
 INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

# GUIA PLAN DE RECUPERACIÓN ANTE DESASTRES

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23


## 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** Líder de Seguridad de la información.

**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)
<b>Aplicaciones</b>	- Pagina Web Icultur	24 horas ((1 día hábil)
	-Sisbibliored Sistema de bibliotecas	24 horas (1 día hábil)
	- PQRS Sistema de atención al ciudadano	24 horas (1 día hábil)
<b>Mensajería</b>	- Correo Electrónico	24 horas ((1 día hábil)
<b>Comunicaciones</b>	- Switch Core	24 horas ((1 día hábil)
	- Enlace con Internet	
	- Enlaces con intendencias	
<b>Servicios</b>	- DNS	24 horas ((1 día hábil)

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

#### 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.

**BIA:** Sigla en inglés (Business Impact Analysis), 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.

**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.


**ERA:** Sigla en inglés (Environment Risk Analysis), 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.

**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.

**RPO:** Sigla en inglés (Recovery Point Objective), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.

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

**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.

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23


## 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 y no ha sido afectados por el desastre.

- El desastre no afectó simultáneamente el Centro de cómputo principal y el Centro de Cómputo Alterno.
- El Centro de Cómputo Alterno estará habilitado para un promedio de 100 usuarios concurrentes.

- Solo el funcionario responsable activará el DRP.
- Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- 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 con líneas punteadas, dependen de adquisición y funcionalidad de las estrategias de continuidad con la infraestructura contingente correspondiente.**

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

### 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:

##### Infraestructura de Comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en:

- SWITCH CORE
- ROUTER CORE
- SWITCH DE PISO
- ENLACES DE COMUNICACIÓN CON ISP
- FIREWALL



	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23


### Infraestructura de Bases de datos. Almacenamiento y Respaldo

No disponibilidad de datos e información por:

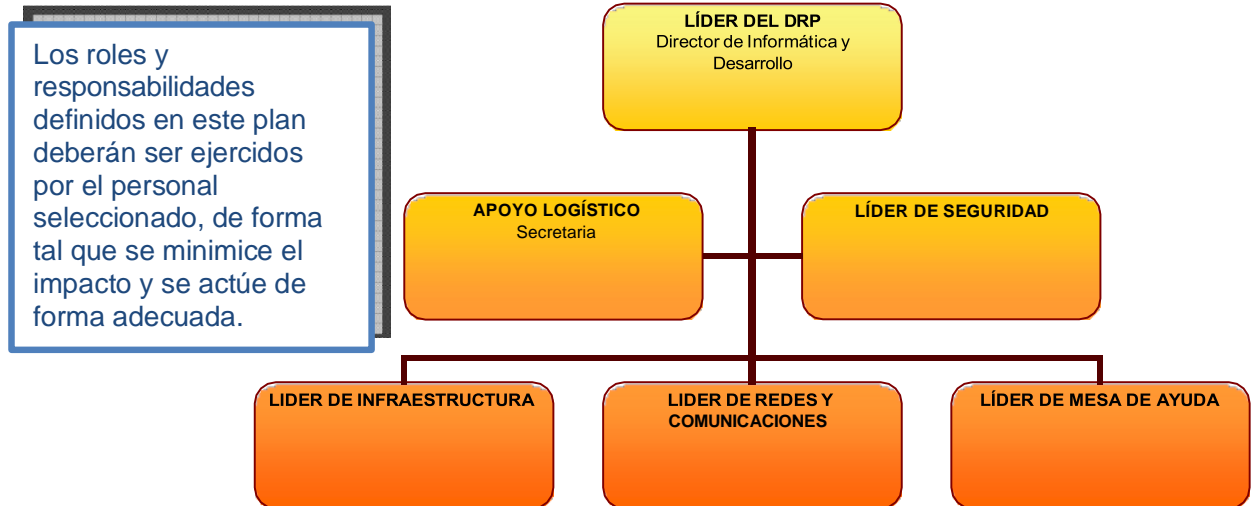
- **CORRUPCIÓN DE LA BASE DE DATOS**
- **BORRADO O PÉRDIDA DE DATOS**
- **FALLA TOTAL O PARCIAL DE LA SAN SUN 6140**
- **FALLA TOTAL O PARCIAL DE LA SAN IBM DS 4300**
- **FALLA EN SWITCH CONEXIÓN A LA SAN**
- **FALLA TOTAL O PARCIAL DEL SERVIDOR DE RESPALDO**



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


	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

### 3.2. ROLES Y RESPONSABILIDADES




Las responsabilidades definidas para cada rol son:

ROL	ANTES DEL EVENTO	DURANTE EL EVENTO	DESPÚES DEL EVENTO
	INTERRUPCIÓN	INTERRUPCIÓN	INTERRUPCIÓN
<b>Líder del DRP</b>	<ul style="list-style-type: none"> <li>- Velar por la actualización del DRP y recursos requeridos.</li> <li>- Velar por la actualización, distribución y pruebas del DRP</li> <li>- Gestionar la consecución de los recursos para el DRP.</li> <li>- Comunicar a las personas que corresponda sobre la situación de contingencia.</li> </ul>	<ul style="list-style-type: none"> <li>- Evaluar y activar el DRP y las estrategias de recuperación y contingencia.</li> <li>- Comunicar al Director General sobre el estado de la operación de Contingencia.</li> <li>- Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio</li> <li>- Liderar la operación bajo contingencia.</li> <li>- Comunicar a la dirección el desastre, interrupción o evento contingente.</li> <li>- Liderar el retorno a la normalidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Velar por la actualización del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción.</li> <li>- Informar al Director General sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.</li> </ul>
<b>Líder de infraestructura, Líder de Redes y Comunicaciones, y Líder de Mesa de ayuda</b>	<ul style="list-style-type: none"> <li>- Comunicar necesidades de ajuste</li> <li>- Participar en la ejecución de las pruebas al DRP</li> </ul>	<ul style="list-style-type: none"> <li>- Evaluar el desastre, interrupción o evento contingente.</li> <li>- En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución.</li> <li>- Comunicar el evento al Líder del DRP</li> <li>- Verificar disponibilidad y notificar</li> </ul>	<ul style="list-style-type: none"> <li>- Reportar los inconvenientes y oportunidades de mejora del DRP</li> </ul>

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

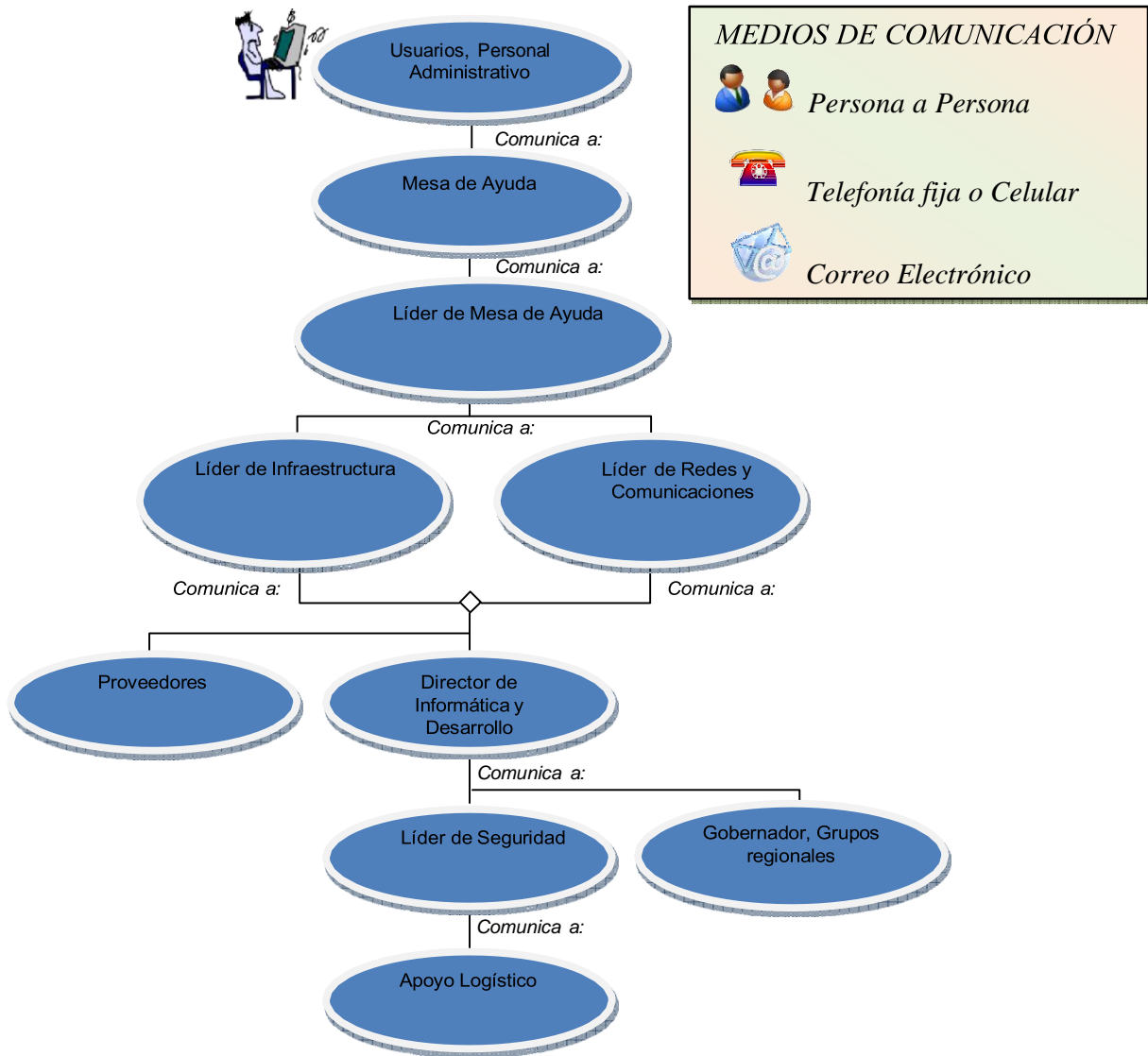
ROI	ANTES DEL EVENTO INTERRUPCIÓN	DURANTE EL EVENTO INTERRUPCIÓN	DESPÚES DEL EVENTO INTERRUPCIÓN
		<ul style="list-style-type: none"> <li>al personal requerido para atender el evento.</li> <li>- Ejecutar las guías de contingencia y recuperación.</li> <li>- Comunicar a los proveedores la activación del DRP.</li> <li>- Solicitar la corrección del componente afectado y realizar seguimiento de la solución.</li> <li>- Estar atentos para dar una correcta información a las personas que lo requieran.</li> <li>- Mantener informado al Líder del DRP</li> </ul>	
<b>Líder de Seguridad</b>	<ul style="list-style-type: none"> <li>- Coordinar actividades de entrenamiento, documentación y actualización del DRP.</li> <li>- Coordinar las actividades de pruebas del DRP.</li> <li>- Identificar los recursos requeridos para la operación del DRP.</li> </ul>	<ul style="list-style-type: none"> <li>- Proveer soporte a los profesionales especializados.</li> <li>- Notificar al proveedor de Centro de Cómputo Alterno (si aplica).</li> <li>- Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno.</li> <li>- Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno, de los funcionarios que activarán la infraestructura. (Si aplica)</li> <li>- Mantener informado al Líder del DRP</li> </ul>	<ul style="list-style-type: none"> <li>- Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.</li> </ul>
<b>Apoyo Logístico</b>	<ul style="list-style-type: none"> <li>- Participar en la ejecución de las pruebas al DRP</li> </ul>	<ul style="list-style-type: none"> <li>- Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia, entre otras.</li> <li>- Suministro de información de contrato</li> <li>- Logística de desplazamiento, si es requerido</li> <li>- Contacto de proveedores, si es requerido</li> </ul>	<ul style="list-style-type: none"> <li>- Reportar los inconvenientes y oportunidades de mejora del DRP</li> </ul>




	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

### 3.3. ÁRBOL DE LLAMADAS

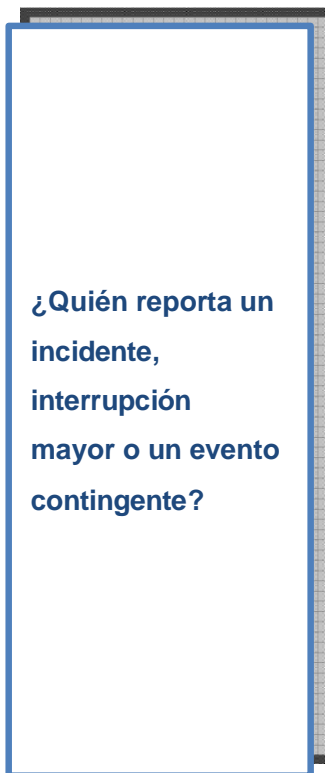
Cuando se presente un desastre, interrupción o evento contingente, se debe seguir la siguiente cadena de llamadas:



	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

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



**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


**b. El personal administrativo (vigilancia, servicios generales) debe reportar el incidente a Mesa de Ayuda o Líder de Centro de Cómputo cuando:**

- SUENA la alarma del centro de cómputo
- HAY inundación en cualquier piso
- HAY un conato de incendio en el piso donde se encuentre ubicado el centro de computo
- CUALQUIER otro evento que afecte o pueda afectar el centro de cómputo

**c. La mesa de ayuda debe atender el incidente de acuerdo a lo establecido en los Procedimientos de Mantenimiento preventivo, correctivo y soporte técnico, y se continúa con la ejecución si:**

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados.

En cualquiera de los casos, debe escalarlo a los funcionarios responsables.

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

**d. 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.

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

**¿Cuándo se debe activar el Centro de Cómputo Alterno?**

**e. El Director de Informática y Desarrollo, define si se activa o no el Centro de Cómputo Alterno, teniendo en cuenta los siguientes aspectos:**


- Si el evento afectó considerablemente el Centro de Cómputo Principal
- Si la solución en sitio dura más de **24 horas**.

**f. En caso de que se active, el líder de seguridad debe comunicar la activación al proveedor, teniendo en cuenta:**

- Fecha y hora a partir de la cual se da inicio a la activación.
- Funcionarios de la entidad que estarían en el proceso de activación, para que se tramiten los permisos de acceso correspondientes.

**g. El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Centro de Cómputo Alterno, teniendo en cuenta:**

- Enrutamiento y activación de las comunicaciones hacia el Centro de Cómputo Alterno.
- Detención de la replicación de datos
- Verificación de la disponibilidad de información en el Centro de Cómputo Alterno
- Activación servicio de controladores de dominio y sistema operativo en servidores
- Activación servicio de bases de datos y aplicaciones

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

**h. El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el Centro de Cómputo Alterno, teniendo en cuenta:**

- Acceder a los sistemas de información
- Realizar pruebas sobre los sistemas de información

**i. El Director de Informática y Desarrollo, define si comunica o no el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.**


**j. El Líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:**

*Si es un evento que afectó las comunicaciones,*

- Configurar el Switch de contingencia, en caso de falla en el switch de Core.
- Contactar al proveedor de comunicaciones, en caso de falla en router de conexión con intendencias, falla en router ubicado en cada intendencia, falla en enlaces con ISP, o falla en enlace con intendencias regionales.
- Enrutar el tráfico por los demás switch que componen el stack, en caso de una falla de la fibra óptica de uno de ellos.
- Utilizar el switch de piso como contingencia ante falla de un switch de piso en un centro de cableado..

**¿Qué actividades paralelas se deben realizar, luego de activado el Centro de Cómputo Alterno?**

- Configurar el firewall de contingencia, en caso de falla del equipo principal.

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

*Si es un evento que afectó la infraestructura de servidores,*


- Configurar el servidor de contingencia en el BladeServer utilizando la plantilla predefinida, en caso de falla de alguno de los siguientes servidores: DOCSERVER, DOCUMENTSERVER, SQLSERVER, SUPERWEB, WEBLINUX, OLDWAS, APLSERVER, SBITACO31, Y SUPERCORREO.
- Configurar el servidor de contingencia en el BladeServer utilizando la plantilla predefinida, en caso de falla de alguno de los siguientes servidores: DSA\_Super y WAS.
- Activar el servidor de contingencia, anta falla del servidor SUPERDOMINIO.

*Si es un evento que afectó Infraestructura de Bases de datos, Almacenamiento y Respaldo*

- Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de la base de datos, y borrado o pérdida de datos.
- Utilizar los discos de contingencia ante una falla en la SAN IBM DS 4300
- Configurar el servidor de contingencia el servidor F80 como servidor de respaldo, en caso de falla del principal.

**¿Qué hacer en caso de que la falla afectó un equipo que no se encuentra en garantía, o mantenimiento correctivo?**

- k. El Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.**
- l. El Director de Informática y Desarrollo realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.**
- m. El Líder responsable de la plataforma afectada coordina la solución con el proveedor contratado.**

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

**n. El Director de Informática y Desarrollo comunica la solución del incidente a la entidad**

**o. El Director de Informática y Desarrollo, en conjunto con los profesionales especializados, definen la estrategia de retorno a la normalidad, , teniendo en cuenta:**

- Fecha del retorno a operación normal.
- Consideraciones especiales a aplicar en el proceso de retorno.
- Consideraciones especiales con respecto a la recuperación de la información y mantener la integridad de los datos, cuando aplique.
- Sincronización entre los centros de cómputo, cuando se operó en el Centro Alterno de Cómputo, si aplica.

**p. El Líder de Seguridad, en conjunto con los funcionarios que participaron en la atención del incidente, documentan el incidente e identifican oportunidades de mejora para fortalecer el DRP.**

**q. Se realiza el cierre del incidente, interrupción mayor o evento contingente, y se continúa con la ejecución del procedimiento de acciones preventivas y correctivas del SGSI.**


### **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.**

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

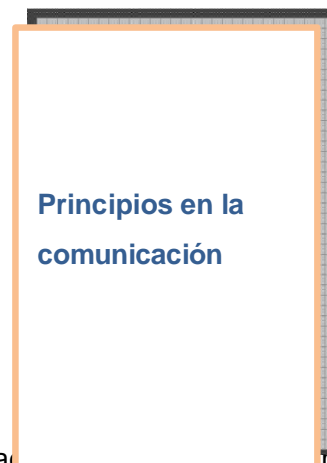
c. La Alta Dirección, a través de los voceros o funcionarios delegados, comunicará la crisis a nivel interno y externo, en caso de ser requerido, teniendo en cuenta los siguientes aspectos:




- ¿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)?

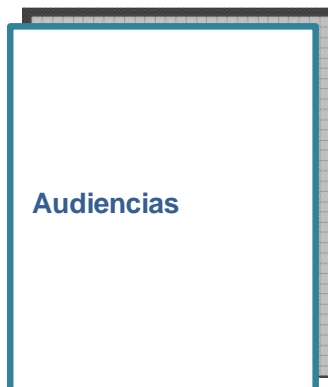
La comunicación de la crisis deberá considerar los siguientes principios:

- **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. No se debe ocultar información 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.



	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

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



- Sociedades inspeccionadas, vigiladas y/o controladas
- Usuarios externos de los productos y/o servicios de la entidad.
- Funcionarios
- Opinión Pública
- Gobierno y Autoridades
- Líderes de Opinión
- Contratistas y Proveedores

**d. La Alta Dirección, o los funcionarios designados por esta, deberá realizar monitoreo permanente de la crisis y tomar las decisiones que correspondan para continuar con la mitigación del mismo. Se debe tener en cuenta:**

- ¿Qué información circula en los medios de comunicación?
- ¿Qué información circula a nivel interno?
- ¿Qué impacto sobre la crisis tiene la información que está circulando en los medios?
- ¿Se requerirá realizar nuevos comunicados?

### **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:



	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

No	Actividad	Responsable	Frecuencia
1.	Actualización de los procedimientos de recuperación y contingencia de la plataforma tecnológica	Lideres 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 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 Infraestructura 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

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23


- 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.

### 3.9. RECURSOS MÍNIMOS REQUERIDOS


La infraestructura necesaria para soportar los procesos misionales de la entidad que serán recuperados en una contingencia es:

Cant.	Servidor	Marca	Procesadores	Memoria	Almacenamiento	Servicios y Software Instal
1	DSA_Super - Base de datos Informix	IBM Power6 550	4 Proc Quad 3,5 GHz, version Pw6	32 GB	<u>Interno:</u> 300 GB RAID 10. <u>Externo:</u> SAN 4TB	<ul style="list-style-type: none"> <li>- Unix AIX 5.3</li> <li>- Informix Dynamic Server versión 10.</li> <li>- BD Storm</li> <li>- BD SIGS</li> <li>- BD BE Sociedades</li> <li>- BD B Generales</li> <li>- BD Kactus</li> <li>- BD STONE</li> <li>- BD Inversión y Deuda Externa</li> </ul>
1	Docserver - Servidor de archivos del sistema de información documental	DELL Power Edge 6600	2 Proc 3.0 Ghz, Pentium Xeon	4 GB	<u>Interno:</u> Cuatro (4) discos de 36 GB SCSI Ultra 320 15K rpm <u>Externo:</u> SAN 600 GB	<ul style="list-style-type: none"> <li>- Windows 2003 Server Standard</li> <li>- Informix Connect,</li> <li>- HUMMINGBIRD DM y componente de radicación y flujo de procesos.</li> <li>- IBM Tivoli Client</li> </ul>
1	Documentserver - Servidor Base de datos SQL Server	HP DL 580 G3	4 Proc 3.0 Ghz, Pentium Xeon MP	4 GB	<u>Interno:</u> Dos (2) discos de 36 GB SCSI Ultra 320 15K rpm <u>Externo:</u> SAN 150 GB	<ul style="list-style-type: none"> <li>- Windows 2003 Server Standard</li> <li>- SQLServer 2000 Standard.</li> <li>- BD Baranda Virtual</li> <li>- BD SID</li> <li>- IBM Tivoli Client</li> </ul>
1	SQL SERVER - Base de datos SQL Server	HP Proliant ML370 G3	4 Proc 3.4 Ghz, Pentium Xeon	4 GB	<u>Interno:</u> Cuatro (4) discos de 36 GB SCSI Ultra 320 15K rpm. <u>Externo:</u> SAN 100 GB (4300 IBM)	<ul style="list-style-type: none"> <li>- Windows 2003 Server Standard</li> <li>- Microsoft SQL Server 2000 Standard,</li> <li>- BD Stone</li> </ul>
1	Superweb - Servidor de IIS del portal de la entidad	HP ML370 G4	2 Proc 3.2 Ghz x86-64 bits, Pentium Xeon DP	4 GB	<u>Interno:</u> Dos (2) discos de 72 GB SCSI Ultra 320	<ul style="list-style-type: none"> <li>- Windows 2003 Server Standard</li> <li>- Informix Dinamyc Server 9.4</li> </ul>

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR					Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO					
	PROCESO: GESTIÓN DE INFRAESTRUCTURA					Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP					Número de página 1 de 23
Cant.	Servidor	Marca	Procesadores	Memoria	Almacenamiento	Servicios y Software Instal
					15K rpm	<ul style="list-style-type: none"> <li>- Data Director for web 2.0</li> <li>- Internet information server</li> <li>- IBM Tivoli Client</li> </ul>
1	Superdominio – Servidor de	HP Proliant ML370 G3	4 Proc 3.4 Ghz, Pentium	4 GB	<u>Interno:</u> Cuatro (4) discos	<ul style="list-style-type: none"> <li>- Windows 2003</li> </ul>

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR		Fecha: 05 de Febrero de 2023			
	SISTEMA GESTIÓN INTEGRADO					
	PROCESO: GESTIÓN DE INFRAESTRUCTURA		Versión: 001			
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP		Número de página 1 de 23			

Cant.	Servidor	Marca	Procesadores	Memoria	Almacenamiento	Servicios y Software Instal
	controlador de dominio e impresión		Xeon		de 36 GB SCSI Ultra 320 15K rpm Externo: SAN - 130 GB	Server Standard - Jet Admin
1	Firewall - Servidor de seguridad de equipos corta-fuegos	Proventia MX5010	-	-	-	-

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

#### **4. ACTIVIDADES DE RECUPERACIÓN Y CONTINGENCIA**


A continuación se definen las guías o pasos a seguir para recuperar los componentes de la plataforma tecnológica:

##### **4.1. ¿Cómo configurar el switch de contingencia en caso de falla del switch core?**

- a. Desconectar de cada uno de los centros de cableado los cables de fibra de los switch 2,3, 4 y si hay otros en stack.
- b. Obtener la documentación de operación en contingencia del Switch de Core.
- c. Encendido de los switch de contingencia
- d. Desconexión de servidores y fibras No.1 de conexión de los centros de cableado del switch de core y conexión al switch de contingencia, de acuerdo a la documentación.
- e. Reinicio de servidores en este caso todos.
- f. Orden de mantenimiento correctivo del switch de core.
- g. Comunicación a los funcionarios y personas correspondientes sobre la operación en contingencia.
- h. Una vez corregida la falla del Switch de Core y cuando este se encuentre en operación normal.
- i. Obtener la documentación de retorno a la normalidad del Switch de Core.
- j. Programar la fecha de retorno y las consideraciones necesarias para garantizar la disponibilidad de las comunicaciones.
- k. Apagar los servidores y otros equipos con sus respectivos servicios.
- l. Conectar y prender el Switch de Core y verificar su funcionamiento.
- m. Conectar los cables de fibra de Switches 2,3,4 y otros del Stack en cada centro de cableado
- n. Volver a conectar los servidores y las fibras No. 1 de los centros de cableado al Core, de acuerdo a la documentación.
- o. Verificar su funcionalidad.
- p. Comunicar a los funcionarios y personas correspondientes del retorno a la operación normal y el agradecimiento por su comprensión y apoyo.

##### **4.2. Cómo utilizar el switch de contingencia ante una falla de un switch de piso en Centro de Cableado en la sede de Bogotá?**


- a. Ubicar el switch de contingencia en el centro de cableado correspondiente.
- b. Conectar el switch de contingencia en el Centro de Cableado

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

- c. Conectar con un patchcore un punto de un switch funcional por el frente y desconectar el cable de fibra del switch dañado.
- d. Verificar la conectividad con la operación de los lets.
- e. Desconectar el cable de stack de la parte posterior del Switch.
- f. Conectar todos los puntos del switch que está fallando al switch de contingencia.
- g. Verificar conectividad.
- h. Tramitar el arreglo o compra del switch defectuoso.
- i. Ubicar y configurar el switch nuevo o ajustado.
- j. Conectar el stack, y la fibra óptica.
- k. Mover los parch core del switch de contingencia al switch
- l. Verificar conectividad.
- m. Comunicar el restablecimiento del servicio en contingencia.
- n. Programar la fecha de retorno y las consideraciones necesarias para garantizar la disponibilidad de las comunicaciones
- o. Ubicar y conectar el nuevo switch de piso.
- p. Conectar el cable de stack de la parte posterior del switch.
- q. Verificar conectividad.
- r. Desconectar y conectar todos los puntos del switch de contingencia al switch.
- s. Comunicar del restablecimiento del servicio.

#### **4.3. Cómo utilizar el switch de contingencia ante una falla de un switch de la intendencia Regional?**

- a. Conectar el cable del Router del equipo de comunicaciones de Telecom.
- b. Verificar que el servicio de comunicaciones.
- c. Mover los patc core del switch dañado al de contingencia.
- d. Verificar los servicios de comunicaciones
- e. Retirar y Enviar el switch para el arreglo..
- f. Configurar el nuevo switch
- g. Tramitar el arreglo o compra del switch defectuoso
- h. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes
- i.

	INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR	Fecha: 05 de Febrero de 2023
	SISTEMA GESTIÓN INTEGRADO	
	PROCESO: GESTIÓN DE INFRAESTRUCTURA	Versión: 001
	GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP	Número de página 1 de 23

#### 4.4. ¿Cómo utilizar el switch de contingencia como contingencia ante una falla del switch del firewall?

- a. Obtener la documentación de operación del switch de contingencia para el switch de firewall
- b. Desconectar la salida de Internet.
- c. Ubicar y conectar el switch de contingencia.
- d. Verificar que este operativo el firewall
- e. Retirar el switch del firewall que falló y reemplazarlo por el switch de contingencia.
- f. Verificar conectividad hacia Internet
- g. Tramitar el arreglo o compra del switch defectuoso.
- h. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes

## 5. ANEXOS Y REGISTROS

## 6. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de cambios	Responsable
001	05-02-2023	05-02-2024	Creación del documento	Líder de Seguridad de la información

Elaboró : Profesional Contratista Dirección de Informática  
Fecha : 05-02-2023

Revisó: Líder de Seguridad de la Información  
Fecha : 05-02-2023

Aprobó: Líder de Seguridad de la Información  
Fecha : 05-02-2023