
# GUIA PLAN DE RECUPERACIÓN ANTE DESASTRES

## *1. INFORMACIÓN GENERAL*

**1.1. OBJETIVO**

Definir el conjunto de actividades, roles y responsabilidades que permitan mantener la continuidad de la plataforma tecnológica de la entidad, en caso de la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente.

**1.2. RESPONSABLE**

Equipo IT.

**1.3. ALCANCE**

Esta guía se enmarca en la protección de los sistemas y plataformas tecnológicas descritas a continuación y que soportan los procesos misionales de la entidad:

| Tipo de Componente | Descripción | Tiempo de Interrupción Tolerable (RTO) |
|---|---|---|
| **Aplicaciones** | - Spotify API | 1 hora |
| | - AWS Rekognition | 1 hora |
| | - Web App propia | 5 minutos |
| **Comunicaciones** | - Enlace con Internet | 24 horas ((1 día hábil) |
| **Servicios** | - DNS | 5 minutos |
| **Infraestructura** | - Infraestructura en la nube | 5 minutos |

| | |
|---|---|
| **1.4. DEFINICIONES** | **BCP:** Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.<br><br>**BIA**: Sigla en inglés (Business Impact Analisys), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.<br><br>**DRP**: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.<br><br>**ERA**: Sigla en inglés (Environment Risk Analisys), Análisis de Riesgos Ambientales en español, y hace referencia a un documento que relaciona los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.<br><br>**RAS**: Sigla en inglés (Response Alternative and Solutions), y hace referencia a un documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.<br><br>**RPO:** Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.<br><br>**RTO**: Sigla en inglés (Recovery Time Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.<br><br>**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 críticos para soportar los procesos y servicios de la entidad. |

## *2. CONDICIONES GENERALES*

*2.1.* El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales de inspección, vigilancia y control, y procedimientos mercantiles.

2.2. Supuestos: La efectividad en la ejecución de este documento guía, ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente que afecte la plataforma tecnológica, se fundamenta en los siguientes supuestos:

- Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- Los funcionarios que ejecutan esta guía, o sus suplentes, se encuentran disponibles para proveer apoyo y no han sido afectados por el desastre.
- El desastre no afectó simultáneamente la zona hábil principal y la zona hábil alterna.
- El centro de cómputo alterno estará habilitado para un promedio de 100 usuarios concurrentes.
- Solo el funcionario responsable activará el DRP.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

**Nota: Los aspectos que se encontrarán en esta guía, encerrados en un recuadro rojo con líneas punteadas, dependen de adquisición y funcionalidad de las estrategias de continuidad con la infraestructura contingente correspondiente.**

## *3. GUIA DEL PLAN DE RECUPERACIÓN ANTE DESASTRES*

### *3.1.* ESCENARIOS DE DESASTRE

Los escenarios de desastre, interrupción mayor o un evento contingente que contempla este documento guía son:

## Centro de Cómputo:

No disponibilidad del centro de cómputo (centro AWS) por:

- **ATENTADO TERRORISTA**
- **INCENDIO**
- **DESASTRE NATURAL**
- **DAÑO A SISTEMA DE REFRIGERACIÓN**
- **DAÑO EN SUMINISTRO ELÉCTRICO**

- **Ataque Informatico**

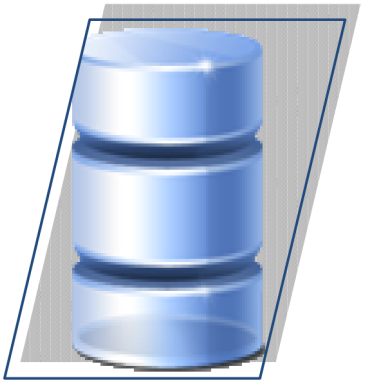
## Infraestructura de Comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en:

- **SWITCH CORE**
- **FIBRAS ÓPTICAS DE CONEXIÓN CON CENTROS DE CABLEADO**
- **ROUTER CORE**
- **ROUTER DE LA REGIONAL**
- **SWITCH DE PISO**
- **ENLACES DE COMUNICACIÓN CON ISP**
- **ENLACES DE COMUNICACIÓN CON REGIONALES**
- **SWITCH DE COMUNICACIÓN CON REGIONALES**
- **SWITCH DE UNA REGIONAL**
- **SWITCH DEL FIREWALL**
- **FIREWALL**

## Infraestructura de Bases de datos, Almacenamiento y Respaldo

No disponibilidad de datos e información por:

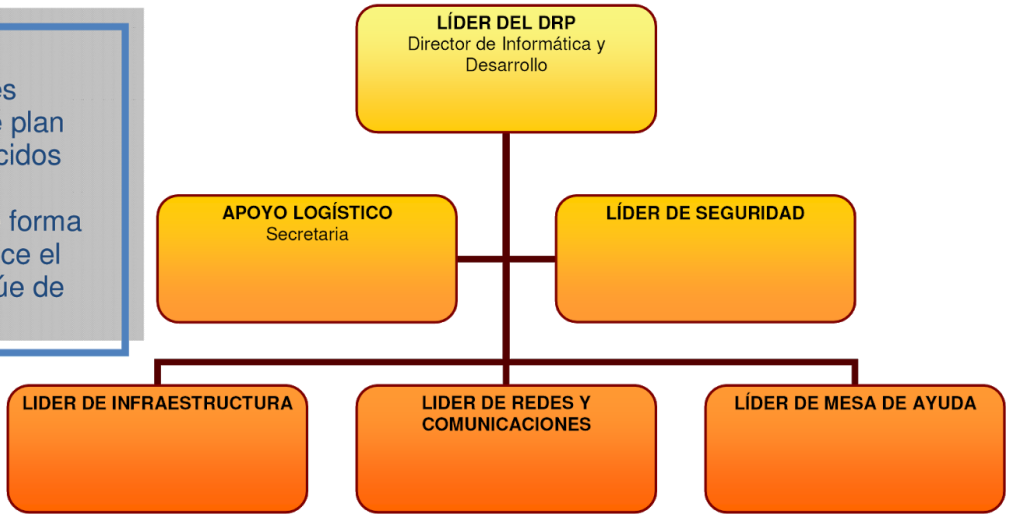


- **CORRUPCIÓN DE LA BASE DE DATOS**
- **BORRADO O PÉRDIDA DE DATOS**

**CUALQUIER ESCENARIO NO MENCIONADO ANTERIORMENTE, NO HA SIDO CONSIDERADO EN EL PRESENTE DOCUMENTO GUÍA.**

## *3.2.* ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada.



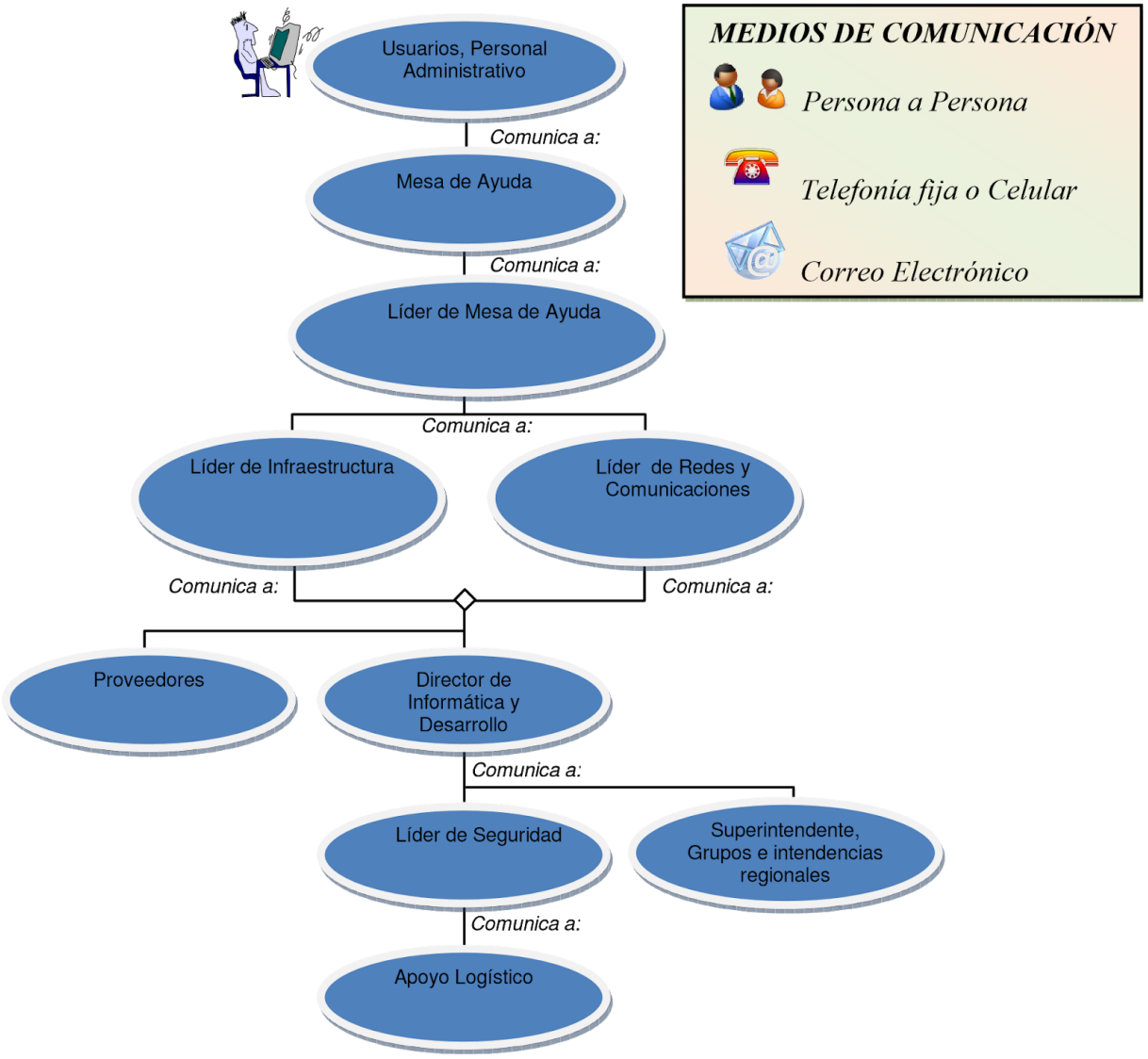
Las responsabilidades definidas para cada rol son:

| ROL | ANTES DEL EVENTO INTERRUPCIÓN | DURANTE EL EVENTO INTERRUPCIÓN | DESPUÉS DEL EVENTO DE INTERRUPCIÓN |
|---|---|---|---|
| **Líder del DRP** | - Velar por la actualización del DRP y recursos requeridos.<br>- Velar por la actualización, distribución y pruebas del DRP<br>- Gestionar la consecución de los recursos para el DRP.<br>- Comunicar a las personas que corresponda sobre la situación de contingencia. | - Evaluar y activar el DRP y las estrategias de recuperación y contingencia.<br>- Comunicar al Secretario General sobre el estado de la operación de Contingencia.<br>- Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio<br>- Liderar la operación bajo contingencia.<br>- Comunicar a la dirección el desastre, interrupción o evento contingente.<br>- Liderar el retorno a la normalidad. | - Velar por la actualización del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. |
| **Lider de infraestructura, Lider de Redes y Comunicaciones, y Lider de Mesa de ayuda** | - Comunicar necesidades de ajuste<br>- Participar en la ejecución de las pruebas al DRP | - Evaluar el desastre, interrupción o evento contingente.<br>- - Comunicar el evento al Líder del DRP<br>- Verificar disponibilidad y notificar | - Reportar los inconvenientes y oportunidades de mejora del DRP |

| ROL | ANTES DEL EVENTO INTERRUPCIÓN | DURANTE EL EVENTO INTERRUPCIÓN | DESPUÉS DEL EVENTO DE INTERRUPCIÓN |
|---|---|---|---|
| **Líder de Seguridad** | - Coordinar actividades de entrenamiento, documentación y actualización del DRP.<br>- Coordinar las actividades de pruebas del DRP.<br>- Identificar los recursos requeridos para la operación del DRP. | - Proveer soporte a los profesionales especializados. - Notificar al proveedor de Centro de Cómputo Alterno (si aplica).<br>- Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno.<br>- Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno, de los funcionarios que activarán la infraestructura. (Si aplica)<br>- Mantener informado al Líder del DRP | - Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. |
| **Apoyo Logístico** | - Participar en la ejecución de las pruebas al DRP | - Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia, entre otras. - Suministro de información de contrato<br>- Logística de desplazamiento, si es requerido<br>- Contacto de proveedores, si es requerido | - Reportar los inconvenientes y oportunidades de mejora del DRP |

## *3.3.* ÁRBOL DE LLAMADAS

Cuando se presente un desastre, interrupción o evento contingente, se debe seguir la siguiente cadena de llamadas:




Los datos de contacto para los funcionarios que ejercen estos roles se encuentra en los documentos de la Dirección de Informática y Desarrollo.

### *3.4.* ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP

**¿Quién reporta un incidente, interrupción mayor o un evento contingente?**

**a. Los usuarios deben reportar el incidente a la mesa de ayuda cuando:**

- NO se pueden utilizar los sistemas de información.
- NO hay red de comunicaciones.
- NO hay servicio de correo electrónico.
- NO hay acceso a los archivos electrónicos centralizados
- CUALQUIER otro evento de tecnología que afecte la prestación del servicio.

**¿Quién evalúa la magnitud e impacto del incidente?**

**b.El profesional especializado de la plataforma afectada, debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:**

- Naturaleza e impacto del incidente.
- Estrategias definidas en el DRP aplicables u otras soluciones potenciales
- Tiempo estimado de solución del incidente.

Finalmente, comunicarse con el Director de Informática y Desarrollo para informar los resultados del diagnóstico.

### 3.5. ACTIVIDADES DE MANEJO DE CRISIS

A continuación se listan las actividades y consideraciones necesarias para el manejo de una crisis que afecte o pueda afectar la reputación, imagen, u operación de la Superintendencia de Sociedades.

a. **El Director de Informática y Desarrollo comunica a la Alta Dirección , teniendo en cuenta los siguientes aspectos:**
   - Sistemas y servicios afectados
   - Resultados del diagnóstico
   - Acciones realizadas
   - Tiempo estimado para normalización
   - Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
   - Decisiones que debe tomar la alta dirección.

b. **La Alta Dirección (Equipo de Manejo de Crisis) evalúa la crisis y el impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontar la crisis.**

c. **La Alta Dirección, a través de los voceros o funcionarios delegados, comunicará la crisis a nivel interno y externo, en caso de ser requerido, teniendo en cuenta los siguientes aspectos:**


- ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
- ¿Qué información está en proceso de verificación e investigación?
- ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
- ¿Qué información se debe manejar al interior de la entidad?
- ¿Quiénes fueron afectados por la crisis (audiencia)?
- ¿Qué otras audiencias deberían saber sobre la crisis?
- ¿Cómo se comunicará la información a los interesados o afectados (medio)?

**La comunicación de la crisis deberá considerar los siguientes principios:**


- **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.

- **Decir la verdad**: Ser honestos en los comunicados, sin embargo no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.

- **Emitir reportes lo más exactos posible**: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

**Las audiencias a considerar en la comunicación de la crisis son:**


servicios de la entidad.

- Usuarios externos de los productos y/o

- Gobierno y Autoridades

### 3.6. ACTIVIDADES DE MANTENIMIENTO

Es responsabilidad del Líder de Seguridad la actualización de las nuevas versiones al DRP, y la comunicación de las mismas a todos los funcionarios involucrados en el mismo.

La actualización y mantenimiento al DRP se debe realizar:

- Cuando ha transcurrido un año desde la última actualización.
- Cuando han ocurrido cambios en la plataforma tecnológica objeto del alcance de esta guía.
- Cuando los resultados de las pruebas requieren actualización del DRP o sus procedimientos.
- Cuando hay cambios en el personal que operaría el DRP.
- Cuando los resultados de auditorías así lo indican.

Algunas actividades a realizar para mantener vigente el DRP, son:

| No | Actividad | Responsable | Frecuencia |
|---|---|---|---|
| 1. | Actualización de los procedimientos de recuperación y contingencia de la plataforma tecnológica | Líderes de los procesos | Cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia |
| 2. | Sincronización de la configuración de la infraestructura respaldada en el Centro de Cómputo Alterno (Incluyendo replicación de data) | Lider de Infraestructura<br><br>Lider de redes y comunicaciones | Permanente |
| 3. | Monitoreo de la infraestructura respaldada en el Centro de Cómputo Alterno, para verificar su disponibilidad en caso de que se presente un evento | Lider de Infraestructura | Permanente |
| 4. | Ejecución de pruebas periódicas para verificar el correcto funcionamiento de los sistemas respaldados | Profesionales Especializados | Cada trimestre |
| 5. | Ejecución del procedimiento de respaldo de datos de la infraestructura tecnológica | Lider de Infraestructura | Permanente |

| | | | |
|---|---|---|---|
| 6. | Obtener imagen del sistema de servidores y equipos de red. | Lider de Infraesetructura<br><br>Lider de redes y comunicaciones | Semestral o cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia |

### 3.7. ACTIVIDADES DE PRUEBA

La programación y metodología a utilizar en la realización de pruebas al DRP están relacionadas en el Procedimiento de Gestión al Plan de Recuperación ante Desastres.

### 3.8. DISTRIBUCIÓN DE LA GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES

Este documento guía deberá ser entregado bajo las siguientes consideraciones:

- Se debe entregar una copia final COMPLETA del DRP a:
  - Director de Informática y Desarrollo
  - Líder de Seguridad de la Información
  - Líder de Infraestructura
  - Administrador de Redes y Comunicaciones
- Se debe enviar una copia final COMPLETA del DRP a:

- Proveedor de Centro de custodia.

Las diferentes copias del documento guía deben ser controladas, y cada que se cambie de versión, se deberá recoger las versiones anteriores.