

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 1 de 23



Superintendencia de Sociedades



GUIA PLAN DE CONTINGENCIA BPM

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 2 de 23

1. INFORMACIÓN GENERAL

1.1 OBJETIVO

Dar a conocer el proceso contingencia ante la falla de la plataforma BPM generando indisponibilidad en los procesos automatizados

1.2 RESPONSABLE

Coordinador de Innovación, Desarrollo y Arquitectura de Aplicaciones.

1.3 ALCANCE

Este documento enmarca las actividades a ejecutar ante la indisponibilidad de los procesos automatizados sobre la plataforma BPM, permitiendo mantener en la entidad, la continuidad en la operación y gestión de estos procesos. Asimismo, en la protección de los sistemas y plataformas tecnológicas descritas en el siguiente link:

[Catalogo Aplicaciones_01_2023.xlsx \(sharepoint.com\)](#)

Servicios Tecnológicos:

- Correo Electrónico
- Intranet
- Internet
- Portal WEB
- VPN
- Telefonía
- Streaming

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

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 3 de 23

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: 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.

BPM: Sigla en inglés (Business Process Management), y hace referencia a una nueva categoría de software empresarial que permite a las empresas modelizar, implementar y ejecutar conjuntos de actividades interrelacionadas –es decir, Procesos– de cualquier naturaleza.

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.

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.

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 4 de 23

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.

2. CONDICIONES GENERALES

El Plan De Contingencia está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales de la Superintendencia de Sociedades.

2.1. 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 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 desastre no afectó simultáneamente el Centro de cómputo principal y el Centro de Cómputo Alterno.
- El Centro de Cómputo Alterno estará habilitado para un promedio de 100 usuarios concurrentes.
- Solo el funcionario responsable activará el plan de contingencia.
- Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.
- La realización de respaldos de las bases de datos e información se realiza de acuerdo a los procedimientos y frecuencias establecidas.

3. GUIA DEL PLAN DE CONTINGENCIA BPM

3.1. ESCENARIOS DE DESASTRE

Los escenarios de interrupción mayor o un evento contingente que contempla este documento guía se presentan ante no disponibilidad de la plataforma BPM por:

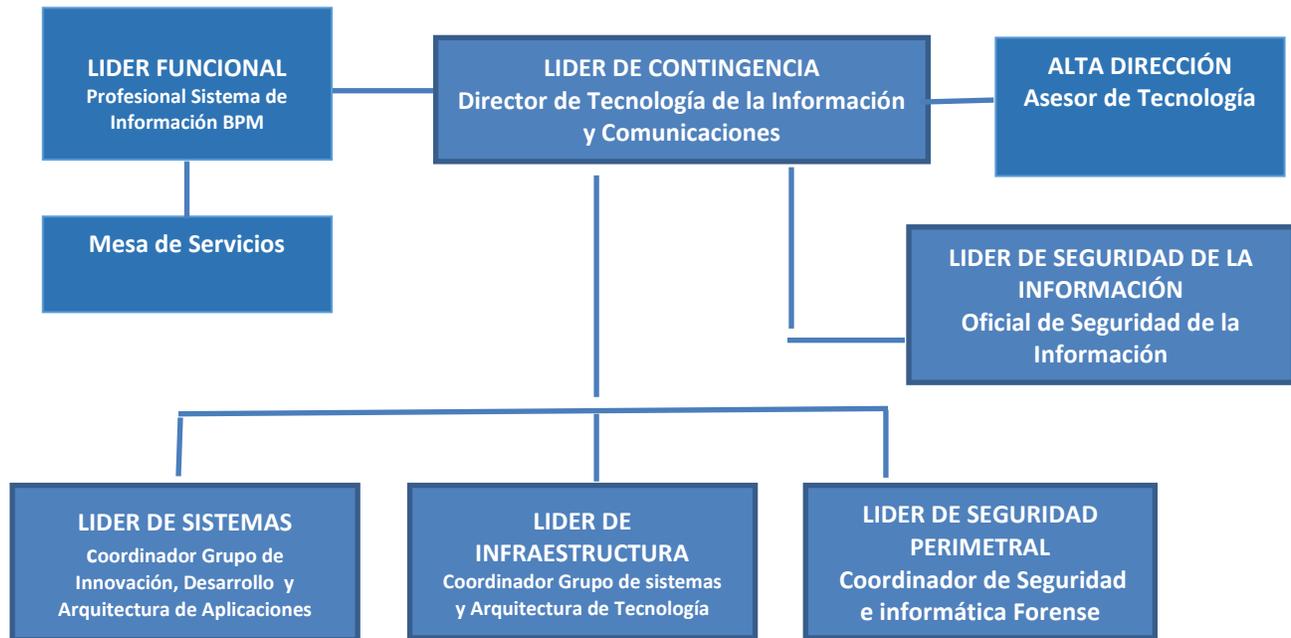
- Fallas técnicas en servidores de aplicación

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 5 de 23

- Fallas técnicas en servidores de Bases de datos
- Fallas técnicas en redes de comunicaciones
- Ataques informáticos

3.2. 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
LIDER FUNCIONAL Profesional Sistema de Información BPM	- Estar pendiente de las situaciones y eventos que puedan generar indisponibilidad de servicios de la aplicación de BPM.	- Comunicar al líder de Sistemas el evento de indisponibilidad que se presente. - Verificar la disponibilidad de la infraestructura propia asociada a los servicios de BPM para contingencia.	- Confirmar que todos los servicios requeridos para BPM estén funcionando. - Reportar los inconvenientes y

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 6 de 23

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	<ul style="list-style-type: none"> - Apoyar, conocer y dar Vo.Bo, al plan de contingencia de BPM. - Determinar la configuración técnica requerida para establecer una respuesta a contingencia de BPM. - Estar atento a los cambios en la infraestructura tecnológica, funcionarios y en los aplicativos conexos a BPM , a fin de actualizar el plan de recuperación ante desastres. 	<ul style="list-style-type: none"> - 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 Sistemas el estado de la contingencia durante el evento. 	<ul style="list-style-type: none"> - oportunidades de mejora del plan de contingencia de BPM respecto a las actividades a realizar con su equipo de trabajo. - Comunicar al líder de Seguridad de la Información, las lecciones aprendidas.
<p>LIDER DE SISTEMAS</p> <p>Coordinador de Innovación, Desarrollo y Arquitectura de Aplicaciones.</p>	<ul style="list-style-type: none"> - Asegurar el monitoreo del sistema de BPM. - 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 BPM. - Informar los resultados del monitoreo de los servicios de BPM. - Velar y conocer los resultados del soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de BPM. 	<ul style="list-style-type: none"> - Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. - Participar en la evaluación del evento contingente. - Coordinar la ejecución de las actividades de contingencia y recuperación de su equipo de trabajo. - Comunicar a los proveedores relacionados con el evento sobre la activación del plan de contingencia de BPM. - Mantener informado al Líder de Contingencia sobre el estado de contingencia y avance de las actividades de sus equipos de trabajo. - Colaborar con la información correspondiente para realizar las configuraciones requeridas en la activación de componentes alternos durante la contingencia 	<ul style="list-style-type: none"> - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de BPM respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de BPM que se hayan detectado respecto a la infraestructura tecnológica. - Entregar al líder de seguridad de la información las lecciones aprendidas del evento.

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 7 de 23

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	<ul style="list-style-type: none"> - Participar en el Análisis de impacto de eventos de servicios de BPM el RTO y RPO. - Contar con los ambientes de contingencia en caso de eventos de indisponibilidad de BPM. 		
<p>LIDER DE CONTINGENCIA</p> <p>Director de Tecnología de la Información y Comunicaciones</p>	<ul style="list-style-type: none"> - Velar por la actualización del plan de contingencia de BPM. - Velar por la actualización, distribución y pruebas del DRP - Gestionar la consecución de los recursos para el plan de contingencia de BPM. - Conocer a quien debe comunicar sobre la situación de contingencia. 	<ul style="list-style-type: none"> - Evaluar y activar el plan de contingencia para el evento de contingencia que se presente en BPM. - 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. 	<ul style="list-style-type: none"> - 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.
<p>LÍDER DE INFRAESTRUCTURA</p> <p>Coordinador Sistemas y Arquitectura de Tecnológica</p>	<ul style="list-style-type: none"> - Asegurar el monitoreo de los sistemas y componentes de la plataforma tecnológica de BPM. - Mantener la configuración técnica de la conectividad, bases de datos y servidores requerida en los servicios de BPM. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de los eventos 	<ul style="list-style-type: none"> - Participar en la evaluación del evento contingente. - Verificar por disponibilidad de la infraestructura propia asociada a los servicios de BPM 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 BPM. - Estar atentos para dar una correcta información a las personas que están 	<ul style="list-style-type: none"> - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de BPM respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de BPM que se hayan detectado respecto a la

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 8 de 23

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	<p>que ocurran en el sistema de BPM.</p> <ul style="list-style-type: none"> - Informar los resultados del monitoreo de los servicios de BPM. - Velar por el soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de BPM. - Participar en el Análisis de impacto de eventos de servicios de BPM para determinar el RTO y RPO. - Asegurar el respaldo de información y aplicación de BPM. - Contar con los ambientes de contingencia en caso de eventos de indisponibilidad de BPM. 	<p>participando en el plan de contingencia.</p> <ul style="list-style-type: none"> - 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. 	<p>infraestructura tecnológica.</p>
<p>LÍDER DE SEGURIDAD E PERIMETRAL</p> <p>Coordinador Grupo de Seguridad e Informática Forense.</p>	<ul style="list-style-type: none"> - Asegurar el monitoreo técnico de BPM. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de contingencia sobre BPM. - Coordinar el registro de los incidentes y su atención que se presenten sobre BPM. 	<ul style="list-style-type: none"> - Participar en la evaluación del evento contingente. - Verificar disponibilidad de los recursos involucrados en el sistema de información que se encuentran en contingencia y notificar a su personal para atender el evento. - 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. 	<ul style="list-style-type: none"> - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de BPM. - Solicitar, revisar y aprobar los cambios en la guía de contingencia de BPM. - Comunicar al líder de seguridad de la información, las lecciones aprendidas del evento.

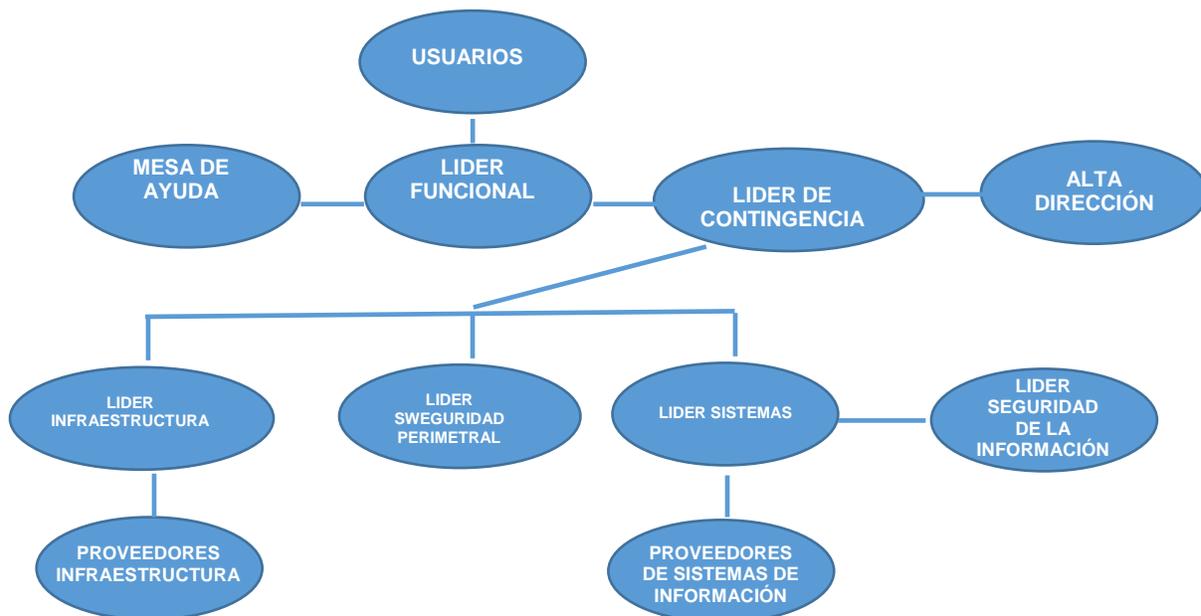
	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 9 de 23

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
<p>LIDER DE SEGURIDAD DE LA INFORMACIÓN</p> <p>Oficial de Seguridad de la Información</p>	<ul style="list-style-type: none"> - Liderar la creación del plan de contingencia de BPM y el Análisis de impacto para determinar el RTO y RPO. - Coordinar la publicación del plan de contingencia de BPM. - Gestionar la lectura y conocimiento del plan de contingencia para BPM, por parte de los grupos involucrados. 	<ul style="list-style-type: none"> - 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. 	<ul style="list-style-type: none"> - Verificar si se actualizó la guía de contingencia, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. - Verificar que las lecciones aprendidas están siendo actualizadas en la herramienta definida.
<p>MESA DE AYUDA</p>	<ul style="list-style-type: none"> - Conocer los planes de contingencia que existan y cuál es su participación. - Contar con un sistema de registro de eventos con un ticket automático. - Contar con los medios de comunicación efectivos para los funcionarios que desean reportar eventos. 	<ul style="list-style-type: none"> - Registrar los eventos que le reporten. - Reportar información sobre el Ticket asignado al evento. - Estar atentos a realizar actividades de remediación que les soliciten. 	<ul style="list-style-type: none"> - Cerrar evento cuando se lo comuniquen. - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia.

3.3. ÁRBOL DE LLAMADAS

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

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 10 de 23



Medios de comunicación: Correo electrónico, teléfono, celular, 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.

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

3.4.1 ¿Quién reporta un incidente, interrupción mayor o un evento Contingente?

- Por lo regular, los usuarios que utilizan el aplicativo BPM digital, deben reportar todos los eventos que se presenten sobre el funcionamiento o eventos que se presenten, acorde con los referenciado en el punto 3.1.1 escenarios de contingencias y que generen la indisponibilidad de estos servicios.
- 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

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 11 de 23

- Se disparen alarmas ambientales
- c. La mesa de ayuda debe atender el incidente de acuerdo a lo establecido en el Procedimiento GINT-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.

3.4.2 ¿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 en el 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.

- b. El Director de Tecnología de la Información y las Comunicaciones, en conjunto con los Coordinadores, 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 respecto 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.

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 12 de 23

3.4.3 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 servicio de:

RTO: 16 horas

RPO: 16 horas

3.5. 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.

- 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?

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACIÓN	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 13 de 23

- ¿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 por 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 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?

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 14 de 23

3.6. ACTIVIDADES DE MANTENIMIENTO

Es responsabilidad del Líder del plan de contingencia la actualización de las nuevas versiones y del envío de 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 sistema de BPM.	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 BPM.
2.	Cambio en el aplicativo de BPM 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 BPM 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 sistema de BPM

3.7. ACTIVIDADES DE PRUEBA

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 15 de 23

La programación y método por utilizar, en la realización de pruebas a la continuidad se deben relacionar en el formato GINT-F-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.

Pruebas de seguridad de la información a realizar

Las siguientes pruebas entre otras que se puedan desarrollar de seguridad de la información, deben tenerse en cuenta durante el desarrollo del plan de contingencia:

- El control de acceso físico
- El control de acceso lógico a las diferentes aplicaciones o infraestructuras involucradas 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.

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

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.

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 16 de 23

3.9. RECURSOS MÍNIMOS REQUERIDOS

La infraestructura mínima necesaria para soportar los procesos misionales de la entidad que serán recuperados en una contingencia es:

Cantidad	Componente	Descripción
2	Servidor base de datos	LSSVSQCL17\BPM LSSVSQCL04\BPM
4	Bases de datos	SQL SERVER 2016
4	Servidores de aplicación	SSWV1-BPM01 SSWV1-BPM02 SSWV1-BPM03 SSWV1-BPM04

4. ACTIVIDADES DE CONTINGENCIA

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

4.1. Proceso de Contingencia.

4.2. Actividades de contingencia funcionales:

Durante el tiempo de indisponibilidad de los procesos BPM, se deben llevar a cabo las siguientes actividades funcionales:

Proceso	Sistema	Actividad	Responsable
Radicación por Ventanilla	Postal	<ol style="list-style-type: none"> Los documentos de entrada que ingresen a través de ventanilla deben ser radicados y digitalizados a través de postal. Se debe enviar a las personas de soporte BPM el reporte de radicados indicando el proceso BPM al cual debe ser asociado. 	Gestión Documental
Gestión de procesos	Postal	<p>Debe usarse Postal como sistema de contingencia, para realizar las siguientes actividades:</p> <ol style="list-style-type: none"> Consulta de radicados de entrada y salida por sociedad o persona natural Proyección de borradores Revisión y firma de firma de documentos de salida Se debe enviar a las personas de soporte BPM la relación de documentos de salida indicando el 	Ponentes y coordinadores de Grupo

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 17 de 23

		número de radicado y el proceso al cual debe ser asociado.	
Pagos PSE	Manual	Se debe generar las cuentas de cobro manualmente y luego asociar los pagos a la plataforma BPM	Grupo de Cartera – Grupo de Tesorería

Actividades de contingencia tecnológicas:

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Soporte de BPM	<ol style="list-style-type: none"> 1. Informar al Líder funcional sobre el evento de indisponibilidad de BPM. 2. Realizar pruebas de funcionalidad técnica de BPM antes y después de un evento. 3. Informar al líder funcional sobre el retorno a la normalidad. 	Líder de Sistemas
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e 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 BPM. 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
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	<ol style="list-style-type: none"> 3. Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. 4. Comunicar al líder Seguridad de la Información sobre la situación que se presenta y confirmar si el evento supera el RTO. 	Líder Sistemas

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 18 de 23

Proceso	Subproceso	Actividad	Responsable
		<ol style="list-style-type: none"> Comunicar al Líder de Contingencia, la situación de contingencia presentada. Informar a los equipos de trabajo para actuar en contingencia. Coordinar ejecución y reporte de resultados, de las actividades de contingencia de su grupo de trabajo. 	
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	<ol style="list-style-type: none"> Evaluar reporte recibido y activar el plan de contingencia para el evento de contingencia que se presente. 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. 	Líder Contingencia
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura Tecnológica	<ol style="list-style-type: none"> Verificar funcionamiento de canales de comunicación. Verificar funcionamiento de switch CORE. Verificar funcionamiento de switchs de Piso. Verificar funcionamiento de red WAN con regionales. Verificar funcionamiento de la plataforma de distribución F5. Informar a líder de Seguridad Perimetral sobre estado de las comunicaciones en periodo de contingencia. Preparar la plataforma tecnológica requerida para el funcionamiento de contingencia de BPM. 	Líder Infraestructura
Gestión de Tecnología de la Información	Coordinador de Sistemas y	<ol style="list-style-type: none"> Registrar reporte de evento presentado y escalar hacia el área 	Coordinador de mesa de ayuda

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 19 de 23

Proceso	Subproceso	Actividad	Responsable
y las Comunicaciones	Arquitectura de Tecnología	encargada de solucionar problema. 2. Informar al líder funcional el número de tiquete asignado. 3. Registrar cierre del evento cuando lo reporten.	
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.	Oficial de Seguridad de la Información
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Innovación y Arquitectura de Aplicaciones	1. Realizar las pruebas de funcionamiento de los sistemas de información misionales y de apoyo. 2. Coordinar la ejecución de las guías de contingencia y pruebas. 3. Comunicar a los proveedores o desarrolladores la activación del plan de contingencia BPM. 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 Sistemas de Información

5. RETORNO A LA NORMALIDAD.

5.1. Actividades funcionales:

Una vez se restablezca la plataforma BPM y se tengan en operación los procesos BPM, se deben ejecutar las siguientes actividades:

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 20 de 23

Proceso	Sistema	Actividad	Responsable
Asociar Radicados de Entrada a Procesos	BPM	<ol style="list-style-type: none"> Se relacionan los documentos radicados de entrada y de salida a través del proceso administrativo de BPM. En caso de que correspondan a solicitudes nuevas se da inicio a un nuevo proceso, por el contrario, si corresponde a procesos existentes, se sube el documento al proceso correspondiente con su información de radicación. Se envía comunicación a las personas responsables del proceso informando la asociación de los radicados para continuar su gestión a través de BPM. 	Gestión Documental

5.2. Actividades Tecnológicas:

Una vez se restablezca el funcionamiento del sistema de BPM 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	<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 Oficial de seguridad de la información las lecciones aprendidas del evento. 	Líder Sistemas
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. Comunicar a Oficial de seguridad de la información las lecciones aprendidas del evento. 	Líder Contingencia
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. 	Líder Seguridad de la Información

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGÍAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 21 de 23

Proceso	Subproceso	Actividad	Responsable
		2.Velar porque se registren las lecciones aprendidas en la herramienta existente para este fin.	
Gestión de Tecnología de la Información y las Comunicaciones	Mesa de ayuda	1.Registrar el cierre del evento. 2.Informar al líder funcional sobre el cierre del evento.	Coordinador de mesa de ayuda
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1.Verificar monitoreo de servidores de aplicación de BPM.	Líder Seguridad perimetral

6. REGISTROS

- Formato GINT-F-004 Plan, Diseño, Ejecución y Evaluación de pruebas.
- Formato GINT-F-005 Análisis de impacto.

7. ANEXOS

- Anexo 1. Directorio Telefónico

8. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	27-09-2019	27-12-2020	Creación del documento	Líder de Seguridad de la información
002	8-12/2020	22-12-2021	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) en el punto 1.3, publicada en el SharePoint y la cual se encuentra actualizada. Se definen las pruebas de seguridad a realizar si es el caso	Coordinador grupo Innovación, Desarrollo Y Arquitectura De Aplicaciones
003	23-12-2021	27-06-2024	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. Se	Coordinador grupo Innovación, Desarrollo Y Arquitectura De Aplicaciones

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 22 de 23

			retiran actividades de la oficina asesora de planeación.	
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 GINT-G-010 Plan de recuperación ante desastres BPM por a GINT-G-010 PLAN DE CONTINGENCIA BPM. Se actualiza el Directorio Telefónico por cambios en estructura funcional y nuevos miembros de equipos. Cambio logo institucional.	Coordinador grupo Innovación, Desarrollo Y Arquitectura De Aplicaciones

Elaboró: Contratista de Seguridad e Informática Forense	Revisó: Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones	Aprobó: Directora de Tecnología de la Información y las Comunicaciones
Fecha: 26 de junio de 2024	Fecha: 27 de junio de 2024	Fecha: 27 de junio de 2024

	SUPERINTENDENCIA DE SOCIEDADES	Código: GINT-G-010
	SISTEMA GESTIÓN INTEGRADO	Fecha: 28 de junio de 2024
	PROCESO: GESTIÓN DE INFRAESTRUCTURA Y TECNOLOGIAS DE INFORMACION	Versión: 004
	GUIA: PLAN DE CONTINGENCIA BPM	Número de página 23 de 23

ANEXOS

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No.	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director Informática y Desarrollo	Mayra Isabel Gonzalez Núñez Mi Gonzalez@SUPERSOCIEDADES.GOV.CO	Director	3000
2	Oficial de Seguridad de la Información	Ivan ALEXIS Ontibon Roja iontibon@supersociedades.gov.co	Oficial de Seguridad de la Información	
3	Coordinación Innovación, Desarrollo y Arquitectura de Aplicaciones	Marisol Castiblanco Calixto MarisolCC@supersociedades.gov.co	Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones	3301
4	Coordinación de Sistemas y Arquitectura de Tecnología	Anderson López Cruz AndersonL@supersociedades.gov.co	Coordinador Grupo de Sistemas y Arquitectura de la Información.	3153
5	Grupo Seguridad e Informática Forense	Jeny Shirley Díaz González JenyD@supersociedades.gov.co	Coordinador de Seguridad e Informática Forense	4030
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