Política

Continuidad del negocio y recuperación de desastres

Revisó: Comité de Seguridad de la Información y Continuidad del Negocio- Comité de Riesgo **Fecha: 21-11-2024** **Fecha: 26-11-2024**	**Aprobó: Consejo de Administración** **Fecha: 11-12-2024**

1. INTRODUCCIÓN

La Misión de Ahorrocoop es “ofrecer soluciones rápidas y seguras a sus asociados”, mediante sus servicios financieros. Para poder dar cumplimiento a ello, la cooperativa reconoce la importancia de garantizar la continuidad operacional y recuperación ante desastre, asegurando la disponibilidad de los servicios a sus socios y colaboradores. Por lo tanto, esta política establece los lineamientos y acciones para mantener operativo el negocio.

En este sentido, todos los colaboradores de la cooperativa son responsables de proteger los procesos y activos relacionados a la continuidad del negocio, utilizando los canales de comunicación formales para notificar cualquier evento que podría transgredir esta materia. Al mismo tiempo, los colaboradores deben respetar y cumplir las normativas internas y externas relacionadas con la continuidad del negocio y la recuperación de desastres.

Este documento se encuentra alineado con los objetivos de la cooperativa y la Política del sistema de Gestión integrado, donde la Alta Dirección define un marco referencial para el cumplimiento de los objetivos en materia de continuidad del negocio.

2. OBJETIVO GENERAL

Garantizar la continuidad del negocio, minimizando el impacto de incidentes en los servicios y procesos críticos de Ahorrocoop. Esto mediante un sistema de gestión integrado (SGI), adoptando las buenas prácticas de la norma ISO 22301 continuidad del negocio.

Esta política se basa en marcos, estándares internacionales y regulaciones locales, tales como la ISO 31000 (Gestión de Riesgos), 22301 (Gestión de Continuidad del Negocio) y la Recopilación Actualizada de Normas (RAN) de la CMF. Su propósito es enfrentar los desafíos actuales y futuros mediante una gobernanza efectiva, la identificación, protección y detección temprana de amenazas, asegurando una respuesta y recuperación ante incidentes y garantizar la continuidad del negocio.

2.1. OBJETIVO ESPECIFICO

a. Garantizar la Resiliencia Operacional de Ahorrocoop

- Establecer procesos resilientes que aseguren la capacidad de Ahorrocoop para resistir interrupciones significativas en sus operaciones, manteniendo la continuidad de los servicios esenciales a través de medidas preventivas y proactivas.
- Implementar infraestructura redundante que permita la rápida recuperación de sistemas y procesos críticos en caso de interrupciones.

b. Identificar y Priorizar Procesos Críticos

- Realizar un Análisis de Impacto en el Negocio (BIA) para identificar los procesos clave y determinar los servicios que deben ser restaurados según nivel de importancia en caso de pérdida de la continuidad del negocio.
- Clasificar y priorizar los servicios críticos en función de su importancia para las operaciones diarias, asegurando que las medidas de continuidad se enfoquen en protegerlos.

c. Minimizar el Impacto de Interrupciones en los Servicios

- Desarrollar e implementar planes de contingencia que reduzcan al mínimo el impacto de posibles interrupciones, asegurando que los servicios de mayor valor para Ahorrocoop puedan estar operativos en el menor tiempo posible.
- Establecer tiempos de recuperación claros (RTO y RPO) para los procesos críticos, asegurando que las operaciones puedan restaurarse dentro de límites exigidos por el Consejo de Administración.

d. Asegurar la Disponibilidad de la información y activos Críticos

- Mantener políticas de respaldo y recuperación de datos que permitan restaurar la información sin pérdida significativa y con la mínima interrupción.
- Implementar soluciones de alta disponibilidad para los activos críticos, incluyendo redundancia de hardware, software y centros de datos, para minimizar el tiempo de inactividad.

e. Fortalecer la Preparación ante Emergencias a través de Capacitación y Simulacros

- Desarrollar programas de capacitación y concienciación que aseguren que todos los colaboradores comprendan su rol y responsabilidad en caso de un evento de interrupción.
- Realizar simulacros para probar la efectividad del Plan de Continuidad del Negocio (BCP) y entrenar a los equipos responsables en la respuesta ante emergencias, ajustando los planes según los resultados de estas pruebas.

f. Establecer Protocolos de Comunicación Efectiva en Situaciones de Crisis

- Definir procedimientos claros de comunicación interna y externa que aseguren la difusión de información precisa y oportuna durante una interrupción, manteniendo informados a todos los interesados, incluidos colaboradores, socios, proveedores y organismos fiscalizadores.
- Desarrollar un plan de comunicación de crisis que incluya métodos de notificación rápida y canales alternativos para la coordinación durante emergencias.

g. Garantizar la Recuperación de la continuidad operacional

- Crear y mantener planes de recuperación ante desastres (DRP) que permitan restaurar los servicios según prioridad en caso de pérdida de la continuidad del negocio por incidentes, desastres, fallos de infraestructura o ataques de ciberseguridad.
- Integrar estrategias de recuperación en el BCP, asegurando que todas las actividades de recuperación de los servicios tecnológicos y operativos estén para una recuperación sin problemas.

h. Alinear la Continuidad del Negocio con Normativas y Estándares Internacionales

- Asegurar el cumplimiento con la norma ISO 22301, RAN de continuidad operacional, leyes vigentes y otras regulaciones aplicables, integrando las mejores prácticas internacionales y nacionales en la planificación y gestión de la continuidad del negocio.
- Realizar revisiones y auditorías para verificar el cumplimiento de la política de continuidad del negocio y los estándares adoptados, como también las normativas y leyes chilenas.

i. Mejora Continua del sistema de gestión integrado donde incluye Continuidad del Negocio

- Establecer un proceso de mejora continua para revisar, actualizar y optimizar el BCP basándose en nuevas amenazas, cambios legales, cambios de normativas internas y cambios tecnológicos.
- Monitorear e implementar innovaciones tecnológicas que puedan mejorar la resiliencia operativa y la capacidad de recuperación de la cooperativa.

3. ALCANCE

El alcance de esta política aplica a todos los colaboradores, activos de información, proveedores, terceros y cualquier entidad que acceda, maneje o utilice los recursos tecnológicos y activos de información de Ahorrocoop, también incluye los servicios entregados a los a los socios, sistemas e infraestructura tecnológica que soporta la continuidad del negocio, que estén en las dependencias de sus oficinas fuera de ellas

a. Cobertura de Operaciones y Procesos Críticos

- La política abarca todos los procesos, servicios y operaciones esenciales para el funcionamiento de Ahorrocoop. Esto incluye todas las áreas operativas críticas que, en caso de interrupción, podrían afectar la capacidad de la cooperativa para proporcionar servicios financieros a sus clientes (socios).
- Los procesos cubiertos incluyen, servicios que afectan a los socios, operaciones de crédito y ahorro, gestión de pagos de proveedores y terceros, recaudación, soporte tecnológico, y servicios de seguridad de la información, entre otros.

b. Activos de Información y Tecnología

- Se incluyen todos los activos de información, como; bases de datos, servidores, redes, dispositivos de comunicación, sala de servidores, software crítico, seguridad entre otros.
- El alcance también abarca la protección y recuperación de los activos de información, asegurando la disponibilidad, integridad y confidencialidad de los datos durante y después de una interrupción.

c. Cobertura Geográfica

- La política es aplicable a la oficina central, a las oficinas sucursales de Ahorrocoop.
- También se extiende a las transacciones realizadas de forma remota, asegurando que las medidas de continuidad y recuperación puedan implementarse, sin importar dónde se encuentren los colaboradores y socios en el momento de una interrupción.

d. Colaboradores y Equipos de Respuesta

- Todos los colaboradores de Ahorrocoop, incluyendo contratistas, están sujetos a esta política. Cada colaborador debe estar preparado para desempeñar su rol asignado en el Plan de Continuidad del Negocio (BCP) en caso de la perdida de continuidad del negocio.
- El alcance incluye la formación de equipos especializados para la gestión de crisis, la recuperación y la continuidad operativa. Estos equipos serán responsables de ejecutar las acciones establecidas en los planes de respuesta.

e. Proveedores, Socios y Terceros

- La política se extiende a todos los proveedores y terceros que brinden servicios críticos a Ahorrocoop. Esto incluye a los proveedores de tecnología, servicios de comunicaciones, gestión de datos, logística, y otros servicios esenciales que son fundamentales para la continuidad del negocio en la cooperativa.
- Se requiere que estos terceros cumplan con los requisitos establecidos en los acuerdos de continuidad del negocio y que participen en ejercicios de simulación y pruebas, según sea necesario, para asegurar la preparación conjunta.

f. Escenarios de Riesgo y Tipos de Interrupciones

La política cubre una amplia gama de posibles eventos de interrupción, tales como;

- **Desastres Naturales:** terremotos, inundaciones, incendios, tormentas u otros eventos climáticos severos que puedan afectar la operación física de la cooperativa.
- **Interrupciones Tecnológicas:** fallas en sistemas, pérdida de datos, cortes de electricidad, ciberataques, y otras amenazas a la infraestructura tecnológica.
- **Incidentes de Seguridad**: situaciones de emergencia que incluyan amenazas físicas o de seguridad, tales como incendios, vandalismo, ataques físicos o disturbios que afecten las instalaciones.
- **Problemas de Salud Pública:** pandemias, brotes de enfermedades u otras crisis sanitarias que puedan limitar la capacidad de los colaboradores para acceder a las oficinas o desempeñar sus funciones normales.
- **Otros Riesgos:** cualquier otro tipo de evento que pueda comprometer la capacidad de Ahorrocoop para operar normalmente, como fallos en la cadena de suministro o la pérdida de recursos clave.

4. ROLES Y RESPONSABILIDADES

En esta política se definen los roles y responsabilidad de las partes internas que participan en el cumplimiento a la gestión de continuidad del negocio. Estos roles y responsabilidades aseguran que Ahorrocoop tenga una estructura clara y efectiva para gestionar la continuidad del negocio. Cada nivel de la cooperativa, desde el Consejo de Administración hasta los colaboradores individuales, tienen un papel importante que realizar en esta materia, lo que permite una respuesta coordinada y eficiente durante las situaciones de interrupción, garantizando la resiliencia de Ahorrocoop.

a. Consejo de Administración

Rol: Máxima autoridad en la supervisión y aprobación de la estrategia de continuidad del negocio.

El Consejo de Administración es la máxima autoridad de Ahorrocoop y tiene la responsabilidad de definir, supervisar y aprobar la estrategia y políticas de continuidad operacional de la cooperativa, asegurándose de que esté alineada con los objetivos estratégicos.

Responsabilidades

Aprobar la política de continuidad del negocio: Evaluar y aprobar la estrategia general de continuidad del negocio, asegurando que esté alineada con los riesgos, el entorno operativo y los objetivos estratégicos de la cooperativa.

Revisar y aprobar los informes: evaluar y aprobar informes de evaluación de riesgos y los planes de mitigación propuestos por el Comité de Seguridad en esta materia.

Monitorear los indicadores: revisar y evaluar indicadores de desempeño y la efectividad de los controles para velar por la continuidad del negocio y la recuperación ante desastres.

Supervisión del cumplimiento: Monitorear el cumplimiento de normativas, regulaciones y mejores prácticas internacionales, ISO 31000 e ISO 22301, relacionadas con la continuidad del negocio y recuperación de desastres.

Asignación de recursos: Aprobar la asignación de recursos financieros y humanos necesarios para implementar y mantener las medidas de continuidad del negocio y recuperación ante desastres.

Evaluación de riesgos: Revisar regularmente los riesgos relacionados a la continuidad del negocio, asegurándose de que se implementen controles para mitigarlos adecuadamente.

Revisión periódica: Garantizar que la política de continuidad del negocio y la recuperación de desastres se revise y actualice para abordar nuevos riesgos y desafíos tecnológicos.

b. Gerencia General

Rol: La Gerencia General es responsable de implementar y ejecutar de la política aprobada por el Consejo de Administración, velando que la continuidad del negocio y recuperación de desastres sean aspectos claves en la gestión diaria de Ahorrocoop.

Responsabilidades:

Implementación de políticas: Asegurar que la política de continuidad del negocio y recuperación de desastres se apliquen correctamente a nivel transversal, mediante la coordinación con el Comité de seguridad de la información.

Informe de resultados al Consejo: Presentar al Consejo de Administración informes regulares sobre el estado de cumplimiento de la política de continuidad del negocio y recuperación de desastres.

Liderar la cultura de seguridad: Fomentar una cultura de seguridad de la información, mediante la sensibilización y la formación continua de los colaboradores.

Gestión de riesgos operativos: Supervisar los procesos de gestión de riesgos asociados a la seguridad y ciberseguridad, y coordinar la implementación de medidas correctivas en caso de vulnerabilidades.

Garantizar los recursos: garantizar que los recursos humanos, tecnológicos y financieros estén disponibles para la implementación de las medidas de continuidad del negocio y recuperación de desastres.

c. Comité de Seguridad y Continuidad del Negocio

Rol: El Comité de Seguridad es un equipo multidisciplinario especializado, que tiene como rol principal la planificación, desarrollo y supervisión del sistema de gestión integrado en materia de continuidad operacional y recuperación de desastres.

Responsabilidades:

Desarrollar y mantener BCP: Proponer al Consejo de Administración un plan de continuidad, permitiendo mantener la continuidad del negocio.

Desarrollar y mantener BIA: Proponer al Consejo de Administración el Análisis de Impacto (BIA) que permita evaluar y entender el impacto de la interrupción en los procesos y servicio de la cooperativa, para definir acciones y prioridades de recuperación ante desastres.

Definir y priorizar controles: Definir y priorizar controles relacionados con la continuidad del negocio y recuperación desastres, basados en evaluación de riesgos.

Pruebas y revisiones: R Realizar y evaluar pruebas de continuidad y recuperación para revisar la efectividad el plan de continuidad y recuperación de desastres.

Elaborar informes: realizar y presentar informes mensuales del estado y progreso de la continuidad y recuperación a la alta gerencia, Comité de Riesgos y el Consejo de Administración.

d. Subgerencia de Operaciones y TI (CTO)

Rol: La Subgerencia de Operaciones y TI, tiene el rol de gestionar la infraestructura tecnológica e implementar medidas tecnológicas para asegurar la continuidad del negocio y recuperación ante desastres.

Responsabilidades

Implementación de medidas de disponibilidad y recuperación: asegurar la disponibilidad y recuperación de las tecnologías que soportan el negocio.

Monitoreo de sistemas: Monitorear continuamente los activos de información para detectar posibles anomalías, vulnerabilidades y amenazas que atenten contra la continuidad del negocio.

Gestionar medidas de respaldo: desarrollar e implementar medias de alta disponibilidad, respaldo y recuperación de información, que permitan resguardar y recuperación el negocio en el tiempo indicado por el Consejo de Administración.

Actualización de infraestructuras: Gestionar la actualización continua de la infraestructura relacionada cona la continuidad del negocio y recuperación de desastres.

Evaluar tecnologías: Evaluar y seleccionar nuevas tecnologías para mejorar y mantener la continuidad del negocio y recuperación de desastres.

Aplicar controles: gestionar y aplicar controles técnicos tales como firewalls, sistema de prevención de intrusos, cifrados, entre otros.

e. Oficial de Seguridad de la Información (CISO)

Rol: El Oficial de Seguridad de la Información (CISO) es el responsable de garantizar que las actividades de seguridad y ciberseguridad de la información estén integradas en el plan de continuidad del negocio y recuperación de desastres.

Responsabilidades

Coordinar: Coordinar la integración de seguridad y ciberseguridad en todas las actividades de continuidad del negocio y recuperación de desastres, asegurando que los controles y medidas de seguridad de mantengan durante una crisis.

Gestión de riesgos de continuidad: Identificar y gestionar los riesgos que afecten a la continuidad del negocio.

Reporte a la alta dirección: reportar directamente al Comité de seguridad, Informar a la Gerencia General y al Consejo de Administración sobre el estado de la continuidad del negocio.

Supervisar y coordinar la respuesta de incidentes: supervisar y gestionar la respuesta ante incidentes que puedan atentar la continuidad del negocio.

f. Oficial de Cumplimiento

Rol: El Oficial de Cumplimiento se encarga de asegurar que Ahorrocoop cumpla con todas las normativas y leyes relacionadas con la continuidad del negocio.

Responsabilidades

Cumplimiento normativo: Asegurarse de que Ahorrocoop cumpla con las normativas legales y las mejores prácticas relacionadas con la ciberseguridad, como ISO 27001 e ISO 22301, RAN entre otras.

Mantener requisitos regulatorios: mantener actualizados todas los requisitos legales y normativos en función de las leyes vigentes y asesorar a las distintas áreas de la cooperativa sobre las implicaciones normativas.

g. Usuarios Finales y Colaboradores

Rol: Todos los colaboradores y usuarios de los sistemas en la cooperativa tienen como rol fundamental entender y aplicar las actividades del plan de recuperación de desastres, mientras dure la crisis.

Responsabilidades

Cumplir con la política: los colaboradores deben cumplir con la política de continuidad del negocio y recuperación de desastres.

Informar cualquier actividad sospechosa: todos los colaboradores deben informar de inmediato cualquier actividad sospechosa o posible incidente que pueda comprometer la continuidad del negocio.

Participar capacitación: participar en los programas de capacitación y concientización sobre continuidad del negocio y recuperación de desastres.

h. Subgerentes y jefes de departamentos:

Rol: Ejecutar los planes de continuidad respectivos a su subgerencia y departamentos relacionados, garantizando la que sus equipos estén disponibles y preparados ante una crisis.

Responsabilidades

Cumplir con la política: verificar que sus colaboradores cumplan con la política de continuidad del negocio y recuperación de desastres.

Informar cualquier actividad sospechosa: informar de inmediato cualquier actividad sospechosa o posible incidente que pueda comprometer la continuidad del negocio.

Participar capacitación: participar en los programas de capacitación y concientización sobre continuidad del negocio y recuperación de desastres.

Desarrollar planes específicos: desarrollar planes específicos para sus departamentos, los cuales deben estar alineados con el plan de recuperación general. Estos planes deben ser presentados y coordinados con el Comité de seguridad y continuidad.

i. Equipo de Crisis

Rol: Coordinar la respuesta inmediata ante un incidente que afecte la continuidad del negocio.

Responsabilidades

Activar Plan: responsable de activar plan de continuidad cuando sea necesario, gestionando la comunicación y coordinación de la respuesta a la crisis interna y externa.

Contactar: Mantener contacto con todas las partes interesadas internas y externas, asegurando que éstas estén informadas durante la crisis.

Coordinar: Dirigir, coordinar los esfuerzos de recuperación, monitorear el progreso y ajustar estrategias según las necesidades inmediatas durante la crisis.

j. Departamento de TI

Rol: tiene el rol de gestionar, proteger y asegurar la infraestructura del tecnológica del negocio, garantizando que los sistemas y servicios críticos sean resilientes, estén respaldados y puedan ser recuperados rápidamente en caso de interrupciones Su rol es esencial para asegurar la continuidad del negocio durante la crisis.

Responsabilidades

Gestionar infraestructura critica: implementar y mantener la infraestructura tecnológica que soporta al negocio, asegurando su disponibilidad y recuperación.

Desarrollar e implementar medidas de alta disponibilidad y redundancia para minimizar el impacto ante fallos o cortes de servicios.

Respaldos y recuperación de información: Asegurar que los sistemas y servicios críticos cuenten con contingencias de alta disponibilidad.

Mantener respaldos de información almacenados en lugares seguros y listos para realizar recuperación ante una crisis.

Implementación de planes de recuperación: Desarrollar, implantar y mantener el plan técnico de recuperación de desastres (DRP) que permita recuperar los sistemas, servicios e informacion en caso de incidente que afecte a la continuidad del negocio. Realizar pruebas de recuperación para evaluar la efectividad del plan de recuperación, realizando ajustes según resultados.

Monitoreo continuo: Monitorear en forma continua los servicios tecnológicos (redes, servidores, aplicaciones y otros activos de información) para detectar posibles amenazas que afecten a la continuidad del negocio. Implementar herramientas de monitoreo y alerta para identificar y responder rápidamente ante incidentes técnicos o ciberataques.

Actualizar parches: Gestionar las actualizaciones de parches de los sistemas operativos, software, antivirus, aplicaciones y otros para proteger contra vulnerabilidades y minimizar el riesgo de pérdida de continuidad por un incidente de ciberseguridad. Asegurar que todos los sistemas operativos y aplicaciones críticas estén actualizados con las versiones actuales del proveedor.

Coordinación Comité de seguridad y continuidad: Trabajar y coordinar con el equipo de crisis para garantizar que las acciones de recuperación estén alineadas con el plan de recuperación ante desastres. Coordinar con otros departamentos y equipos las acciones para garantizar la recuperación de los servicios.

Soporte técnico: Proveer soporte técnico durante incidentes y emergencias para asegurar la solución de problemas y continuidad del negocio. Tener colaboradores técnicos preparados para actuar en caso de incidentes que afecten la continuidad de los servicios TI.

Documentación y mejora continua: Pro mantener documentado y actualizado los procedimientos y procesos e TI relacionados con la continuidad del negocio y recuperación de desastre.

k. Departamento de Auditoría

Rol: El rol principal del departamento de Auditoría es evaluar la efectividad de los controles y procesos implementados en relación a la continuidad del negocio y recuperación de desastres.

Responsabilidades

Revisión de auditorías de continuidad y recuperación: Realizar auditorías y evaluar la eficiencia de los controles relacionados en esta materia.

Emitir informes y recomendaciones: Emitir informes con recomendaciones, relacionadas a correcciones o mejoras en los procesos y actividades de continuidad y recuperación de desastres.

l. Departamento de Riesgo Operacional

Rol: El departamento de riesgo operacional es asegurar que la gestión de continuidad y recuperación sea eficiente y efectiva, planificando y realizando revisiones y pruebas en esta materia.

Responsabilidades

Evaluación de riesgos de ciberseguridad: Realizar evaluaciones de riesgos para identificar amenazas potenciales que afecten a la continuidad del negocio.

Gestión de riesgos estratégicos: Garantizar que los riesgos asociados a la continuidad operacional estén alineados con la estrategia de riesgos de la cooperativa.

5. DOCUMENTOS RELACIONADOS

- PO-SG-01 Política del sistema de gestión integrado.
- M-SG-05 Plan de Continuidad del Negocio
- M-SG-05-D-01 Programa de Sensibilización Continuidad del Negocio
- M-SG-05-D-05 Contingencia
- M-SG-05-D-01 Funcionamiento de las Sucursales en Contingencia
- RAN 20-8 Información de Incidentes Operacionales
- RAN 20-9 Gestión de la Continuidad de Negocios
- RAN 20-10 Gestión de Seguridad de la Información y Ciberseguridad
- Ley 21459 ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS
- P-RI-09 Envío de Incidentes Operacionales a la CMF
- P-SG-09 Investigación y Tratamiento de Incidentes
- P-ADM-03-D-29 Archivo I12 Incidentes de Ciberseguridad

6. DEFINICIONES

- **Activo:** Conjunto de bienes, derechos o recursos que posee una empresa u organización, del que se espera que sea utilizado para la obtención de beneficios económicos en el futuro.
- Análisis de impacto: Documento derivado del Plan de Continuidad, donde la Alta Dirección determina formalmente la criticidad de sus procesos y activos. Esta información será esencial para que la organización pueda definir las estrategias que permitirán enfrentar los riesgos que provoquen una pérdida de la continuidad del negocio.
- **Ciberseguridad**: Conjunto de acciones de seguridad que están destinadas a proteger la información almacenada en medios tecnológicos.
- **Comité de Seguridad de la Información y Operaciones**: Comité de la Cooperativa Ahorrocoop, creado con la finalidad de que asegurar los activos de información que circulen por los sistemas informáticos, procesos de negocio y redes de comunicación sean adecuados respecto a la confidencialidad, integridad y disponibilidad, para garantizar que los clientes-usuarios de la organización los utilicen de manera efectiva, ajustadas a la Política de Calidad y Seguridad de la Información.
- **Continuidad del Negocio**: es la capacidad de la organización para continuar suministrando sus productos y/o servicios a niveles predefinidos aceptables durante y después de un desastre que impida su funcionamiento normal.

- Plan de continuidad de negocios: Un plan que contiene procedimientos documentados, recursos y sistemas que conducen a que la organización pueda responder, recuperar, reanudar y restaurar sus procesos de negocio a un nivel de operación predefinido ante una emergencia de manera adecuada, logrando así el mínimo impacto posible.
- **Plan de contingencia:** Es un subconjunto de un plan de continuidad de negocio, que contempla como reaccionar ante una contingencia específica que pueda afectar alguno de los servicios ofrecidos por los proveedores, tanto internos como externos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, etc.
- **Plan de Recuperación frente a Desastres:** Es aquella parte del plan de continuidad de negocio, que define un conjunto de recursos humanos, físicos y técnicos y de procedimientos orientados a recuperar, dentro de tiempos y costos definidos, una actividad interrumpida por una emergencia o desastre.
- **Política del Sistema de Gestión Integrado:** Marco de lineamientos de la Cooperativa Ahorrocoop, autorizada por Gerencia General y ratificada por el Directorio, que tiene por finalidad dar cumplimiento a los requisitos de las normativas ISO 9001:2015 y ISO 27001:2013 e ISO 20000-1:2015 referentes a la calidad del producto/servicio de los procesos de TI y la seguridad de la información, determinando objetivos para su medición.
- **Proceso de Negocio**: Conjunto de actividades sucesivas que genera un producto y/o servicio clave para el funcionamiento de la organización.
- **Riesgo**: Posibilidad de que un evento se produzca y provoque un impacto que altere la normalidad de una actividad.
- **Seguridad**: Condición conseguida cuando los activos están protegidos contra los riesgos.
- **Gestión de la Continuidad del Negocio:** proceso integral de gestión que identifica las amenazas potenciales y sus impactos en las operaciones del negocio, que considera una planificación y análisis y como se podría ver comprometida la infraestructura.

7. PRINCIPIOS

Los principios de la Política de continuidad de Ahorrocoop proporcionan la base para gestionar los riesgos de manera eficaz, garantizar el cumplimiento normativo y proteger los activos de información. Estos principios aseguran que todos los colaboradores entiendan sus responsabilidades y que la cooperativa mantenga un enfoque proactivo y dinámico frente a las amenazas de seguridad, protegiendo en forma continua la continuidad del negocio.

Esta política se sustenta en principios para la protección de la continuidad del negocio basado en la norma ISO 22301 Continuidad del negocio y las normas RAN del organismo fiscalizador CMF. Estos guían la implementación y gestión de la política de continuidad del negocio en Ahorrocoop, asegurando que la cooperativa esté preparada para enfrentar desafíos operativos, protegiendo sus activos de informacion, la confianza de sus socios y organismos fiscalizadores. Están diseñados para fomentar la resiliencia, la responsabilidad y la mejora continua, alineándose con las mejores prácticas internacionales y el cumplimiento normativo y legal vigente, estos principios son los siguiente:

a. Proactividad y Preparación

- Adoptar un enfoque preventivo que permita anticiparse a posibles amenazas e interrupciones, identificando riesgos y tomando medidas preventivas para minimizar su impacto.

- Desarrollar y mantener planes de continuidad bien definidos que permitan a Ahorrocoop estar preparado para responder de manera rápida y efectiva ante cualquier eventualidad.

b. Resiliencia Operacional

- Asegurar que los procesos críticos y los servicios tecnológicos de Ahorrocoop sean resilientes frente a interrupciones, permitiendo que las operaciones continúen o se restauren rápidamente tras un incidente.
- Implementar infraestructura redundante y soluciones tecnológicas de alta disponibilidad para garantizar la continuidad de servicios esenciales, incluso en condiciones adversas.

c. Responsabilidad y Rendición de Cuentas

- Establecer roles y responsabilidades claras para la gestión de la continuidad del negocio, asegurando que cada miembro del equipo de Ahorrocoop entienda sus funciones y pueda actuar de manera eficiente durante una crisis.
- Fomentar una cultura de responsabilidad compartida, donde todos los colaboradores comprendan la importancia de la continuidad del negocio y participen activamente en su implementación y mejora.

d. Protección de los Intereses de los Clientes (Socios) y de la Cooperativa

- Priorizar la protección de los intereses y datos de los clientes (socios) durante cualquier incidente, garantizando la disponibilidad, seguridad de los servicios que dependen de Ahorrocoop.
- Asegurar la sostenibilidad y estabilidad a largo plazo de la cooperativa, manteniendo la confianza y la lealtad de los socios incluso durante situaciones de emergencia.

e. Cumplimiento Normativo y Conformidad

- Cumplir con todas las regulaciones, leyes vigentes y estándares internacionales aplicables, como la norma ISO 22301, asegurando que la continuidad del negocio y el SGI estén alineados con las mejores prácticas del sector.
- Realizar auditorías regulares para verificar el cumplimiento y asegurar que los procesos de continuidad estén actualizados y ajustados a los cambios regulatorios.

f. Mejora Continua

- Implementar un proceso de mejora continua para revisar y actualizar los planes de continuidad, aprendiendo de incidentes pasados, simulacros y cambios en el entorno de riesgos.
- Adaptar el BCP a riesgos emergentes y a innovaciones tecnológicas que puedan mejorar la eficiencia y efectividad del plan de recuperación y continuidad.

g. Colaboración y Comunicación

- Promover la comunicación y colaboración interna y externa, asegurando que todos los equipos y partes interesadas claves estén alineados y preparados para actuar en caso de pérdida de continuidad operacional.
- Establecer canales claros y efectivos para la comunicación de crisis, permitiendo la rápida difusión de información a colaboradores, clientes (socios), proveedores y autoridades regulatorias, según sea necesario.

h. Capacitación y Concienciación

- Desarrollar programas de capacitación y concienciación regulares para todos los colaboradores, asegurando que comprendan sus roles en el BCP y estén preparados para responder eficazmente durante una crisis.

- Fomentar una cultura organizacional que valore la preparación y la resiliencia, destacando la importancia de la continuidad del negocio como parte fundamental de la gestión de la cooperativa.

i. Flexibilidad y Adaptabilidad

- Asegurar que los planes de continuidad del negocio sean lo suficientemente flexibles para adaptarse a diferentes tipos de emergencias e interrupciones, permitiendo respuestas personalizadas según la naturaleza del evento.
- Evaluar y ajustar las estrategias de continuidad para reflejar los cambios en la estructura operativa, las tecnologías emergentes y los riesgos del entorno.

8. COMPROMISOS

La Política de continuidad operacional incluye compromisos que reflejan el enfoque integral de Ahorrocoop en la gestión de la continuidad del negocio, asegurando que esté preparada para enfrentar y superar incidentes o desastres de cualquier naturaleza, para mantener la continuidad y asegurar la recuperación en el menor tiempo (según lo mandatado por el Consejo de administración), permitiendo mantener la confianza de los clientes (socios) y organismos fiscalizadores. Estos compromisos están alineados con los alineados con los objetivos estratégicos, las mejores prácticas internacionales y las leyes vigentes.

a. Compromiso con la Resiliencia Operacional

- Ahorrocoop se compromete a garantizar la resiliencia de sus procesos y servicios críticos, asegurando la capacidad de recuperación rápida y eficiente frente a interrupciones inesperadas.
- Ahorrocoop se componente a mantener una infraestructura redundante para minimizar el impacto de eventos adversos en la operación diaria de la cooperativa.

b. Compromiso con la Protección de Clientes (Socios) y Partes Interesadas

- La cooperativa se compromete a proteger los intereses de sus clientes (socios) asegurando la disponibilidad y seguridad de los servicios el mayor tiempo según acuerdo del consejo.
- Ahorrocoop se esforzará por mantener la confianza de los socios, partes interesadas y organismos fiscalizadores al proporcionar respuestas perdida de continuidad del negocio.

c. Compromiso con la Mejora Continua

- Ahorrocoop se compromete a adaptarse a un enfoque de mejora continua para evaluar, probar y actualizar el Plan de Continuidad del Negocio (BCP), asegurando visualizar nuevas amenazas y cambios en el entorno.
- Ahorrocoop se compromete a aprender de incidentes previos y ejercicios de simulacro, implementando mejoras basadas en lecciones aprendidas para fortalecer el plan de continuidad del negocio.

d. Compromiso con el Cumplimiento Normativo

- Ahorrocoop se compromete que el sistema de gestión de continuidad del negocio cumplirá con las normativas locales e internacionales aplicables, incluyendo la norma ISO 22301.
- Ahorrocoop se compromete a realizarán revisiones y auditorías internas o externas para verificar que las políticas, procesos y controles relacionados con la continuidad del negocio se cumplen y estén alineados con los estándares y regulaciones vigentes.

e. Compromiso con la Capacitación de Colaboradores

- La cooperativa se compromete a proporcionar programas regulares de capacitación y simulacros para que todos los colaboradores estén preparados para actuar de manera efectiva durante una pérdida de continuidad del negocio.
- Ahorrocoop se compromete que los colaboradores comprendan sus roles específicos dentro del BCP y estén equipados con las habilidades necesarias para manejar situaciones de crisis.

f. Compromiso con la Comunicación Eficaz

- Ahorrocoop se compromete a establecer y mantener canales de comunicación claros y efectivos para la gestión de crisis, asegurando que la información clave se difunda rápidamente a colaboradores, socios, proveedores y autoridades reguladoras durante una emergencia.
- Ahorrocoop se compromete a mantener planes de comunicación bien definidos para coordinar las respuestas ante incidentes, durante y después de un incidente

g. Compromiso con la Colaboración con Terceros y Proveedores

- Ahorrocoop se compromete de que los proveedores y otras partes interesadas que son críticos estén alineados con sus planes de continuidad del negocio y cumplan con los estándares establecidos en los acuerdos de nivel de servicio (SLAs).
- Ahorrocoop se compromete a trabajar para mantener una estrecha colaboración con terceros para realizar evaluaciones de riesgos conjuntas, ejercicios de simulacro y revisiones periódicas para garantizar la preparación y la resiliencia de toda la cadena de suministro.

h. Compromiso con la Flexibilidad y Adaptabilidad

- Ahorrocoop se compromete a mantener la flexibilidad en sus planes de continuidad, adaptándolos a diferentes tipos de interrupciones, desde desastres naturales hasta incidentes tecnológicos y amenazas de seguridad.
- Ahorrocoop se compromete a evaluar sus planes de continuidad para reflejar los cambios de contexto, los riesgos y las tecnologías.

9. ACCIONES DE CONTINUIDAD DEL NEGOCIO

Prevenir: Implementar medidas preventivas para reducir la probabilidad de interrupción de las operaciones y sistemas tecnológicos.

Detectar: Establecer sistemas de monitoreo y alerta temprana es una acción específica diseñada para identificar posibles problemas antes de que ocurran

Responder: Desarrollar planes de acción claros para responder ante interrupciones es una actividad que forma parte del plan de continuidad del negocio.

Recuperar: Implementar procesos para restaurar rápidamente las operaciones y sistemas tecnológicos a su estado normal después de un incidente que interrumpa la continuidad del negocio.

Aprender: Realizar evaluaciones periódicas para identificar áreas de mejora y ajustar los planes de acción para mejorar la continuidad del negocio.

10. REVISIÓN Y ACTUALIZACIÓN

La política se revisa a lo menos una vez al año o cuando el contexto lo amerite, con el fin de asegurar su vigencia y adecuación a los cambios en el entorno legal y económico.

Esta política es comunicada a todos los socios, colaboradores y proveedores.

CONTROL DE CAMBIOS

1. Control de Cambios

Versión Vigente	Página(s) de cambio	Cambio Efectuado
01 (08-09-2010)	No aplica	Creación del Documento
02 (11-03-2016)	5	Se actualiza Roles y Responsabilidades incorporando la responsabilidad de actualizar la política por lo menos una vez al año.
03 (30-08-2016)	No Aplica	Se actualiza formato de la política según procedimiento P-SG-01 Elaboración y control de documentos.
03	5	Se elimina duplicidad de párrafo.
04 (12-05-2017)	4	La Alta Dirección del SGI, debe desarrollar un Plan de Continuidad del Negocio que cubra los aspectos críticos y esenciales de la actividad de la Cooperativa.
05 (16-05-2018)	2	Se agrega el punto “Introducción”. Además, se definen los Objetivos de la Política de Continuidad de Negocio y se especifica el alcance de este documento, considerando los procesos críticos del negocio.
05	2-3	Se cambia título de “Terminologías” por “Definiciones”. En este punto, se agregan algunos conceptos que son “Activo”, “Comité de Seguridad de la Información y Operaciones”, “Continuidad de Negocio”, “Política de Calidad y Seguridad de la Información”, “Proceso de Negocio”, “Riesgo” y “Seguridad”. Se modifican las definiciones de “Análisis de Impacto”, “Plan de Continuidad del Negocio”, “Plan de Contingencia” y “Plan de Recuperación frente a Desastres”.
05	4	Se agrega el documento M-SG-05 Plan de Continuidad y el documento M-SG-05-D-01 Programa de Sensibilización Continuidad del Negocio como documentos referenciales.

INFORMACIÓN INTERNA

05	4-5	Se agrega el punto “Principios y Compromisos”. Se modifica el punto “Responsabilidades”, asignando roles al Comité de Crisis y al Consejo de Administración.
05	No Aplica	Se eliminan los siguientes puntos: “Objetivo”, “Elementos Adicionales a la Política General”, “Violaciones a la Política”, “Inicio del Plan de Continuidad del Negocio”, “Desarrollo y Administración del Plan de Continuidad del Negocio”, “Evaluación de Riesgo del Plan de Continuidad del Negocio”, “Características del Plan de Continuidad del Negocio”, “Entrenamiento y Concientización del Plan de Continuidad del Negocio, “Prueba del Plan de Continuidad del Negocio” y “Mantenimiento y Actualización del Plan de Continuidad del Negocio”.
06 (10-07-2019)	2	Se actualiza la redacción a Sistema de Gestión Integrado.
07 (13-05-2020)	3	Se cambia el nombre la Política de Calidad y Seguridad de la Información a Política de Gestión Integrado de Información
07	4	Se incorpora dentro del punto de principios y compromisos los Recursos técnicos y financieros para llevar a cabo la política de continuidad.
08 (12-04-2021)	2	Se realiza ajuste en el párrafo del alcance, donde ahora se indica que: esta política aplicará para todo el personal que preste servicio en, o, para Ahorrocoop Ltda.
09 (13-06-2022)	No Aplica	Revisión sin Cambios
10 (10-05-2023)	4	Se incorpora información asociada a la Gestión de la Continuidad del Negocio
11 (12-06-2023)	2-3	Se efectúan ajustes en relación con el concepto de ciberseguridad.
12 (14-02-2024)		
13 (11-12-2024)	Todo el Documento	Se realiza ajuste en relación con observación de la CMF
13	Todo el Documento	Se separa el objetivo general con el especifico, mejora en el alcance, se especifican los roles y responsabilidades de todas las partes interesadas, se separan los principios de los compromisos