





Cooperativa de  
Ahorro y Crédito Societaria  
"Virgen de los Remedios RL."



# ESTRATEGIAS DEL PLAN 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.

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 <p><b>NO DISPONIBILIDAD DE LOS RESPONSABLES DE LOS PROCESOS (RR.HH.)</b></p>	<ul style="list-style-type: none"> <li>• Incendio</li> <li>• Terremoto</li> <li>• Actos de Violencia</li> <li>• Cierre parcial</li> <li>• Ausencia (Fallecimiento)</li> <li>• Intoxicación Colectiva</li> <li>• Indisposición de Personal responsable de proceso (Ausencia, renuncia repentina)</li> <li>• Pandemia</li> </ul>	<ul style="list-style-type: none"> <li>• Definición de árboles de llamada</li> <li>• Capacitación de personal alternativo</li> <li>• Documentación de procedimientos o manuales operativos.</li> </ul>
 <p><b>NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA</b></p>	<ul style="list-style-type: none"> <li>• Incendio</li> <li>• Inundación</li> <li>• Actos de violencia</li> <li>• Sismo o Terremoto</li> <li>• Explosión (Atentado)</li> </ul>	<ul style="list-style-type: none"> <li>• Teletrabajo</li> <li>• Respaldo entre sedes (Entre Oficina central y Agencia del Mercado Campesino)</li> <li>• Centro de Procesamiento de Datos Alterno (CPDA)</li> </ul>
 <p><b>NO DISPONIBILIDAD DE LOS RECURSOS TECNOLÓGICOS</b></p>	<ul style="list-style-type: none"> <li>• Falla eléctrica</li> <li>• Incendio</li> <li>• Inundación</li> <li>• Sismo o Terremoto</li> <li>• Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones</li> <li>• Ciberataque</li> </ul>	<ul style="list-style-type: none"> <li>• Estrategia de Recuperación</li> <li>• Plan de Contingencia Tecnológica</li> <li>• Procedimiento Alternativo manual para la atención a los socios y socias.</li> </ul>



ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 <p><b>NO DISPONIBILIDAD DE INFORMACIÓN</b></p>	<ul style="list-style-type: none"> <li>• Falla eléctrica</li> <li>• Incendio</li> <li>• Inundación</li> <li>• Sismo o Terremoto</li> <li>• Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones</li> <li>• Error humano</li> <li>• Hurto o robo</li> </ul>	<ul style="list-style-type: none"> <li>• Respaldo de información clave del proceso (BackUp): Copias diarias del sistema CORE.</li> <li>• Respaldo (Backup) de la información crítica de estaciones de trabajo y sistemas.</li> <li>• Procedimientos de resguardo y recuperación</li> <li>• Procedimiento de Digitalización de documentación crítica.</li> </ul>
 <p><b>NO DISPONIBILIDAD DE PROVEEDORES Y/O TERCEROS</b></p>	<p>No disponibilidad del Proveedor por eventos propios de su operación:</p> <ul style="list-style-type: none"> <li>• Falla eléctrica</li> <li>• Incendio</li> <li>• Inundación</li> <li>• Sismo o Terremoto</li> <li>• Falla Tecnológica</li> <li>• Pandemia</li> <li>• Actos de Violencia</li> <li>• Quiebra financiera del proveedor</li> <li>• Ciberataque</li> </ul>	<ul style="list-style-type: none"> <li>• Acuerdos de Niveles de Servicio SLA</li> <li>• Lista de proveedores alternos</li> </ul>

- ✓ 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.



## 1: ESTRATEGIAS A NIVEL DE CONTINGENCIA

### a) **ESTRATEGIA DE SITIO ALTERNO**

El sitio alternativo (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.

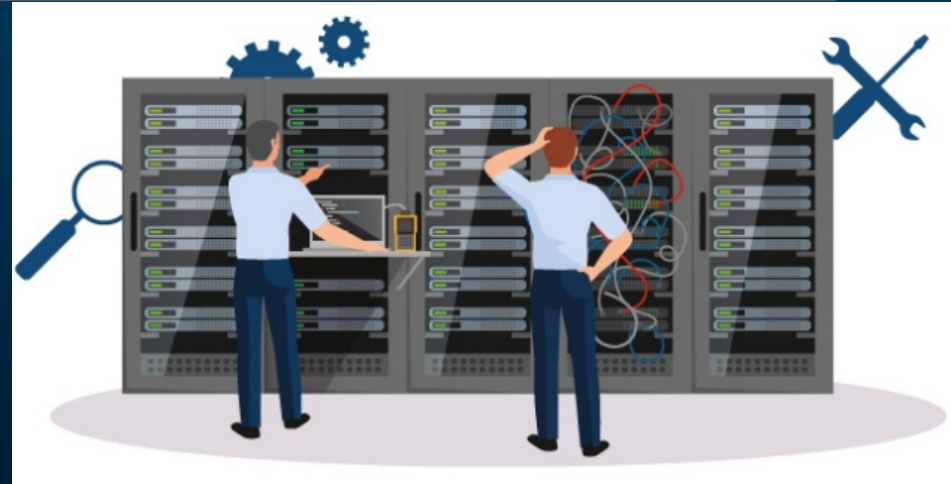


Los Criterios de Activación, están dadas de acuerdo a lo mencionado anteriormente como ser: Desastres Naturales, cortes de energía prolongados, ciberataques o falas críticas de la infraestructura en Oficina Central.

## 1: ESTRATEGIAS A NIVEL DE CONTINGENCIA

### b) **ESTRATEGIA TECNOLÓGICA: 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.



**EL PLAN DE CONTINGENCIA TECNOLÓGICA**, es activada por la unidad de sistemas siendo el responsable de su aplicación. Se tiene las estrategias para los recursos más críticos:

**Restauración o recuperación de las bases de datos**

**Estrategia de Recuperación del Servicio del Internet**

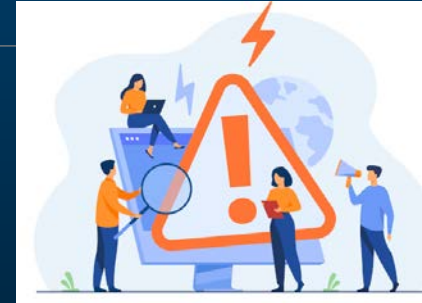
**Restauración de la Comunicación de la red interna**

**Recuperación de los Sistemas Operativos**

## 1: ESTRATEGIAS A NIVEL DE CONTINGENCIA

### C) **ESTRATEGIA CONTINGENCIA OPERATIVA MANUAL**

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, que permita la minimización del impacto tras la realización de eventos no deseados o disruptivos.



Esta estrategia será aplicada en eventos de interrupción de las operaciones o funciones críticas, como:

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

Es fundamental que el personal se involucre y cumpla 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

*Las estrategias de emergencia protegen a las personas y reducen los riesgos inmediatos en situaciones críticas, priorizando siempre la seguridad humana, es decir, 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. Por tanto, se debe contar:*



- 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 COMUNICACIÓN

Esta estrategia se enfoca 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 tres ejes:

**Comunicación  
interna**

**Comunicación  
externa**

**Herramientas y  
Soporte**



**¡¡¡Gracias por la  
atención!!!**

