GUIA PLAN DE RECUPERACIÓN DE DESASTRES

INFORMACIÓN GENERAL

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.

RESPONSABLE

Jefe de Informática y Sistemas / Oficial de Seguridad de la información.

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	eSigna	24 horas ((1 día hábil)
	STORM - Contraloria Gral de la Nacion	24 horas ((1 día hábil)
	Acreditación Personal Operativo - APO	24 horas ((1 día hábil)
	Renova	24 horas ((1 día hábil)
	SIIF	24 horas ((1 día hábil)
	Orfeo	24 horas ((1 día hábil)
	SEVEN - Informacion Financiera	24 horas ((1 día hábil)
	Número de Registro Oficial - NRO	24 horas ((1 día hábil)
	Humano - Soporte Logico Nomina	24 horas ((1 día hábil)
	Pagina WEB	24 horas ((1 día hábil)
Mensajería	- Correo Electrónico	24 horas ((1 día hábil)
Comunicaciones	- Switch Core - Enlace con Internet - Enlaces MPLS	24 horas ((1 día hábil)
Servicios	- DNS	24 horas ((1 día hábil)
Infraestructura	- Sistema de Aire Acondicionado - UPS	24 horas ((1 día hábil)

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 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.

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.

RPO: Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

perder un proceso o servicio.

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.

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.

CONDICIONES GENERALES

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales de Inspección, Vigilancia y Control.

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 los administradores de la plataforma, se encuentran disponibles y no ha sido afectados por el desastre.
- El desastre no afectó simultáneamente el Centro de cómputo principal y el Sitio Alterno (Azure) donde residen las aplicaciones críticas.
- Se contará con un Centro de Alterno (Azure) y estará habilitado en caso de contingencia.
- 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.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

GUIA DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

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 por:

- **ATENTADO TERRORISTA**
- **INCENDIO**
- **INUNDACIÓN**
- **DAÑO SISTEMA AIRE ACONDICIONADO**
- **DAÑO EN SUMINISTRO ELÉCTRICO**

Infraestructura de Comunicaciones: No disponibilidad de los servicios de comunicaciones por fallas en:

- **SWITCH CORE**
- **FIBRAS OPTICAS DE CONEXIÓN**
- **ROUTER**
- **ENLACES DE COMUNICACIÓN CON ISP**
- **FIREWALL**

Infraestructura de Servidores: No disponibilidad de la infraestructura por fallas en los servidores identificados como críticos en el inventario actualizado de servidores.

Infraestructura de Bases de datos, Almacenamiento y Respaldo No disponibilidad de datos e información por:

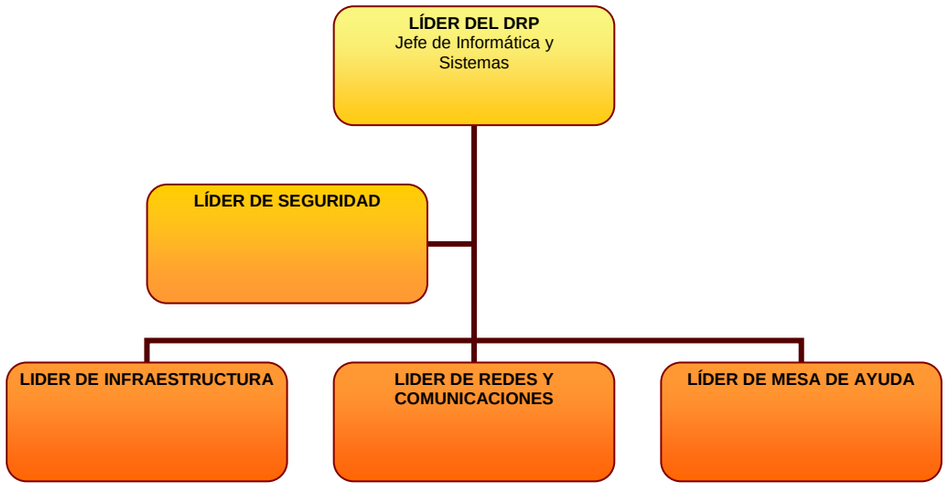
- **CORRUPCIÓN DE LA BASE DE DATOS**
- **BORRADO O PÉRDIDA DE DATOS**
- **FALLA TOTAL O PARCIAL DE LA SAN**
- **FALLA TOTAL O PARCIAL DE LA SAN**
- **FALLA EN SWITCH CONEXIÓN A LA SAN**
- **FALLA TOTAL O PARCIAL DEL SERVIDOR DE RESPALDO**

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

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

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	DESPÚES DEL EVENTO DE INTERRUPCIÓN
Líder del DRP	- Velar por la actualización del DRP y recursos requeridos. - Velar por la actualización, distribución y pruebas del DRP - Gestionar la consecución de los recursos para el DRP. - Comunicar a las personas que corresponda sobre la situación de contingencia.	- Evaluar y activar el DRP y las estrategias de recuperación y contingencia. - Comunicar al Secretario General sobre el estado de la operación de Contingencia. - Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio - Liderar la operación bajo contingencia. - Comunicar a la dirección el desastre, interrupción o evento contingente. - 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. - Informar al Secretario General sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
Lider de infraestructura, Lider de Redes y Comunicaciones, y Lider de Mesa de ayuda	- Comunicar necesidades de ajuste - Participar en la ejecución de las pruebas al DRP	- Evaluar el desastre, interrupción o evento contingente. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución. - Notificar al proveedor de Centro de Cómputo Alterno (Azure) (si aplica). - Comunicar el evento al Líder del DRP - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Ejecutar las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP. - Solicitar la corrección del componente afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las perso-	- Reportar los inconvenientes y oportunidades de mejora del DRP

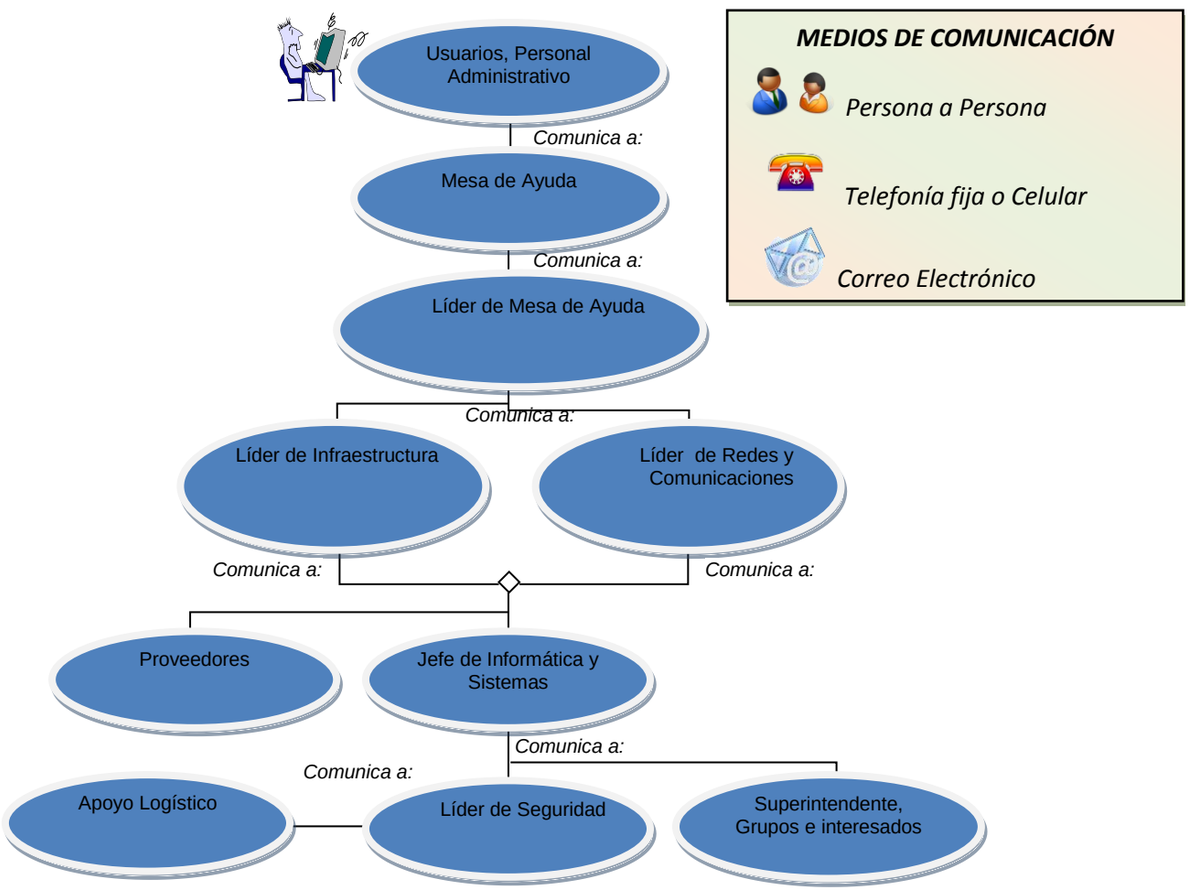
FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

ROL	ANTES DEL EVENTO INTERRUPCIÓN	DURANTE EL EVENTO INTERRUPCIÓN	DESPÚES DEL EVENTO DE INTERRUPCIÓN
		nas que lo requieran. - Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno (Azure), de los funcionarios que activarán la infraestructura. (Si aplica) - Mantener informado al Líder del DRP	
Líder de Seguridad	- Coordinar actividades de entrenamiento, documentación y actualización del DRP. - Coordinar las actividades de pruebas del DRP. - Identificar los recursos requeridos para la operación del DRP.	- Proveer soporte a los profesionales especializados. - Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno (Azure). - 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 - Logística de desplazamiento, si es requerido - Contacto de proveedores, si es requerido	- Reportar los inconvenientes y oportunidades de mejora del DRP

ÁRBOL DE LLAMADAS

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



FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Los datos de contacto para los funcionarios que ejercen estos roles se encuentra en la oficina de informática y sistemas.

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

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 el Procedimiento definido para Mantenimiento preventivo, correctivo y soporte técnico, y se continúa con la ejecución de esta guía 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.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

¿Quién evalúa la magnitud e impacto del incidente?

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 Jefe de Informática y Desarrollo para informar los resultados del diagnóstico.

¿Cuándo se debe activar el Centro de Cómputo Alterno?

El Jefe de Informática y Sistemas, define si se activa o no el Centro de Cómputo Alterno (Azure) , 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**.

e. En caso de que se active, se 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.

f. El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Centro de Cómputo Alterno (Azure), teniendo en cuenta:

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

El Líder de infraestructura, verifica la disponibilidad de la plataforma desde entro de Cómputo Alterno (Azure), teniendo en cuenta:

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

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

h. El Jefe de Informática y Sistemas, define si comunica o no el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.

i. 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 Swicth de contingencia, en caso de falla en el switch de Core.
- Contactar al proveedor de comunicaciones, en caso de falla en router

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

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

Si es un evento que afectó la infraestructura de servidores,

- Configurar el servidor de contingencia utilizando la plantilla predefinida, en caso de falla de alguno de los siguientes servidores: mencionados como críticos en el inventario.
- Activar el servidor de contingencia, anta falla del servidor de DOMINIO.

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
- Configurar el servidor de contingencia un servidor Alterno (Azure) 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?

j. El Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.

k. El Jefe de Informática y Sistemas realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.

l. El Líder responsable de la plataforma afectada coordina la solución con el proveedor contratado.

m. El Jefe de Informática y Sistemas comunica la solución del incidente a la entidad

n. El Jefe de Informática y Sistemas, 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 respectos 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 (Azure) de Cómputo, si aplica.

o. 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.

p. 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.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

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.

El Jefe 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.

a. 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.

b. 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:

Comunicación de la crisis

- ¿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:

Principios en la comunicación

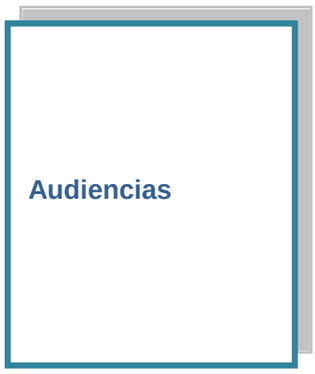
- **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos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

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

- **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:



- 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

c. **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?

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	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 (Azure) (Incluyendo replicación de data)	Lider de Infraestructura Lider de redes y comunicaciones	Permanente

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

No	Actividad	Responsable	Frecuencia
3.	Monitoreo de la infraestructura respaldada en el Centro de Cómputo Alterno (Azure) , 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 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

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.

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:
  - Jefe de Informática y Sistemas
  - Líder de Seguridad de la Información
  - Líder de Infraestructura

- Administrador de Redes y Comunicaciones
  - Se debe enviar una copia final COMPLETA del DRP a:
- Provedor de Centro Alterno (Azure).

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

RECURSOS MÍNIMOS REQUERIDOS

La infraestructura necesaria para soportar los procesos misionales de la entidad que serán recuperados en una contingencia es similar a la mencionada en el inventario actualizado de servidores.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

ACTIVIDADES DE RECUPERACIÓN Y CONTINGENCIA

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

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

a. Desconectar del centro de cableado los cables de fibra de los switch core 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 de conexión de los centros de del centro 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 otros Switches y otros del Stack en cada centro de cableado
n. Volver a conectar los servidores y las fibras 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.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Eusebio Cordero Orjuela
Revisado para firma por	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co