ESTRATEGIAS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Objetivo:

Identificar las estrategias implementadas para continuar operaciones.

Contenido:

- ✓ Estrategias generales de continuidad (ej. redundancia, respaldo, personal clave)
- ✓ Reubicación a centros alternos o trabajo remoto
- ✓ Reposición tecnológica y recuperación de información

¿QUÉ ES UNA ESTRATEGIA DE CONTINUIDAD DEL NEGOCIO?

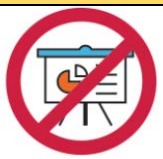
Una estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de los procesos y actividades críticas de una determinada organización frente a un desastre o una interrupción mayor.

La Cooperativa ha analizado las necesidades de recuperación no solo desde el punto de vista tecnológico, sino también desde el punto de vista del negocio, por lo que a partir del Análisis de Impacto del negocio y el Análisis de Riesgos con relación a la afectación de la continuidad del negocio, ha definido procedimientos y planes que establecen cómo la Cooperativa mantendrá sus operaciones esenciales y se recuperará de interrupciones inesperadas como desastres naturales, ciberataques o fallas de infraestructura.

Determinación de escenarios

Los escenarios identificados están relacionados a la Infraestructura o instalaciones físicas de la Cooperativa, Tecnologías de la Información (TI), Recursos Humano o personal Crítico (RR.HH.), Proveedores e Información clasificada. A continuación, se define la relación de alternativas operacionales que tiene la Cooperativa, para recuperar la funcionalidad de sus procesos críticos en términos de la ausencia de alguno(s) de los recursos claves, estas estrategias pueden permitir la continuidad de las operaciones más importantes en un nivel aceptable con el fin de cumplir y satisfacer los requerimientos del servicio solicitado por los socios (as) después de un evento de interrupción.

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 **NO DISPONIBILIDAD DE LOS RESPONSABLES DE LOS PROCESOS (RR.HH.)**	• Incendio • Terremoto • Actos de Violencia • Cierra parcial • Ausencia (Fallecimiento) • Intoxicación Colectiva • Indisposición de Personal responsable de proceso (Ausencia, renuncia repentina) • Pandemia	• Definición de árboles de llamada • Capacitación de personal alterno • Documentación de procedimientos o manuales operativos.
 **NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA**	• Incendio • Inundación • Actos de violencia • Sismo o Terremoto • Explosión (Atentado)	• Teletrabajo • Respaldo entre sedes (Entre Oficina central y Agencia del Mercado Campesino) • Centro de Procesamiento de Datos Alterno (CPDA)
 **NO DISPONIBILIDAD DE LOS RECURSOS TECNOLÓGICOS**	• Falla eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones • Ciberataque	• Estrategia de Recuperación • Plan de Contingencia Tecnológica • Procedimiento Alternativo manual para la atención a los socios y socias.

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 **NO DISPONIBILIDAD DE INFORMACIÓN**	• Falla eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones • Error humano • Hurto o robo	• Respaldo de información clave del proceso (BackUp): Copias diarias del sistema CORE. • Respaldo (Backup) de la información crítica de estaciones de trabajo y sistemas. • Procedimientos de resguardo y recuperación • Procedimiento de Digitalización de documentación crítica.
 **NO DISPONIBILIDAD DE PROVEEDORES Y/O TERCEROS**	No disponibilidad del Proveedor por eventos propios de su operación: • Falla eléctrica • Incendio • Inundación • Sismo o Terremoto • Falla Tecnológica • Pandemia • Actos de Violencia • Quiebra financiera del proveedor • Ciberataque	• Acuerdos de Niveles de Servicio SLA • Lista de proveedores alternos

RECURSOS PARA LAS ESTRATEGÍAS DE RECUPERACIÓN:

Se consideran los siguientes recursos mínimos ya sean internos o externos:

- ✓ Personal capacitado.
- ✓ Información y datos.
- ✓ Infraestructura e instalaciones de soporte.
- ✓ Equipamiento y bienes.
- ✓ Sistemas informáticos de Tecnologías de la información.
- ✓ Copias de respaldo de bases de datos de los Sistemas de información.
- ✓ Copias de respaldo de configuraciones de dispositivos críticos.
- ✓ Copias de la data de estaciones de trabajo críticos.
- ✓ Transporte y logística.
- ✓ Finanzas.
- ✓ Socios y proveedores.

Para la recuperación se ha definido dentro de las estrategias, procedimientos para llevar a cabo tareas, clasificándolas tipos de estrategias.

TIPOS DE ESTRATEGIAS:

1) ESTRATEGIAS A NIVEL DE CONTINGENCIA.

Son las medidas que se aplican cuando ocurre una interrupción que afecta procesos o recursos críticos, con el fin de **mantener la continuidad operativa en un nivel aceptable**. Las estrategias de contingencia permiten que la Cooperativa siga funcionando aun cuando sus recursos principales (tecnológicos, humanos o físicos) no estén disponibles, asegurando la atención a los socios.

Para ello se ha establecido las siguientes estrategias:

1.1. ESTRATEGIA DE SITIO ALTERNO

El **sitio alterno (o Centro de Procesamiento de Datos Alterno – CPDA) es una estrategia porque es una alternativa predefinida y preparada** para que la entidad pueda seguir operando aun cuando su sitio principal no esté disponible.

Los Criterios de Activación, están dadas de acuerdo a lo mencionado anteriormente como ser: Desastres Naturales, cortes de energía prolongados, ciberataques o falas críticas de la infraestructura en Oficina Central.

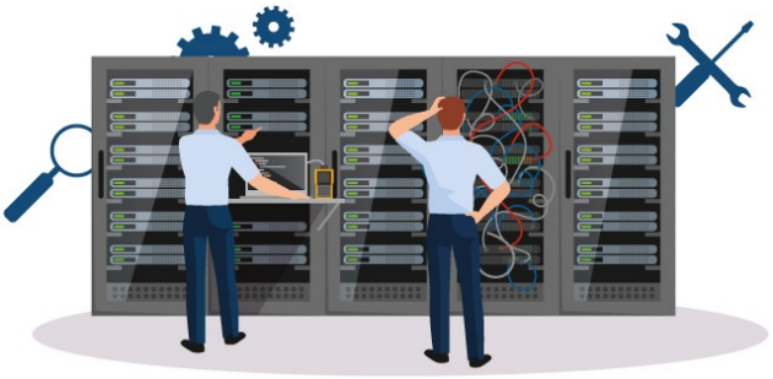
La ubicación del CPDA se encuentra dentro de la Agencia del Mercado Campesino, la cual tiene para la atención a los socios, un equipo de CAJA y un equipo para la responsable de la Agencia (Plataforma/Créditos) así como el mobiliario respectivo para la atención.

Los responsables son:

- **Jefe de Sistemas:** Responsable de Activar el CPDA, en coordinación con el Oficial de Seguridad de la Información, así mismo es responsable de migrar y levantar los servicios en el CPDA. También es responsable de restaurar los servicios en el CPD, una vez que pase el incidente.
- **Encargado de Seguridad Física y Soporte**: Responsable de revisar las estaciones de trabajo dando soporte a cualquier requerimiento técnico.
- **Gerencia General**: Responsable de Autorizar la activación del CPDA.
- **Oficial de Seguridad de la Información**: Coordina y supervisa el proceso de la activación del CPDA hasta su restauración del CPD principal.
- **Unidades de Control**: Supervisan la aplicación del procedimiento de la contingencia a través de la Activación del CPDA.
- **Personal Operativo**: En caso de traslado de personal los mismo deben conocer el procedimiento a seguir.

1.2. ESTRATEGIA TECNOLOGICA: PLAN DE CONTINGENCIA TECNOLÓGICA

Esta estrategia constituye la forma planificada y documentada en la que la Cooperativa garantiza que su plataforma tecnológica continúe operando aun ante eventos de falla o desastre, asegurando la disponibilidad de los sistemas crítico en los tiempos establecidos en el Análisis BIA.



Este tipo de contingencia se presenta cuando el hardware y/o software presenta fallas, o por interrupción prolongada de las comunicaciones, en este sentido se activa el **PLAN DE CONTINGENCIA TECNOLÓGICA**, el cual es responsable la unidad de sistemas de su aplicación en su mayor parte, por lo que ésta toma en cuenta, las estrategias para los recursos más críticos:

a) Estrategia tecnológica para la recuperación de las bases de datos
b) Estrategia Tecnológica para recuperar el servicio de Internet
c) Estrategia Tecnológica para la recuperación de la comunicación de la Intranet (LAN)
d) Estrategia Tecnológica para la recuperación de los Sistemas Operativos

1.3. ESTRATEGIA CONTINGENCIA OPERATIVA MANUAL

La Autoridad de Supervisión del Sistema Financiero (ASFI) establece que las Entidades Financieras deben elaborar y cumplir, políticas y normas que permitan adoptar acciones oportunas que tiendan a garantizar la continuidad de las operaciones, en un ámbito que permita a los consumidores financieros utilizar los servicios de una manera eficiente y segura y permita la minimización del impacto tras la realización de eventos no deseados o disruptivos. En tal sentido se define Proceso alterno manual de las operaciones, en casos que la entidad sea afectada su continuidad operativa en cuanto a los servicios que se brinda.

La activación del Plan de contingencia será aplicada en eventos de interrupción de las operaciones o funciones críticas, como:

1) Cortes de energía eléctrica prolongado
2) Pérdidas parciales de capacidad de procesamiento (Sistemas, equipos, servidores, cajas/Plataforma)
3) Caída del Sistema SFI hasta su restauración en servidor contingente.

En caso de contingente Operativa, es fundamental que el personal se involucre y cumpla rigurosamente con el protocolo establecido:

- En Oficina Central: Captaciones / Cajeros(as) / Analistas de créditos / Jefa Comercial
- En Agencia Mercado Campesino: Área Caja / Personal de Plataforma /Encargada de Agencia

2) ESTRATEGIAS A NIVEL DE EMERGENCIA.

Son los planes y protocolos diseñados para **proteger la vida y la integridad de las personas** ante eventos inesperados y peligrosos (sismos, incendios, robos, accidentes), por lo que incluyen evacuaciones, brigadas de emergencia, uso de extintores y primeros auxilios.

Las estrategias de emergencia protegen a las personas y reducen los riesgos inmediatos en situaciones críticas, priorizando siempre la seguridad humana.

Ante cualquier incidente que de manera inesperada afecte o ponga en riesgo la vida de los empleados, usuarios clientes y/o asociados que se encuentren en las instalaciones de la Cooperativa, se cuenta con un plan de emergencia para la respuesta a este tipo de incidentes.

- Procedimiento de evacuación
- Plan de emergencia en caso de incendio
- Plan de emergencia en caso de sismo o terremoto
- Plan de emergencia en caso de robo y/o asalto
- Plan de Primeros Auxilios
- Plan de Factor Pandemia / Epidemia

3) ESTRATEGIAS A NIVEL DE COMUNICACIONES.

En un Plan de Continuidad del Negocio (BCP), las estrategias de comunicación se enfocan en garantizar que la información fluya de manera rápida, clara, oportuna y confiable durante una interrupción, es decir, las **estrategias de comunicación** buscan evitar la desinformación y mantener confianza, asegurando que cada público (interno y externo) reciba la información adecuada, por el canal correcto y en el momento oportuno.

Se consideran generalmente tres ejes:

a) **Comunicación Interna**:
   - Se definen canales oficiales: Correo Corporativo, WhatsApp Business, llamadas telefónicas e intranet.
   - Se establece un árbol de llamadas o cadena de comunicación para notificar al personal clave.
   - Se determinan mensajes estandarizados para:
     - ☞ Notificación de la interrupción.
     - ☞ Instrucciones sobre continuidad de operaciones.
     - ☞ Estado de la emergencia y tiempo estimado de recuperación.

b) **Comunicación Externa:**
   - Se Identifican voceros oficiales (ej. Gerente General, Encargado de Riesgos, etc.).
   - Se establecen lineamientos para comunicar a:
     - ☞ Socios/Clientes: estado de los servicios, alternativas disponibles.
     - ☞ Entidades Reguladoras (ASFI, Banco Central, etc.): reportes de incidentes según normativa.
     - ☞ Medios de comunicación y redes sociales: solo a través de canales autorizados.

c) **Herramientas y Soporte:**
   - Se preparan mensajes prediseñados para emergencias.
   - Se debe asegurar múltiples vías de contacto en caso de falla de una (ej. internet vs. telefonía).
   - Realizar pruebas periódicas del plan de comunicación.