# PLAN DE CONTINUIDAD DEL NEGOCIO EMCANDELARIA S.A.S. E.S.P

## INTRODUCCION

Hoy en día la información es unos de los activos más importantes de cualquier organización o entidad, ya sea esta pública privada. Puesto que es la herramienta fundamental para garantizar el desarrollo de los procesos, permitiendo a las organizaciones su funcionamiento, continuidad y seguridad del negocio.

Para poder restablecer estos servicios y mitigar los riesgos, es necesario llevar a cabo unos pasos como son planear, desarrollar, probar y llevar a cabo procedimientos que se aseguren la continuidad eficiente de estos activos de la información.

La necesidad de implementar un plan o proceso para recuperar los servicios de cómputo se contempla desde que ocurra un incidente o evento que parcialmente o por un breve periodo de tiempo interrumpa las actividades diarias de la entidad o, por el contrario, impida la continuidad del negocio en su totalidad.

## OBJETIVO

Diseñar el plan de continuidad del negocio ante desastres tecnológicos (DRP) de EMCANDELARIA S.A.S E.S.P, en caso de un siniestro o un evento que genere interrupción de los servicios tecnológicos de la entidad.

Responsable:

Líder: jefe de la Oficina de Tecnologías de la Información

Equipo de respuesta Oficina TIC

## ALCANCE

Este documento tiene como finalidad la rápida respuesta a incidentes que afecten la continuidad de los servicios en la entidad. Con el desarrollo de estrategias en la recuperación de los activos de información en el menor tiempo posible y así disminuir la perdida de los recursos.

## GLOSARIO

**Activo de información**: Se refiere al activo que contiene información o elementos relacionados con el manejo de la información (sistemas, soportes, edificios, personas…) y que se caracteriza por tener valor para la organización o entidad (ISO/IEC 27000).

**Análisis del impacto:** al negocio (BIA por sus siglas en inglés): Proceso del análisis de actividades, las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22300).

**Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. Nota 1: El análisis de riesgo proporciona las bases para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. Nota 2: El análisis del riesgo incluye la estimación del riesgo. [Norma ISO 31000:2011, Capítulo 2, Términos y definiciones, numeral 2.21].

**Continuidad del negocio**: Capacidad de la organización de continuar entregando productos y servicios a niveles aceptables predefinidos después de que ocurra un evento.

**Desastre:** Un evento repentino, no planeado y catastrófico que causa daño o pérdida no aceptable a una organización.

**Directorio activo:** Base de datos distribuida que permite almacenar información relativa a los recursos de una red (objetos, dominios, árboles y bosques) con el fin de facilitar su localización y administración, el cual ofrece la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa.

**DRP:** Sigla en inglés (Disaster Recovery Plan) Plan de Recuperación ante Desastres de Tecnología: Información documentada que define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

**Infraestructura:** Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. [Norma ISO 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.20].

**Interrupción:** Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de

tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

**Plan de continuidad de negocio:** Procedimientos documentados que guían u orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción.

**Plan de contingencia:** Define los procedimientos y medidas que se deben tomar para que las organizaciones puedan continuar operando en caso de una situación de desastre o emergencia.

**Plataforma tecnológica crítica:** Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son esenciales para soportar los procesos y servicios de la entidad.

**Procesos críticos:** Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

**Proveedor:** Persona, natural o jurídica, responsable de suministrar bienes y servicios.

**RAS:** Sigla en inglés (Response Alternative and Solutions): documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

**Respuesta a incidentes:** Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable.

**RTO:** Sigla en inglés (Recovery Time Objetive): tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

**RPO:** Sigla en inglés (Recovery Point Objetive): cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio cuando se presenta un evento alterador del normal funcionamiento.

## GENERALIDAD DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Análisis del impacto del negocio

En este análisis se intenta presentar la relación de los componentes específicos de EMCANDELARIA S.A.S E.S.P (Seguridad digital, equipos de cómputo, correos, interfaces de software y las áreas involucradas), con sus servicios esenciales; y con base a esta información determinamos las necesidades y prioridades de contingencia.

Este plan contempla el hecho de que por alguna situación interna o externa ocurra un incidente menor o mayor afectado los servicios tecnológicos por completo por un periodo inaceptable de tiempo.

Qué aspectos se evalúan:

- ✔ Daños físicos
- ✔ Tiempo estimado de recuperación
- ✔ Acciones específicas a seguir de acuerdo con el tipo de incidente.

Identificación de Procesos Críticos

- ✔ la Infraestructura que la soporta (Servidores, Redes y Telecomunicaciones)
- ✔ Procesos financieros, contables y administrativos que dependen de plataformas de terceros (Proveedores)
- ✔ Seguridad de la información con la creación de políticas y la auditoria de ejecución y cumplimiento de las mismas al interior de la entidad.

Funciones críticas

- ✔ Personal disponible para mesa de ayuda
- ✔ Disponibilidad de la infraestructura tecnológica (Servidores, almacenamiento y conectividad)

- ✔ Disponibilidad de telefonía IP
- ✔ Disponibilidad de canales de internet
- ✔ Disponibilidad de canales de chat, o redes sociales para comunicación entre EMCANDELARIA S.A.S E.S.P y los clientes.

Funciones esenciales

- ✔ Disponibilidad de correo electrónico institucional
- ✔ Disponibilidad de internet
- ✔ Disponibilidad de Chat y portales de servicio

Funciones necesarias

- ✔ Disponibilidad de acceso a Plataforma ANSOFT

Tiempos estimados de recuperación:

- ✔ Criticas 5 Horas
- ✔ Esenciales 2 horas
- ✔ Necesarias 1 hora

Prioridades de Recuperación

las prioridades de recuperación durante el plan de contingencia son:

Prioridad alta:

• Infraestructura de Red Local (Switches, Firewall, plantas, etc)

• Canales de comunicación (WhatsApp, Facebook)

• Infraestructura de apoyo (Telefonía/telecomunicaciones y aplicaciones)

• Herramientas de Gestión de Servicios ANSOFT (Bases de Datos)

• Correo electrónico Colombian Hosting

• Canal de Internet Proveedor Claro

Prioridad Media

• Aplicaciones de negocio, proyectos, etc.

Prioridad Baja

• Ambientes de prueba y desarrollo

## RIESGOS ASOCIADOS A LA CONTINUIDAD DEL NEGOCIO

Está ligado a la gestión de riesgos empresariales cuya finalidad es analizar los riesgos a que están expuestos los negocios y las operaciones, así como las consecuencias que provocarían dichos riesgos, centrándose en el impacto de la interrupción del negocio.

Entre ellos tenemos:

1. Interrupciones no planificadas en TI y telecomunicaciones.
2. Ciberataques.
3. Brechas de datos.
4. Malas condiciones climatológicas.
5. Interrupción del suministro de red.
6. Fuego.
7. Incidentes de seguridad.
8. Incidentes de salud y seguridad.
9. Actos de terrorismo.
10. Nuevas leyes o regulaciones.

Enmarcadas en algunas de estas áreas, encontramos una serie de **situaciones de peligro frecuentes y recurrentes**:

- Un deficiente control de acceso a los sistemas informáticos.
- Existencia de vulnerabilidades web.
- Falta de formación y concienciación entre los trabajadores.
- Procesos de gestión ante incidentes de seguridad ineficaces o mal planteados.
- Problemas de adaptación a los cambios regulatorios y normativos.
- Inexistencia o insuficiente control del acceso a la red de los usuarios internos y terceros, tales como proveedores o invitados a la red corporativa.
- Fugas de información.
- Existencia de vulnerabilidades en los filtros informativos que provocan fraudes y robos de información.
- Uso de software inseguro.
- Falta de planificación en la continuidad de negocio.

**IMPACTO**

**Nivel 5 - Extremo**. Es un riesgo que puede representar pérdidas para la organización si se materializa con un impacto crítico o grave, y se debe mitigar por medio de planes de acción.

**Nivel 4 - Alto**. Es un riesgo que puede representar pérdidas para la organización si se materializa con un impacto alto y se debe mitigar por medio de planes de acción.

**Nivel 3 - Medio**. Es un riesgo que representa un nivel moderado y se debe controlar para que no aumente.

**Nivel 2 - Bajo**. Es un riesgo que se debe monitorear, pero está dentro del riesgo para la entidad.

**Nivel 1 – Muy Bajo**. Es un riesgo que se debe monitorear, pero está dentro del riesgo para la entidad.

Para el monitoreo preventivo del ejercicio de continuidad del negocio y del servicio EMCANDELARIA S.A.S E.S.P cuenta con los siguientes riesgos existentes:

| Clasificación del riesgo | Nombre del Riesgo | Descripción |
|---|---|---|
| Comunicación | Uso inadecuado de los canales de comunicación | Comprende el mal uso de los canales de comunicación para difundir un mensaje, reportar un dato o información. |
| Imagen | Pérdida de Credibilidad y confianza | Relacionado con la percepción y confianza de los ciudadanos hacia EMCANDELARIA |
| Información | Perdida de la información | Se asocia con pérdida o robo de la información, ya sea física o digital |
| Operativo | Daños o deterioro de los activos tangibles. | Daño o deterioro de los bienes muebles |

| | | |
|---|---|---|
| Tecnológico | Acceso no autorizado | Acceso a bases de datos o servidores. Servidores de correo sin autorización previa |

## PRUEBAS Y REVISIÓN PERIÓDICA DEL PLAN

En las reuniones de comité de MIPG, se revisará, aprobará monitoreará el plan de continuidad del negocio, las acciones preventivas se llevarán a cabo según la planificación de Talento Humano, administrativas relacionadas con la infraestructura, las cuales estarán coordinadas por la Gerencia, el grupo de apoyo de mesa de ayuda, el líder u oficial de seguridad de la información. Durante esta planificación se definirán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, esto se hará con base en los recursos económicos presupuestados para cada vigencia y debe hacerse como mínimo dos (2) veces al año.

## PASO A PASO PARA SEGUIR EL PLAN

Una vez construido y aprobado el plan por Gerencia y el comité de MIPG, se deben emprender acciones necesarias para socializarlos con todos los funcionarios, contratistas, terceros y proveedores, para estar preparados para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible los servicios con el siguiente check list:

- Analizar daños (elaborar lista de chequeo) Comité MIPG
- Llamado al equipo de restablecimiento
- Llamado al personal interno y comunicación de acción a seguir – Restablecimiento de los sistemas de información según el plan –Coordinador Grupo de Sistemas
- Re establecimiento gradual de la información - Grupo de mesa de ayuda
- Análisis de situación – Gerencia y comité
- Establecer plan de mejoramiento a partir del análisis de lo ocurrido

## NOTIFICACIÓN DE INFORMACIÓN A LOS FUNCIONARIOS

Con base en su cargo o puesto de trabajo dentro de la entidad, se le pondrá en contacto a través del coordinador o líder del área para que le informe:

- La naturaleza de la emergencia o evacuación
- Estimación de daños ocurridos
- Punto de encuentro

Cada coordinador de área o líder, será el punto de contacto con su equipo de apoyo, hará llegar la información necesaria y las instrucciones a su equipo y será responsable de un informe sobre la situación correcta de los progresos en su equipo.

## DECIDIR DONDE REINICIAR LABORES U OPERACIONES

Es necesario establecer si las operaciones de infraestructura estropeadas se pueden reparar, dependiendo del daño. Lo anterior deberá decidirse entre el Coordinador del plan de continuidad (en este caso es el mismo líder del Grupo de Sistemas).

## REGRESO DEL PERSONAL A LAS ÁREAS DE TRABAJO O PISOS

Una vez se realicen los trabajos de reparación de las operaciones estropeadas, el Coordinador del plan de continuidad notificarán a los lideres de cada área de cada piso el momento a partir del cual los funcionarios puedan regresar a las instalaciones para reanudar la entrega del servicio.

## RESTABLECER LAS OPERACIONES NORMALES DE LA ENTIDAD

Con el personal ubicado y operando en cada lugar que le corresponde en las instalaciones recuperadas, el Coordinador del plan de continuidad, procederán a evaluar y monitorear la entrega de los servicios afectados con el objetivo del menor tiempo posible y llegar a los niveles de entrega satisfactorios anteriores a la interrupción.

## REANUDACIÓN DE LAS OPERACIONES EN LOS NIVELES ANTERIORES A LA INTERRUPCIÓN

Al conseguir operar a los niveles previos a la interrupción, el líder o profesional encargado del BCP y el Gestor de Incidentes notificarán al Comité de Gerencia el retorno a normalidad en la entrega de los servicios afectados vía correo electrónico y por este mismo medio se procederá con la notificación a los clientes o proveedores externos afectados por la interrupción.

| **Fecha** | **Versión** | **Cambios** |
|---|---|---|
| 19/08/2022 | 1 | Adopción procedimiento |
| Elaboró<br>Cristian Bravo | Revisó<br>Control Interno | Aprobó |