Superintendencia de Sociedades

PLAN DE CONTINGENCIA SISTEMA SIIF

1. INFORMACIÓN GENERAL

1.1 OBJETIVO

Oficializar la guía del plan de contingencia para el sistema SIIF generado por materialización de riesgos que generen indisponibilidad para el servicio.

1.2 RESPONSABLE

Dirección Financiera.

1.3 ALCANCE

Este documento enmarca las actividades a ejecutar ante la indisponibilidad del Sistema Integrado de Información Financiera (SIIF), que pertenece y es administrado por el Ministerio de Hacienda y por el cual se procesa toda la información financiera (contabilidad, presupuesto, tesorería) de la Superintendencia de Sociedades.

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

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

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

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

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

DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

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

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.

Plataforma tecnológica crítica: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

RAS: Sigla en inglés (Response Alternative and Solutions), y hace referencia a un documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

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

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

SIIF: Sistema Integrado de Información Financiera Nación es un sistema que coordina, integra, centraliza y estandariza la gestión financiera pública nacional, con el fin de propiciar una mayor eficiencia y seguridad en el uso de los recursos del Presupuesto General de la Nación.

2. CONDICIONES GENERALES

El contenido está enfocado no solo a la contingencia sobre la plataforma tecnológica que soporta el proceso Financiero y Contable de la Superintendencia de Sociedades, sino, a los aspectos funcionales de continuidad en el caso de no ser posible la conexión al Sistema de Información Integrado Financiero de la Nación (SIIF).

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

y el oportuno registro de la información financiera en el sistema SIIF, 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 la contingencia.
- Solo el funcionario responsable activará la 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.
- El sistema SIIF siempre estará en funcionamiento.

3. GUIA DEL PLAN DE CONTINGENCIA PARA EL SISTEMA SIIF.

3.1. ESCENARIOS DE CONTINGENCIAS

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

3.1.1. Infraestructura Física:

No disponibilidad de acceso por diferentes motivos como emergencias sanitarias, asonadas, desorden público y paros, a:

- Sector del Centro Administrativo Nacional (CAN)
- Edificio Supersociedades
- Oficina de Dirección Financiera

3.1.2. Infraestructura de Comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en:

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

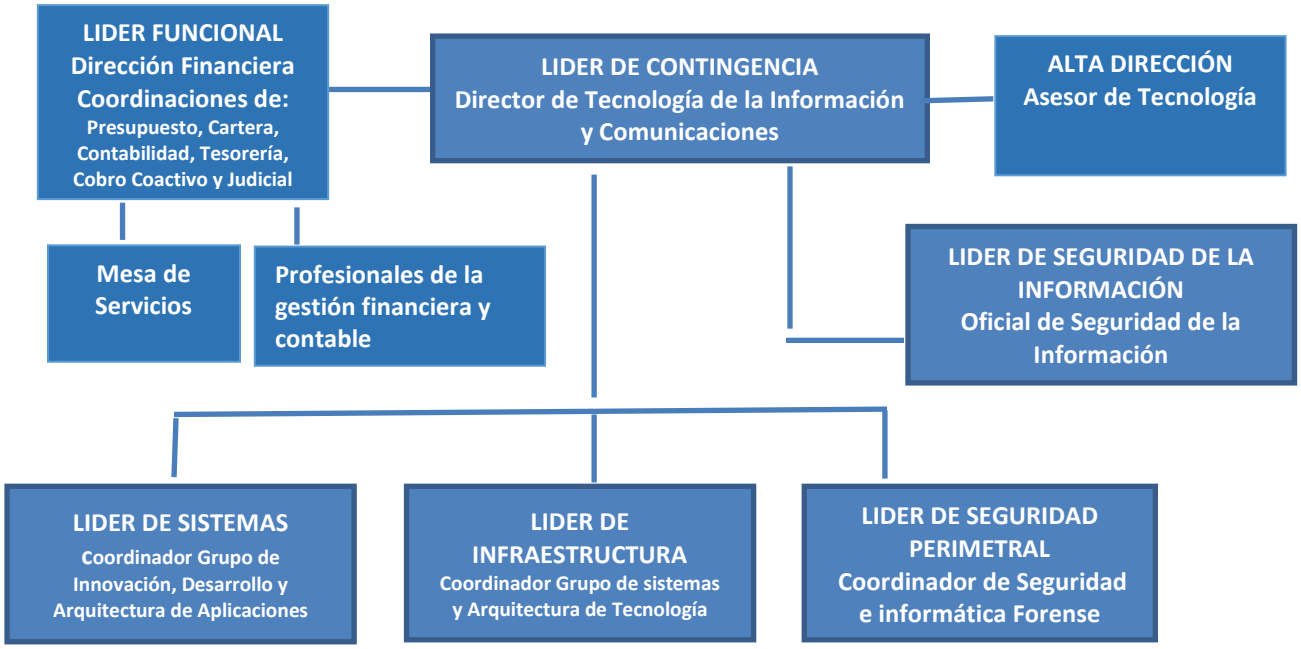
3.1.3. Servicios tecnológicos.

No disponibilidad del Sistema SIIF por:

- Bloqueo de usuarios
- Virus informáticos en equipos de funcionarios
- Fallas en sistemas operativos
- Daño en certificados digitales (tokens)

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 Dirección Financiera	- Estar pendiente de las situaciones y eventos que puedan generar indisponibilidad del sistema SIIF. - Conocer las actividades del plan de continuidad en caso de indisponibilidad del sistema SIIF y otros sistemas soporte de la actividad financiera y contable SIIF. - Tramitar trabajo en casa para profesionales del área que trabajen con SIIF.	- Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. - Comunicar al líder de Continuidad del negocio sobre cualquier indisponibilidad que se presente y confirmar si el evento supera el RTO. - Preparar los equipos de trabajo para actuar en contingencia por teletrabajo.	Confirmar que todos los servicios requeridos para para el uso del sistema SIIF funcionan.
LIDER DE SISTEMAS Coordinador de Innovación, Desarrollo y Arquitectura de Aplicaciones.	- Asegurar el monitoreo del sistema SIIF. - 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 SIIF. - Informar los resultados del monitoreo de los servicios de SIIF. - Velar y conocer los resultados del soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de SIIF. - Participar en el Análisis de impacto de eventos de servicios de SIIF el RTO y RPO. - Contar con los ambientes de	- 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 SIIF. - 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	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de SIIF respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de SIIF que se hayan detectado respecto a la infraestructura tecnológica. - Entregar al líder de seguridad de la información las lecciones aprendidas del evento.

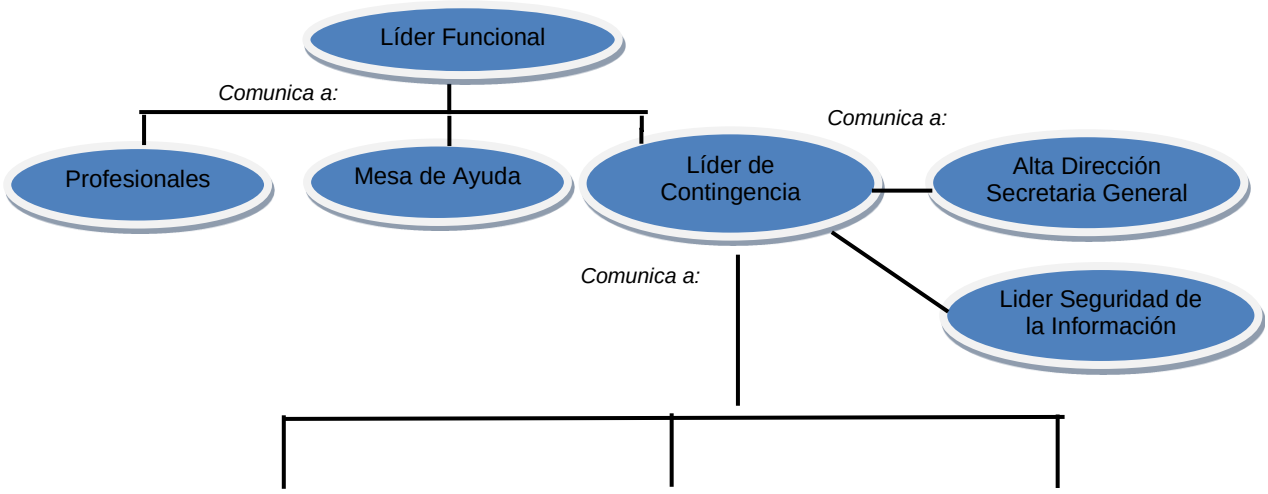
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	contingencia en caso de eventos de indisponibilidad de SIIF.		
LIDER DE CONTINGENCIA Director de Tecnología de la Información y Comunicaciones	- Velar por la actualización del plan de contingencia de SIIF. - Velar por la actualización, distribución y pruebas del plan de contingencia. - Gestionar la consecución de los recursos para el plan de contingencia de SIIF. - 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 SIIF. - Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. - Liderar la operación bajo contingencia. - Comunicar a la alta dirección y Secretaria General 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.
LÍDER DE INFRAESTUCTURA Coordinador Sistemas y Arquitectura de Tecnológica	- Asegurar el monitoreo de los sistemas y componentes de la plataforma tecnológica de SIIF. - Mantener la configuración técnica de la conectividad, bases de datos y servidores requerida en los servicios de SIIF. - 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 SIIF. - Informar los resultados del monitoreo de los servicios de SIIF. - Velar por el soporte y mantenimiento vigente para la infraestructura Tecnológica de servicios de SIIF. - Participar en el Análisis de impacto de eventos	- Participar en la evaluación del evento contingente. - Verificar la disponibilidad de la infraestructura propia y de comunicaciones asociada a teletrabajo y sus servicios involucrados en SIIF 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 SIIF. - Monitorear trabajo en casa de los funcionarios del área financiera durante la 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.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de SIIF respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de SIIF 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
	de servicios de SIIF para determinar el RTO y RPO. - Asegurar el respaldo de información y aplicación de SIIF. - Contar con los ambientes de contingencia en caso de eventos de indisponibilidad de SIIF.		
LÍDER DE SEGURIDAD E PERIMETRAL Coordinador Grupo de Seguridad e Informática Forense.	- Asegurar el monitoreo técnico de SIIF. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de contingencia sobre SIIF. - Coordinar el registro de los incidentes y su atención que se presenten sobre SIIF.	- Participar en la evaluación del evento contingente. - Verificar disponibilidad de los recursos involucrados en el sistema SIIF 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.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de SIIF. - Solicitar, revisar y aprobar los cambios en la guía de contingencia de SIIF. - Comunicar al líder de seguridad de la información, las lecciones aprendidas del evento.
LIDER DE SEGURIDAD DE LA INFORMACIÓN Oficial de Seguridad de la Información	- Liderar la creación del plan de contingencia de SIIF y el Análisis de impacto para determinar el RTO y RPO. - Coordinar la publicación del plan de contingencia de SIIF. - Gestionar la lectura y conocimiento del plan de contingencia para SIIF, 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 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.
MESA DE AYUDA	- Conocer los planes de contingencia que existan y cuál es su participación.	- Registrar los eventos que le reporten.	- Cerrar evento cuando se lo comuniquen.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	- 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.	- Reportar información sobre el ticket asignado al evento. - Realizar actividades de remediación que les soliciten.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia.
Profesionales de la Gestión Financiera y contable	- Conocer el plan de continuidad a aplicar en caso de contingencia - Participar en las pruebas del plan de continuidad. - Probar el funcionamiento de los computadores personales asignados para el trabajo normal o teletrabajo o trabajo en casa.	- Iniciar actividades alternas de operación del SIIF. - Realizar pruebas de acceso y funcionamiento de los sistemas e infraestructura alterna de operación del SIIF. - Certificar conexión al SIIF, acorde con las actividades alternas. - Iniciar uso del sistema SIIF en contingencia. - Probar certificados y firmas digitales. - Informar a líder funcional sobre funcionamiento de actividades alternas de operación del SIIF.	- Reportar los inconvenientes y oportunidades de mejora del plan de continuidad o del DRP.

3.3. ÁRBOL DE LLAMADAS

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



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

Los datos de contacto para los funcionarios que ejercen estos roles se encuentran en los documentos de la Dirección de Tecnología de la Información y las Comunicaciones, ver Anexo 1.

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

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

Los funcionarios de la Dirección Financiera, Coordinadores de grupos de Presupuesto Cartera, Contabilidad, Tesorería y Cobro Coactivo y Judicial:

a. deben reportar a la mesa de ayuda el incidente cuando:

- No es posible la conexión a la plataforma SIIF.
- No hay red de comunicaciones.
- No hay servicio de internet.
- No funcionen los certificados digitales
- No funcionen las firmas digitales
- CUALQUIER otro evento de tecnología o funcional que afecte el uso del sistema SIIF.

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

- Se detecta caída de servicios de comunicaciones que afecte el uso de sistema SIIF.
- Se detecta mal funcionamiento de infraestructura critica (servidores, dispositivos de comunicaciones, conexiones remotas, Firewall)

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 la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al sistema SIIF.

En cualquiera de los casos, debe escalarlo a los funcionarios responsables.

3.4.2 ¿Quién evalúa la magnitud e impacto del incidente?

a. Para el caso de un evento tecnológico, 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.

b. Para el caso de un evento funcional, el Subdirector Financiero o los coordinadores de Presupuesto, Tesorería, Contabilidad, Cartera, Cobro Coactivo y Judicial, deben realizar un diagnóstico sobre el incidente presentado, teniendo y ejecutar las siguientes acciones:

- Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta.
- Comunicar al líder de Continuidad sobre la situación de indisponibilidad que se presenta.
- Preparar los equipos de trabajo para actuar en contingencia.
- Tiempo estimado de solución del incidente.

3.4.3 Análisis de Impacto.

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

RPO: 0 - 8 horas
RTO: 0 - 8 horas

Este RPO y RTO se asigna a cada uno de los sistemas de información involucrado en el servicio de Gestión Financiera y contable, tal como se refleja en el anexo 1 numeral **Tipo de componente: Aplicaciones.**

De acuerdo con esto, si se debe activar el plan de contingencia, la responsabilidad recaería de la siguiente manera:

a. En caso de evento tecnológico:

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

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

El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma tecnológica no disponible, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones alternas.
- Realizar pruebas sobre los sistemas de comunicación.
- Configuración de componentes alternos para SIIF.

El Director de Tecnología de la Información y las Comunicaciones, comunica el incidente al líder funcional, indicando el nivel y tiempo de atención del incidente.

b. En caso de evento funcional:

El Subdirector Financiero o los coordinadores de Presupuesto, Tesorería, Contabilidad, Cartera, Cobro Coactivo y Judicial, definen si se activa el plan de contingencia, teniendo en cuenta los siguientes aspectos:

- El evento de no uso del sistema SIIF va a durar más de 8 horas.
- La afectación de componentes propios de la operación por más de 8 horas.
- Imposibilidad de acceso a las oficinas de la Dirección.
- Regulaciones emitidas por el gobierno nacional en caso de emergencias sanitarias, económicas, ambientales o de conflictos.

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

a. En caso de un evento tecnológico:

El Líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:

Si el evento afectó las comunicaciones.

- Configurar el Switch de contingencia, en caso de falla en el switch de Core.
- Contactar al proveedor de comunicaciones, en caso de falla en router de conexión con intendencias, falla en router ubicado en cada intendencia, falla en enlaces con ISP, o falla en enlace con intendencias regionales.

- Enrutar el tráfico por los demás switches que componen el stack, en caso de una falla de la fibra óptica de uno de ellos.
- Utilizar el switch de piso como contingencia ante falla de un switch de piso en un centro de cableado.
- Configurar el firewall de contingencia, en caso de falla del equipo principal.

Si el evento no afectó las comunicaciones, pero no se puede acceder físicamente a las instalaciones.

Configurar los componentes de seguridad perimetral, antivirus, navegadores, tokens y firmas digitales requeridos en los computadores personales.

b. En caso de un evento funcional:

Si el evento afecto la infraestructura física o el acceso a las áreas de la Dirección Financiera y Contable, el lider, El Subdirector Financiero o los coordinadores de Presupuesto, Tesorería, Contabilidad, Cartera, Cobro Coactivo y Judicial, deben realizar las actividades de conexión desde los computadores personales.

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.

3.5.1 Para el caso de eventos tecnológicos:

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

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

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

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

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

3.5.2 Para el caso de eventos funcionales:

a. El Subdirector Financiero, comunica a la Alta Dirección, teniendo en cuenta los siguientes aspectos:

- Evento presentado
- Hora de inicio
- Posible duración
- Promedio diario de atención
- Hora de inicio de la operación de contingencia

b. 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?

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 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 por considerar en la comunicación de la crisis pueden ser:

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

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 POSTAL.	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 POSTAL.
2.	Cambio en el aplicativo de POSTAL por nuevas versiones o reemplazo.	Lideres de los grupos de la Dirección de Tecnología de la	Cuando se realice cambio de versión del sistema de POSTAL o nueva aplicación

No	Actividad	Responsable	Frecuencia
		Información y las Comunicaciones. Oficial de Seguridad de la Información	
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 POSTAL
4.	Cambios en la configuración de SIIF Nación de acuerdo con el documento **MANUAL TÉCNICO DE RECOMENDACIONES DE CONFIGURACIÓN SIIF NACIÓN**	Lider de Infraestructura Lider de redes y comunicaciones	Permanente
5.	Cambios en el esquema de conexión con SIIF Nación o en la configuración de VPNSSL con el Ministerio de Hacienda, acorde con lo establecido en el documento: **Instructivo para la configuración de Clientes del SIIF Nación**	Lider de Infraestructura Lider de redes y comunicaciones	Permanente
6.	En el momento en que se presente una falla en el canal del Ministerio de Hacienda y Crédito Público MHCP – Sitio Principal, acorde con el documento: **Canales de Contingencia para SIIF Nación**	Lider de Infraestructura Lider de redes y comunicaciones	Permanente
7.	Actualizaciones a la conectividad – SIIF Nación, siguiendo las recomendaciones del documento:	Lider de Infraestructura Lider de redes y comunicaciones	Semestral o cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia.

No	Actividad	Responsable	Frecuencia
	Actualizar Conectividad - SIIF Nación		

3.7. ACTIVIDADES DE PRUEBA

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 CONTINUIDAD SIIF.

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.

3.9. RECURSOS MÍNIMOS REQUERIDOS

La infraestructura necesaria para soportar el proceso de uso del sistema SIIF es la siguiente la cual está definida en los instructivos y manuales emitidos por el Ministerio de Hacienda y Crédito Público – SIIF Nación:

3.9.1. Requisitos técnicos de hardware para configuración de clientes SIIF Nación.

Los requisitos mínimos de Hardware con los que debe contar una máquina ***cliente*** del SIIF NACION para operar adecuadamente el aplicativo son:

Un portátil o equipo de cómputo de escritorio que este configurado con la línea base de la Superintendencia de Sociedades (hardware y software) y que preferiblemente sea suministrado por la entidad. Este equipo debe tener los siguientes requisitos acorde con el "**Instructivo para la configuración de Clientes del SIIF Nación"** entregado por el Ministerio de Hacienda y Crédito público.

- **Procesador**: Mínimo 1.2 GHz. Recomendable 2.2 GHz o superior para descargar reportes
- **Memoria**: Mínimo 4 GB. Se recomienda 8 GB o Superior para la exportación de reportes y carga de archivos.
- **Pantalla**: Resolución Mínima de 1600 x 900 Pixeles o Superior
- **Tarjeta de red**: Ethernet 10/100/1000 o Inalámbrica 802.11b/g/a/n (según infraestructura de cada cliente)
- **Disco Duro**: Mínimo 100 MB libres.
- **Puerto USB:** para soportar certificados Digitales en físico.

3.9.2. Requisitos técnicos de software para configuración de clientes SIIF Nación.

El software base con el que debe contar una estación cliente para operar adecuadamente el SIIF Nación y las configuraciones que deben estar habilitadas en dicha máquina son:

- **Navegador:** Google Chrome (RECOMENDADO) e Internet Explorer 11.

- **Actualizaciones:**

a) Windows 8.1, deben tener instalado todos los parches. Este Sistema Operativo tiene soporte extendido oficial por Microsoft hasta el 10 de enero del 2023.

b) Windows 10, deben tener instalado todos los parches

- **Instalar el componente para la firma digital**

Leer y seguir la guía de instalación y configuración "SIIF - Guía para Actualizar Componente de Firma Digital" publicada en la página Web del SIIF Nación ubicada en Aspectos Técnicos.

- **Controlador del dispositivo de almacenamiento del certificado digital (Token)**

Los usuarios del SIIF Nación que utilizan como medio de almacenamiento del certificado digital un dispositivo criptográfico (token), previo a su utilización en el SIIF Nación, deben solicitar al personal de soporte técnico de la entidad usuaria realizar la instalación de los controladores de acceso al dispositivo. Estos controladores y el soporte para su instalación los deberá proveer la Autoridad de Certificación Digital emisora del certificado digital.

- **Herramienta para la firma digital de archivos utilizados para cargas masivas de datos al SIIF Nación**

Los usuarios del SIIF Nación que utilizan los procesos de carga masiva de datos al SIIF Nación, deben firmar digitalmente los archivos a cargar. Por lo cual el soporte técnico de la entidad usuaria deberá realizar la instalación del aplicativo suministrado por la Entidad Certificadora para tal fin.

Este aplicativo y el soporte para su instalación los deberá proveer la Autoridad de Certificación digital emisora del certificado.

- **Navegador.**

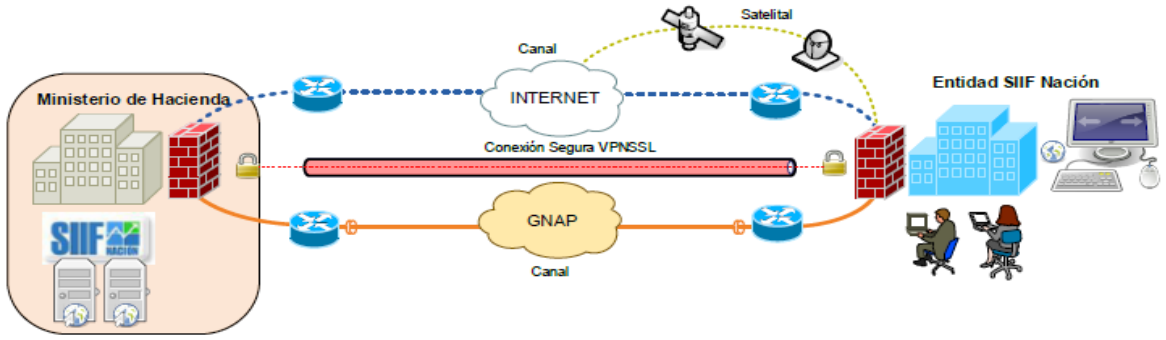
De acuerdo con el Instructivo para la configuración de Clientes del SIIF Nación, se deben verificar los siguientes aspectos:

- Verificar versión del navegador
- Configuración de PopUp:
- Vista de compatibilidad.

- Barras de Google y Yahoo! estén bloqueadas
- Activación Active X
- Eliminar Caché
- Verificar que Opción de Autocompletar no este chequeada
- Configuración de los Sitios de confianza

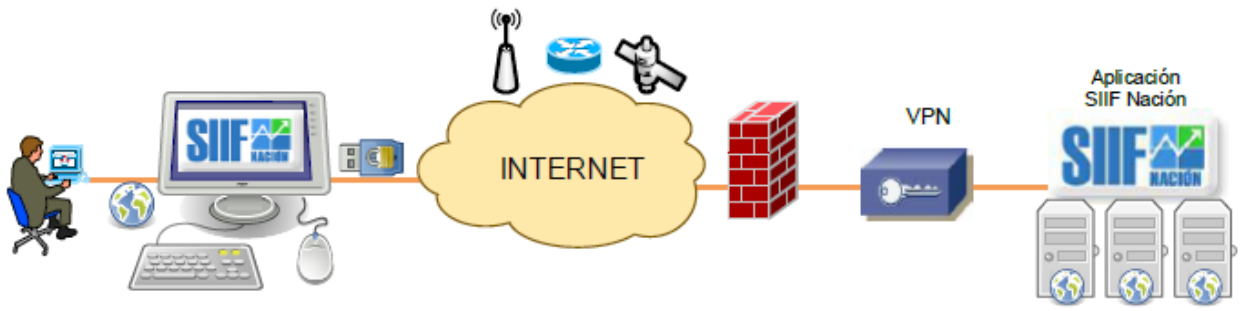
3.9.3.Requisitos de Comunicación.

El Sistema Integrado de Información Financiera de la Nación (SIIF Nación) es un sistema centralizado, soportado sobre una solución WEB administrada por el Ministerio de Hacienda y Crédito Público. En el siguiente grafico se refleja esta situación:



La Superintendencia de Sociedades accederá al SIIF Nación por medio un Portal Seguro, con una Red Virtual Privada (VPN SSL) donde los datos viajan cifrados y encapsulados a través de Internet, de esta manera se garantiza que los datos no puedan ser descifrados, leídos o modificados durante su trasmisión.

En el caso de la Superintendencia de Sociedades, como se usa el canal de Internet, se debe verificar esta configuración y su seguridad. El siguiente grafico refleja la conectividad:



Las verificaciones por realizar son:

En caso de que la salida a Internet y/o GNAP sea a través de un **Firewall o un servicio proxy server** este debe verificar:

Para **portal2.siifnacion.gov.co**
Dirección Destino: 190.60.77.91
Puerto de Servicio: TCP 443 (https), TCP 80 (http)

4. ACTIVIDADES DE CONTINGENCIA

A continuación, se definen las guías o pasos a seguir para trabajar en contingencia mientras se recuperan los componentes de la plataforma tecnológica afectados:

4.1. Infraestructura Física:

4.1.1 No disponibilidad de acceso a área de trabajo por diferentes motivos como emergencias sanitarias, asonadas, desorden público, paros y otros eventos de conmoción publica, a:

EVENTO	ESTRATEGIA
Sector del Centro Administrativo Nacional (CAN)	Trabajo en casa
Edificio Supersociedades	Trabajo en casa
Oficina de Dirección Financiera	Trabajo en casa

4.1.2 Actividades Funcionales.

Proceso	Subproceso	Actividad	Responsable
Gestión Financiera y Contable	Contabilidad, Presupuesto, Tesorería, Cartera, Cobro Coactivo y Judicial	1. Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. 2. Comunicar al líder de Continuidad del negocio sobre la situación que se presenta y confirmar si el evento supera el RTO.	Subdirector Financiero

Proceso	Subproceso	Actividad	Responsable
		3. Comunicar a Director Operativo de SIIF Nación, la situación de contingencia presentada. 4. Preparar los equipos de trabajo para actuar en contingencia	
Gestión Financiera y Contable	Contabilidad, Presupuesto, Tesorería, Cartera, Cobro Coactivo y Judicial	1. En caso de activación del plan de contingencia, dirigirse a sus hogares. 2. Realizar Pruebas de funcionamiento de equipos personales y la conexión al SIIF 3. Realizar pruebas de funcionamiento de certificado digital (token) y de firma digital (para autorizados). 4. Realizar pruebas de funcionamiento de aplicativo SIIF. 5. Probar acceso con usuarios normales. 6. Probar opciones autorizadas o perfil autorizado. 7. Trabajar bajo modalidad de contingencia.	Subdirector Financiero Coordinadores de grupo Equipos de trabajo

4.1.3 Actividades Funcionales.

Proceso	Subproceso	Actividad	Responsable
Coordinación de Sistemas y Arquitectura de Tecnología	Mesa de Ayuda	1. Registrar reporte de indisponibilidad y escalar hacia el área encargada de solucionar problema. 2. Realizar revisión técnica de los recursos mínimos requeridos en los equipos de los funcionarios que trabajaran desde el hogar, acorde con el numeral 3.9 del presente documento. (tarea a realizar por acceso remoto).	Coordinador de Sistemas y Arquitectura de Tecnología

4.2. Infraestructura de comunicaciones:

No disponibilidad de los servicios de comunicaciones por fallas en Switchs core, Fibras ópticas de conexión con centros de cableado, Switch de piso, Enlaces de comunicación con ISP, Firewall, Falla en la conexión con Internet.

4.2.1 Actividades Tecnológicas.

Proceso	Subproceso	Actividad	Responsable
Coordinación de Sistemas y Arquitectura de Tecnología	Seguridad Perimetral	1. Verificar funcionamiento de conexión VPN con SIIF nación Ministerio de Hacienda y Crédito Público. 2. Verificar funcionamiento Firewall principal, en caso de fallas realizar conexión de firewall alterno hacia SIIF Nación. 3. Si no hay conectividad, informar por correo electrónico a la Coordinación de Sistemas y Arquitectura de Tecnología.	Líder Seguridad Perimetral
Coordinación de Sistemas y Arquitectura de Tecnología	Comunicaciones	1. Verificar funcionamiento de canal principal de canal de internet en caso de falla activar alterno. 2. Verificar switch CORE en caso de fallas de switch principal realizar la conexión a switch alterno. 3. Verificar switch de Piso en caso de fallas realizar actividades de cambio de switch y configuración para los equipos de los funcionarios de la Dirección Financiera y Contable. 4. En caso de falla total de comunicaciones y cuya solución dure más de 8 horas, reportar a la Coordinación de Sistemas y Arquitectura de Tecnología, para que se coordine actividades de trabajo desde el hogar.	Líder Comunicaciones
Coordinación de Sistemas y Arquitectura de Tecnología	Mesa de Ayuda	1. Registrar reporte de evento presentado y escalar hacia el área encargada de solucionar problema.	Coordinador de Sistemas y Arquitectura de Tecnología

Proceso	Subproceso	Actividad	Responsable
		2. Realizar revisión de los requisitos mínimos de hardware, software y comunicaciones en los equipos de los funcionarios de la Dirección Financiera y Contable. 3. Informar al Coordinador de sistemas y Arquitectura de Tecnología los resultados de la revisión.	
Líder de Contingencia	Coordinación de Seguridad e Informática Forense	1. Comunicar al líder funcional el estado de contingencia y el avance de actividades de contingencia. 2. Liderar actividades de contingencia tecnológica.	Coordinador de Seguridad e Informática Forense
Líder Funcional	Dirección Financiera y Contable	1. Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. 2. Comunicar al líder de Continuidad del negocio sobre cualquier contingencia que se presente, su estado y confirmar si el evento supera el RTO. 3. Preparar los equipos de trabajo para actuar en contingencia	Subdirector Financiero
Líder de Continuidad Tecnológica y Seguridad de la Información.	Gestión de Infraestructura y Tecnologías de la Información	1. Determinar el arranque del plan de contingencia. 2. Verificar ejecución del plan de contingencia. 3. Participar en la toma de decisiones que se den para ajustar el plan de contingencia durante su ejecución. 4. Informar a la alta dirección sobre estado de contingencia. 5. Coordinar retorno a la normalidad.	Director de Tecnología de la Información y las Comunicaciones
Gestión Financiera y Contable	Coordinaciones de Contabilidad, Presupuesto,	- Iniciar actividades alternas de operación del SIIF.	Profesionales de la Gestión Financiera y contable

Proceso	Subproceso	Actividad	Responsable
	Tesorería, Cartera, Cobro Coactivo y Judicial	- Realizar pruebas de acceso y funcionamiento de los sistemas e infraestructura alterna de operación del SIIF. - Certificar conexión al SIIF, acorde con las actividades alternas. - Iniciar uso del sistema SIIF en contingencia. - Probar certificados digitales y firmas digitales. - Informar a líder funcional sobre funcionamiento de actividades alternas de operación del SIIF.	

5. RETORNO A LA NORMALIDAD.

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

5.1 Actividades de retorno Funcional.

Una vez se restablezca la situación de acceso al CAN, a la Superintendencia de Sociedades y a las oficinas de la Dirección Financiera, los funcionarios del proceso de Gestión Financiera y Contable deben ejecutar las siguientes actividades:

Proceso	Subproceso	Actividad	Responsable
Gestión Financiera y Contable	Contabilidad, Presupuesto, Tesorería, Cartera, Cobro Coactivo y Judicial	1. Acudir al sitio de trabajo en las oficinas habituales. 2. Realizar Pruebas de funcionamiento de equipos de trabajo de oficina y la conexión al SIIF 3. Realizar pruebas de funcionamiento de certificado digital (token) y de firma digital (para autorizados). 4. Realizar pruebas de funcionamiento de aplicativo SIIF. 5. Probar acceso con usuarios normales. 6. Probar opciones autorizadas o perfil autorizado. 7. Trabajar bajo modalidad de contingencia. 8. Iniciar labores normales.	Director Financiero Coordinadores de grupo Funcionarios del proceso de Gestión Financiera y Contable

Proceso	Subproceso	Actividad	Responsable
Coordinación de Sistemas y Arquitectura de Tecnología	Mesa de ayuda	1. Cerrar reporte de evento registrado 2. Informar a Coordinador correspondiente.	Coordinador de Sistemas y Arquitectura de Tecnología

5.2 Actividades de retorno tecnológico.

Una vez se restablezca el servicio en los componentes afectados de la plataforma tecnológica, se deben ejecutar las siguientes actividades:

Proceso	Subproceso	Actividad	Responsable
Coordinación de Sistemas y Arquitectura de Tecnología	Seguridad Perimetral	1. Verificar funcionamiento Normal de conexión VPN con SIIF nación Ministerio de Hacienda y Crédito Público. 2. Verificar funcionamiento Firewall principal para la conexión con SIIF Nación. 3. Revisar funcionamiento de Internet, en ruta normal.	Coordinador de Sistemas y Arquitectura de Tecnología
Coordinación de Sistemas y Arquitectura de Tecnología	Comunicaciones	1. Verificar funcionamiento de canal principal. 2. Verificar switch CORE principal. 3. Verificar switch de Piso y configuración para los equipos de los funcionarios de la Dirección Financiera y Contable.	Coordinador de Sistemas y Arquitectura de Tecnología
Coordinación de Sistemas y Arquitectura de Tecnología	Mesa de ayuda	1. Realizar cierre de los registros de los eventos. 2. Registrar lecciones aprendidas en el sistema de gestión de incidentes. 3. Realizar revisión normal de: - Usuario - Revisión Antivirus. - Revisión de sistema operativo. - Revisión token 4. Solicitar actualización del inventario de equipos y token en caso de ser necesario. 5. Informar a Coordinador correspondiente	Coordinador de Sistemas y Arquitectura de Tecnología

5.3 Actividades de cierre del evento de contingencia.

Una vez se restablezca el servicio del sistema SIIF en el proceso de Gestión Financiera y Contable, el líder de contingencia debe ejecutar las siguientes actividades:

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

6. REGISTROS

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

7. ANEXOS

- Anexo 1. Directorio Telefónico

8. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	28-12-2020	22-12-2021	Creación del documento	Líder de Contingencia
002	23-12-2021	29-12-2022	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 retiran actividades de la oficina asesora de planeación.	Director de Tecnología de la Información y las Comunicaciones
003	30-12-2022	27-06-2024	Se elimina del anexo 2. Directorio Telefónico el nombre del funcionario y correo. Se adecuan los nombres de los grupos frente a la nueva estructura de la	Director de Tecnología de la Información y las Comunicaciones

			Entidad. Se incluye la sugerencia de crear un grupo de chat ya sea por TEAMS o por WhatsApp. Se adecua el nombre del documento con el de la caracterización.	
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 actualiza el Directorio Telefónico por cambios en estructura funcional y nuevos miembros de equipos.	Director de Tecnología de la Información y las Comunicaciones

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

ANEXOS

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No.	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director Informática y Desarrollo	Mayra Isabel Gonzalez Núñez Migonzalez@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	3029
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