



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

ESTRATEGIAS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

¿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.

ESCENARIO DE INTERRUPCIÓN	AMENAZAS	ALTERNATIVAS OPERATIVAS
 <p>NO DISPONIBILIDAD DE LOS RESPONSABLES DE LOS PROCESOS (RR.HH.)</p>	<ul style="list-style-type: none"> • Incendio • Terremoto • Actos de Violencia • Cierra parcial • Ausencia (Fallecimiento) • Intoxicación Colectiva • Indisposición de Personal responsable de proceso (Ausencia, renuncia repentina) • Pandemia 	<ul style="list-style-type: none"> • Definición de árboles de llamada • Capacitación de personal alterno • Documentación de procedimientos o manuales operativos.
 <p>NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA</p>	<ul style="list-style-type: none"> • Incendio • Inundación • Actos de violencia • Sismo o Terremoto • Explosión (Atentado) 	<ul style="list-style-type: none"> • Teletrabajo • Respaldo entre sedes (Entre Oficina central y Agencia del Mercado Campesino) • Centro de Procesamiento de Datos Alterno (CPDA)
 <p>NO DISPONIBILIDAD DE LOS RECURSOS TECNOLÓGICOS</p>	<ul style="list-style-type: none"> • Falla eléctrica • Incendio • Inundación • Sismo o Terremoto • Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones • Ciberataque 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• Falla eléctrica• Incendio• Inundación• Sismo o Terremoto• Fallas Tecnológicas en: Hardware, Software, Base de Datos y Comunicaciones• Error humano• Hurto o robo	<ul style="list-style-type: none">• 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	<p>No disponibilidad del Proveedor por eventos propios de su operación:</p> <ul style="list-style-type: none">• Falla eléctrica• Incendio• Inundación• Sismo o Terremoto• Falla Tecnológica• Pandemia• Actos de Violencia• Quiebra financiera del proveedor• Ciberataque	<ul style="list-style-type: none">• Acuerdos de Niveles de Servicio SLA• Lista de proveedores alternos

- ✓ 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 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.

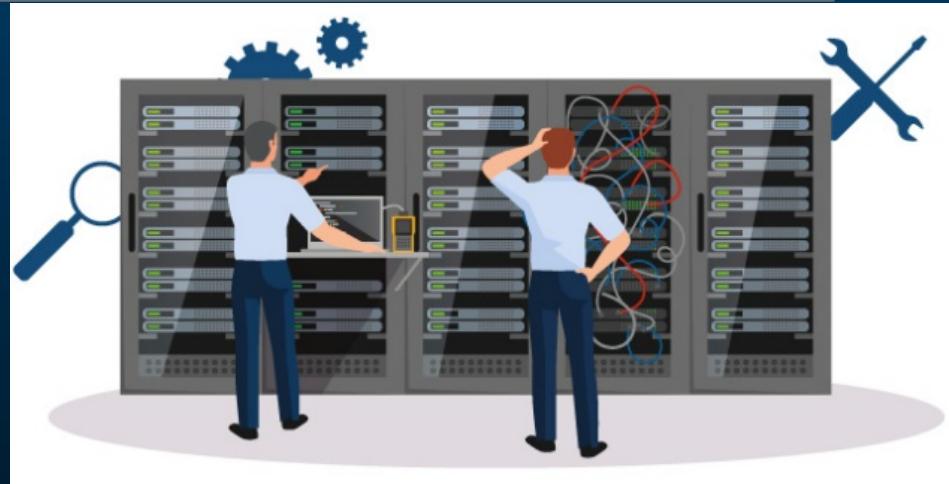


Los Criterios de Activación, están dadas de acuerdo a lo mencionado anteriormente como ser: Desastres Naturales, cortes de energía prolongados, ciberataques o falas críticas de la infraestructura en Oficina Central.

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!!!

