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 indisponibilidad, interrupción mayor o un evento contingente.

2. ALCANCE

Esta guía se enmarca en la protección del nivel de disponibilidad de los sistemas y plataformas tecnológicas descritas en el presente documento.

3. RESPONSABLE

Dirección de Tecnología de la Información y las Comunicaciones

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.

ERA: Sigla en inglés (Environment Risk Analisys), Análisis de Riesgos Ambientales en español, y hace referencia a un documento que relaciona los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.

Evento: Suceso imprevisto que puede ocurrir en un espacio y tiempo específico, generando impactos sobre los activos tecnológicos y activos del negocio.

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.

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.

5. CONTENIDO

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales de la Superintendencia de Sociedades basados en la alta disponibilidad.

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 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 evento afectó infraestructura localizada en el Centro de cómputo principal.
- Solo el funcionario responsable activará el DRP o los planes de contingencia.
- Se han realizado las pruebas de alta disponibilidad de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- Los funcionarios responsables de los planes de contingencia han participado en las pruebas.
- Se cuenta con planes de contingencia documentados
- La realización de respaldos de las bases de datos e información se realiza de acuerdo con los procedimientos y frecuencias establecidas.

5.2. GUIA DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

5.2.1. ESCENARIOS DE DESASTRE

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

5.2.1.1. Centro de Cómputo:

No disponibilidad de los servicios misionales por:

- Falla de uno o más componentes de la infraestructura tecnológica
- Daño sistema aire acondicionado
- Daño en suministro eléctrico

No se cuenta con las capacidades tecnológicas para eventos relacionados con:

- Destrucción total del Centro de Cómputo por eventos como:
- Atentado terrorista
- Incendio
- Inundación

5.2.1.2. Infraestructura de Comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en componentes como:

- Switchs core

- Fibras ópticas de conexión con centros de cableado
- Switch Red Borde – Red LAN
- Router proveedor de servicio ISP
- Router de la regional
- Access Point - Red WIFI
- Enlaces de comunicación con ISP
- Enlaces de comunicación con regionales ISP
- Switch de comunicación con regionales
- Plataforma de seguridad perimetral (Firewall, WAF, SandBox, NAC)
- VPN

5.2.1.3. Infraestructura de Servidores

No disponibilidad de la infraestructura por fallas en servidores como:

- Clúster de Hiperconvergencia
- Enclosure DELL
- Servidores DELL
- Clúster Openshift
- Plataforma de Virtualización Red Hat
- Plataforma de Virtualización Hyper – V
- Plataforma de Virtualización Acrópolis
- Servidores de Base de Datos
- Servidores virtuales de aplicaciones
- Servidores de Controlador de Dominio

5.2.1.4. Infraestructura de Bases de datos, Almacenamiento y Respaldo

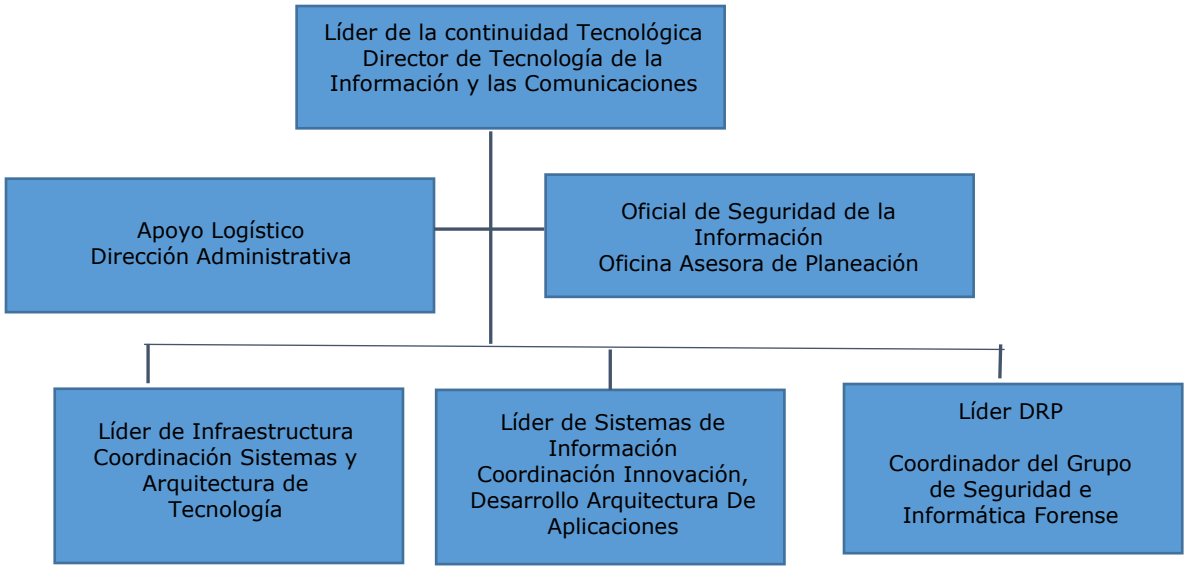
No disponibilidad de datos e información por:

- Corrupción de la base de datos
- Borrado o pérdida de datos
- Falla de parcial de los nodos de Clúster Hiperconvergente
- Falla total o parcial del almacenamiento SAN DELL
- Falla en switch conexión a la SAN
- Falla total o parcial de la plataforma de Backups

5.2.1.5. Infraestructura de Aplicaciones

No disponibilidad de la aplicación por:

- No conexión con otras aplicaciones
- Borrado o pérdida de datos
- Integridad de los datos



5.2.1.6. Servicios tecnológicos

No disponibilidad de la aplicación por:

- Bloqueo de puertos
- Fallas en servidores de aplicaciones
- Malware, Ramsomware
- Ataques de denegación de servicio
- Exfiltración de Datos
- Accesos no autorizados

5.2.2. ROLES Y RESPONSABILIDADES:

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

Las responsabilidades definidas para cada rol son:

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
LÍDER 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. - Comunicar a las personas que corresponda sobre la situación de contingencia.	- Evaluar y activar el DRP y las estrategias de recuperación y contingencia. - Informar el momento en que opera en contingencia y que puede suceder con la prestación del Servicio - Liderar la operación bajo contingencia. - 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. - Apoyar la construcción del informe de la Prueba de Contingencia en el GTI-FM-032 Informe Pruebas de Contingencia

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
Oficial de Seguridad de la Información	- Mantener actualizado el Plan de Continuidad el Negocio - Identificar los activos críticos de la Entidad - Identificar los Riesgos de Seguridad de la Información sobre los activos críticos - Participar en las pruebas de Contingencia tecnológica - Definir los requisitos de seguridad para las pruebas realizadas	- Participar activamente en el proceso, para garantizar la protección de la información. - Identificar los controles necesarios para mantener la seguridad de la información durante el evento. - Identificar mejoras al proceso - Verificar ejecución del plan de contingencia. - Participar en la toma de decisiones que se den para ajustar el plan de contingencia durante su ejecución. - Coordinar que todo el personal involucrado este participando. - Revisar el registro de la contingencia acorde con el procedimiento o guía de gestión de incidentes. - Garantizar que se cumplan los requisitos de seguridad identificados	- Validar el cumplimento de los requisitos de Seguridad definidos - Apoyar la construcción de las lecciones aprendidas - Identificar oportunidades de mejora - Gestionar el plan de mejoramiento y la implementación de nuevos controles - Verificar si se actualizó la guía de contingencia, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. - Apoyar la calificación de la prueba - Apoyar la construcción del informe de la Prueba de Contingencia

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
			en el GTI-FM-032 Informe Pruebas de Contingencia
Líder de infraestructura Tecnológica **Coordinador sistemas y Arquitectura de Tecnológica**	- Asegurar el monitoreo de los sistemas y componentes de la plataforma tecnológica de la entidad - Asegurar la entrega mensual de informe de incidentes, disponibilidad y cambios de la plataforma tecnológica de la entidad - Comunicar necesidades de ajuste al Plan DRP y alta disponibilidad - Coordinar la ejecución de las pruebas al DRP, alta disponibilidad con informe de resultados. - En caso de no contar con un contrato de	- Evaluar el desastre, interrupción o evento contingente. - Comunicar el evento al Líder del DRP - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Velar por la ejecución de las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP o alta disponibilidad. - Gestionar el alistamiento y disponibilidad de la plataforma o del sitio a utilizar como contingencia - Solicitar la corrección del componente afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las personas que lo requieran.	- Reportar los inconvenientes y oportunidades de mejora del DRP o plan de alta disponibilidad - Solicitar los cambios en el plan de recuperación - Apoyar la construcción del informe de la Prueba de Contingencia en el GTI-FM-032 Informe Pruebas de Contingencia -

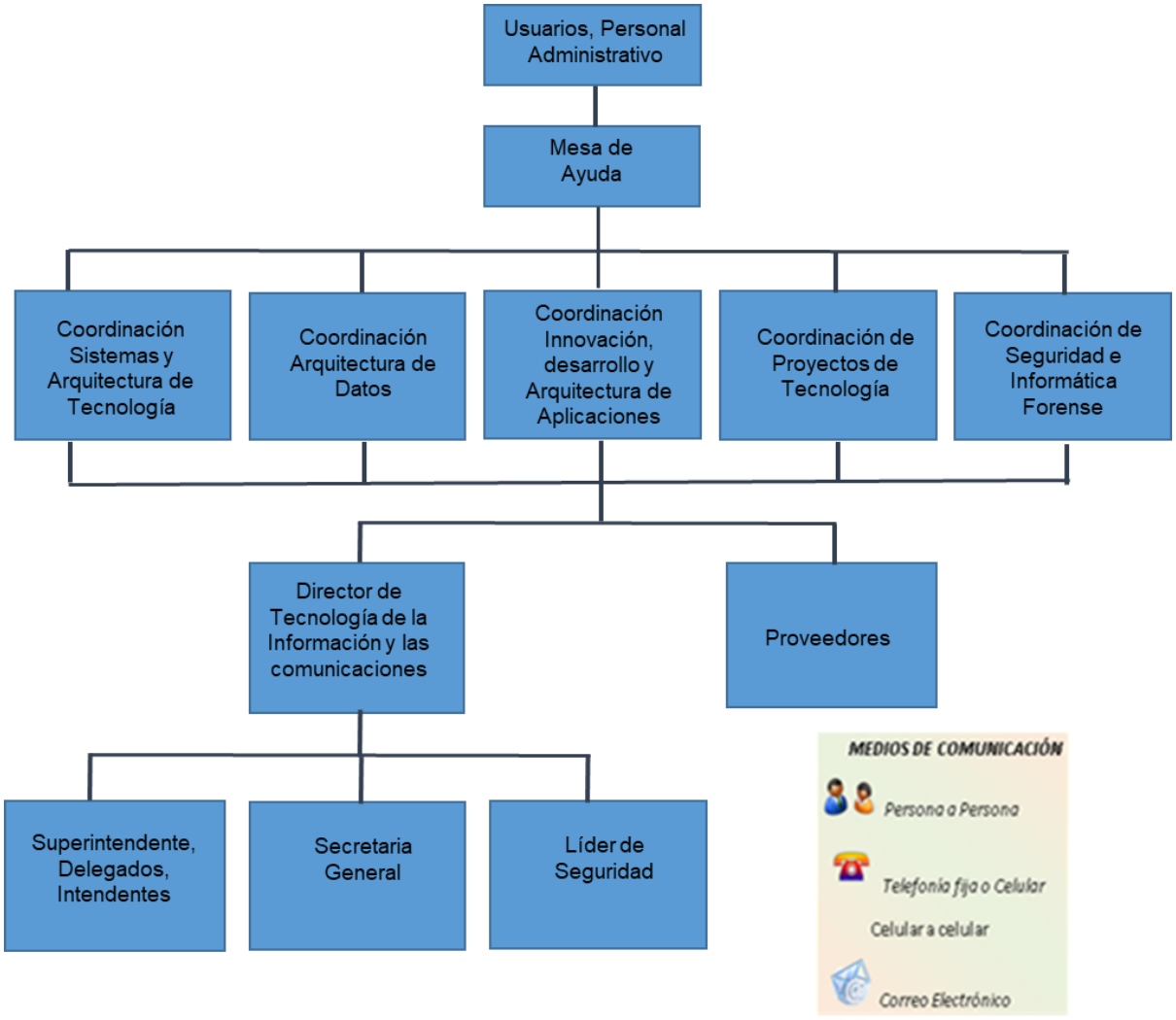
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	mantenimiento vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución.	- Mantener informado al Líder del DRP - Coordinar con los responsables el desplazamiento al sitio a utilizar como Centro de Cómputo, de los funcionarios que activarán la infraestructura. (Si aplica)	
Líder de Sistemas de Información. **Coordinador Grupo de Innovación, Desarrollo y Arquitectura de aplicaciones**	- Asegurar el monitoreo de los sistemas de información de la entidad - Asegurar la entrega mensual de informe de incidentes, disponibilidad y cambios en los sistemas de información de la entidad - Comunicar necesidades de ajuste al Plan DRP - Coordinar la ejecución de las pruebas al DRP y entregar a la dirección informe de resultados. - En caso de no contar con un contrato de mantenimiento	- Evaluar el desastre, interrupción o evento contingente. - Comunicar el evento al Líder del DRP - Verificar disponibilidad y notificar al personal requerido para atender el evento. - Velar por la ejecución de las guías de contingencia y recuperación. - Comunicar a los proveedores la activación del DRP. - Gestionar el alistamiento y disponibilidad de los ambientes de desarrollo y pruebas. - Solicitar la corrección del sistema afectado y realizar seguimiento de la solución. - Estar atentos para dar una correcta información a las personas que lo requieran.	- Reportar los inconvenientes y oportunidades de mejora del DRP - Solicitar los cambios en el plan de recuperación o plan de disponibilidad - Apoyar la construcción del informe de la Prueba de Contingencia en el GTI-FM-032 Informe Pruebas de Contingencia -

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	vigente se debe tener un listado de posibles proveedores de acciones correctivas de solución.	- Mantener informado al Líder del DRP	
Líder de Continuidad Tecnológica **Director de Tecnología de la Información y las Comunicaciones**	- 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.	- Verificar ejecución del plan de recuperación de desastres. - Participar en la toma de decisiones que se den pro-ajustes durante la ejecución del plan. - Coordinar que todo el personal involucrado este participando. - Comunicar al secretario general sobre el estado de la operación de Contingencia - Comunicar a la alta dirección el desastre, interrupción o evento contingente. -	- Verificar si se actualizó el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. - Verificar que las lecciones aprendidas están siendo actualizadas en la herramienta definida. - Apoyar la construcción del informe de la Prueba de Contingencia

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
			en el GTI-FM-032 Informe Pruebas de Contingencia
Apoyo Logístico **Dirección Administrativa**	- Participar en la ejecución de las pruebas de Aires acondicionados y fluido eléctrico.	En sitio 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

5.2.3. ÁRBOL DE LLAMADAS

Cuando se presente un desastre, interrupción o evento tecnológico, se debe seguir el siguiente plan de comunicación:



Los datos de contacto para los funcionarios que ejercen estos roles se encuentran en los documentos de la Dirección de Tecnología de la Información y Comunicaciones, Sin embargo, se cuenta con grupo en WhatsApp denominado DITC, para realizar la comunicación de los eventos.

5.3. ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DE LOS PLANES DE CONTINGENCIA TECNOLOGICA

5.3.1. ¿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 Infraestructura tecnológica. 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 cómputo y
- CUALQUIER otro evento que afecte o pueda afectar el centro de cómputo

c. El personal de tecnología encargado de monitoreo de plataforma (infraestructura tecnológica, infraestructura de comunicaciones, infraestructura de datos) deben reportar el incidente a Mesa de Ayuda o Líder de Infraestructura tecnológica.

- Se detecta caída de servicios,
- Se detecta mal funcionamiento de infraestructura critica (servidores, dispositivos de comunicaciones, bases de datos, almacenamiento)
- Se disparen alarmas ambientales

d. La mesa de ayuda debe atender el incidente de acuerdo con lo establecido en el Procedimiento GTI-PR-002- Mantenimiento preventivo, soporte técnico y mantenimiento correctivo de la infraestructura tecnológica, 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.

e. Se debe generar el correspondiente incidente de Seguridad de la información, de acuerdo con la guía GTI-GU-006_Gestión de Incidentes.

5.3.2. ¿Quién evalúa la magnitud e impacto del incidente?

a. 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 o plan de contingencia aplicables u otras soluciones potenciales
- Tiempo estimado de solución del incidente.

Finalmente, comunicarse con el director de Tecnología de la Información y las Comunicaciones para informar los resultados del diagnóstico.

5.3.3. ¿Cuándo se deben activar los planes de contingencia?

a. El Director de Tecnología de la Información y las Comunicaciones, define si se activan o no las contingencias tecnológicas de acuerdo con el proceso afectado teniendo en cuenta los siguientes aspectos:

- Si el evento afectó considerablemente el Centro de Cómputo Principal
- Si la solución dura más del tiempo definido en el **Anexo No. 1. RTO de Sistemas y plataformas tecnológicas que soportan los procesos misionales en la Superintendencia de Sociedades**

b. En caso de que se active, el líder de infraestructura debe comunicar la activación a los proveedores requeridos, teniendo en cuenta:

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

c. El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones hacia el sitio a utilizar como centro de cómputo.
- Detención de la replicación de datos.
- Verificación de la disponibilidad de información en el sitio a utilizar como centro de Cómputo.
- Activación servicio de controladores de dominio y sistema operativo en servidores
- Activación servicio de bases de datos y aplicaciones

d. El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el sitio a utilizar como centro de Cómputo, teniendo en cuenta:

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

f. El director de Tecnología de la Información y las Comunicaciones, comunica el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.

g. Se realiza la ejecución de los planes de contingencia, teniendo en cuenta la información consignada en los documentos:

- GTI -GU-007 Plan de contingencia para expediente digital
- GTI -GU-010 Plan de contingencia BPM
- GTI -GU-015 Plan de Contingencia Firewall
- GTI -GU-017 Plan de contingencia Switch Core
- GTI -GU-018 Guía plan de contingencia aplicaciones en la nube
- GTI-GU-024 Plan de contingencia Gestor Documental

3.4.4 ¿Qué actividades paralelas se deben realizar, luego de activado el plan de contingencia?

a. 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 el 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.
- 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 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
- Configurar el servidor de contingencia el servidor F80 como servidor de respaldo, en caso de falla del principal.

b. En caso de que la falla afecte un equipo que no se encuentra en garantía o mantenimiento correctivo, el Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.

c. El director de Tecnología de la Información y las Comunicaciones realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.

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

e. El director de Tecnología de la Información y las Comunicaciones comunica la solución del incidente a la entidad.

f. El director de Tecnología de la Información y las Comunicaciones, 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 por 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.

g. 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.

h. 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.

5.4. 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 Tecnología de la Información y las Comunicaciones comunica a la Alta Dirección, teniendo en cuenta los siguientes aspectos:

- Sistemas y servicios afectados
- Resultados del diagnóstico
- Acciones realizadas
- Tiempo estimado para normalización
- Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
- Decisiones que debe tomar la alta dirección.

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

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

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

La comunicación de la crisis deberá considerar los siguientes principios:

- **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar 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 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?

5.5. ACTIVIDADES DE MANTENIMIENTO

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

La actualización y mantenimiento al DRP y a los planes de contingencia tecnológico 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, a los planes de contingencia o sus procedimientos.
- Cuando hay cambios en el personal que operaría el DRP o el plan de contingencia.
- Cuando los resultados de auditorías así lo indican.
- Cuando el área de planeación haga entrega de un nuevo Análisis de Impacto de Negocio- BIA

Algunas actividades para mantener vigente el DRP y los planes de contingencia, son:

No	Actividad	Responsable	Frecuencia
1.	Actualización de las guias de contingencia de la plataforma tecnológica	Lideres de los procesos	Cada vez que se realice un cambio a la infraestructura de producción que amerite modificaciones sobre los planes definidos o se realice una prueba de

No	Actividad	Responsable	Frecuencia
			contingencia y su resultado sea una actualización al plan
2.	Pruebas de las copias de respaldo de la infraestructura respaldada	Lider de Infraestructura Lider de redes y comunicaciones	Permanente
3.	Monitoreo de la infraestructura respaldada en la nube, para verificar su disponibilidad en caso de que se presente un evento, dependiendo del criterio definido de recuperación (prendido o apagado)	Lider de Infraestructura	Permanente
4.	Ejecución de pruebas periódicas a los planes de contingencia para verificar el correcto funcionamiento de los sistemas que estan en alta disponibilidad	Profesionales Especializados	Cada semestre y sobre aplicativos específicos.
5.	Ejecución del procedimiento de respaldo de datos de la infraestructura tecnológica	Lider de Infraestructura	Permanente

5.6. ACTIVIDADES DE PRUEBA

Anualmente se debe realizar la programación de las pruebas a través del formato GTI-FM-004 Plan de Pruebas de Contingencia Tecnológica.

Los requisitos de seguridad que se evaluarán durante las pruebas serán solicitados por correo electrónico al Oficial de Seguridad de la información, quien de acuerdo con el escenario de la prueba definirá y evaluará el resultado de la prueba y el cumplimiento de los requisitos de seguridad los cuales serán consignados en el Formato GTI-FM-032 Informe de Pruebas de contingencia.

A continuación, se relacionan requisitos de seguridad junto con los que defina el Oficial de Seguridad de la información para garantizar la seguridad de la información en la prueba deben considerarse durante la ejecución del plan de contingencia:

Fase	Requisito	Evaluación
1. Requisitos Previos a las Pruebas		¿Se identificaron los módulos o funciones a probar?
	1.1. Definición del alcance	¿Se definieron los objetivos específicos de las pruebas?
		¿Se documentaron los tipos de prueba (unitarias, integración, etc.)?
	1.2 Validación del entorno de pruebas	¿El entorno de pruebas está completamente aislado del entorno de producción?
		¿Se replicó la configuración técnica del entorno real?
		¿Se documentó la arquitectura técnica del entorno?
		¿Se etiquetaron claramente los elementos del entorno como 'de pruebas'?
		¿Se validó la estabilidad operativa del entorno antes de las pruebas?
	1.3 Datos para las pruebas	¿Se utilizaron datos anonimizados, sintéticos o generados para pruebas?
		¿Los datos cubren casos positivos, negativos y extremos?
		¿Se eliminarán los datos de prueba al finalizar la actividad?
	1.4 Respaldos y contingencia	¿Se realizó y validó el backup completo del sistema y sus bases de datos?
		¿Existe un plan de restauración probado recientemente?
		¿Están definidos los procedimientos de reversión ante errores?
		¿Se asignaron responsables para la activación del plan de contingencia?
	1.5 Documentación del plan de pruebas	¿El plan de pruebas incluye trazabilidad con los requisitos?
		¿Se establecieron criterios de aceptación y de salida?

Fase	Requisito	Evaluación
		¿Se cuenta con un control de versiones del plan?
		¿Fue aprobado el plan por las áreas responsables?
	1.6 Evaluación de riesgos	¿Se identificaron y clasificaron los riesgos asociados a la prueba?
		¿Se definieron medidas de mitigación y protocolos de respuesta?
		¿Se asignaron responsables para el seguimiento de riesgos?
	1.7 Monitoreo y trazabilidad	¿Se activaron los logs y mecanismos de auditoría?
		¿Se implementaron alertas automáticas ante eventos críticos?
		¿Se documentan correlaciones entre actividades y resultados?
	1.8 Comunicación con partes interesadas	¿Se elaboró un plan de comunicaciones para las pruebas?
		¿Se notificó a todas las partes involucradas?
		¿Se documentan acuerdos y decisiones tomadas?
	1.9 Reporte y validación de resultados	¿Se usaron plantillas estandarizadas para los hallazgos?
		¿Se clasificaron los hallazgos por criticidad?
		¿Los resultados fueron validados por los responsables del sistema?
2. Requisitos Durante la Ejecución de las Pruebas	2.1 Supervisión en tiempo real	¿Está el equipo responsable disponible durante toda la prueba?
		¿Se realiza seguimiento a los indicadores establecidos?
	2.2 Registro de incidencias y hallazgos	¿Se documentan los hallazgos con fecha, descripción y evidencia?
		¿Se gestiona una bitácora con control de versiones?
	2.3 Comunicación permanente	¿Se mantienen canales de comunicación activos y seguros?
		¿Se registran decisiones y alertas durante la ejecución?

Fase	Requisito	Evaluación
	2.4 Cumplimiento del plan	¿Se siguen los escenarios definidos sin desviaciones?
		¿Se documentan y aprueban los cambios justificados?
	2.5 Protección de la información	¿Se aplican medidas de seguridad como cifrado y control de acceso?
		¿Se evita el uso de datos sensibles fuera del entorno controlado?
	2.6 Monitoreo y performance	¿Se recopilan métricas clave como tiempos de respuesta y uso de CPU?
		¿Se identifican y documentan comportamientos anómalos?
3. Requisitos Posteriores a la Ejecución de las Pruebas	3.1 Análisis de resultados	¿Se consolidaron los hallazgos en un informe estructurado?
		¿Se compararon los resultados con los criterios de aceptación?
	3.2 Evaluación de impacto	¿Se revisó si hubo afectaciones al entorno de pruebas?
		¿Se validó que no persistan efectos adversos?
	3.3 Gestión de hallazgos y acciones correctivas	¿Se asignaron responsables y plazos de corrección?
		¿Se documenta la trazabilidad del hallazgo hasta su cierre?
	3.4 Lecciones aprendidas y mejora continua	¿Se realizó una sesión de cierre para identificar aprendizajes?
		¿Se documentaron oportunidades de mejora institucional?
	3.5 Reversión de configuraciones temporales	¿Se eliminaron accesos, datos y configuraciones temporales?
		¿Se dejó evidencia del restablecimiento del entorno?
	3.6 Comunicación y cierre	¿Se comunicó formalmente el cierre de la fase de pruebas?
		¿Se obtuvo la validación de los resultados por los responsables?

5.7. DISTRIBUCIÓN DE LA GUIA: PLAN DE RECUPERACIÓN ANTE DESASTRES

Se debe contar con acceso al Documento DRP a:

- Director de Tecnología de la Información y las Comunicaciones
- Líder de Seguridad de la Información
- Líder de Infraestructura
- Administrador de Redes y Comunicaciones
- Proveedor de Centro de custódia.

6. ACTIVIDADES DE RECUPERACIÓN Y CONTINGENCIA

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

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

a. Activar el GTI -GU-017 Plan de Contingencia Switch Core, Esta ddocumentación debe estar actualizada.

b. Verificación la recuperación de los servicios de red por parte del switch activo. Acondicionar cableado de servicio de voz, videoconferencia y activar puerto de contingencia para la gestión de la red WiFi.

c. Iniciar proceso de aplicación de garantía y soporte sobre switch afectado.

d. Una vez corregida la falla del Switch de Core principal

- De ser necesario actualizar la documentación de mapa de conexión de dispositivos al CORE.
- Reconectar el Switch afectado y de ser necesario reconectar servicio de voz, videoconferencia y activar puerto de contingencia para la gestión de la red WiFi.
- Conectar cables según mapa de conectividad de dispositivos al CORE.
- Prender el Switch de Core.

e. Verificar su funcionalidad y todos los servicios.

f. Comunicar a los funcionarios y personas correspondientes del retorno a la operación normal.

6.2. 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
c. Conectar con un patchcore un punto de un switch funcional y desconectar el cable de fibra del switch dañado.
d. Verificar la conectividad con la operación de los leds.
e. Desconectar el cable de stack del Switch.
f. Conectar todos los puntos del switch que está fallando al switch de contingencia.
g. Verificar conectividad.
h. Tramitar soporte o garantía 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 afectado
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 del switch.
q. Verificar conectividad.
r. Desconectar y conectar todos los puntos del switch de contingencia al switch.
s. Comunicar del restablecimiento del servicio.

6.3. 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 del ISP.
b. Verificar el servicio de comunicaciones.
c. Mover los patch core del switch dañado al de contingencia.
d. Verificar los servicios de comunicaciones
e. Retirar y Enviar el switch para soporte y garantía.
f. Configurar el nuevo switch

g. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes

6.4. ¿Cómo utilizar el firewall contingente como contingencia ante una falla del firewall principal?

a. Activar el GTI -GU-015 Plan de Contingencia Firewall, Esta documentación debe estar actualizada.
b. Desconectar la salida de Internet.
c. Desconectar el HA del FW, para dejar operativo el equipo secundario
d. Verificar conectividad hacia Internet
e. Tramitar el arreglo o compra del equipo defectuoso.
f. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes

6.5. ¿Cómo utilizar el WAF de contingente como contingencia ante una falla del del WAF principal?

g. Activar el GTI -GU-015 Plan de Contingencia Firewall, esta documentación debe estar actualizada.
h. Desconectar del FW principal.
i. Desconectar el HA del WAF, para dejar operativo el equipo secundario
j. Verificar conectividad del equipo
k. Tramitar el arreglo o compra del equipo defectuoso.
l. Realizar el retorno a la operación normal de acuerdo con las recomendaciones correspondientes.

6.6. ¿Cómo reportar y atender clientes externos ante fallas del portal institucional.?

Sin que sea un evento de desastre, los servicios expuestos hacia los clientes externos son de gran importancia para la Supersociedades. Por eso se deben atender de manera especial cuando existan indisponibilidades del servicio. Para esto existen las siguientes instancias y canales de atención al ciudadano:

Línea de atención al ciudadano:

Es el medio de comunicación externo con el cual un ciudadano puede reportar un hecho irregular o deficiente funcionamiento de enlaces del Portal WEB, o sugerencias de mejoras de los servicios expuestos de la Superintendencia de Sociedades. Se encuentra en la parte inferior izquierda de la página web.

Dirección: Av. El Dorado No. 51-80 Bogotá, D.C.
Código Postal: 111321
Horario de Atención: Lunes a Viernes de 8:00 am a 5:00 pm
Teléfono Conmutador: +57(601) 220 10 00
Correo Institucional: webmaster@supersociedades.gov.co
Correo de notificaciones judiciales: notificacionesjudiciales@supersociedades.gov.co

Modulo de Servicios al Ciudadano.

En el menu de acceso que aparece en el portal WEB, se encuenta al lado derecho, la opción de Servicios al Ciudadano, donde se presentan a los diferentes modulos que puede acceder. Uno de ellos es "**Atención y servicios a la ciudadanía** ", que genera la presentación grafica de los servicios a los cuales puede acceder, incluidos los canales de atención. Otro de ellos el "**Modulo de PQRS**".

Al dar clik sobre la opcion de **Atención y servicios a la ciudadanía ,** aparecen de manera grafica los canales de atención e información adicional que puede ser de utilidad al ciudadano.

Los canales de atención son:

- **Modulo de PQRS.** Formulario donde los ciudadanos pueden informarnos, en cumplimiento de su deber de solidaridad, la existencia de hechos irregulares o deficiente funcionamiento de enlaces del Portal WEB, o sugerencias de mejoras de los servicios expuestos de la Superintendencia de Sociedades.
- **Chat.** Chat de Orientación General. Formulario que permite la comunicación en linea de los ciudadanos con un Contac Center para realizar peticiones, informar fallas, sugerencias y por el cual recibiran instrucciones inmediatas para solucionarlos o en caso contrario realizar escalamiento hacia el área correspondiente.
- **Buzon de Contáctenos.** Opción que permite la conexión de los diferentes servicios de correo electronico que puedan tener los ciudadanos para envio de sus solicitudes, sugerencias, reportes de fallas y cualquier petición que deseen realizar.

7. REGISTROS

- Herramienta de gestión de incidentes.
- Formato GTI-FM-004 Plan de pruebas
- Formato GTI-FM-032 Informe de pruebas de Contingencia
- GTI -GU-007 Plan de contingencia para expediente digital
- GTI -GU010 Plan de contingencia BPM
- GTI -GU-015 Plan de Contingencia Firewall
- GTI -GU-017 Plan de Contingencia Switch Core
- GTI -GU-018 Plan de contingencia aplicaciones en la nube
- GTI -GU-024 Plan de Contingencia Gestor Documental

8. *ANEXOS*

- Anexo Tablas y Directorio.

9. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	24-02-2014	Creación del documento
002	19-02-2018	Actualización documento. Se actualizó RTO por aplicación incluyendo todas las aplicaciones, se incluye la infraestructura por aplicativos. Se definen nuevos escenarios de desastre. Se actualizó el árbol de roles y responsabilidades. Se incluye lista de funcionarios involucrados en el DRP y sus datos de contacto. Se mejoran actividades y se incluyen las de pruebas. Se revisaron y actualizaron actividades de recuperación y contingencia.
003	26-02-2018	Inclusión de reporte y atención a clientes externos, en caso de falla del portal. Inclusión de campos de correo electrónico y extensión y funcionarios de otras áreas en el Anexo 2.
004	12/07/2018	Se modificaron las actividades del numeral 4.1 ¿Cómo configurar el switch de contingencia en caso de falla del switch core? Se incluyó en la matriz de infraestructura necesaria en el numeral 3.9 RECURSOS MÍNIMOS REQUERIDOS, los dispositivos de comunicaciones involucrados.

005	27/09/2019	Se actualiza anexo de Directorio Telefónico por cambios en la dirección de Informática y Desarrollo. Se actualiza numeral 4.1 ¿Cómo configurar el switch de contingencia en caso de falla del switch core?, ya que se implementa alta disponibilidad en el dispositivo
006	14/08/2020	Se actualiza anexo de Directorio Telefónico por cambios en el líder de Seguridad de la información y Dirección de Informática y Desarrollo, y se anexan funcionarios de Arquitectura de datos. Se elimina el anexo de infraestructura y se cambia por el link del catálogo de aplicaciones (por plataforma), publicada en el SharePoint y la cual se encuentra actualizada.
007	28/12/2020	Se actualiza anexo de Directorio Telefónico eliminando datos personales de los funcionarios (Número Celular). Se integran los controles de seguridad de la información a desarrollar y probar durante una contingencia.
008	23/12/2021	Se adecua a los nombres de los grupos de tecnología actuales. Se cambia lo correspondiente al centro de cómputo alterno por sitio a utilizar como centro de cómputo. Se actualiza el anexo de Directorio Telefónico por cambios en estructura funcional y nuevos miembros de equipos. Se agrupan los anexos 1 y 2 en Anexo Plataformas y Directorio
009	30/12/2022	Se elimina del anexo 2. Directorio Telefónico el nombre del funcionario y correo. Se incluye la sugerencia de crear un grupo de chat ya sea por TEAMS o por WhatsApp. Se adecua el nombre del documento con el de la caracterización
010	28/04/2025	Se actualiza alcance y actividades, se modifica la plantilla de acuerdo con la nueva imagen institucional
011	11/06/2025	Se incluye la infraestructura de los Sistemas de Información, se actualizan requisitos de seguridad para las pruebas se incluye formato de informe de pruebas de contingencia.
012	06/05/2026	Se actualizan los planes de contingencia, se retira anexo de infraestructura

Elaboró	Revisó	Aprobó

Nombre: Jeny Díaz Cargo: Coordinadora de Grupo de Seguridad e informática Forense Fecha: 20/04/2026	Nombre: Diego Franco Cargo: Coordinador Grupo de Sistemas y Arquitectura de Tecnología – Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones Fecha:22/04/2026	Nombre: Ricardo Rios Rosales Cargo: director de Tecnología de la información y las comunicaciones Fecha:06/05/2026

Anexos No. 1. RTO de Sistemas y plataformas tecnológicas que soportan los procesos misionales en la Superintendencia de Sociedades

Descripción	RTO - HORAS	Tiempo de interrupción tolerable (RTO)
PORTAL WEB	**12**	**12 horas ((1/2 día hábil)**
SIGS	24	24 horas ((1 día hábil)
Sistema de Información Documental (Gedess)	24	24 horas ((1 día hábil)
Kactus	24	24 horas ((1 día hábil)
Sistema General de Sociedades (SGS - Auxiliares de la justicia)	48	48 horas ((2 días hábiles)
Correo Masivo	48	48 horas ((2 días hábiles)
Baranda Virtual	48	48 horas ((2 días hábiles)
Estado de Cuenta y Contribución - Pago PSE	48	48 horas ((2 días hábiles)
SISTEMA INTEGRADO DE REPORTES FINANCIEROS (SIRFIN)	48	48 horas ((2 días hábiles)
Firma Digital	48	48 horas ((2 días hábiles)
Genesys Cloud (PureCloud)	72	72 horas (3 días hábiles)

Descripción	RTO - HORAS	Tiempo de interrupción tolerable (RTO)
Registro de usuarios	72	72 horas (3 días hábiles)
Consulta General Sociedades	72	72 horas (3 días hábiles)
Módulo de Insolvencia	72	72 horas (3 días hábiles)
Tesauros	72	72 horas (3 días hábiles)
Sistema integrado de Información societaria (SIIS)	72	72 horas (3 días hábiles)
Alertas tempranas	72	72 horas (3 días hábiles)
Aplicación Movil Modulo Insolvencia (SingApp)	72	72 horas (3 días hábiles)
Sistema de Administración Integral del Riesgo (SAIR)	72	72 horas (3 días hábiles)
Sistema para la promoción de empresas (Rueda de Negocio)	72	72 horas (3 días hábiles)
Digiturno	72	72 horas (3 días hábiles)
Sistema Integrado de Información Financiera - SIIF Nación, http://www.minhacienda.gov.co/HomeMinhacienda/SIIF	72	72 horas (3 días hábiles)
Procesos Judiciales (Delegaturas)	72	72 horas (3 días hábiles)
Reorganización Empresarial (BPM)	72	72 horas (3 días hábiles)
Liquidación Judicial por Insolvencia (BPM)	72	72 horas (3 días hábiles)
Intervenidas (BPM)	72	72 horas (3 días hábiles)
Conciliar (BPM)	72	72 horas (3 días hábiles)

Descripción	RTO - HORAS	Tiempo de interrupción tolerable (RTO)
Instalación de tribunales de arbitraje (BPM)	72	72 horas (3 días hábiles)
Correspondencia (BPM)	72	72 horas (3 días hábiles)
Sofia - Inventarios	120	120 horas (1 semana hábil)
Sistema de Administración de Biblioteca - Documanager	120	120 horas (1 semana hábil)
Ventana de Enseñanza Empresarial (MOODLE) intranet/extranet ventana empresarial	120	120 horas (1 semana hábil)
correo electrónico certificado (Rmail)	120	120 horas (1 semana hábil)
muestraSociedades	120	120 horas (1 semana hábil)
Expediente Digital	120	120 horas (1 semana hábil)
Documentos adicionales	120	120 horas (1 semana hábil)
Régimen cambiario	120	120 horas (1 semana hábil)
Intranet	120	120 horas (1 semana hábil)
Control muestra de sociedades (Muestra de sociedades)	120	120 horas (1 semana hábil)
SistemaPQRSEar	120	120 horas (1 semana hábil)
VisualizacionEstados	120	120 horas (1 semana hábil)
Calendario Eventos	120	120 horas (1 semana hábil)
STORM	120	120 horas (1 semana hábil)
Certificaciones en Línea	120	120 horas (1 semana hábil)

Descripción	RTO - HORAS	Tiempo de interrupción tolerable (RTO)
SPSS	120	120 horas (1 semana hábil)
STONE	120	120 horas (1 semana hábil)
Sistema de Gestión de Riesgos y Auditorias -ITS	120	120 horas (1 semana hábil)
Archivos Históricos (Gestion Documental)	120	120 horas (1 semana hábil)
Radicador de salida masivo (Gestion Documental)	120	120 horas (1 semana hábil)
Radicador de salida masivo Coactivo (Gestion Documental- Grupo Coactivo)	120	120 horas (1 semana hábil)
Radicación y Reparto (Gestión Documental 4-72)	120	120 horas (1 semana hábil)
consulta Personas Naturales y/o Jurídicas	120	120 horas (1 semana hábil)

No.	Cargo	Rol	Extensión
1	Director Tecnología de la Información y las Comunicaciones	Líder de Continuidad Tecnológica	3000
2	Jefe Oficina Asesora de Planeación	Líder estratégico	2079
3	Coordinador grupo Administrativo	Apoyo logístico	4074
4	Coordinación Innovación, Desarrollo y Arquitectura de Aplicaciones	Líder de sistemas de información	3301
5	Coordinación Proyectos de Tecnología	Coordinador	3010
6	Coordinación de Sistemas y Arquitectura de Tecnología	Líder de infraestructura	3013
7	Coordinación de Seguridad e Informática Forense	Coordinador	4030
8	Coordinación de la Coordinación de Arquitectura de Datos	Coordinador	4148
9	Funcionario de la Coordinación de Arquitectura de Datos	Funcionario	3011
10	Funcionario de Coordinación de Arquitectura de Datos	Funcionario	4065
11	Funcionario de la Coordinación Proyectos de Tecnología	Funcionario	1006
12	Funcionario de la Coordinación de Seguridad e Informática Forense	Funcionario	3226
13	Funcionario de la Coordinación de Seguridad e Informática Forense	Funcionario	3098
14	Funcionario de la Coordinación de Seguridad e Informática Forense	Funcionario	4030
15	Funcionario del Grupo de Innovación, Desarrollo y Arquitectura Aplicaciones	Funcionaria	3092
16	Funcionario del Grupo de Proyectos de Tecnología	Funcionario	3007
17	Funcionario del Grupo Sistemas y Arquitectura de Tecnología	Funcionario	3009
18	Funcionario del Grupo Sistemas y Arquitectura de Tecnología	Funcionario	3037