GUIA PLAN DE CONTINGENCIA PARA EXPEDIENTE DIGITAL

1. OBJETIVO

Definir el conjunto de actividades, roles y responsabilidades que permitan activar el proceso de contingencia del Sistema Expediente Digital (ED), en caso de la ocurrencia de un evento que genere indisponibilidad de la aplicación.

2. ALCANCE

Este documento describe las actividades a realizar ante la indisponibilidad del aplicativo Expediente Digital, permitiendo mantener la continuidad de la operación y la gestión de los procesos de la entidad.

3. RESPONSABLE

Coordinador del Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones.

4. DEFINICIONES

BCP: Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact 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.

Contingencia: Cualquier evento o situación imprevista relacionada con los sistemas informáticos y tecnológicos de una organización. Esto puede incluir desde fallos en el sistema, ciberataques, pérdida de datos, hasta problemas con proveedores de servicios tecnológicos.

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.

Plan de contingencia: Es una estrategia diseñada para ayudar a las empresas a responder eficazmente a eventos negativos o incidentes que puedan suceder en el futuro. Este plan contiene medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones en el ámbito de la informática o las tecnologías.

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.

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.

Expediente digital: Expediente Digital es un sistema de la Superintendencia de Sociedades en el cual se intenta optimizar la generación de documentos resolutivos de los procesos aceptados y radicados a la entidad, la generación de cuadernos, Asociar abogados a las partes y autenticación vía web para terceros.

Expediente jurisdiccional (Expediente digital): Sistema que presta los siguientes servicios a los usuarios internos: flujo de procesos, radicación de documentos, generación de documentos automáticos entre otras funcionalidades.

Expediente jurisdiccional (Expediente digital WEB): Permite la radicación, consulta y seguimiento de las solicitudes relacionadas con procedimientos mercantiles, atención de demandas mercantiles, procesos verbal y verbal sumario.

5. CONTENIDO

El Plan de Contingencia tiene como objetivo asegurar la continuidad operativa de los procesos asociados al **aplicativo Expediente Digital**, estableciendo estrategias y procedimientos para minimizar el impacto de posibles incidentes que puedan comprometer su disponibilidad, integridad o funcionamiento. Además, se establecen mecanismos de recuperación para garantizar la pronta restauración del servicio, reduciendo al máximo las interrupciones y afectaciones a los usuarios.

5.1. SUPUESTOS:

La efectividad en la ejecución de este documento, 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 tecnológica y recursos que soportan las estrategias de contingencia y recuperación para los procesos críticos.
- Los funcionarios que ejecutan esta guía, o sus suplentes, se encuentran disponibles y no han sido afectados por la contingencia.
- Solo el funcionario responsable activará la contingencia y el equipo encargado del plan podrá actuar según los procedimientos establecidos en este documento
- Se han realizado pruebas de las estrategias y actividades al menos 1 vez al año, y han funcionado.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- El sistema de seguridad perimetral siempre deberá estar en funcionamiento.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.
- Se considera que los protocolos de comunicación interna y externa funcionarán según lo planeado.

5.2. GUIA DEL PLAN DE CONTINGENCIA PARA EL APLICATIVO DE EXPEDIENTE DIGITAL.

5.2.1. ESCENARIOS DE CONTINGENCIAS

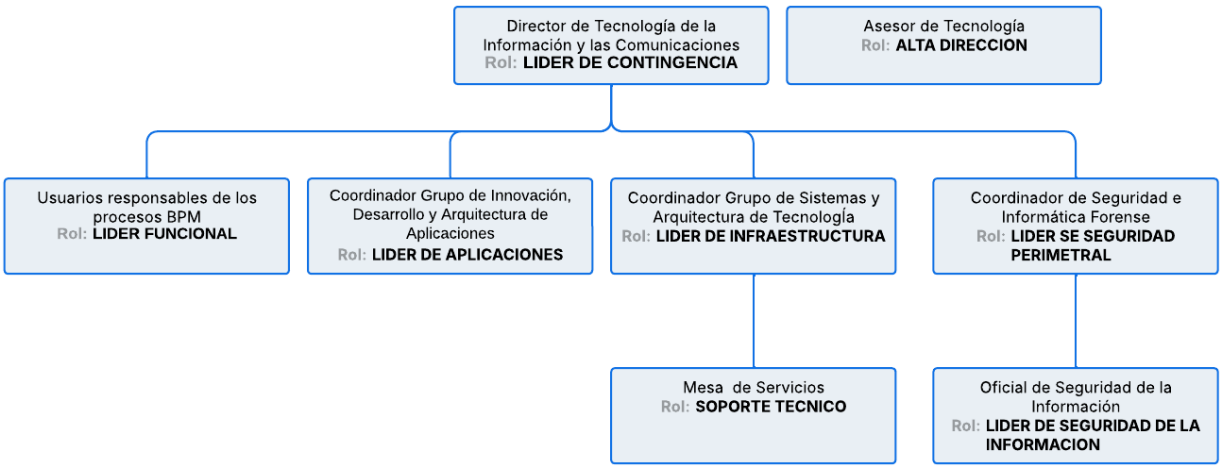
Los escenarios de interrupción mayor o un evento contingente que contempla este documento guía se presentan ante no disponibilidad del aplicativo Expediente Digital por:

- Virus informáticos
- Daño en certificados digitales (tokens)
- Fallas técnicas en servidores de aplicación
- Fallas técnicas en servidores de Bases de datos
- Fallas técnicas en redes de comunicaciones
- Ataques informáticos

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. En la siguiente imagen se definen los roles responsables del plan de contingencia del aplicativo Expediente Digital:



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 Usuarios Responsables de los procesos gestionados en Expediente Digital	- Estar pendiente de las situaciones y eventos que puedan generar indisponibilidad de servicios del aplicativo expediente digital. - Apoyar, conocer y dar Vo.Bo, al plan de contingencia de expediente digital. - Determinar la configuración técnica requerida para establecer una respuesta a la contingencia de Expediente Digital.	- Comunicar al líder de Aplicaciones el evento de indisponibilidad que se presente. - Preparar los equipos de trabajo para actuar en contingencia. - Ejecutar las actividades del plan de contingencia o sus pruebas, que le correspondan. - Informar al líder de Aplicaciones el estado de la contingencia durante el evento.	- Confirmar que todos los servicios y funcionalidades de Expediente Digital estén funcionando. - Comunicar al líder de Seguridad de la Información, las lecciones aprendidas. - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	- Estar atento a los cambios en la infraestructura tecnológica, funcionarios y en los procesos de Expediente Digital, a fin de actualizar el plan de recuperación ante desastres.		expediente digital respecto a las actividades a realizar con su equipo de trabajo.
LIDER DE APLICACIONES Coordinador de Innovación, Desarrollo y Arquitectura de Aplicaciones.	- Asegurar el monitoreo del aplicativo expediente Digital. - Apoyar el desarrollo de las actividades a ejecutar por su equipo de trabajo en caso de un evento de indisponibilidad o en la ejecución de las pruebas de contingencia. - Velar por la existencia de soporte técnico y mantenimiento evolutivo del sistema de expediente digital. - Informar los resultados del monitoreo de los servicios de expediente digital. - Velar y conocer los resultados del	- Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. - Participar en la evaluación del evento contingente. - Verificar la disponibilidad de la infraestructura propia asociada a los servicios de expediente digital para contingencia. - Coordinar la ejecución de las actividades de contingencia y recuperación con su equipo de trabajo. - Comunicar a los proveedores relacionados con el evento sobre la activación del plan de contingencia de expediente digital. - Mantener informado al Líder de Contingencia sobre el estado de contingencia y avance de las actividades de sus equipos de trabajo.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de expediente digital respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de expediente digital que se hayan detectado respecto a la infraestructura tecnológica.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de expediente digital. - Participar en el Análisis de impacto de eventos de servicios de expediente digital el RTO y RPO. - Contar con los ambientes de contingencia en caso de eventos de indisponibilidad de expediente digital.	- Colaborar con la información correspondiente para realizar las configuraciones requeridas en la activación de componentes alternos para expediente digital.	- Entregar al líder de seguridad de la información las lecciones aprendidas del evento.
LIDER DE CONTINGENCIA Director de Tecnología de la Información y Comunicaciones	- Velar por la actualización del plan de contingencia de Expediente Digital. - Velar por la actualización, distribución y pruebas del plan de contingencia - Gestionar la consecución de los recursos para activar el plan de contingencia de expediente digital. - Conocer a quien debe comunicar sobre la situación de contingencia.	- Evaluar y activar el plan de contingencia para el evento de contingencia que se presente en expediente digital. - Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. - Liderar la operación bajo contingencia. - Comunicar a la alta dirección el estado de contingencia y el avance de actividades de contingencia.	- Velar por la actualización del plan de continuidad acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. - Informar a la alta dirección sobre el retorno a la normalidad.

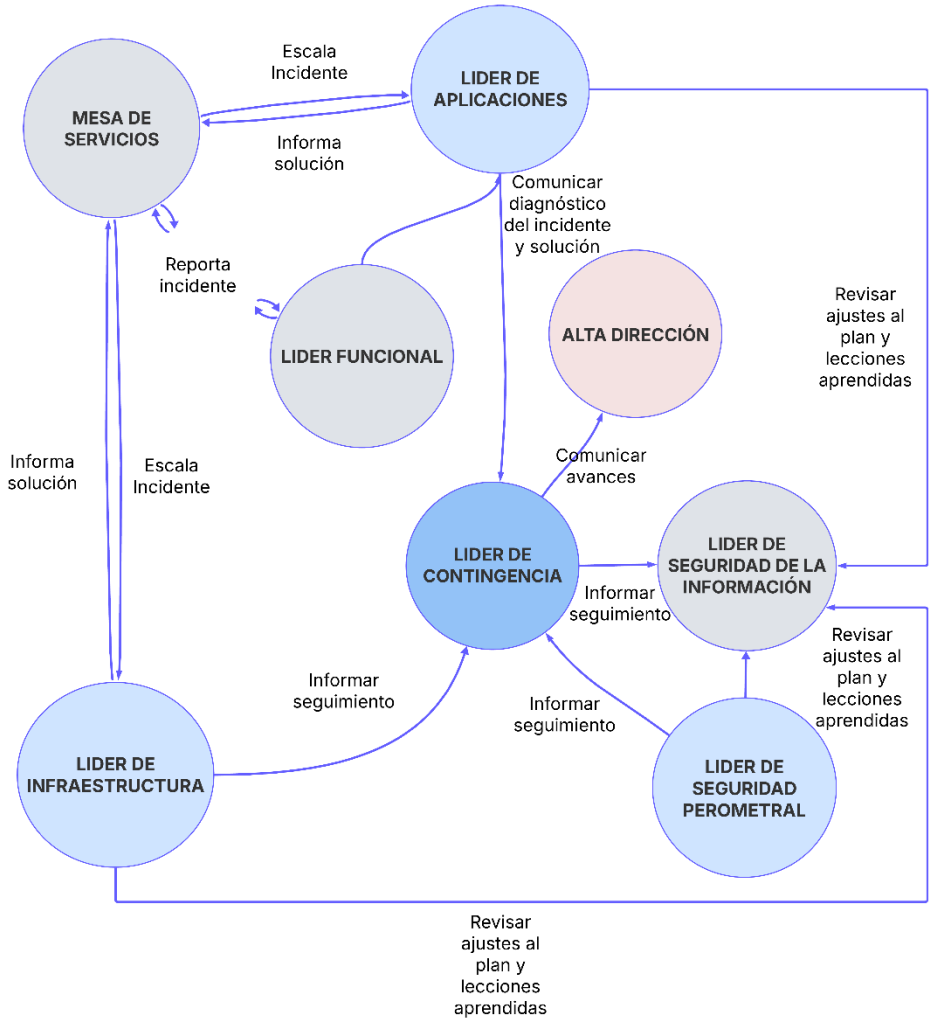
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
LÍDER DE INFRAESTUCTURA Coordinador Sistemas y Arquitectura de Tecnológica	- Asegurar el monitoreo de los procesos y componentes de la plataforma tecnológica de expediente digital. - Mantener la configuración técnica de la conectividad requerida en los servicios de expediente digital - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de los eventos que ocurran en el sistema de expediente digital. - Informar los resultados del monitoreo de los servicios de expediente digital. - Velar por el soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de expediente digital. - Participar en el Análisis de impacto de eventos de	- Participar en la evaluación del evento contingente. - Verificar por disponibilidad de la infraestructura propia asociada a los servicios de expediente digital para contingencia. - Velar por la ejecución de las actividades de contingencia y recuperación, con su equipo de trabajo. - Comunicar a los proveedores relacionados con el evento sobre la activación del plan de contingencia de expediente digital. - Estar atentos para dar una correcta información a las personas que están participando en el plan de contingencia. - Mantener informado al Líder de Contingencia sobre el estado de contingencia y avance de las actividades de sus equipos de trabajo. - Realizar las configuraciones requeridas para activar componentes alternos requeridos.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de expediente digital respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de expediente digital que se hayan detectado respecto a la infraestructura tecnológica.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	servicios de expediente digital el RTO y RPO. - Asegurar el respaldo de información y aplicación de expediente digital. - Contar con los ambientes de contingencia en caso de eventos de indisponibilidad de expediente digital.		
LÍDER DE SEGURIDAD E PERIMETRAL Coordinador Grupo de Seguridad e Informática Forense.	- Asegurar el monitoreo técnico de expediente digital. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de contingencia sobre expediente digital. - Coordinar el registro y la gestión de los incidentes relacionados con Expediente Digital, asegurando su correcta atención y resolución	- Participar en la evaluación del evento contingente para determinar su impacto y posibles soluciones. - Verificar la disponibilidad de los recursos de Expediente Digital y notificar al personal responsable para su atención. - Realizar con su equipo de trabajo las actividades que les correspondan en el plan de contingencia. - Mantener informado al Líder de contingencia de los resultados de las actividades realizadas.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de expediente digital. - Solicitar, revisar y aprobar los cambios en la guía de contingencia de expediente digital. - Comunicar al líder de seguridad de la información, las lecciones aprendidas del evento.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
LIDER DE SEGURIDAD DE LA INFORMACIÓN Oficial de Seguridad de la Información	- Liderar la creación del plan de contingencia de expediente digital y el Análisis de impacto para determinar el RTO y RPO. - Coordinar la publicación del plan de contingencia de expediente digital. - Gestionar la socialización y conocimiento del plan de contingencia para expediente digital, por parte de los grupos involucrados.	- Participar en el proceso de prueba del plan de continuidad. - 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.	- Verificar si se actualizó el plan de contingencia, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. - Verificar que las lecciones aprendidas están siendo actualizadas en la herramienta definida.
MESA DE SERVICIOS Soporte Técnico	- Conocer el plan de contingencia vigente y comprender su rol de participación en este. - Disponer de un sistema de registro de eventos mediante tickets. - Contar con los medios de comunicación efectivos para que los funcionarios puedan reportar eventos de maneraa oportuna.	- Registrar los eventos reportados de manera precisa. - Informar sobre el estado y detalles del ticket asignado a cada evento. - Estar atentos para realizar actividades de remediación que les soliciten.	- Cerrar el evento una vez haya recibido la confirmación correspondiente. - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia.

5.3. ÁRBOL DE LLAMADAS

En la siguiente gráfica se puede observar las comunicaciones que deben ejecutarse durante un evento que afecte la disponibilidad del aplicativo expediente digital.



Los medios de comunicación para atender estos eventos son los siguientes: correo electrónico, teléfono, celular, Microsoft Teams.

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 las Comunicaciones, ver Anexo 1.

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

5.4.1 ¿Quién reporta un incidente, interrupción mayor o un evento contingente de expediente digital?

a. Por lo regular, los usuarios que utilizan el aplicativo de expediente digital, deben reportar todos los eventos que se presenten sobre el funcionamiento o eventos que se presenten.

b. El personal de tecnología encargado de monitoreo de plataforma (infraestructura de técnica, infraestructura de comunicaciones, infraestructura de datos) deben reportar el incidente a Mesa de Ayuda o Líder de Centro de Cómputo cuando:

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

c. La mesa de ayuda debe atender el incidente de acuerdo a lo establecido en el Procedimiento GTI-PR-002- Mantenimientos preventivos y correctivos, y se continúa con la ejecución de esta guía asi:

- El incidente afecta la disponibilidad del aplicativo Expediente Digital a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.

En cualquiera de los casos, se debe escalar el incidente a los funcionarios responsables

5.4.2 ¿Quién evalúa la magnitud e impacto del incidente?

a. Para el caso de un evento de indisponibilidad del aplicativo de Expediente digital el líder funcional realizará con su equipo de trabajo el análisis y diagnóstico sobre el incidente presentado, teniendo en cuenta:

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

Finalmente debe comunicarse con el Director de Tecnología de la Información y las Comunicaciones para informar los resultados del diagnóstico, en caso de que el incidente sea crítico, deberá evaluar el impacto junto con los demás lideres y activar el plan de contingencia correspondiente.

b. El director de Tecnología de la Información y las Comunicaciones, en conjunto con los demás lideres, definen la estrategia de retorno a la normalidad, una vez se haya dado solución al incidente presentado, 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.
- Sincronización entre los centros de cómputo, cuando se operó el sitio a utilizar como Centro de Cómputo, si aplica.

5.4.3 Análisis de Impacto.

De acuerdo con las pruebas de contingencia realizadas anteriormente a los sistemas de información, el tipo de funcionalidad y el tiempo utilizado para la recuperación de los servicios, se ha definido un tiempo de recuperación del aplicativo Expediente Digital de:

RTO: 6 horas
RPO: 6 horas

5.5. ACTIVIDADES DE MANEJO DE CRISIS

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

5.5.1. Para el caso de eventos tecnológicos:

a. El líder de Contingencia 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 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.

Los grupos de interés a considerar en la comunicación de la crisis pueden ser:

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

- Gobierno, Autoridades y Entes de Control
- Contratistas y Proveedores
- Medios de comunicación

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 de este. 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?

5.6. ACTIVIDADES DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA

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

La actualización y mantenimiento a la presente guía se debe realizar cuando exista:

No	Actividad	Responsable	Frecuencia
1.	Cambios en la plataforma Tecnológica de la entidad que involucre modificaciones en la configuración del aplicativo de expediente digital.	Lideres de los grupos de la Dirección de Tecnología de la Información y las Comunicaciones. Oficial de Seguridad de la Información	Cada vez que se realice un cambio a la infraestructura tecnológica del sistema de expediente digital.
2.	Cambio en el aplicativo de expediente digital por nuevas versiones o reemplazo.	Lideres de los grupos de la Dirección de Tecnología de la Información y las Comunicaciones. Oficial de Seguridad de la Información	Cuando se realice cambio de versión del sistema de expediente digital o nueva aplicación
3.	Cuando los resultados de las pruebas de contingencia que	Lideres de los grupos de la Dirección de Tecnología de la	Posterior a las pruebas de contingencia que se

No	Actividad	Responsable	Frecuencia
	se realicen requieran una actualización de la guía	Información y las Comunicaciones. Oficial de Seguridad de la Información	realicen sobre el sistema de expediente digital

5.7. ACTIVIDADES DE PRUEBA

La programación y método por utilizar en la realización de pruebas a la continuidad se deben relacionar en el formato GTI-FM-004 Plan, Diseño, Ejecución y Evaluación de pruebas. Las actividades deben estar acordes los roles y responsabilidades incluidas en el numeral 3.2 de la presente guía.

Las siguientes pruebas, junto con otras que puedan desarrollarse para garantizar la seguridad de la información, deben considerarse durante el desarrollo del plan de contingencia:

- El control de acceso físico
- El control de acceso lógico al aplicativo o la infraestructura involucrada en pruebas de eventos tecnológicos.
- Pruebas a la disponibilidad de la información.
- Uso aceptable de los activos durante la prueba.
- Ejecución de la gestión de cambios para la prueba.
- Tratamiento de la seguridad dentro de los acuerdos con proveedores participantes en las pruebas
- La integridad de las bases de datos y archivos de información.
- La disponibilidad y configuración de la infraestructura involucrada.
- La confidencialidad de la información involucrada en la prueba.
- La trazabilidad de las actividades realizadas en la prueba sobre la infraestructura, las bases de datos y las comunicaciones.

5.8. DISTRIBUCIÓN DE LA GUIA: PLAN DE CONTINUIDAD DE EXPEDIENTE DIGITAL.

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.
- Usuarios.

5.9. RECURSOS MÍNIMOS REQUERIDOS

La infraestructura necesaria para soportar el aplicativo Expediente digital en caso de un evento crítico de infraestructura. es:

Cant.	Aplicació	Servidor	Base de Datos
1	Expediente Jurisdiccion (Expediente digital)	SSSHP-VA15 SSSHP-VA16 SSSHP-VA17 SSSHP-VA18 SSSHP-VA09	Microsoft SQL Server 2012 (SP3) (KB3072779) - 11.0.6020.0 (X64) Oct 20 2015 15:36:27 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows NT 6.3 <X64> (Build 9600:) (Hypervisor)
2	Expediente Jurisdiccion (Expediente digital WEB	SSSHP-VA15 SSSHP-VA16 SSSHP-VA17 SSSHP-VA18 SSSHP-VA09	

5.10. ACTIVIDADES DE CONTINGENCIA

A continuación, se definen los pasos a seguir para recuperar los componentes de la plataforma tecnológica en caso de evento de indisponibilidad de expediente digital:

5.10.1. ACTIVIDADES DE CONTINGENCIA FUNCIONALES

Durante el tiempo de indisponibilidad del aplicativo Expedinte Digital, se deben llevar a cabo las siguientes actividades funcionales:

Proceso	Sistema	Actividad	Responsable

Radicación por Ventanilla	Gestor Documental	1. Los documentos de entrada que ingresen a través de ventanilla deben ser radicados y digitalizados a través de GEDESS. 2. Se debe enviar a las personas de soporte de Expediente Digital el reporte de radicados indicando el proceso al cual debe ser asociado.	Gestión Documental
Gestión de Procesos	Gestor Documental	Debe usarse GEDESS como sistema de contingencia, para realizar las siguientes actividades: 1. Consulta de radicados de entrada y salida por sociedad o persona natural 2. Proyección de borradores 3. Revisión y firma de documentos de salida 4. Se debe enviar a las personas de soporte de Expediente Digital la relación de documentos de salida indicando el número de radicado y el proceso al cual debe ser asociado.	Ponentes y Coordinadores de Grupo

5.10.2. ACTIVIDADES DE CONTINGENCIA TECNOLÓGICAS.

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Soporte de expediente digital	1. Informar al líder funcional sobre el evento de indisponibilidad de expediente digital. 2. Realizar pruebas de funcionalidad técnica de expediente digital antes y después de un evento. 3. Informar al líder funcional sobre el retorno a la normalidad.	Líder de Aplicaciones
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Preparar las condiciones de seguridad para la plataforma de contingencia que se implemente en caso de incidente de indisponibilidad de expediente digital. 2. Coordinar la ejecución de las actividades de prueba de	Líder Seguridad Perimetral

Proceso	Subproceso	Actividad	Responsable
		funcionalidad que le correspondan a su equipo de trabajo dentro de esta guía. 3. Informar al líder de contingencia del resultado de las pruebas que le correspondan. 4. Entregar al líder funcional las evidencias de las pruebas realizadas.	
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	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 Contingencia, la situación de contingencia presentada. 4. Informar a los equipos de trabajo para actuar en contingencia mediante el uso del Gestor Documental GEDESS. 5. Coordinar ejecución y reporte de resultados, de las actividades de contingencia de su grupo de trabajo.	Líder aplicaciones
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 de contingencia que se presente. 2. Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. 3. Liderar la operación bajo contingencia. 4. Comunicar a la alta dirección el estado de contingencia y el	Líder Contingencia

Proceso	Subproceso	Actividad	Responsable
		avance de actividades de contingencia.	
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. Verificar el funcionamiento de la infraestructura del Gestor Documental como sistema de contingencia. 7. Informar a líder de Seguridad Perimetral sobre estado de las comunicaciones en periodo de contingencia. 8. Revisar y garantizar el correcto funcionamiento del aplicativo Expediente Digital de acuerdo con las causas del incidente presentado para dar la respectiva solución.	Líder Infraestructura
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. 3. Registrar cierre del evento cuando se confirme la solución.	Líder de Infraestructura - Coordinador de mesa de servicios
Gestión de Tecnología de la Información y las Comunicaciones	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.	Líder de Seguridad de la Información

Proceso	Subproceso	Actividad	Responsable
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. Coordinar la ejecución de las guías de contingencia y pruebas. 3. Comunicar a los proveedores o desarrolladores la activación del plan de contingencia expediente digital. 4. Revisar disponibilidad de los ambientes de desarrollo y pruebas, en caso de ser necesario. 5. Informar al Líder de contingencia sobre el evento. 6. Informar al Líder de seguridad de la información sobre el evento.	Líder de Aplicaciones

5.11. RETORNO A LA NORMALIDAD.

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

5.11.1. ACTIVIDADES FUNCIONALES

Una vez se restablezca el aplicativo de Expediente Digital y se tengan en operación los procesos, se deben ejecutar las siguientes actividades:

Proceso	Sistema	Actividad	Responsable
Asociar Radicados de Entrada a Procesos	Expediente Digital	1. Se relacionan los documentos radicados de entrada y de salida a los procesos de Expediente Digital, ya sea porque corresponden a solicitudes nuevas, o porque corresponden a procesos existentes, se debe relaciona el radicado al proceso correspondiente.	Gestión Documental

		2. Se envía comunicación a las personas responsables del proceso informando la asociación de los radicados para continuar su gestión a través de BPM.	

5.11.2. ACTIVIDADES TECNOLÓGICAS

Una vez se restablezca el funcionamiento del sistema de expediente digital se deben ejecutar las siguientes actividades:

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	1. Solicitar a mesa de ayuda sobre el cierre del evento. 2. Informar al Líder de Contingencia sobre retorno a la normalidad 3. Informar a Líder de Seguridad de la Información sobre retorno a la normalidad. 4. Informar a usuarios finales el fin de la contingencia. 5. Comunicar a Líder de Seguridad de la Información las lecciones aprendidas del evento.	Líder de Aplicaciones
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	1. Comunicar a la alta dirección la finalización de la contingencia y retorno a la operación normal. 2. Comunicar al Líder de Seguridad de la información las lecciones aprendidas y el informe de cierre del evento.	Líder Contingencia
Oficina Asesora de Planeación	Oficial de Seguridad de la Información	1. Consolidar a información de las lecciones aprendidas del evento. 2. Velar porque se registren las lecciones aprendidas en la	Líder Seguridad de la Información

Proceso	Subproceso	Actividad	Responsable
		herramienta existente para este fin y se actualice la documentación correspondiente con el fin de fortalecer el presente plan de continuidad	
Gestión de Tecnología de la Información y las Comunicaciones	Mesa de servicios	1. Registrar el cierre del evento. 2. Informar al líder funcional sobre el cierre del evento.	Coordinador de mesa de servicios
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Verificar monitoreo de servidores de aplicación de expediente digital.	Líder Seguridad perimetral

6. REGISTROS

Formato GTI-FM-004 Plan, Diseño, Ejecución y Evaluación de pruebas.
Formato GTI-FM-005 Análisis de impacto.

7. ANEXOS

Anexo 1. Directorio Telefónico

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	28/06/2018	Creación del documento. Se definió la infraestructura tecnológica, nombre de base de datos y servidor de base de datos de la aplicación. Se definieron escenarios de desastre, las infraestructuras que interactúan con expediente digital, el árbol de roles y responsabilidades, se incluyen actividades de recuperación y contingencia, y recursos mínimos requeridos.
002	28/12/2020	Se actualizan 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. Se definen las pruebas de seguridad a realizar si es el caso.
003	23-12-2021	Se adecua a los nombres de los grupos de tecnología actuales. Se actualiza el Directorio Telefónico por cambios en estructura funcional y nuevos miembros de equipos.
004	28-06-2024	Se estandariza el documento al formato de los otras guías de contingencia. Se estandarizan los roles y responsabilidades, árbol de llamadas y recursos

		mínimos requeridos. Se cambia el nombre del documento de GTI-GU-007 Plan Recuperación Expediente Digital a GTI-GU-007 PLAN DE CONTINGENCIA EXPEDIENTE DIGITAL. Se actualiza el Directorio Telefónico por cambios en estructura funcional y nuevos miembros de equipos. Cambio logo institucional.
005	28-04-2025	Se actualizan las imágenes de roles y responsabilidades, así como el árbol de llamadas. Además, se realizan ajustes generales de forma. También se actualiza el Directorio Telefónico debido a cambios en la estructura funcional y la incorporación de nuevos miembros a los equipos.

Elaboró	**Revisó**	**Aprobó**
Nombre: Marisol Castiblanco Cargo: Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones Fecha: 25/03/2025	Nombre: Marisol Castiblanco Cargo: Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones Fecha:12/04/2025	Nombre: Ricardo Fernelix Ríos Rosales Cargo: director de Tecnología de la Información comunicaciones Fecha:25/04/2025

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director de Tecnología de la Información y comunicaciones	Ricardo Rios Rosales Rrios@supersociedades.gov.co	Líder de Contingencia	3000
2	Oficial de Seguridad de la Información	Ivan Alexis Ontibon Rojas iontibon@supersociedades.gov.co	Líder de Seguridad de la Información	
3	Coordinación Innovación, Desarrollo y Arquitectura de Aplicaciones	Marisol Castiblanco Calixto MarisolCC@supersociedades.gov.co	Líder de Aplicaciones	3301
4	Coordinación de Sistemas y Arquitectura de Tecnología	Amanda Rocio Fernández Rico AmandaF@supersociedades.gov.co	Líder de Infraestructura	3013
5	Coordinación de Seguridad e Informática Forense	Jeny Shirley Díaz González JenyD@supersociedades.gov.co	Líder de Seguridad Perimetral	4030
7	Soporte Técnico	Mesa de ayuda soporte@supersociedades.gov.co	Mesa de Servicios	3020-