	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

1. OBJETIVO

Dar a conocer el proceso contingencia ante las posibles fallas técnicas y funcionales que se puedan presentar en GESTOR DOCUMENTAL.

2. ALCANCE

Este documento enmarca las actividades a ejecutar ante posibles eventos tecnológicos y funcionales que afecten la disponibilidad de la aplicación o componentes necesarios para apoyar la gestión funcional que se presenten en el GESTOR DOCUMENTAL, permitiendo mantener en la entidad, la continuidad en la operación y gestión de estos procesos.


3. RESPONSABLES

Director de Tecnología de la Información y las comunicaciones.
 Coordinador Grupo de Proyectos de Tecnología.
 Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones.
 Coordinador Grupo de Sistemas y Arquitectura Tecnológica
 Coordinador de Seguridad e Informática Forense.
 Coordinador Grupo de Gestión Documental
 Coordinador Grupo de Relación Estado – Ciudadano
 Coordinador Grupo de Notificaciones Administrativas
 Coordinador Grupo de Apoyo Judicial
 Gerente de proyecto de SGDEASS

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 plan de contingencia, planes de

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact Analysis), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a los usuarios internos y externos.

CAP: Centro Alternativo 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 Alternativo 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.

PLAN DE CONTINGENCIA: Conjunto de actividades que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio, las operaciones de una compañía u organización, el funcionamiento de un sistema o aplicación que han sufrido en una situación inesperada que afecta disponibilidad de los servicios de una entidad.

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.

DEL GESTOR DOCUMENTAL: Sistema de gestión documental que tiene como función: administrar, gestionar y controlar el flujo de documentos recibidos y emitidos y la ejecución de todos los asuntos o trámites que se manejan, a través de archivos con cualquier medio o formato (escrito, fax, correo electrónico, Internet, voz y video entre otros), situación que inicia desde el

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

momento mismo en que la correspondencia se radica a la entrada o a la generación y salida de la Entidad.

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

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


5. CONDICIONES GENERALES

El plan de contingencia está enfocado a tener en cuenta posibles escenarios de riesgo que se pueden presentar sobre el GESTOR DOCUMENTAL – GeDeSS y estar preparados para solventar estos eventos garantizando la prestación del servicio de la entidad.

5.1. Supuestos:

La efectividad en la ejecución de las actividades registradas en este documento se fundamenta en los siguientes supuestos:

- Se dispone de la infraestructura y recursos que soportan la plataforma requerida por el SGDEASS.
- Ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente que afecte la plataforma tecnológica
- Los funcionarios que ejecutan estas actividades o sus suplentes se encuentran disponibles.
- Solo el funcionario responsable activará el plan de contingencia.
- Se deben realizar las actividades previstas de manera ordenada.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo con los procedimientos y frecuencias establecidas.
- Se tendrá acompañamiento del proveedor que brinda el soporte del Gestor Documental.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

- Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- Se tendrá acompañamiento de los proveedores de aplicativos que se integran al GeDeSS.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

5.2. GUIA DEL PLAN DE CONTINGENCIA PARA DEL GESTOR DOCUMENTAL

5.2.1. ESCENARIOS DE CONTINGENCIA


Los escenarios de interrupción mayor o eventos contingentes que contempla este documento guía se presentan ante no disponibilidad de la plataforma del GESTOR DOCUMENTAL por:

5.2.2. Fallas técnicas en servidores de aplicación.

- Problemas del sistema operativo.
- Problemas de conectividad de red que afectan la comunicación entre el servidor de aplicación y otros componentes de la infraestructura como, cortes de red, congestión de la red, configuración incorrecta de redes virtuales.
- Errada configuración como: configuración incorrecta de parámetros de inicio y configuración de límites de recursos (CPU, memoria) incorrectos.
- Línea base requerida en los servidores no implementada.
- Inconvenientes de Hardware.
- DeadLook de los hilos de procesamiento.

5.2.3. Fallas técnicas en la plataforma de contenerización

- Errores en configuración del entorno.
- Problemas de conectividad de red que afectan la comunicación entre el servidor de aplicación y otros componentes de la infraestructura


	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

como, cortes de red, congestión de la red, configuración incorrecta de redes virtuales.

- Problemas de almacenamiento (Errada configuración como: configuración incorrecta de parámetros de límites de recursos de espacio)
- Problemas de lentitud: Contenedores que experimentan rendimiento lento debido a recursos insuficientes asignados, como CPU, memoria o E/S.
- Problemas de escalabilidad: Dificultades para escalar los contenedores horizontal o verticalmente para satisfacer la demanda de carga de trabajo.
- Problemas en el gestor de contenedores: Fallas en la plataforma de orquestación (por ejemplo, Kubernetes, Docker Swarm) que pueden afectar la gestión y disponibilidad de los contenedores.
- Problemas de balanceo de carga: Errores en la distribución del tráfico entre los contenedores o en la configuración de los servicios de balanceo de carga.
- Problemas de registro (logging): Fallas en la recopilación o visualización de registros desde los contenedores, lo que dificulta la detección y resolución de problemas.
- Problemas de monitorización: Falta de visibilidad adecuada sobre el estado y el rendimiento de los contenedores, lo que dificulta la detección temprana de problemas.
- Incompatibilidad de versiones: Problemas debido a la incompatibilidad entre las versiones de las imágenes de los contenedores y las bibliotecas o dependencias utilizadas por la aplicación
- Línea base requerida en los servidores no implementada.
- Inconvenientes de comunicación entre los Pots.
- Inconsistencia en las imágenes de los contenedores
- Sobrecarga de contenedores

5.2.4. Fallas técnicas en estaciones de trabajo.

- Problemas del sistema operativo.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

- Problemas de conectividad de red que afectan la comunicación entre la estación de trabajo y la aplicación, el servidor de aplicación y otros componentes de la infraestructura.
- Errada configuración como: configuración incorrecta de parámetros de inicio y configuración de límites de recursos (CPU, memoria) incorrectos.
- Línea base requerida no implementada.
- Requerimientos mínimos para el GEDESS no implementada.

5.2.5. Fallas críticas del aplicativo.


- Incompatibilidad con el entorno de producción.
- Problemas de configuración (puertos, protocolos de seguridad, protocolos de cifrado).
- Versión desactualizada respecto a las pruebas ya realizadas.
- Errores de funcionalidad.
- Problemas de lentitud

5.2.6. Problemas de Bases de datos.

- Fallas en el registro de la trazabilidad y auditorias.
- Falta de sintonización.
- Configuración errada.
- Degradación en el rendimiento de consultas y transacciones
- Desoptimización de índices
- Tablas referenciales no creadas o migradas.
- Sobrecarga de recursos
- Parametrización errada de tamaños de las tablas.
- Configuración insegura.
- Fallos en los procesos de copia de seguridad.
- Bloqueos masivos de usuario
- Problemas de escalabilidad de la base de datos
- DeadLock de la base de datos

5.2.7. Problemas de Seguridad

- Fallas en el registro de la trazabilidad y auditorias.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública

- Explotación vulnerabilidad SQL injection.
- Errores de XSS Cross-site scripting.
- Configuración insegura.
- Exposición de datos sensibles.
- Uso de componentes con vulnerabilidades conocidas.
- Rupturas de control de acceso.
- Rupturas de autenticación.
- Vulnerabilidades tipo XXE.
- Errores de validación de datos.

5.2.8. Pérdida de datos o corrupción de datos

- Errores en los scripts de migración de datos.
- Falta de backups actualizados.
- Problemas de sincronización entre bases de datos.
- Inadecuada configuración de copias de seguridad.

5.2.9. Problemas de escalabilidad


- Diseño incorrecto de la arquitectura en producción o diferente a la probada en ambiente de pruebas.
- Subestimación de la carga esperada.
- Problemas de gestión de capacidad de recursos (CPU, memoria).

5.2.10. Fallas de disponibilidad

- Errores en la configuración del balanceador de carga.
- Fallos en la infraestructura de red.
- Problemas con los proveedores de servicios.

5.2.11. Fallas en la integración con sistemas externos

- Problemas de interoperabilidad con sistemas externos o servicios.
- Cambios inesperados en las APIs externas.
- Versiones incompatibles entre sistemas.
- Problemas de comunicación.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

5.2.12. Fallas en la aplicación Móvil

- Cierres inesperados
- Congelamiento
- Errores de carga
- Errores de interfaz de usuario
- Lentitud y/o consumo excesivo de recursos
- Fallas de conexión
- Errores de sincronización
- Funcionalidades que no funcionan como se espera: Ej: Problemas con la autenticación, la carga de contenido, la reproducción de medios.
- Inconsistencia en el comportamiento: La aplicación se comporta de manera inconsistente en diferentes dispositivos o situaciones.
- Problemas de seguridad (fuga de información).
- Errores específicos de la versión del sistema operativo, diferentes dispositivos.
- Problemas relacionados con las actualizaciones
- Errores de integración con otros servicios o APIs
- Errores en la gestión de errores y logs.


5.2.13. Errores humanos durante la implementación

- Falta de capacitación del personal funcional.
- Falta de capacitación del personal técnico.
- Procedimientos de implementación inexistentes o mal definidos.
- Manuales técnicos y funcionales no entregados o desactualizados.

5.2.14. Desastres naturales o problemas de infraestructura

- Cortes de energía y/o aire acondicionado.
- Errores en el mantenimiento de la infraestructura física.
- Incendios o conatos de incendio.
- Desordenes, huelgas, motines, Etc

5.2.15. Errores en Infraestructura o Aplicaciones que interactúan con el gestor documental:

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

- No disponibilidad de la aplicación por:
- No conexión con otras aplicaciones
- Borrado o pérdida de datos
- Integridad de los datos
- Comunicación con otros sistemas como
- Errores con Directorio activo
- Errores con SIGS
- Registros en bases de datos


5.3. ROLES Y RESPONSABILIDADES:

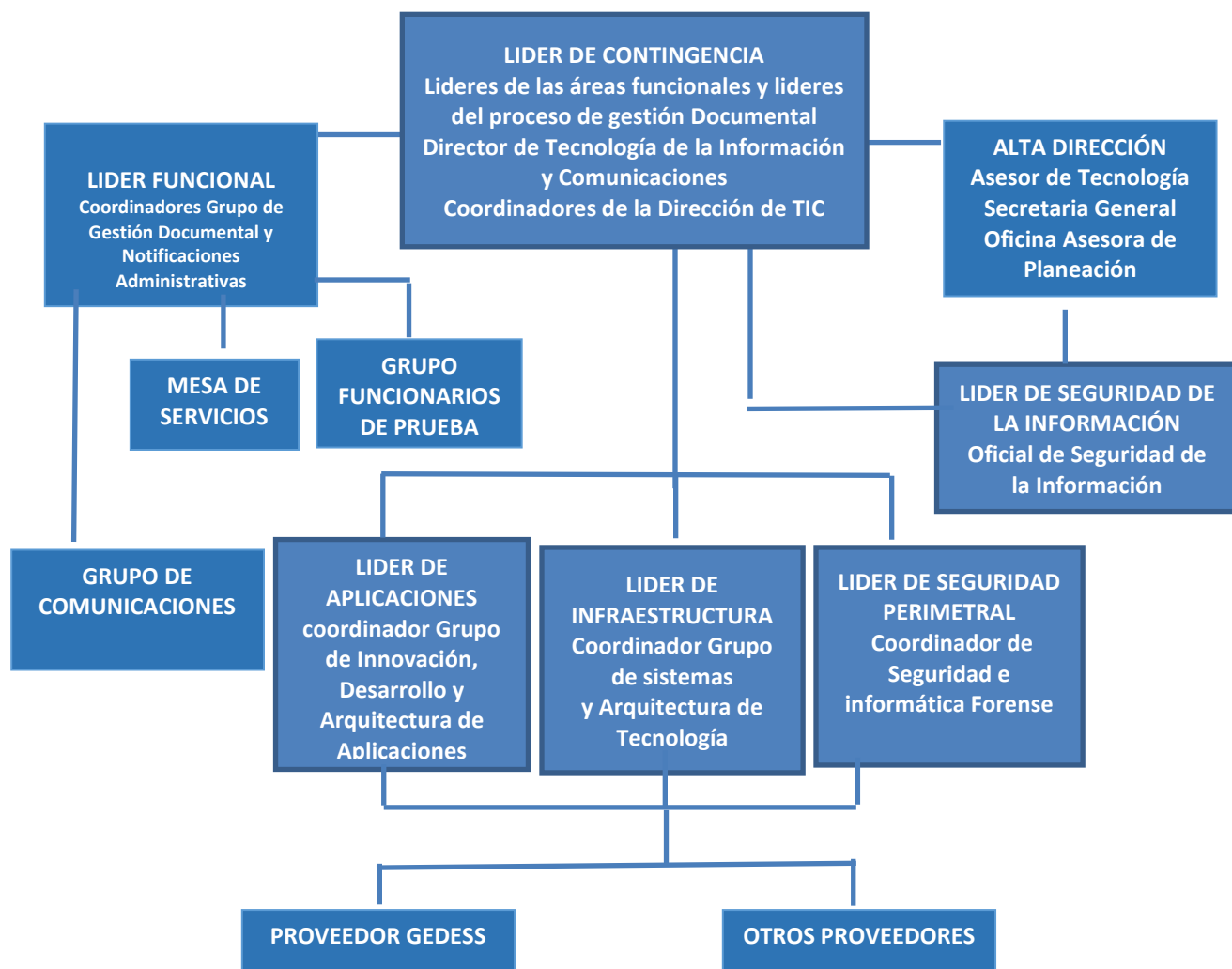
5.3.1. Comité de Crisis.

En el marco del plan de contingencia se debe conformar un comité multidisciplinario el cual debe estar conformado por:

- Líderes del proceso de gestión documental acorde con el Modelo operativo por procesos y a su caracterización (Código: GDOC-C-001)
- Director o quien haga sus veces en el marco del liderazgo de la dirección de DTIC
- Líderes funcionales y de negocio
- Grupos de trabajo de la dirección de DTIC (coordinación de innovación y desarrollo y arquitectura de aplicaciones, Grupo de sistemas de Arquitectura de tecnología, Grupo de seguridad informática y forense, grupo de arquitectura de datos.
- Gerencia de proyectos de la DTIC.
- Funcionario y Contratista de la Superintendencia involucrado.


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.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública



Las responsabilidades definidas para cada rol son:

Rol	Responsabilidades Principales
Líder de Contingencia	Autorizar activación del protocolo, coordinar a todos los grupos, tomar decisiones de retorno o marcha atrás.
Líder Funcional	Implementar procedimientos alternos de radicación manual, garantizar continuidad funcional, custodiar la documentación física.


	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

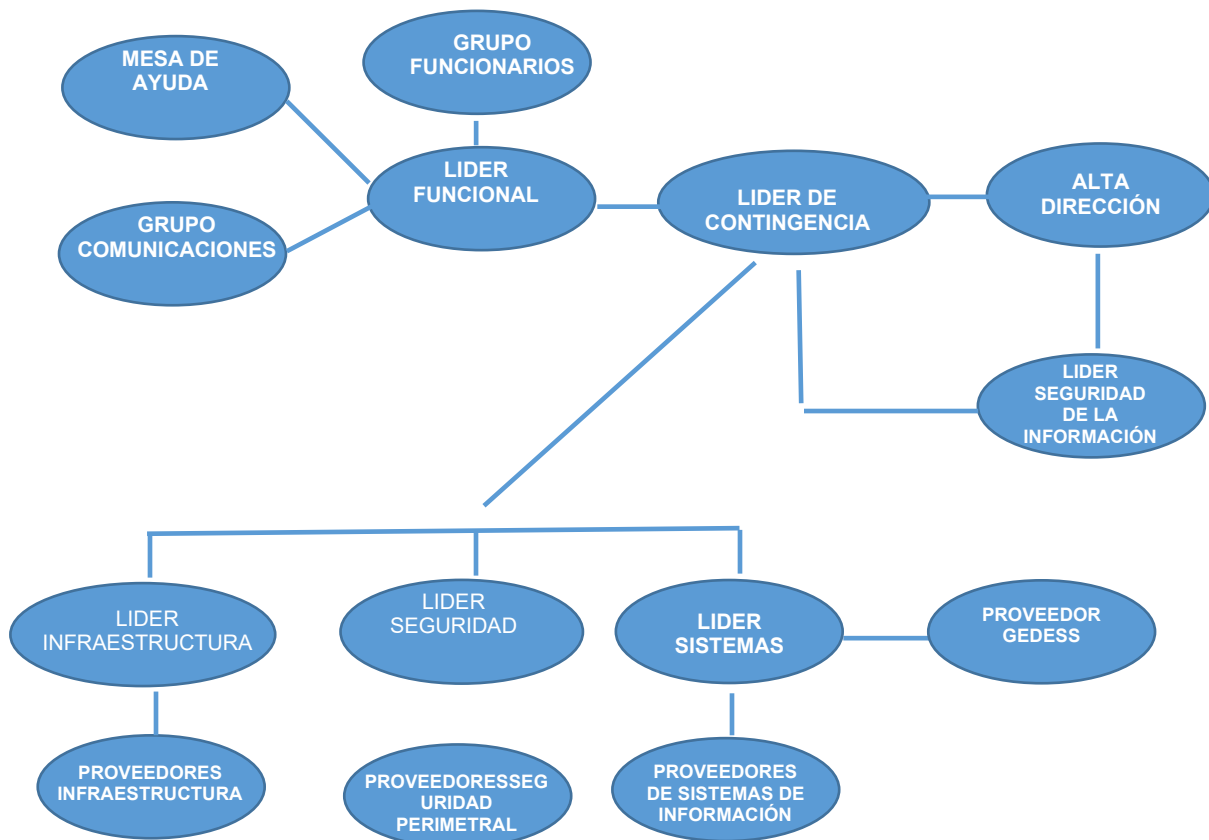
Líder de Infraestructura	Identificar y resolver fallas técnicas, ejecutar respaldos, coordinar recuperación de servicios.
Líder de Aplicaciones	Diagnosticar errores de software, coordinar correcciones con proveedor, instalar parches.
Líder de Seguridad de la Información	Evaluar riesgos de seguridad, identificar y reportar vulnerabilidades, para mitigación al proveedor y realizar monitoreo de amenazas.
Líder de Seguridad	Gestionar las herramientas de seguridad perimetral para validar el estado actual e implementar medidas
Grupo de Comunicaciones	Emitir comunicados internos y externos sobre el estado del servicio y acciones temporales.
Mesa de Ayuda	Recibir, registrar y escalar incidentes, asistir a usuarios en la operación manual.
Proveedor SGDEASS	Brindar soporte técnico y funcional, realizar correcciones urgentes, entregar parches o versiones corregidas.

5.3.2. ÁRBOL DE LLAMADAS

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

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.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024	
		Versión:	001	
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025	
		Clasificación de Información	Pública	



Medios de comunicación: Correo electrónico, teléfono, celular, teams, reuniones presenciales


5.3.3. 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 SGDEASS de:

RTO: 24 horas

RPO: 24 horas

5.3.4. ACTIVIDADES DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA


	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

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 Gestor Documental - GeDeSS	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 aplicativo Gestor Documental - GEDESS
2.	Cambio en el aplicativo Gestor Documental - GEDESS 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 aplicativo Gestor Documental - GEDESS o nueva aplicación
3.	Cuando los resultados de las pruebas de contingencia que se realicen requieran una actualización de la guía	Lideres de los grupos de la Dirección de Tecnología de la Información y las Comunicaciones. Oficial de Seguridad de la Información	Posterior a las pruebas de contingencia que se realicen sobre el aplicativo Gestor Documental - GEDESS

5.3.4.1. ACTIVIDADES DE PRUEBA

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

La programación de las pruebas de contingencia se debe relacionar en el formato Formato GTI-FM-004_PlanPruebasde Contingencia Tecnológica. Las actividades deben estar acordes los roles y responsabilidades incluidas en el numeral 6.2 de la presente guía.

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 el sistema GEDESS y por defecto la reputación, imagen u operación de la Superintendencia de Sociedades.

a. Se establece un comité de crisis conformado por:

- Director de Tecnología de la Información y las Comunicaciones.
- Coordinadora Grupo de Gestión Documental.
- Gerente de proyecto GEDESS.
- Coordinador Grupo de Sistemas y Arquitectura de Tecnología (GSAT).
- Coordinador Grupo de Innovación, desarrollo y arquitectura de Aplicaciones (GIDDA).
- Coordinador Grupo de proyectos de Tecnología de la Información.
- Gerente de proyecto por parte del proveedor.
- Representantes del grupo de arquitectos de tecnología determinados por el director de TIC.
- Representantes de las coordinaciones de la DTIC que estos determinen.
- Oficial de Seguridad de la Información.

Este comité tiene la responsabilidad de:


- Evaluar las diferentes situaciones que se presenten en el gestor documental, reportadas por los grupos de trabajo y evaluar el impacto de estas situaciones.
- Solicitar las correcciones necesarias o su escalamiento.
- Tomar las decisiones de espera y alto de la operación dependiendo de las situaciones presentadas.
- Determinar los reportes a la alta gerencia.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

- b. El Director de Tecnología de la Información y las Comunicaciones comunica a la Alta Dirección, el estado de funcionamiento del gestor documental y entrega el informe de los eventos que se han presentado. Informar:
- Sistemas y servicios afectados
 - Resultados del diagnóstico
 - Acciones realizadas
 - Tiempo estimado para normalización
 - Riesgos a los que está expuesta la entidad por las situaciones presentadas, y las alternativas disponibles.
 - Decisiones que debe tomar la alta dirección.
- c. 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.
- d. 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

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.

- **Decir la verdad:** Ser honestos en los comunicados. Sin embargo, no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.
- **Emitir reportes lo más exactos posible:** Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

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

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

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

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

A continuación, se describe el procedimiento de actuación en un plan de contingencia.

5.5.1. Activación


- El incidente es detectado por monitoreo, reporte de usuario o evento crítico.
- La Mesa de Ayuda genera ticket y notifica al Líder de Contingencia.
- El Líder de Contingencia evalúa el impacto y decide activar el protocolo.
- Se informa a todos los líderes de grupo y se convoca al Comité de Crisis.
- Se registra en el Formato GTI-FM-025 Registro tratamiento de incidentes la hora de activación y condiciones iniciales.

5.5.2. Ejecución de la contingencia operativa

5.5.2.1. Actividades funcionales


Una vez se ha dado el aviso de implementar contingencia por parte de la Dirección de Tecnología de la Información y las Comunicaciones debido a que se presentan fallas del sistema y no se ha logrado el proceso normal de radicación, se debe aplicar el plan de contingencia registrado en la Guía de Recuperación de Desastres que hace parte del Sistema de Gestión Integrado. Sin embargo, el Coordinador de Gestión Documental debe dar aviso a los radicadores del plan de contingencia, en el cual se debe tener en cuenta:

1. Para las radicaciones de entrada se le debe recibir al usuario el documento y se debe plasmar el sello de recibido de correspondencia, con fecha hora, folios y quien recibe el documento en un lugar visible del documento sin dañar el contenido de este, sin tachones ni enmendaduras.
2. Al usuario se le debe colocar en la copia del mismo sello de recibido de correspondencia, con fecha hora, folios y quien recibe el documento en un


	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública

lugar visible del documento sin dañar el contenido de este, sin tachones ni enmendaduras

3. Una vez restituido el servicio se debe radicar en el mismo orden de llegada los documentos (Acuerdo 001 de 2024 del AGN) velando así por la transparencia de la actuación administrativa. Para lo cual en el campo de referencia externa el radicador deberá dejar la anotación de la hora en que se recibió el documento, la fecha y de ver sello de recibido
4. Una vez restablecido el servicio, mediante correo electrónico institucional se le debe notificar al usuario el número de radicado al que pertenece su solicitud. Por parte del Grupo de Gestión Documental.
5. Para los casos de radicación de salida muy urgentes como: Contestación de tutelas o documentos que no den espera al restablecimiento del sistema, se debe gestionar el el documento por parte del área competente, de manera manual en formatos de la entidad, incorporar la firma manual o electrónica y entregarlo en el área de radicación de la entidad con el fin de plasmar el sello con hora, fecha, folios, y una vez restablecido el servicio se procederá a radicar dejando la anotación en el campo de referencia externa dentro del SID.
6. Una vez los documentos de salida cuentan con los sellos a través de las cuentas de correo electrónico certificado de la entidad por parte del Grupo de Gestión Documental se procederá con él envío de la documentación. Para ello desde el área de radicación se le debe notificar al área de correspondencia o donde corresponda según el tipo de envío.
7. Para todos los documentos que se reciban mediante esta contingencia prevalecerá la fecha y hora del sello. Para ello desde el Grupo de Gestión Documental se debe tener un control de los documentos recibidos.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


8. Para el caso de documentos de entrada urgentes allegados mediante correos electrónico institucional como: webmaster@supersociedades.gov.co el Grupo de Gestión Documental le pondrá una etiqueta al correo electrónico identificándolo como urgente y lo notificará al Coordinador de Grupo y al enrutador mediante correo electrónico o mediante la aplicación teams, o aquella aplicación que se encuentre disponible para su gestión.
9. Una vez restablecido el servicio se procederá con la radicación de aquellos correos electrónicos etiquetados como urgentes por parte del Grupo de Gestión Documental. En concordancia al (Acuerdo 001 de 2024 del AGN) velando así por la transparencia de la actuación administrativa. Para lo cual en el campo de referencia externa el radicador deberá dejar la anotación de la hora en que se recibió el documento, la fecha y de ver sello de recibido
10. En caso de presentarse pérdida de información por catástrofe natural u ocasionada por personas o deterioro de documentos por inadecuadas condiciones de preservación, se procedimientos a seguir implementados junto a la Dirección de Tecnología de la Información y las Comunicaciones, publicado en la caracterización del proceso de Gestión de Infraestructura y tecnologías de la información identificado como en GINT-G-008 Plan Recuperación.
11. Los documentos que se gestionen durante la contingencia manejarán el nivel de confidencialidad acorde con las tablas de retención documental y a la tabla de trámites de la Superintendencia de Sociedades.
12. Aquellos documentos físicos que cuenten con reserva documental, se deberán manejar en carpetas blancas de cuatro aletas o en su defecto carpetas rojas. Identificados con el rotulo de reserva.

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


13. Por ninguna circunstancia los documentos impresos marcados como confidenciales y/o reservados no deben ser reutilizados para impresión, escritura a mano o cualquier otro propósito.
14. En cada una de las dependencias deberán dar tratamiento especial a los documentos marcados con reserva documental, por el nivel de confidencial que se le ha conferido.
15. Con el propósito de oficializar su trámite y cumplir los términos de vencimiento de las comunicaciones oficiales, la Ley establece que SU RADICACIÓN ES DE CARÁCTER OBLIGATORIO, para lo cual, todos los documentos recibidos durante la contingencia deberán ser incorporados en el gestor documental de la entidad una vez restablecido el servicio.
16. Es claro que en los lineamientos de la entidad se establece que a los trámites que tengan Seguridad solo podrán acceder los funcionarios por su jerarquía, asignación y que por su competencia requieran de su consulta, la cual se podrá realizar de manera manual en los expedientes físicos. Para aquellas consultas muy urgentes que deban darse una prioridad alta y que solo encuentren digitalmente, a través de la Coordinación del Grupo de Gestión Documental y de la Dirección de Tecnología de la Información y las Comunicaciones se contactara al proveedor para su consulta urgente.

5.5.2.2. Actividades de Contingencia Tecnológica


Proceso	Subproceso	Actividad	Responsable
---------	------------	-----------	-------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública


Gestión de Tecnología de la Información y las Comunicaciones	Soporte de Gedess	<ol style="list-style-type: none"> 1. Informar al líder funcional sobre el evento de indisponibilidad del Gestor Documental Gedess. 2. Realizar pruebas de funcionalidad técnica del Gestor Documental Gedess antes y después de un evento. 3. Informar al líder funcional sobre el retorno a la normalidad. 	Líder de Aplicaciones
--	-------------------	---	-----------------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


Gestión de Tecnología de Información y Comunicaciones	de Coordinación de la Seguridad Informática Forense	<ol style="list-style-type: none"> 1. Preparar las condiciones de seguridad para la plataforma de contingencia que se implemente en caso de incidente de indisponibilidad de Gedess. 2. Coordinar la ejecución de las actividades de prueba de 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. 	Líder Seguridad Perimetral
---	---	--	----------------------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


<p>Gestión de Tecnología de Información y Comunicaciones</p>	<p>de la Innovación y de las Arquitecturas de Aplicaciones</p>	<p>de y de</p> <ol style="list-style-type: none"> 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 las actividades Operativas de contingencia definidas. 5. Coordinar ejecución y reporte de resultados, de las actividades de contingencia de su grupo de trabajo. 	<p>Líder aplicaciones</p>
--	--	--	---------------------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


<p>Gestión de Tecnología de Información y Comunicaciones</p>	<p>Director de Tecnología de Información y Comunicaciones</p>	<ol style="list-style-type: none"> 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 avance de actividades de contingencia. 	<p>Líder Contingencia</p>
--	---	--	---------------------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública


<p>Gestión de Tecnología de la Información y las Comunicaciones</p>	<p>Coordinador de Sistemas y Arquitectura Tecnológica</p>	<p>de y</p> <ol style="list-style-type: none"> 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 comunicaciones en periodo de contingencia. 	<p>Líder Infraestructura</p>
---	---	--	------------------------------

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

		7. Revisar y garantizar el correcto funcionamiento del Gestor Documental Gedess de acuerdo con las causas del incidente presentado para dar la respectiva solución.	
Gestión de Tecnología de Información y las Comunicaciones	de Coordinador de Sistemas y de Arquitectura Tecnología	<p>1. Registrar reporte de evento presentado y escalar hacia el área encargada de solucionar problema.</p> <p>2. Informar al líder funcional el número de ticket asignado.</p> <p>3. Registrar cierre del evento cuando se confirme la solución.</p>	Líder de Infraestructura - Coordinador de mesa de servicios
Gestión de Tecnología de Información y las Comunicaciones	de Oficial de Seguridad de la Información	<p>1. Verificar ejecución del plan de contingencia.</p> <p>2. Participar en la toma de decisiones que se den para ajustar el plan contingencia durante su ejecución.</p>	Líder de Seguridad de la Información

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

<p>Gestión de Tecnología de Información y Comunicaciones</p>	<p>de la Innovación y de las Arquitecturas de Aplicaciones</p>	<p>de y de</p> <ol style="list-style-type: none"> 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 del Gestor documental. 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. 	<p>Líder de Aplicaciones</p>
--	--	---	------------------------------


	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública

5.5.3. Recuperación del servicio

Una vez se restablezca el funcionamiento del Gestor Documental se deben ejecutar las siguientes actividades:

5.5.3.1. Actividades de retorno

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	<ol style="list-style-type: none"> Solicitar a mesa de ayuda sobre el cierre del evento. Informar al Líder de Contingencia sobre retorno a la normalidad Informar a Líder de Seguridad de la Información sobre retorno a la normalidad. Informar a usuarios finales el fin de la contingencia. Comunicar a Líder de Seguridad de la Información las lecciones aprendidas del evento. 	Líder de Aplicaciones
Gestión Documental		<ol style="list-style-type: none"> Valida integridad y consistencia de datos. Se cargan al sistema todas las operaciones registradas manualmente. 	Líder Funcional
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador Grupo de Sistemas y arquitectura tecnológica	<ol style="list-style-type: none"> Ejecutar diagnóstico completo para identificar causa raíz. Se realizan correcciones técnicas y pruebas controladas antes de liberar el sistema a producción 	Líder de Arquitectura
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	<ol style="list-style-type: none"> Comunicar a la alta dirección la finalización de la contingencia y retorno a la operación normal. Comunicar al Líder de Seguridad de la información las lecciones aprendidas y el informe de cierre del evento. 	Líder Contingencia

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública

Oficina Asesora de Planeación	Oficial de Seguridad de la Información	<ol style="list-style-type: none"> Consolidar a información de las lecciones aprendidas del evento. Velar porque se registren las lecciones aprendidas en la herramienta existente para este fin y se actualice la documentación correspondiente con el fin de fortalecer el presente plan de continuidad 	Líder Seguridad de la Información
Gestión de Tecnología de la Información y las Comunicaciones	Mesa de servicios	<ol style="list-style-type: none"> Registrar el cierre del evento. 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	<ol style="list-style-type: none"> Verificar monitoreo de servidores del Gestor Documental. 	Líder Seguridad perimetral


5.6. REGISTROS

- Formato GTI-FM-004_PlanPruebasde Contingencia Tecnológica
- Formato GTI-FM-025 Registro tratamiento de incidentes

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	23/12/2025	Se documenta el plan de contingencia del gestor documental

Elaboró	Revisó	Aprobó
Nombre: Fabián Leonardo Cargo: Contratista GIT Gestión de Proyectos de TI Fecha: 13/11/2025	Nombre: María José Rosales López Cargo: Coordinadora (E) Grupo de Gestión de proyectos de Ti Fecha: 13/11/2025	Nombre: Ricardo Fernélix Ríos Cargo: director de Tecnología de la Información y las Comunicaciones Fecha: 23/12/2025

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de la Información	Pública


7. ANEXOS

- Anexo 1. Directorio Telefónico

ANEXOS

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No.	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director Tecnologías de la información y las Comunicaciones	Ricardo Fernelix Ríos Rosales Rrios@supersociedades.gov.co	Director	X53000
2	Oficial de Seguridad de la Información	Ivan Alexis Ontibon Rojas iontibon@supersociedades.gov.co	Oficial de Seguridad de la Información	3118190986
3	Coordinación Innovación, Desarrollo y Arquitectura de Aplicaciones	Marisol Castiblanco Calixto MarisolCC@supersociedades.gov.co	Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones	X53301
4	Coordinación de Sistemas y Arquitectura de Tecnología	Ricardo Fernelix Ríos Rosales Rrios@supersociedades.gov.co	Coordinador Grupo de Sistemas y Arquitectura de la Información.	X53013
5	Apoyo Sistemas y Arquitectura de Tecnología	Deiber Alirio Ramírez daramirez@supersociedades.gov.co	Funcionario Grupo de Sistemas y Arquitectura de la Información.	X53153
6	Grupo Seguridad e Informática Forense	RocioPedrozo rociop@supersociedades.gov.co	Coordinador de Seguridad e Informática Forense	X53029
7	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
8	Grupo de Gestión de Proyectos de TI	Maria José Rosales Lopez mariarl@supersociedades.gov.co	Coordinador del Grupo de Proyectos de Tecnología	X54182

	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Código:	GTI-GU-024
		Versión:	001
	GUIA: PLAN DE CONTINGENCIA DEL GESTOR DOCUMENTAL	Fecha:	23/12/2025
		Clasificación de Información	la Pública