1. OBJETIVO

Diseñar la guía del plan de contingencia para el activo de información SWTCH CORE y documentar todas las actividades que se deben desarrollar para la correcta implementación en caso de que, por la materialización de riesgos, algún evento o incidente de seguridad llegará afectar la correcta operación y disponibilidad del SWTCH CORE.

2. ALCANCE

Actualmente, la Entidad cuenta con una robusta infraestructura de red, que contempla dos switches Huawei S7700 que conforman el CORE de la red y ofrece la conectividad a los equipos de comunicación como los switches de acceso que permiten la conectividad de los dispositivos de usuario como PCs, Portátiles, impresoras, cámaras de seguridad, controles de acceso, switches de acceso de la red inalámbrica, los enrutadores de los proveedores de servicio de conectividad WAN e Internet, la capad de acceso para los servidores legados, los switches TOR que conectan los servidores Enclosure e Hiperconvergencia a la red, el sistema de Telefonía IP, además de soportar la conectividad hacia servicios VPN Sitio a Sitio, conectividad a servicios en la nube como la gestión de la red inalámbrica, Office365 (correo electrónico corporativo y reuniones Teams, entre otros), infraestructura en la nube de AWS (Amazon Web Services) y Azure.

También ofrece conectividad a los Firewalls en alta disponibilidad, el cual realiza la labor de enrutamiento o capa 3 de la red. De esta forma el tráfico es controlado por los Firewalls aplicando políticas de seguridad a los diferentes segmentos de red o zonas de seguridad. Por ejemplo, la red de servidores está separada de la zona de usuarios y protegida por el Firewall.
En la siguiente figura se muestra un diagrama general de la infraestructura TI de la red y los servicios de conectividad de alta disponibilidad ofrecidos por los switches del CORE.

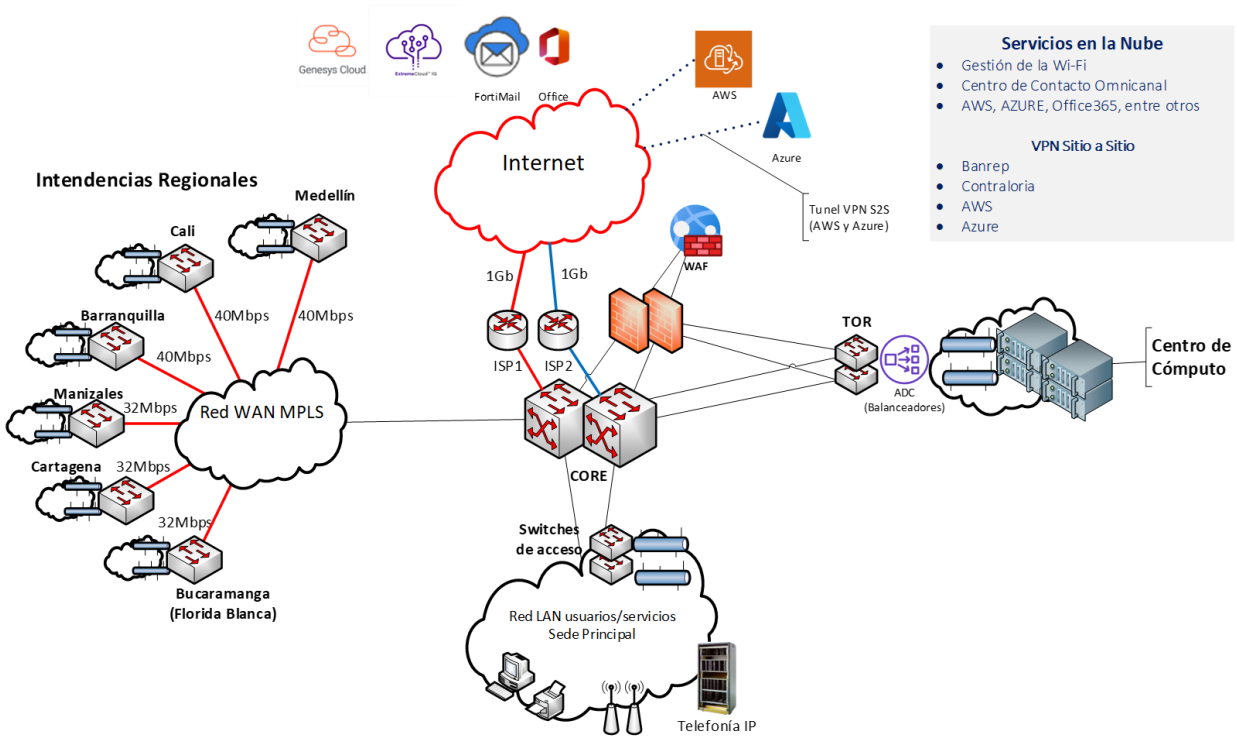


Figura 1 – Diagrama de Conectividad a los switches del CORE

Como se puede observar en la Figura 1, la conectividad a la red de todos los dispositivos de la Entidad, está configurada para ofrecer alta disponibilidad, a través de la doble conectividad a cada uno se los switches de marca Huawei, modelo S7700, que conforman el CORE de la red.

Los switches CORE están configurados para que ambos este de forma activa, de tal forma que cuando uno de ellos presente una falla, el segundo switch S7700 pueda respaldar de manera automática las conexiones a la red, tal como se muestra en la Figura 2.

Cabe señalar que el Firewall en alta disponibilidad provee provee la capa 3 de la red, es decir el enrutamiento de todo el tráfico entre las diferentes sub-redes permitiendo así, establecer reglas y controles de seguridad, tanto perimetral como a nivel de tráfico interno.

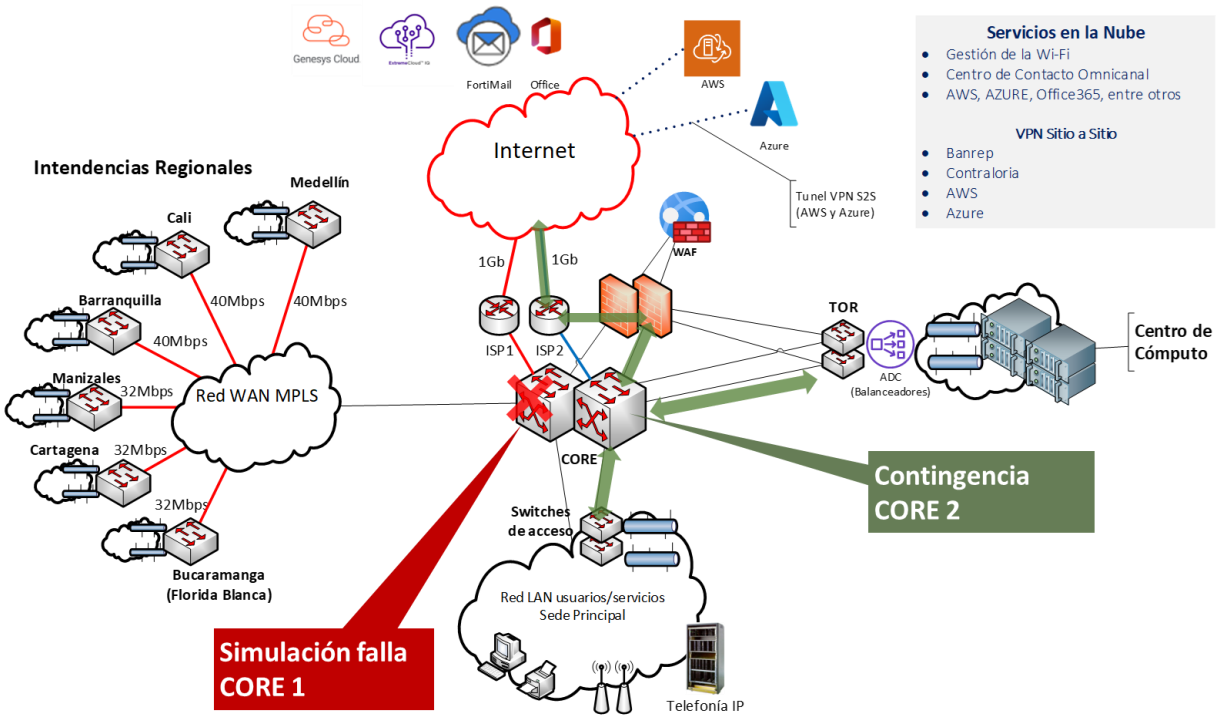


Figura 2 – Contingencia de la conectividad a la red a través del switch CORE 2

En la Figura 2, se presenta como ejemplo, el caso de una falla en el switch CORE1 y como las conexiones a la red son respaldadas por el segundo switch CORE2. De igual forma, si se presentase un daño en el CORE2, el switch CORE1 respaldará las conexiones de los dispositivos a la red.

También cabe señalar, que en caso de falla del CORE1, el Firewall1 se desconectaría de la red (falla lógica) pero sería respaldado por el Firewall 2 el cual esta conectado al CORE2. De esta forma, el enrutamiento de la red no se interrumpirá cuando falle cualquiera de los switches CORE.

La presente guía aplica para todos los administradores del Switch CORE y la Dirección de Tecnologías de la Información y las Comunicaciones.

3. RESPONSABLE

Grupo de Sistemas y Arquitectura Tecnológica.

4. DEFINICIONES

Activos tecnológicos: Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.

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.

CAP: Centro Alterno de Procesamiento. Hace referencia a las instalaciones físicas donde se procesará información en caso de una contingencia mayor en el centro de cómputo principal.

CAO: Centro Alterno de Operación. Hace referencia al sitio donde operará la entidad en caso de que exista un evento que impida la operación en las instalaciones normales.

CCP: Centro de Computo Principal. Hace referencia a las instalaciones físicas donde se procesa normalmente la información y donde se encuentra la infraestructura tecnológica en funcionamiento normal.

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.

Plataforma tecnológica crítica: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos, seguridad y enlaces de comunicación que son críticos para soportar los procesos y servicios 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 Objetive), 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 Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

SWITCH CORE: Los switches Core son un tipo de conmutador de alta capacidad que generalmente se coloca dentro de la red troncal o núcleo físico de una red. Sirven como puerta de acceso a una red de área amplia (WAN) o Internet; proporcionan el punto de acceso final para la red y permiten que varios módulos de agregación trabajen juntos. Debido a la importancia que tiene en las redes, los switches Core debe tener una capacidad de poder significativa para manejar eficientemente la carga que se le envía.
La función básica que realiza es la de trasferir datos entre los diferentes dispositivos de la red, a través del procesamiento de la información que está contenida en las cabeceras de la trama Ethernet. Dentro de una WAN pública, interconecta los switches de borde que se colocan en los bordes de las redes relacionadas, asimismo en una red de área local (LAN), los switches core interconectan los conmutadores de grupo de trabajo.

5. CONTENIDO

CONDICIONES GENERALES

El contenido está enfocado solo a la contingencia sobre el dispositivo de Switch CORE que soporta los servicios de conectividad y flujo de información sobre plataforma tecnológica de la superintendencia de Sociedades.

5.1. Supuestos:

La efectividad en la ejecución de este documento, ante la ocurrencia de un evento de interrupción mayor o un evento contingente que afecte el Switch CORE y el oportuno servicio de la conectividad de la plataforma tecnológica de la Superintendencia de sociedades depende de:

- Se dispone de la infraestructura de comunicación 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 la contingencia.

- Solo el funcionario responsable activará la contingencia.
- Se deben realizar pruebas de las estrategias y actividades al menos 1 vez al año.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- El sistema de conectividad siempre deberá estar en funcionamiento.

5.2. GUIA DEL PLAN DE CONTINGENCIA PARA EL SERVICIO DE CONECTIVIDAD.

5.2.1. ESCENARIOS DE CONTINGENCIAS

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

5.2.1.1. Infraestructura de Comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en:

- Switchs core
- Fibras ópticas de conexión con centros de cableado
- Switch de piso
- Enlaces de comunicación con ISP
- Falla en la conexión con Internet

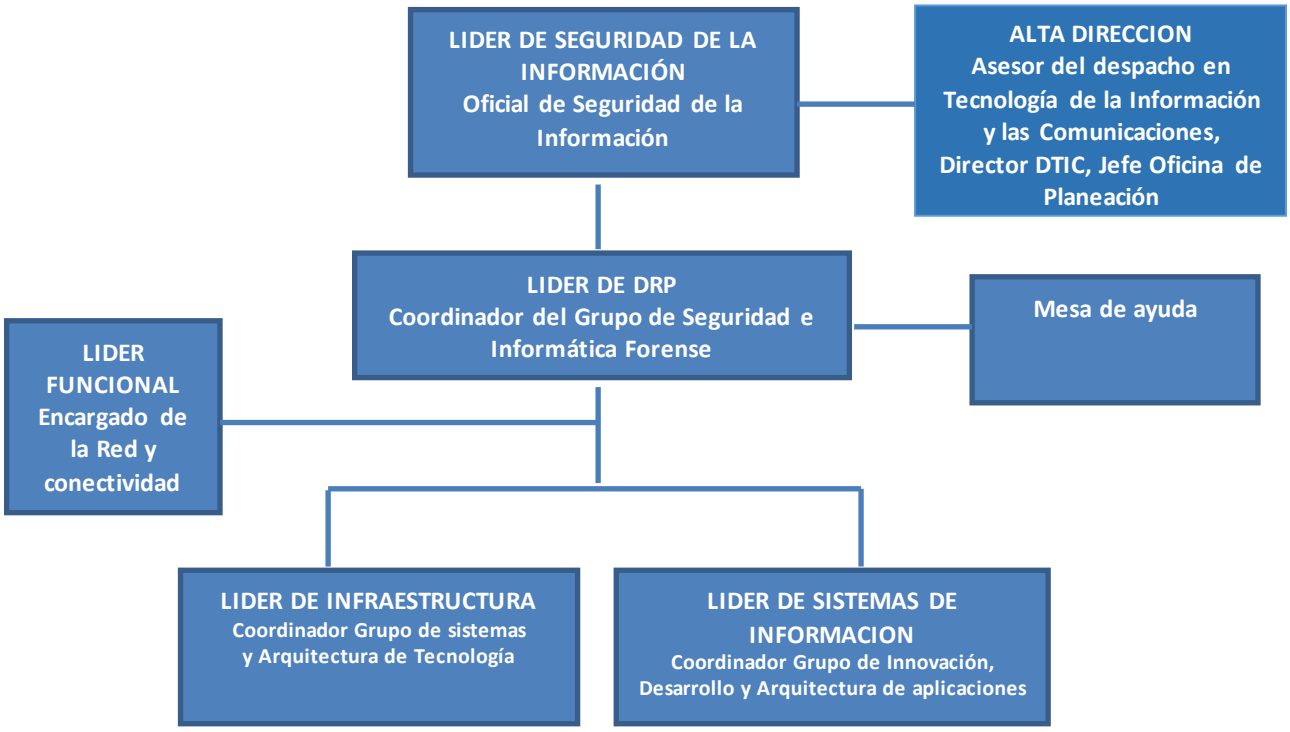
5.2.1.2. Servicios tecnológicos.

No disponibilidad del SWITCH CORE por:

- Bloqueo de usuarios
- Virus informáticos
- Fallas técnicas (sistema operativo, dispositivo)
- Daño en certificados digitales (tokens)

5.3. 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 de interrupción	Durante el evento de interrupción	Después del evento de interrupción
LIDER FUNCIONAL Encargado de la red y la conectividad	- Estar pendiente de las situaciones y eventos que puedan generar indisponibilidad del SWITCH CORE. - Apoyar el diseño del plan de contingencia para Switch CORE y dar Vo.Bo, - Realizar el Análisis de impacto de eventos de SWITCH CORE para determinar el RTO y RPO.	- Reportar a Líder de Infraestructura sobre la situación de indisponibilidad que se presenta. - Preparar los equipos de trabajo para actuar en contingencia. - Preparar la infraestructura de contingencia del Switch CORE. - Reportar a líder de infraestructura el retorno a la normalidad	- Confirmar que todos los servicios requeridos para el servicio del Switch CORE funcionan. - Comunicar al líder de Infraestructura Tecnológica sobre la recuperación de servicios de SWITCH CORE. - Definir mejoras al plan de

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
			contingencia y las lecciones aprendidas.
LIDER DEL DRP. Coordinador de Seguridad e Informática Forense	- 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. - Conocer a quien debe comunicar sobre la situación de contingencia.	- Evaluar y activar el DRP para el evento de contingencia que se presente. - Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. - Informar a mesa de ayuda sobre evento de contingencia y retorno a la normalidad. - Liderar la operación bajo contingencia. - Comunicar al secretario general el estado de contingencia y el avance de actividades de contingencia. - informar el retorno a la normalidad.	- Velar por la actualización del plan de continuidad o del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. - Definir mejoras al plan de contingencia y las lecciones aprendidas.
LÍDER DE INFRAESTUCTURA Coordinador Sistemas y Arquitectura de Tecnológica	- Asegurar el monitoreo de los sistemas y componentes de la plataforma tecnológica de la entidad. - Mantener la configuración técnica de la Infraestructura tecnológica y conectividad, componentes de antivirus, tokens,	- Participar en la evaluación del evento contingente. - Informar a líder de DRP sobre contingencia. - Velar por la ejecución de las actividades de contingencia y recuperación. - Comunicar a los proveedores relacionados con el evento sobre la activación del plan de contingencia del SWITCH CORE, si es necesario. - Mantener informado al	- Reportar los inconvenientes y oportunidades de mejora del plan de continuidad del SWITCH CORE. - Solicitar los cambios en el plan de continuidad del SWITCH CORE. - Participar en la

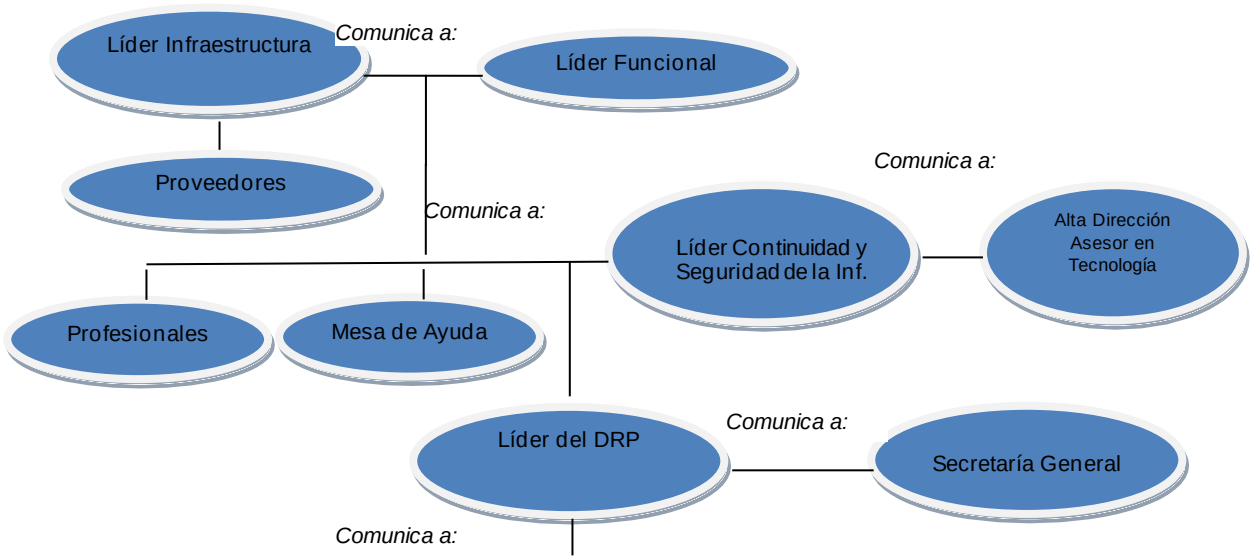
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	Navegadores y firmas digitales. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de los eventos que ocurran sobre el SWITCH CORE e informar los resultados. - Mantener soporte técnico y mantenimiento vigente para la infraestructura de comunicaciones.	Líder del DRP sobre el estado de contingencia y avance de las actividades. - Aprobar las configuraciones requeridas para activar componentes alternos.	revisión de la configuración final de la plataforma del SWITCH CORE contingente y principal
LÍDER DE SISTEMAS DE INFORMACIÓN. Coordinador Grupo de Innovación, Desarrollo y Arquitectura de aplicaciones	- Asegurar el monitoreo de los sistemas de información externos de la entidad. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de los eventos que ocurran sobre el SWITCH CORE e informar los resultados.	- Verificar disponibilidad de los sistemas de información en contingencia y notificar al personal requerido para atender el evento. - Realizar las pruebas de funcionamiento de los sistemas de información misionales y de apoyo en el retorno a la normalidad.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia del SWITCH CORE. - Solicitar los cambios en la guía de contingencia del SWITCH CORE. - Apoyar con las lecciones aprendidas a la contingencia.
LIDER SEGURIDAD DE LA INFORMACIÓN Oficial de Seguridad de la Información	- Participar en la creación del plan de contingencia del SWITCH CORE. - Participar en la definición de las	- Participar en el proceso de prueba del plan de continuidad. - Verificar ejecución del plan de contingencia. - Participar en la toma de	- Verificar si se actualizó la guía de continuidad o el DRP, de acuerdo con los inconvenientes y

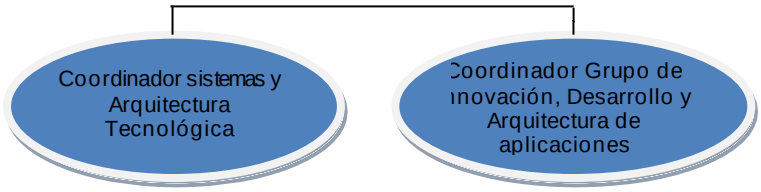
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	actividades a ejecutar en las pruebas de recuperación de eventos del SWITCH CORE.	decisiones que se den para ajustar el plan de contingencia del SWITCH CORE durante su ejecución. - Coordinar que todo el personal involucrado este participando. - Comunicar a la alta dirección sobre el evento de contingencia. - Verificar retorno a la normalidad. - Coordinar el registro del evento en el sistema de gestión de incidentes.	oportunidades de mejora encontrados. - Verificar que las lecciones aprendidas están siendo actualizadas en la herramienta definida. - Informar a la alta Dirección sobre el retorno a la normalidad.
LIDER FUNCIONAL Encargado de la Red y la conectividad Profesional Seguridad e Informática Forense	- Participar y definir las actividades del plan de contingencia del SWITCH CORE. - Participar en el Análisis de impacto de eventos de SWITCH CORE para determinar el RTO y RPO. - Contar con instructivo de revisión de Switch CORE y de sus servicios y/o solicitar soporte a proveedor. - Realizar respaldo de la configuración global del Switch CORE.	- Determinar el tipo de falla o evento que se presenta sobre el SWITCH CORE. - Reportar al líder de Infraestructura la situación de evento de indisponibilidad del SWITCH CORE. - Ejecutar las actividades del plan de contingencia del SWITCH CORE para recuperación de servicios. - Contactar al proveedor del SWITCH CORE en caso de ser necesario. - Reportar al líder de infraestructura la recuperación del evento de contingencia del SWITCH CORE.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia del SWITCH CORE. - Reportar mejoras al plan de pruebas. - Reportar al Líder de continuidad y Seguridad de la Información las lecciones aprendidas del evento.
Profesionales participantes	- Conocer el plan de continuidad a aplicar en caso de	- Realizar las actividades del plan de pruebas asignadas.	- Reportar las oportunidades de mejora al

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	contingencia - Conocer el plan de pruebas a ejecutar.	- Verificar funcionamiento de servicios impactados. - Informar a sus líderes sobre estado de las pruebas realizadas y su recuperación.	plan de continuidad del Switch CORE. - Reportar lecciones aprendidas.
MESA DE AYUDA	- Conocer el plan de contingencia del Switch CORE. - Mantener los canales de comunicación listos para recibir reporte de eventos	- Realizar el registro del evento de indisponibilidad del Switch CORE. - Realizar actividades de primer nivel e Informar a líder del DRP sobre evento de indisponibilidad - Realizar el cierre del evento cuando se reporte vuelta a la normalidad	- Reportar oportunidades de mejora del plan de continuidad del Switch CORE. - Reportar lecciones aprendidas del evento

5.4. ÁRBOL DE LLAMADAS

Cuando se presente un evento tecnológico o funcional sobre el SWITCH CORE, se debe seguir la siguiente cadena de llamadas:





Medios de comunicación: Correo electrónico, teléfono, celular, Persona a persona

Los datos de contacto para los funcionarios que ejercen estos roles se encuentran en los documentos de la Dirección de Informática y Desarrollo, ver Anexo 1.

5.5. ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL PLAN DE CONTINGENCIA

5.5.1. ¿Quién reporta un incidente, interrupción mayor o un evento contingente del SWITCH CORE?

El líder Funcional debe reportar todos los eventos que se presenten sobre el Switch CORE a la mesa de ayuda cuando se afecte alguno de los siguientes aspectos:

- Canales de comunicación.
- Switch CORE.
- Switches de Piso.
- Red WAN con regionales.
- MPLS
- Red LAN
- Plataforma de distribución F5.
- Conexión con regionales.
- Navegación Red Inalámbrica.
- Conexión con ambientes de trabajo (producción, desarrollo, pruebas).

.

Estos eventos pueden afectar la disponibilidad de los servicios tecnológicos a nivel general y dejar a los usuarios sin acceso a estos servicios. En cualquiera de los casos, debe escalarse a los funcionarios responsables.
Para el caso de un evento tecnológico del SWITCH CORE, el Líder Funcional, 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.

5.5.2. Análisis de Impacto.

De acuerdo con el esquema de alta disponibilidad y el análisis de impacto realizado junto con los funcionarios asignados por las coordinaciones y reflejado en el formato GTI-F-005 Analisis de impacto, se ha definido un tiempo de recuperación del servicio de:

RPO: 30 minutos
RTO: 30 minutos

En caso de evento que afecte al SWITCH CORE :

El lider del DRP (Director de Tecnología de la Información y las Comunicaciones), define si se activa el plan de contingencia teniendo en cuenta los siguientes aspectos:

- Si el evento afectó considerablemente los servicios tecnológicos.
- Si el evento afectó la red de comunicaciones e internet.
- Si la solución en sitio dura más del tiempo definido en el RTO y RPO.

5.6. 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.

5.6.1. Para el caso de eventos tecnológicos:

a. El líder del DRP 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 sus asesores. 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 malentendidos, 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 para considerar en la comunicación de la crisis pueden ser:

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

5.7. ACTIVIDADES DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA

Es responsabilidad del Líder de Continuidad y Seguridad de la información, tramitar la actualización de las nuevas versiones al plan de continuidad y planes de contingencia (DRP), y la comunicación de estas a todos los funcionarios involucrados en el mismo.

La actualización y mantenimiento al DRP se debe realizar:

- 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 recomienden.

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 de comunicaciones	LIDER FUNCIONAL Encargado de la Red y la conectividad	Cada vez que se realice un cambio a la infraestructura de producción (COMUNICACIONES) o se realice una prueba de contingencia cuyo resultado involucre cambios a la configuración de comunicaciones.
2.	Cambios en la configuración del SWITCH CORE o de la platraforma de seguridad perimetral.	LIDER FUNCIONAL Encargado de la Red y la conectividad	Permanente
3.	Integraciones a la plataforma tecnológica como procesamiento hibrido con plataformas en la nube.	Lider de Infraestructura Lider de redes y comunicaciones	Permanente

5.8. ACTIVIDADES DE PRUEBA

La programación y método para utilizar en la realización de pruebas a la continuidad se deben relacionar en el formato GTI-F-004 Plan, Diseño, Ejecución y Evaluación de pruebas. Estas pruebas deben incluir escenarios como los definidos en el pun 3.1 Escenarios de Contingencia, del presente documento, como:
Escenarios específicos a fallas tecnológicas:

- Infraestructura de comunicaciones.

5.9. DISTRIBUCIÓN DE LA GUIA: PLAN DE CONTINUIDAD DEL SWITCH CORE

El presente documento se debe publicar en el sistema de Gestión Integrado, proceso de Tecnología de la Información y las Comunicaciones, e informar a los siguientes funcionarios de manera primordial, como involucrados en el proceso.

- Director de Tecnología de la Información y las Comunicaciones
- Oficial de Seguridad de la Información.
- Coordinadores de la Dirección de Tecnología de la Información y las comunicaciones.
- Líderes de Redes y Comunicaciones

5.10. RECURSOS MÍNIMOS REQUERIDOS

La infraestructura necesaria para soportar la plataforma de seguridad perimetral es que exista alta disponibilidad para el Switch CORE.

5.10.1. Requisitos técnicos de hardware y software.

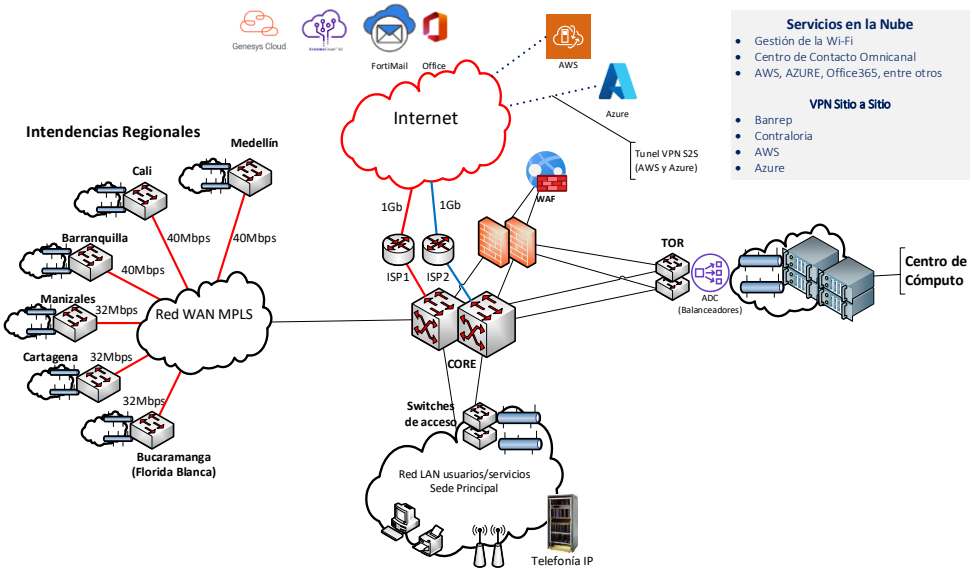
Los requisitos mínimos de Hardware con los que debe contar la plataforma de seguridad perimetral son:

SERIAL EQUIPO	PRODUCTO
2102113305P0D9000445	SWITCH 1 QUIDWAY S5700-ES0B00770600
2102113305P0D9000260	SWITCH 2 QUIDWAY S5700-ES0B00770600

5.10.2. Requisitos de Comunicación.

Los requisitos mínimos de comunicación con los que debe contar la plataforma de seguridad perimetral son:

Diagrama de Red LAN/WAN e Internet de Alto Nivel



5.11. ACTIVIDADES DE CONTINGENCIA

Para los diferentes escenarios de eventos sobre el SWITCH CORE se definen las guías o pasos a seguir para recuperar los servicios que presta este componente.

5.11.1. Actividades Funcionales y tecnológicas.

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Informar a líder funcional sobre falla técnica en Switch CORE y el impacto que se genera. 2. En caso de activación del plan de contingencia, dirigirse al Data Center y realizar pruebas de funcionamiento de dispositivos de Switch CORE principal y secundario. 3. Realizar transferencia de dispositivo principal a dispositivo de contingencia. 4. Realizar pruebas de funcionamiento de dispositivo de contingencia.	Líder de Seguridad Perimetral

		5. Informar sobre funcionamiento de dispositivo de contingencia. 6. Trabajar bajo modalidad de contingencia. 7. Solicitar pruebas de funcionamiento sobre sistemas y servicios reportados en numeral 1.3.	
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. 2. Comunicar al líder Seguridad de la Información sobre la situación que se presenta y confirmar si el evento supera el RTO. 3. Comunicar al Líder de DRP, la situación de contingencia presentada. 4. Informar a los equipos de trabajo para actuar en contingencia.	Coordinador de grupo de Seguridad e Informática Forense
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	1. Evaluar reporte recibido y activar el plan de contingencia para el evento que se presente. 2. Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. 3. Liderar la operación bajo contingencia. 4. Comunicar al Secretario General el estado de contingencia y el avance de actividades de contingencia.	Director de Tecnología de la Información y las Comunicaciones
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura Tecnológica	1. Verificar funcionamiento de canales de comunicación. 2. Verificar funcionamiento de switch CORE. 3. Verificar funcionamiento de switchs de Piso. 4. Verificar funcionamiento de red WAN con regionales. 5. Verificar funcionamiento de la plataforma de distribución F5. 6. Informar a líder de Seguridad Perimetral sobre estado de las	Líder Comunicaciones

		comunicaciones en periodo de contingencia.	
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura de Tecnología	1. Registrar reporte de evento presentado y escalar hacia el área encargada de solucionar problema. 2. Informar al líder funcional el número de tiquete asignado.	Coordinador de mesa de ayuda
Oficina Asesora de Planeación	Oficial de Seguridad de la Información	1. Verificar ejecución del plan de contingencia. 2. Participar en la toma de decisiones que se den para ajustar el plan contingencia durante su ejecución. 3. Informar a la alta dirección sobre evento presentado y su estado	Oficial de Seguridad de la Información
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	1. Realizar las pruebas de funcionamiento de los sistemas de información misionales y de apoyo. 2. Apoyar la ejecución de las guías de contingencia y recuperación que se estén probando. 3. Comunicar a los proveedores la activación del plan de contingencia del SWITCH CORE. 4. Revisar disponibilidad de los ambientes de desarrollo y pruebas, en caso de ser necesario. 5. Informar al Líder del DRP.	Líder de Sistemas de Información
Gestión de Tecnología de la Información y las Comunicaciones	Mesa de ayuda	1. Realizar el registro del evento de indisponibilidad del Switch CORE. 2. Realizar actividades de primer nivel e Informar a líder del DRP sobre evento de indisponibilidad 3. Realizar el cierre del evento cuando se reporte vuelta a la normalidad	Lider Mesa de ayuda

5.12. RETORNO A LA NORMALIDAD.

Una vez es superada la contingencia, se deben realizar actividades de retorno a la normalidad.

5.12.1. Actividades de retorno Funcional y Tecnológicas

Una vez se restablezca el funcionamiento del SWITCH CORE principal deben ejecutar las siguientes actividades:

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Informar sobre la transferencia de dispositivo de contingencia a dispositivo de principal. 2. Reportar a mesa de ayuda sobre el cierre del evento. 3. Comunicar al líder de Seguridad de la Información sobre la solución realizada. 4. Informar a los equipos de trabajo sobre la solución realizada	Coordinador de grupo de Seguridad e Informática Forense
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura Tecnológica	1. Verificar funcionamiento de canales de comunicación. 2. Verificar funcionamiento de switch CORE. 3. Verificar funcionamiento de switchs de Piso. 4. Verificar funcionamiento de red WAN con regionales. 5. Verificar funcionamiento de plataforma de distribución F5. 6. Informar a líder de infraestructura sobre funcionamiento con Switch CORE principal.	Líder Comunicaciones y conectividad
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura de Tecnología	1. Informar a líder del DRP. 2. Informar al líder funcional sobre el cierre del evento.	Sistemas y Arquitectura de Tecnología
Gestión de Tecnología de la Información y las	Oficial de Seguridad de la Información	1. Verificar si se debe ajustar el plan contingencia del SWITCH CORE . 2. Informar a la alta dirección	Oficial de Seguridad de la Información

Comunicaciones		sobre el cierre del evento.	
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	1. Verificar disponibilidad de los sistemas de información en ambiente de producción. 2. Informar al Líder del DRP sobre resultados de la verificación.	Líder de aplicaciones

5.12.2. Actividades de cierre del evento de contingencia.

Una vez se restablezca el servicio del SWITCH CORE, el líder del DRP debe ejecutar las siguientes actividades:

Actividad
a. El Líder del DRP, debe Informar a la alta dirección o a quien esta designe: • La fecha del retorno a operación normal. • Las consideraciones especiales para aplicar en el proceso de retorno. • Emitir informe de cierre del evento. b. El Líder de Seguridad o Continuidad del negocio, coordina en conjunto con los funcionarios que participaron en la atención del incidente, la documentación del incidente e identifican oportunidades de mejora para fortalecer la guía del plan de Continuidad, así como, las lecciones aprendidas.

6. REGISTROS

- Formato GTI-F-004 Plan, Diseño, Ejecución y Evaluación de pruebas.
- Formato GTI-F-005 Analisis de impacto.

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	25-10-2023	Creación del documento
002	01/04/2025	Actualización de Directorio Telefónico, cambio plantilla guía e imagen institucional

Elaboró	Revisó	Aprobó
Nombre: Cargo: Profesional de Grupo de Sistemas y Arquitectura de Tecnología Fecha: 13/02/2025	Nombre: Amanda Rocío Fernández Cargo: Coordinador Grupo de Sistemas y Arquitectura de Tecnología Fecha: 13/02/2025	Nombre: Nubia Xiomara Sepúlveda Cargo: director de Tecnología de la Información y las Comunicaciones Fecha: 01/04/2025

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No.	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director Tecnologías de la información y las comunicaciones	Héctor Jaime Rendón Osorio hrendon@supersociedades.gov.co	Director (E)	3000
2	Oficial de Seguridad de la Información	iontibon@supersociedades.gov.co	Oficial de Seguridad de la Información	
3	Coordinación Innovación, Desarrollo y Arquitectura de Aplicaciones	Marisol Castiblanco Calixto MarisolCC@supersociedades.gov.co	Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones	3301
4	Coordinación de Sistemas y Arquitectura de Tecnología	Amanda Rocio Fernández Rico amandaf@supersociedades.gov.co	Coordinador Grupo de Sistemas y Arquitectura de la Información.	3153
5	Grupo Seguridad e Informática Forense	Jeny Shirley Díaz González JenyD@supersociedades.gov.co	Coordinador de Seguridad e Informática Forense	4030
6	Grupo Sistemas y Arquitectura de Tecnología	Mesa de ayuda soporte@supersociedades.gov.co	Contratista Soporte técnico Grupo de Sistemas y Arquitectura de Tecnología	3020-3022 3024-3026