupción.

El análisis consideró tanto los costos asociados a la implementación de medidas preventivas y correctivas como los beneficios operativos derivados de la reducción de riesgos, la continuidad de las operaciones financieras y la disminución de pérdidas económicas por interrupciones del servicio.

En el marco de las medidas evaluadas, se identificó como prioridad estratégica la implementación de un sistema de respaldo eléctrico mediante generador, debido a que la interrupción del suministro eléctrico fue determinada como uno de los factores de mayor impacto en la continuidad operativa de la sucursal. La dependencia directa de la energía eléctrica para el funcionamiento del servicio de internet, sistemas financieros, estaciones de trabajo y dispositivos de red convierte esta vulnerabilidad en un riesgo crítico para la institución.

El análisis costo - beneficio se centra en evaluar la viabilidad técnica y económica de la adquisición e instalación de una planta eléctrica como mecanismo de mitigación del riesgo. Se consideran los costos asociados a la compra del equipo, instalación, materiales complementarios, mano de obra y mantenimiento preventivo, frente a los beneficios derivados de la reducción de tiempos de inactividad, continuidad en la atención al cliente, estabilidad en las operaciones financieras y protección de la imagen institucional.

También, se realizó un análisis comparativo entre el escenario actual (sin sistema de respaldo eléctrico) y el escenario propuesto (con planta electricidad del negocio).

Tabla 40

Escenario (sin generador vs generador)

Criterio de Evaluación	Sin Generador	Con Generador (12KVA/10KW)
Continuidad operativa	Interrupción total de operaciones ante corte eléctrico.	Operación continua de sistemas críticos (servidor, red, cajas).
Servicio de Internet	Caída inmediata al suspenderse energía eléctrica.	Se mantiene activo al energizar equipos de red.
Área de Cajas	Paralización de transacciones financieras.	Procesamiento continuo de pagos y desembolsos.

Atención al cliente	Retrasos, inconformidad y aumento de quejas.	Atención estable y reducción de tiempos de espera.
Descargue de data de promotores	Imposibilidad de sincronizar información.	Actualización normal de datos comerciales.
Supervisión gerencial	Sin acceso a reportes en tiempo real.	Monitoreo continuo de operaciones.
Pérdidas económicas por hora	Estimado USD 300–500 por paralización.	Mínimas o inexistentes.
Riesgo operativo	Alto (dependencia total de red eléctrica pública).	Bajo (infraestructura respaldada).
Riesgo reputacional	Elevado por fallas recurrentes.	Reducción del impacto en imagen
Protección de activos TI	Exposición a apagados abruptos y daños.	Energía estabilizada y protección de equipos críticos.
Cumplimiento de continuidad del negocio	No cumple buenas prácticas.	Alineado con principios de continuidad operativa.
Inversión inicial	USD 0	USD 9,404.47

Fuente: Elaboración propia con base en análisis técnico y diagnóstico realizado en COOPACRESMHA, sucursal San Juan de la Concepción.

6.34.1. Cálculo de Costos Estimados

- ✓ 2 técnicos
- ✓ 3 días de montaje
- ✓ 8 horas por día
- ✓ \$30 por hora por técnico
- ✓ Alimentación estimada \$15 por persona por día
- ✓ Transporte estimado \$30
- ✓ Materiales eléctricos y accesorios estimados \$750

6.34.2. Cálculo de Mano de Obra

2 técnicos* 8 horas*3 días*\$ 30= \$1,440

Concepto	Descripción	Costo Estimado (USD)
Empresa proveedora	COMCAST NICARAGUA	—
Valor del equipo	Generador 12KVA/10KW	7,064.47
Mano de obra	2 técnicos × 3 días × 8 horas × \$30	1,440.00
Alimentación	2 técnicos × 3 días × \$15	90.00
Transporte	Traslado de equipo y personal	60.00
Materiales eléctricos	Cableado, breakers, tuberías, base, conectores	750.00
Total inversión (estimada)		\$ 9,404.47

Fuente: Elaboración propia en base a cotizaciones

6.35. Plan de Implementación

El plan de implementación establece las actividades necesarias para la puesta en marcha del Plan de Contingencia, definiendo los responsables, indicadores de cumplimiento y los proveedores que brindarán soporte técnico y consultoría. Este plan permite estructurar de manera

ordenada las acciones requeridas para garantizar la continuidad operativa de los servicios tecnológicos.

En la Tabla se presenta el plan de implementación del Plan de Contingencia, detallando las actividades, indicadores de cumplimiento, responsables, proveedores y acción propuesta.

Tabla 41

Plan de implementación del plan de contingencia

Actividad	Indicador de Cumplimiento	Responsable	Proveedor / Oferta	Descripción de la Actividad
Implementación de políticas de respaldo	Políticas formalizadas y aprobadas	Área de TI	Capital Software S.A.	Consultoría para definir políticas y documentación formal de respaldo
Automatización de respaldos	Respaldos automáticos operativos	Área de TI	Cloud Nicaragua S.A.	Implementación de solución de respaldo en la nube y automatización de copias de seguridad
Pruebas de restauración	Registros de pruebas de restauración	Área de TI	Cloud Nicaragua S.A.	Soporte y restauración de datos desde la nube
Definición de roles y responsabilidades	Documento de responsabilidades	Gerencia / TI	Capital Software S.A.	Asesoría para estructurar matriz de responsabilidades
Documentación de procedimientos	Procedimientos documentados	Área de TI	Capital Software S.A.	Elaboración de manuales y protocolos técnicos
Capacitación del personal	Personal capacitado	Gerencia / TI	Capital Software S.A.	Cursos y talleres sobre sistemas y continuidad operativa

Implementación de respaldo en la nube	Backups en la nube disponibles	Gerencia / TI	Cloud Nicaragua S.A.	Servicio de respaldo en la nube con seguridad de datos
Fortalecimiento del respaldo energético	Equipos críticos protegidos	Gerencia Administrativa	UPS Central Managua / UPS	Adquisición de UPS para equipos críticos (APC o Forza)

6.35.1. Presupuesto del Plan de Contingencia

El presupuesto del Plan de Contingencia contempla los costos asociados a la implementación de políticas, automatización de respaldos, capacitación del personal y adquisición de infraestructura tecnológica. Los costos fueron estimados en córdobas nicaragüenses con base en precios del mercado local, lo que permite evaluar la factibilidad económica de la propuesta.

La Tabla muestra el presupuesto estimado del Plan de Contingencia, especificando los proveedores y los costos asociados a cada actividad planificada.

Tabla 42

Presupuesto del plan de contingencia

Actividad	Proveedor	Costo Estimado (C\$)
Implementación de políticas de respaldo	Capital Software S.A.	C\$ 2,500
Automatización de respaldos (anual)	Cloud Nicaragua S.A.	C\$ 9,000 / año
Pruebas de restauración	Cloud Nicaragua S.A.	Incluido en suscripción
Definición de roles y responsables	Capital Software S.A.	C\$ 1,200

Documentación de procedimientos	Capital Software S.A.	C\$ 4,500
Capacitación del personal	Capital Software S.A.	C\$ 10,000
Implementación de respaldo en la nube (anual)	Cloud Nicaragua S.A.	C\$ 9,000 / año
Respaldo energético (UPS)	UPS Central Managua / UPS	C\$ 6,000 – C\$ 20,000

Presupuesto estimado del Plan de Contingencia

6.35.2. Cronograma de Ejecución

El cronograma de ejecución define el tiempo requerido para la implementación de las actividades del Plan de Contingencia, clasificándolas en corto, mediano y largo plazo. Este cronograma permite planificar y priorizar las acciones necesarias para la continuidad operativa del sistema.

En la Tabla se presenta el cronograma de ejecución del Plan de Contingencia, indicando el plazo estimado para cada actividad programada.

Tabla 43

Cronograma de ejecución del plan de contingencia

Actividad	Plazo Estimado
Implementación de políticas de respaldo	Corto plazo (1 mes)
Automatización de respaldos	Corto – Mediano plazo (1–2 meses)
Pruebas de restauración	Permanente (trimestral)
Definición de roles y responsables	Corto plazo (1 mes)
Documentación de procedimientos	Mediano plazo (2–3 meses)
Capacitación del personal	Mediano plazo (3–4 meses)
Implementación de respaldo en la nube	Mediano plazo (3–6 meses)
Fortalecimiento del respaldo energético	Mediano plazo (3–6 meses)

VII. CONCLUSIONES

La presente investigación tuvo como propósito analizar la situación del servicio de conectividad a Internet en la sucursal San Juan de la Concepción, considerando que esta institución financiera depende directamente de los sistemas digitales para ejecutar sus procesos comerciales, financieros y administrativos. A partir del diagnóstico técnico realizado, se evidenció que la continuidad del servicio de Internet es un factor crítico para la operatividad de la sucursal, ya que cualquier interrupción afecta de forma inmediata las transacciones en cajas, la atención a los asociados, la supervisión gerencial y la sincronización de datos de los promotores.

El análisis permitió identificar vulnerabilidades importantes, principalmente la dependencia de un único proveedor de Internet, la ausencia de enlaces de respaldo y la inexistencia de protocolos formales de actuación ante fallas del servicio. Esta situación expone a la cooperativa a riesgos operativos, financieros y reputacionales. Ante este escenario, se diseñó un Plan de Contingencia orientado a reducir el tiempo de inactividad, fortalecer la resiliencia tecnológica y garantizar la continuidad de los procesos comerciales. La propuesta incorpora estrategias como redundancia de conectividad, monitoreo continuo del servicio, definición clara de responsabilidades y capacitación del personal.

Se concluye que la implementación del plan de Contingencia propuesto permite transformar la gestión tecnológica de un enfoque reactivo a un modelo estructurado, alineado con estándares internacionales como ISO 22301, fortaleciendo la continuidad de negocio.

VIII. RECOMENDACIONES

Como resultado del estudio realizado en COOPACRESMHA, Sucursal San Juan de la Concepción, se recomienda aprobar formalmente el Plan de Contingencia como política institucional e integrarlo en la planificación estratégica y el presupuesto anual, asegurando los recursos necesarios para su implementación y actualización continua.

Se sugiere fortalecer la infraestructura tecnológica mediante la contratación de un segundo proveedor de Internet, implementando redundancia real, equipos con failover automático y balanceo de carga, así como sistemas de respaldo eléctrico (UPS o planta eléctrica) que garanticen la continuidad ante fallas de energía.

Asimismo, se recomienda incorporar herramientas de monitoreo en tiempo real, realizar auditorías técnicas periódicas y mantener actualizada una matriz de riesgos tecnológicos. Es importante también definir claramente roles y responsabilidades dentro del plan, establecer indicadores como tiempo de recuperación y nivel de disponibilidad del servicio, todo esto incidente debe de ser documentado para mejorar la gestión preventiva. Desde el ámbito organizacional, se sugiere capacitar anualmente al personal, realizar simulacros de interrupción del servicio y fomentar una cultura orientada a la resiliencia tecnológica.

Finalmente, se recomienda considerar estas acciones como una inversión estratégica preventiva y no como un gasto, ya que contribuyen a reducir pérdidas operativas, proteger la reputación institucional y garantizar la continuidad de los procesos comerciales ante cualquier eventual interrupción del servicio de Internet.

IX. REFERENCIAS BIBLIOGRAFICAS

22301:2019, I. (30 de Octubre de 2019). ISO 22301:2019. Seguridad y Resiliencia, sistema de gestion de continuidad del riesgo, Segunda edicion Ginebra, Suiza.

Bogdan , T. (1987). Metodologia Cuantitativa Chicago, Estados Unidos.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, California, Estados Unidos: SAGE Publications.

Díaz, N. (02 de Noviembre de 2020). Plan de Contingencia de Telcor. (D. I. Barricada, Entrevistador)

García , N. D. (1988). Clasificación de las cooperativas. Clasificación de las cooperativas. Bogota, Colombia: Servicio Nacional de Aprendizaje (SENA).

Hernandez Sampieri, R. (2018). Metodologia de la Investigacion Ciudad de Mexico, Graw Hill Education.

Hernández Sampieri, R., Fernández Collado, C., & B. (2014). Metodología de la investigación (6.^a ed.). Mexico, Mexico: McGraw-Hill Education.

Stallings , W. (2013). Comunicaciones de datos y redes de computadoras. la infraestructura de red constituye el conjunto de dispositivos, medios de transmisión, protocolos y servicios que permiten la comunicación eficiente y segura entre sistemas de información. Boston, Estados Unidos: Madrid, España: Pearson Educación.

Stoneburner, Goguen, & Feringa, . (2002). Guía de gestión de riesgos para sistemas de tecnología de la información. la gestión de riesgos en los sistemas de información permite identificar, evaluar y mitigar amenazas que afectan a los activos organizacionales. Gaithersburg,, Maryland, Estados Unidos.

Taylor, S. J., & Bogdan, R. (1987). Introducción a los métodos cualitativos de investigación:. La investigación cualitativa busca interpretar y comprender los fenómenos sociales desde la perspectiva de los participantes. España: Paidós.

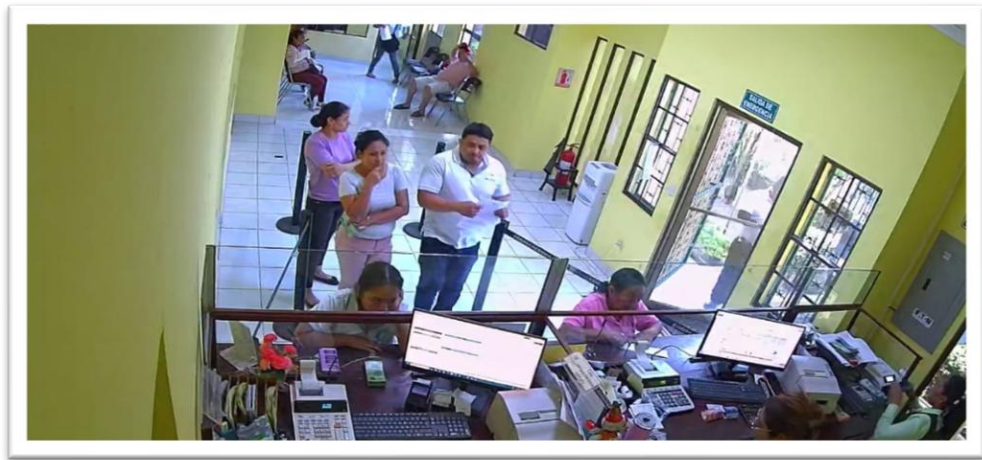
Weill & Ross. (2004). Cómo los mejores empleados gestionan los derechos de decisión de TI para obtener resultados superiores. Señalan que el gobierno de TI define quién toma las decisiones y cómo se monitorean. Harvard Business School Press.

X. ANEXOS

9.1. Punto de Estudio



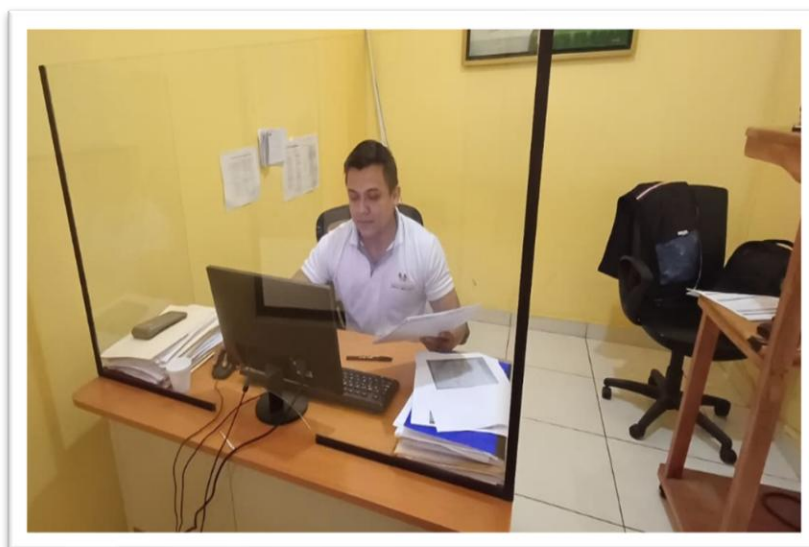
Entrada Principal Sucursal San Juan de La Concepción



Área de Caja

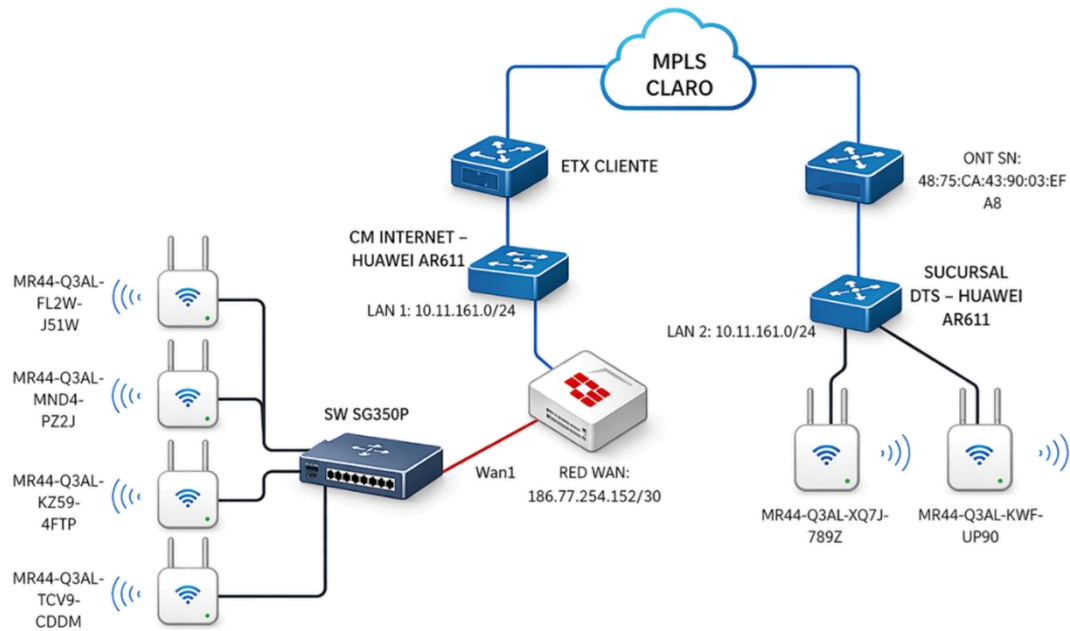


Área de Atención al cliente



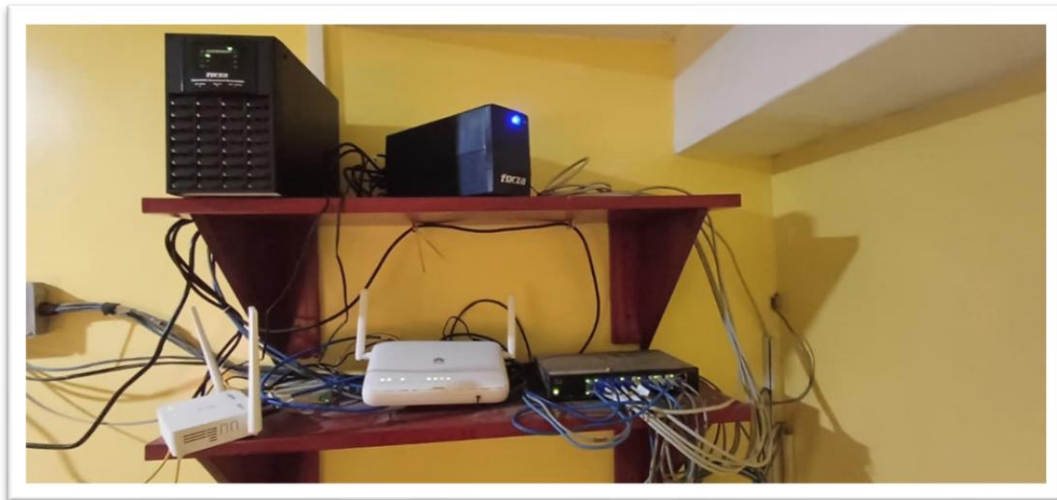
Área de Promotoría

9.2. Infraestructura Tecnológica Actual de COOPACRESMHA

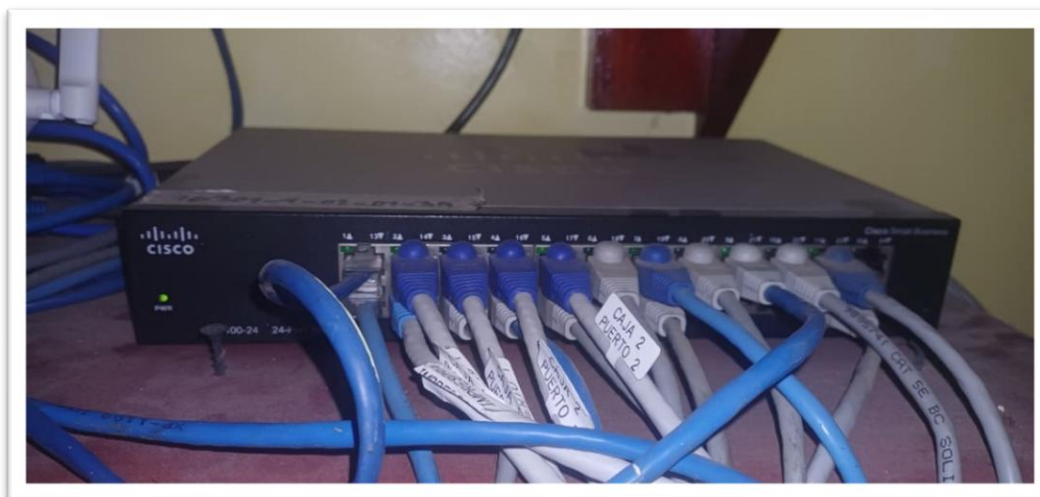


Enlace de Datos con oficina Central

Cliente: COOPERATIVA DE AHORRO, CREDITO Y SERVICIO HUBERTO AGUILAR							
SERVICIO ACTUAL							
ITEM	CONTRATO	PRODUCTO	TECNOLOGIA	PLAN COMERCIAL	DIRECCION	VELOCIDAD / EXTENSION /NUMERO	RENTA
	1074369	5927191	GPON	25461 - INTERNET CLARO GPON A	COLEGIO LA MARIPOSA 50 VRS AL OESTE	10 Mbps Simetrico	\$55.00
	1074369	6181487	GPON	787 - ENLACE METRO CORPORATIVO DEPARTAMENTAL	Del cuadro Deportivo San Juan 150 Mts al sur 25 vrs oeste	10 Mbps	\$105.00
TOTAL ANTES DE IVA							\$160.00



Evidencia del entorno Físico del centro de Datos Local Sucursal San Juan de la Concepción



Switch Cisco para la Distribución de red LAN



Dispositivo Router Huawei AR600 instalado en la Sucursal San Juan



Planta Eléctrica utilizada como respaldo energético en la Sucursal San Juan

Estimado colega

Su opinión es muy importante para nosotros. Le agradeceríamos que dedicara 5 minutos a proporcionarnos sus comentarios, los cuales nos ayudarán a identificar los aspectos problemáticos de su puesto de trabajo y asegurarnos de que nada le impida desempeñar su trabajo de manera efectiva.

Valoramos enormemente su perspectiva y el tiempo que nos dedica.

1. ¿En qué equipo se encuentra usted?

Servicio Financiero ☐

Gerencia ☐

Atención Asociado ☐

Tecnologías de la Información (IT) ☐

Área Caja ☐

Cartera y Cobro ☐

Otro ☐

2. ¿Cuánto tiempo lleva trabajando en COOPACRESMHA?

Menos de 1 año ☐

1 – 2 años ☐

3 – 5 años ☐

Más de 5 años ☐

3. Con que Frecuencia utiliza el servicio de Internet para realizar sus funciones?

Siempre ☐

Frecuentemente ☐

Ocasionalmente ☐

4. ¿Qué tan crítico considera el servicio de Internet para el cumplimiento de sus funciones diarias?

Muy Critico ☐

Critico ☐

Poco Critico ☐

No Crítico ☐

5. ¿Han Experimentado interrupciones del Servicio de Internet durante su Jornada Laboral?

☐ Si

☐ No

6- si la Respuesta es Sí, Con qué frecuencia ocurren estas Interrupciones?

Muy Frecuente ☐

Frecuente ☐

Poco Frecuente ☐

Rara vez ☐

No me doy cuenta ☐

7- Cual ha sido el impacto principal de estas Fallas en los procesos que realizan diarios?

Retrasos en Informes ☐

Interrupciones de Atención al Cliente ☐

Perdida Productividad ☐

otros ☐

8 ¿Existe actualmente algún procedimiento definido para actuar ante una falla en el servicio de Internet?

Si ☐

No ☐

No sé ☐

9. Considera que Proveedor de Servicio actúa de manera rápida cuando se reporta la falla?

Oportuno ☐

No Oportuno ☐

No Opino ☐

10- COOPACRESMHA sucursal San Juan cuenta con un servicio Alternativo de Internet para estos Casos?

SI ☐

No ☐

No Sé ☐

11- Considera Necesario implementar un plan de Contingencia formal para el servicio de Internet?

De Acuerdo ☐

Necesario ☐

No Necesario ☐

Urgente ☐

12-Que medida considera más importante ante una falla del Servicio de Internet?

Enlace de Internet Alterno ☐

Procedimientos Manuales ☐

Entrevista

1. ¿Cuál es su Cargo y área de Trabajo dentro de la Sucursal?
2. ¿Desde Hace Cuanto trabaja en COOPACRESMHA sucursal San Juan?
3. ¿Qué acciones se realizan actualmente cuando ocurre una falla en el Servicio de Internet?
4. ¿Quiénes son los responsables de tomar Decisiones ante una Interrupción de Servicio de Internet?
5. ¿Cuándo se suspende el Servicio de Internet que tan Productivo es en sus Funciones?
6. ¿Han ocurrido casos en donde el Servicio de Internet está por más de 2 Días inaccesible?
7. ¿Considera que cuentan con Infraestructura robusta y que los equipos están bien Protegidos antes bajones de energía?
8. ¿Los Bajones de Energía han ocasionado daños en los equipos que utiliza?
9. ¿La Inestabilidad de Energía ha dañado equipos como Router, Switch?

9.3. Propuestas de mejoras en Infraestructura y Aumento de Internet

COMCAST NIC

Km 9.6 carretera a Masaya
Plaza Guanacaste
Managua
NICARAGUA
+505-5709-5658
admin.nic@comcast-sa.com
www.comcast-sa.com



Cotización 11946

Fecha de Emisión: 2026-02-18 Citar expira fecha: 2026-02-18

Vendido A

COOPERATIVA HUMBERTO AGUILAR
COOPACRESMHA Sucursal San Juan de
Concepción ubicada del campo deportivo
Jarol Rosales 150 mtr al Su
J0110000132772
. 994d1
NICARAGUA
84735895

Enviar A

COOPERATIVA HUMBERTO AGUILAR
COOPACRESMHA Sucursal San Juan de
Concepción ubicada del campo deportivo
Jarol Rosales 150 mtr al Su
J0110000132772
. 994d1
NICARAGUA
84735895

Representante de Ventas: Lenin Cesar

Ln #	Cantidad	Descripción	Precio de Unidad	Total
1	1 Each	CEG-FA12S GENSET 12KVA/10KW standby 120/208v Silent : Generador motor FAWDE 4DW81-28D-YFD10W alternador CEG164ES, 60Hz, DSE6120, YES1-100GA	6143.024 Each	\$6,143.02

Subtotal: \$6,143.02
UPS-GROUND - Envío: \$0.00
Impuesto: \$921.45
Total: \$7,064.47

6 OFERTA ECONÓMICA

6.1 DESCRIPCIÓN COMERCIAL DEL SERVICIO (RECURRENTE MENSUAL)

A continuación, se presenta la oferta económica para el servicio **INTERNET CORPORATIVO**

Servicio como Recurrente Mensual:

DESCRIPCIÓN	MESES DE CONTRATO	RENTA MENSUAL
SERVICIO INTERNET EMPRESARIAL 30 MBPS CONEXIÓN FIBRA OPTICA	24	\$ 150.00
	TOTAL, RECURRENTE MENSUAL	\$ 150.00

Detalles de la oferta económica:

- Servicio Integral de **Internet corporativo** con un monto recurrente mensual de **\$ 150.00**.
- **Precios no incluyen IVA**
- **Los equipos detallados son propiedad de Tigo.**
- **Tiempo de entrega sujeto a disponibilidad de inventario.**
- COOPERATIVA HUMBERTO AGUILAR deberá proveer los puntos y respaldo eléctricos necesarios para la energización de los diferentes equipos a ser instalado.
- Garantía de equipos activa durante la vigencia del contrato.
- Soporte 24/7 durante la vigencia del contrato sobre los equipos rentados.

Oferta de Servicio – COOPACRESMHA R.L

Oferta de Servicio Internet						
Ítem	Sucursal	Cantidad	Servicio	Ancho de Banda-Mbps	Tecnología	Mensualidad
1	BO. GASPAR GARCIA LAVIANA, PALI LA CONCEPCION 1/2C NORTE, 11.934132, - 86.189484	1	Enlace de Datos(Nodo)	30	Fibra óptica	\$ 105.00
2	San Juan de la concepción , Barrio Luis Alfonso Velásquez del campo deportivo 150 más al sur 25 varas al oeste	1	Enlace de Datos	30	Fibra óptica	\$ 150.00
Tota de precios sin IVA						\$ 255.00

Ancho de Banda sin redundancia

Oferta de Servicio – COOPACRESMHA R.L Claro[®]-empresas

Oferta de Servicio Internet						
Ítem	Sucursal	Cantidad	Servicio	Ancho de Banda-Mbps	Tecnología	Mensualidad
1	BO. GASPAR GARCIA LAVIANA, PALI LA CONCEPCION 1/2C NORTE,11.934132, - 86.189484	1	Internet Corporativo	60	Fibra óptica	\$ 1,040.00
2		1	Enlace de Datos(Nodo)	40	Fibra óptica	
3		1	Internet Corporativo/ Respaldo-Pasivo	60	Fibra óptica	
4		1	Enlace de Datos(Nodo) Respaldo-Pasivo	40	Fibra óptica	
5	San Juan de la concepción , Barrio Luis Alfonso Velásquez del campo deportivo 150 más al sur 25 varas al oeste	1	Enlace de Datos	40	Fibra óptica	
Tota de precios sin IVA						\$ 1,040.00

Oferta con Redundancia y Aumento de Ancho de Banda