Superintendencia de Sociedades

GUIA PLAN DE CONTINGENCIA APLICACIONES EN LA NUBE

1. INFORMACIÓN GENERAL

1.1 OBJETIVO

Diseñar la guía del plan de contingencia para los activos de información; servicios en la nube, para los aplicativos Tesauro, SIIS e Insolvencia. Asimismo, documentar las actividades que se deben desarrollar para la correcta implementación en caso de que, por la materialización de riesgos, algún evento o incidente de seguridad llegará afectar la correcta operación y disponibilidad de los aplicativos en la nube referidos anteriormente.

1.2 RESPONSABLE

Grupo de Seguridad e Informática Forense.
Grupo de Sistemas e Arquitectura de Tecnología.
Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones.
Grupo de Seguridad e Informática Forense.
Gerencia de proyecto Servicios en la NUBE.
Oficial de Seguridad de la Información

1.3 ALCANCE

Este documento aplica para los siguientes aspectos y que sería el impacto a considerar:

- Servicios en la nube.
- Alta disponibilidad de los servicios en la nube.
- Aplicativo Tesauro.
- Aplicativo SIIS.
- Aplicativo de insolvencia.
- Modelos de inteligencia artificial y analítica avanzada.
- Administración soporte y mantenimiento de Infraestructura.
- Administración soporte y mantenimiento de sistemas.
- Administración de datos.
- Administración de seguridad.
- Procesamiento en la nube.
- Desarrollo de servicios.

La presente guía aplica para todos los funcionarios involucrados con las aplicaciones en la nube para los aplicativos integrados a estos servicios de la Dirección de Tecnologías de la Información y las Comunicaciones y a los funcionarios que la entidad proveedora de servicios en la nube.

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.

ANALITICA AVANZADA: Conjunto integral de técnicas y métodos analíticos como Big Data, Inteligencia Artificial (IA), Machine Learning, etc. Estas técnicas permiten un mejor análisis predictivo y proporcionan información sobre el cambio tecnológico

AWS: Sigla en inglés (Amazon Web Service) que hace referencia a una colección de servicios de computación en la nube pública que en conjunto forman una plataforma de computación en la nube, ofrecidas a través de Internet por Amazon.com.

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

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

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

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

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

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

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

MODULO DE INSOLVENCIA: Es la herramienta web con inteligencia artificial dispuesta por la Superintendencia de Sociedades para facilitar el trámite de las solicitudes de

admisión a los procedimientos de insolvencia. A través del Módulo de Insolvencia ("MI"), los usuarios podrán diligenciar de forma fácil, estructurada y asistida las solicitudes de admisión a los trámites y procedimientos de insolvencia, reduciendo los tiempos y agilizando el procesamiento de los datos.

INTELIGENCIA ARTIFICIAL: En el contexto de las ciencias de la computación, es una disciplina y un conjunto de capacidades cognoscitivas e intelectuales expresadas por sistemas informáticos o combinaciones de algoritmos cuyo propósito es la creación de máquinas que imiten la inteligencia humana para realizar tareas, y que pueden mejorar conforme recopilen información.

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, seguridad y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

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

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

SIIS: Sigla del Sistema Integrado de Información Societaria.

TECNOLOGÍA EN LA NUBE: Es la disponibilidad bajo demanda de recursos de computación como servicios a través de Internet. Esta tecnología evita que las empresas tengan que encargarse de aprovisionar, configurar o gestionar los recursos y permite que paguen únicamente por los que usen.

TESAURO: Es una aplicación web con inteligencia artificial que permite gestionar información de la doctrina jurídica, ayudando a mejorar los procesos internos de La Superintendencia de Sociedades y permitiendo el procesamiento de toda la información de una manera veraz, permitiendo a su vez el acceso a la información que requieran los ciudadanos.

2. CONDICIONES GENERALES

El contenido está enfocado a la contingencia sobre los servicios en la nube de las aplicaciones de Tesauro, SIIS e Insolvencia que funcionan en la nube Amazon Web Service (AWS) soportados por una entidad proveedora.

Supuestos:

La efectividad en la ejecución de este documento, ante la ocurrencia de un evento de interrupción mayor o un evento contingente que afecte los servicios en la nube referidos anteriormente.

- Contar con un servicio en la nube con alta disponibilidad que además de contar con máquinas virtuales ejecutándose permanentemente en la infraestructura cloud (servidores, redes y seguridad), sincronice las recuperaciones a nivel aplicación y bases de datos.
- Existencia de contrato de Prestación de los servicios de un proveedor de tecnología para la administración, soporte y mantenimiento del sistema de infraestructura, aplicaciones, modelos de inteligencia artificial y analítica avanzada de la Superintendencia de Sociedades en la nube contratada.
- 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 deben realizar pruebas de las estrategias y actividades al menos 1 vez al año.
- Los funcionarios han participado en las pruebas y capacitaciones realizadas.

3. GUIA DEL PLAN DE CONTINGENCIA PARA LAS APLICACIONES EN LA NUBE.

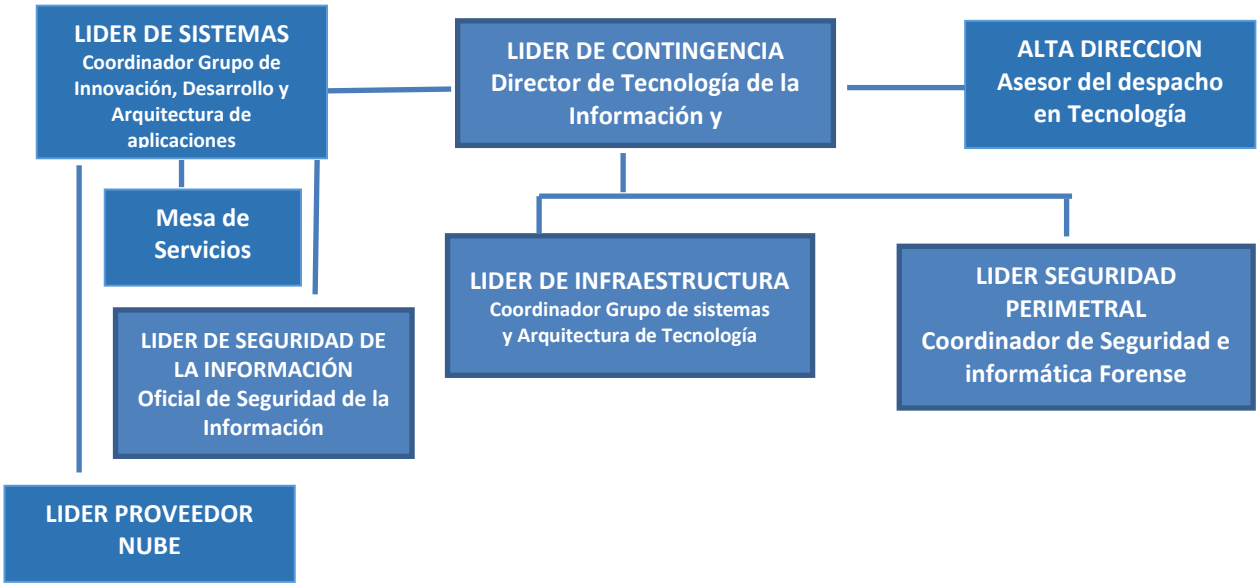
3.1. ESCENARIOS DE CONTINGENCIAS

3.1.1 Contingencias presentadas en proveedor en las aplicaciones en la NUBE.

- Para los servicios y sistemas en la nube, se tendrán en cuenta el escenario de indisponibilidad de la infraestructura tecnológica contratada y asignada, a las aplicaciones de Tesauro, SIIS e Insolvencia.
- Ataques cibernéticos que afecten la infraestructura tecnológica contratada y asignada, a las aplicaciones de Tesauro, SIIS e Insolvencia.

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 DE SISTEMAS Coordinador de Innovación Desarrollo y Arquitectura de Aplicaciones	- Asegurar el monitoreo de los sistemas de información en la nube. - Estar pendiente de las situaciones y eventos que puedan generar indisponibilidad de servicios de las aplicaciones en la NUBE. - Apoyar la elaboración y dar Vo.Bo, al plan de contingencia de servicios en la nube. - Participar en el Análisis de impacto de eventos de servicios en la nube para determinar el RTO y RPO. - Velar por la existencia de soporte técnico y mantenimiento evolutivo de los sistemas en la nube	- Participar en la evaluación del evento contingente. - Reportar a mesa de ayuda sobre la situación de indisponibilidad que se presenta. - Comunicar a los proveedores relacionados con el evento sobre la activación del plan de contingencia de los servicios en la nube. - Comunicar al líder de Contingencia el evento de indisponibilidad que se presente. - Comunicar al líder de Seguridad de la Información sobre cualquier indisponibilidad que se presente y confirmar si el evento supera el RTO. - Preparar los equipos de trabajo para actuar en contingencia. - Coordinar la ejecución de las actividades del plan de contingencia.	- Confirmar que todos los servicios requeridos para los servicios en la nube estén disponibles. - Comunicar al líder de Seguridad de la Información, sobre la recuperación de servicios en la nube. - Comunicar al líder de Contingencia, sobre la recuperación de servicios en la nube.

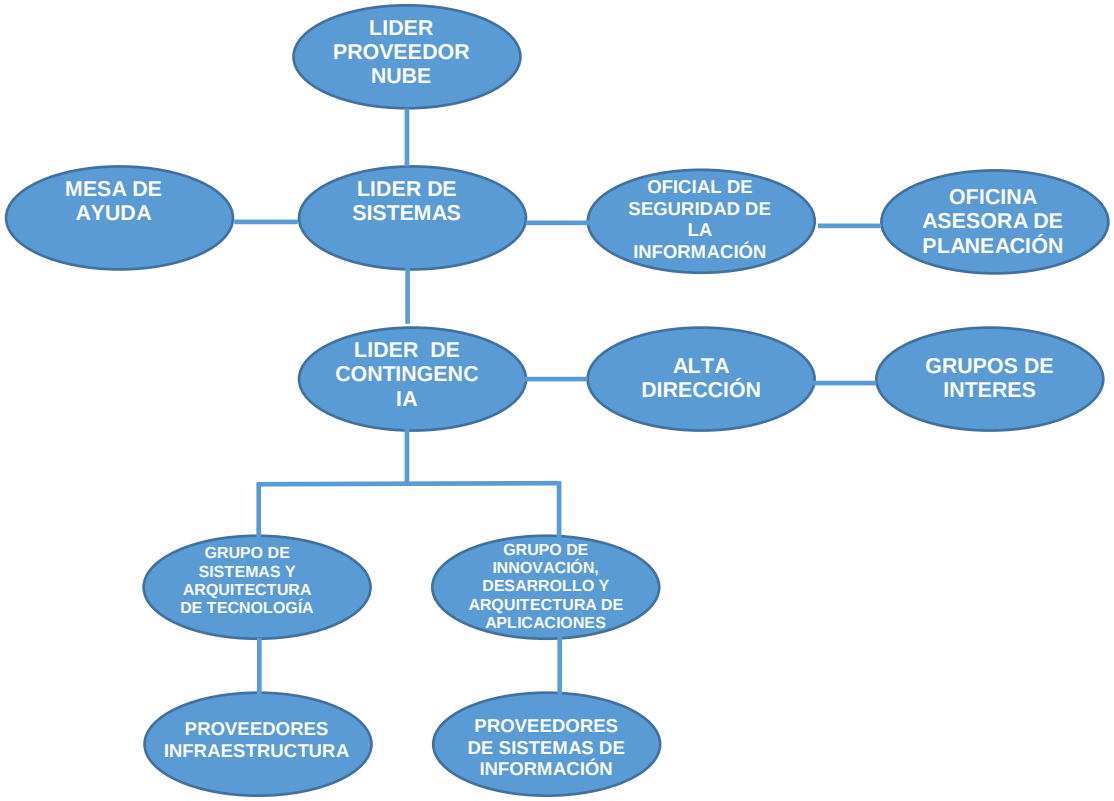
Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
		- Verificar disponibilidad de los sistemas de información que se encuentran en contingencia y notificar al personal requerido para atender el evento. - Realizar con su equipo de trabajo las pruebas de funcionamiento de los sistemas de información en la nube.	
LIDER DE CONTINGENCIA Director de Tecnología de la Información y Comunicaciones	- Velar por la actualización del Plan de Contingencia. - Velar por la actualización, distribución y pruebas del Plan de Contingencia. - Gestionar la consecución de los recursos para el plan de contingencia.	- Evaluar 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. - Liderar el retorno a la normalidad.	- Velar por la actualización del plan de continuidad acorde con los inconvenientes y oportunidades de mejora Visualizados durante el evento de interrupción.
LÍDER DE INFRAESTUCTURA Coordinador Sistemas y Arquitectura de Tecnológica	- Asegurar el monitoreo de los sistemas y componentes de la plataforma tecnológica de la nube. - Mantener la configuración técnica de la conectividad requerida en los servicios en la nube. - Conocer las actividades a desarrollar por su equipo de trabajo en la ejecución de las pruebas de los eventos que ocurran en la nube. - Informar los resultados del monitoreo de los servicios en la nube. - Velar por el soporte y mantenimiento vigente para la infraestructura Tecnológica de	- Participar en la evaluación del evento contingente. - Verificar por disponibilidad de la infraestructura propia asociada a los servicios en la Nube. - Velar por la ejecución de las actividades de contingencia y recuperación de su equipo de trabajo y reporte de resultados. - Mantener informado al Líder de contingencia sobre el estado de contingencia y avance de las actividades de sus equipos de trabajo. - Realizar las configuraciones requeridas para activar componentes alternos requeridos.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de servicios en la nube respecto a las actividades a realizar con su equipo de trabajo. - Solicitar, revisar y aprobar los cambios en el plan de contingencia de servicios en la nube que se hayan detectado respecto a la infraestructura tecnológica.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	servicios en la nube contratada.		
LIDER DE SEGURIDAD DE LA INFORMACIÓN Oficial de Seguridad de la Información	- Liderar la creación del plan de contingencia de servicios en la nube y el Análisis de impacto para los servicios en la nube para determinar el RTO y RPO. - Coordinar la publicación del plan de contingencia de servicios en la nube. - Gestionar la lectura y conocimiento del plan de contingencia para servicios en la nube, por parte de los grupos involucrados. - Revisar el registro de la contingencia acorde con el procedimiento o guía de gestión de incidentes.	- 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.	- Verificar si se actualizó la guía de continuidad o el DRP, 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. - 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.	- Registrar los eventos que le reporten. - Estar atentos a realizar actividades de remediación que les soliciten.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia. - Reportar los inconvenientes y oportunidades de mejora del plan de contingencia.
LIDER PROVEEDOR NUBE	- Conocer el plan de continuidad a aplicar en caso de contingencia .	- Informar sobre la contingencia que se presente al Lider de sistemas. - Coordinar la ejecución de las actividades de contingencia a cargo de los funcionarios del proveedor. - Informar al Lider de Sistemas, el estado de las pruebas durante la contingencia.	- Reportar los inconvenientes y oportunidades de mejora del plan de contingencia de los servicios que administran.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
		- Informar al líder funcional el cierre del evento y vuelta a la normalidad. - Enviar al líder funcional las evidencias de las actividades realizadas.	

3.3. ÁRBOL DE LLAMADAS

Cuando se presente un evento tecnológico o funcional sobre las Aplicaciones en la Nube, se debe seguir la siguiente cadena de llamadas:



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 Informática y Desarrollo, 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 de las aplicaciones en la nube?

El LÍDER DE PROVEEDOR EN LA NUBE, quienes administran los sistemas de Tesauro, SIIS e insolvencia (Justicia Digital) debe reportar todos los eventos que se presenten sobre los servicios en la nube al LÍDER FUNCIONAL, acorde con los referenciado en el punto 3.1.1 Contingencias presentadas en proveedor servicios en la NUBE, y que generen la indisponibilidad de estos servicios.

3.4.2 ¿Quién evalúa la magnitud e impacto del incidente?

Para el caso de un evento de indisponibilidad el LIDER FUNCIONAL realizará con su equipo de trabajo el análisis del evento e informará al LIDER DEL DRP sobre el evento y solicita autorización para el inicio del plan de contingencia. Se debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

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

3.4.3 Análisis de Impacto.

De acuerdo con las pruebas de contingencia realizadas anteriormente a los sistemas de información que se encuentra funcionando en la nube, 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: 30 minutos
RPO: 30 minutos

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 líder del DRP comunica a la Alta Dirección, teniendo en cuenta los siguientes aspectos:

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

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

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

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

La comunicación de la crisis deberá considerar los siguientes principios:

- **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malentendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.

- **Decir la verdad**: Ser honestos en los comunicados, sin embargo, no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.

- **Emitir reportes lo más exactos posible**: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

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

- Ciudadanos, usuarios externos de los productos y/o servicios de la entidad.
- Funcionarios
- Opinión Pública
- Gobierno, Autoridades y Entes de Control
- Medios de comunicación

3.6. ACTIVIDADES DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA

Es responsabilidad del Líder de Seguridad de la información, tramitar la actualización de las nuevas versiones de la presente guía de contingencia (DRP), y la comunicación de las mismas 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 del proveedor que involucre modificaciones en la configuración de las aplicaciones en la nube.	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 solicite al proveedor de servicios en la nube, cambios en la plataforma por mejoras a los aplicativos.
2.	Cambio de proveedor de aplicaciones en la nube.	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 proveedor
3.	Cuando los resultados de las pruebas requieren actualización de la guía	Lideres de los grupos de la Dirección de	Posterior a las pruebas que se realicen

No	Actividad	Responsable	Frecuencia
		Tecnología de la Información y las Comunicaciones. Oficial de Seguridad de la Información	

3.7. ACTIVIDADES DE PRUEBA

La programación y método a utilizar en la realización de pruebas de contingencia, 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.

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 DEL SERVICIOS EN LA NUBE.

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.
- Proveedor de servicios en la nube.

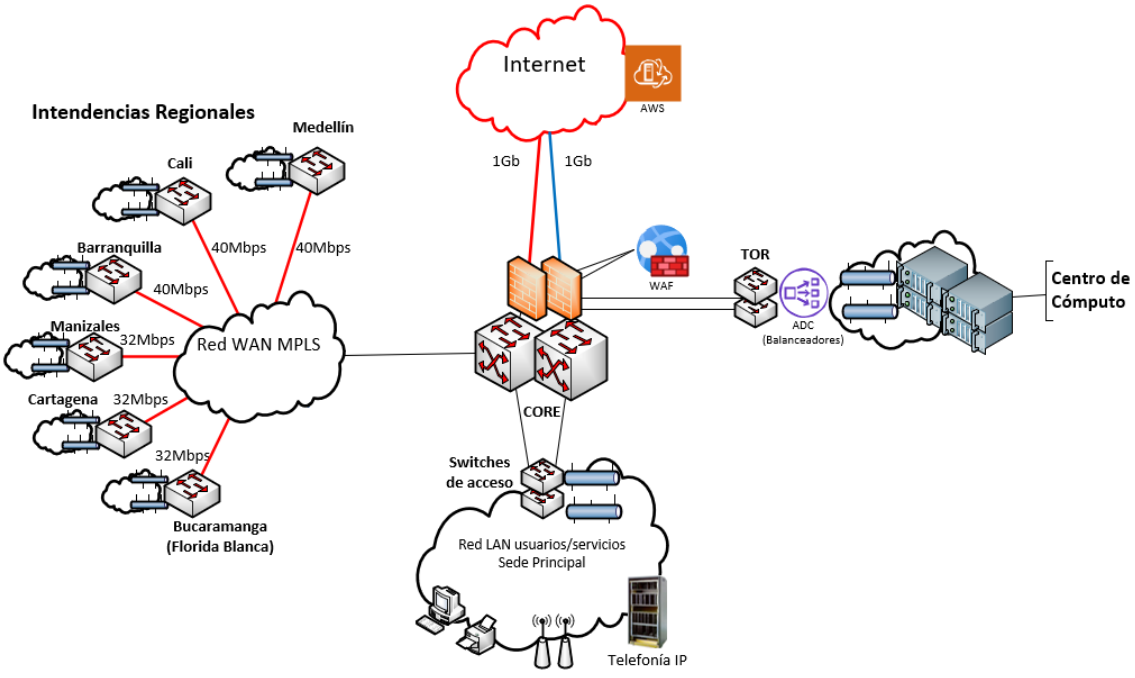
3.9. RECURSOS MÍNIMOS REQUERIDOS

La infraestructura necesaria para soportar los servicios en la nube la siguiente:

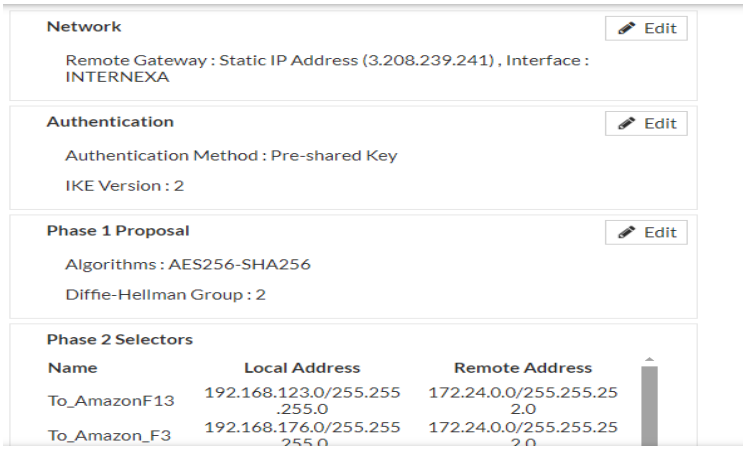
Cantidad de dispositivos	***Sofware Requerido***	***Tipo de Dispositivo***	***Marca***	***Cantidad de Procesadores***	***Memoria***	***Almacenamiento***
1	MI	Servidor	Instancia EC2	2 vCPU	1 GiB	10 GiB
1	Tesauro	Servidor	Instancia EC2	2 vCPU	2 GiB	10 GiB
1	SIIS	Servidor	Instancia EC2	2 vCPU	2 GiB	10 GiB

3.9.1. Requisitos de Comunicación.

Los requisitos mínimos de comunicación con los que debe contar la plataforma de servicios en la nube son:



Se requiere como mínimo un túnel VPN sitio a sitio con la nube AWS, con una velocidad mínima de 200Mbps.
Cabe anotar que tal como se muestra en el diagrama de red, la conectividad actual con la que cuenta la Entidad hacia Internet tiene una capacidad de 1GB y en la actualidad existe un túnel VPN Sitio a Sitio, usando el proveedor Internexa, por lo que el requerimiento se está cumpliendo. A continuación, se muestra la captura de pantalla de la configuración actual del túnel VPN:



4. ACTIVIDADES DE CONTINGENCIA

Para los diferentes escenarios de eventos sobre las Aplicaciones en la Nube se definen las guías o pasos a seguir para recuperar los servicios que presta este componente.

4.1.1 Actividades Funcionales y tecnológicas.

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Servicios en la nube	1. Realizar pruebas de funcionalidad técnica de las aplicaciones en la nube antes y después de un evento. 2. Informar al Lider funcional sobre el evento de indisponibilidad de los servicios en la nube para el aplicativo correspondiente. 3. Informar al líder funcional sobre el retorno a la normalidad.	Lider proveedor servicios en la nube

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de innovación, Desarrollo y Arquitectura de Aplicaciones.	1. Informar a líder de Contingencia sobre la situación de contingencia presentada en las aplicaciones en la nube y el impacto que se genera. 2. Informar a mesa de ayuda para el registro y cierre del evento. 3. Informar a la Oficina Asesora de Planeación (OAP) del evento que se indisponibilidad en prueba. 4. Informar a sus equipos de trabajo para actuar en contingencia.	Líder Sistemas
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Seguridad e Informática Forense	1. Preparar las condiciones de seguridad para la plataforma de contingencia que se implemente en caso de incidente de indisponibilidad de aplicaciones en la nube. 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 de sistemas las evidencias de las pruebas realizadas.	Lider Seguridad Perimetral
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	1. Evaluar reporte recibido y activar el Plan de Contingencia para el evento de contingencia que se presente. 2. Informar a los líderes tecnológicos para que ejecuten actividades de contingencia definidas. 3. Liderar la operación bajo contingencia. 4. Comunicar a la alta dirección el estado de contingencia y el	Lider de Contingencia

Proceso	Subproceso	Actividad	Responsable
		avance de actividades de contingencia.	
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura Tecnológica	1. Verificar funcionamiento de canales de comunicación. 2. Verificar infraestructura tecnológica de la entidad involucrada en la contingencia. 3. Ejecutar actividades de contingencia asignadas a su grupo de trabajo. 4. Informar los resultados de las actividades desarrolladas.	Líder Infraestructura
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Sistemas y Arquitectura de Tecnología	1. Registrar reporte de evento presentado y escalar hacia el área encargada de solucionar problema. 2. Informar al líder funcional el número de tiquete asignado. 3. Ejecutar actividades de contingencia asignadas a su grupo de trabajo. 4. Informar los resultados de las actividades desarrolladas.	Coordinador de mesa de ayuda
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. Apoyar la ejecución de las guías de contingencia y recuperación que se estén probando. 3. Comunicar a los proveedores la activación del plan de contingencia de las aplicaciones en la nube. 4. Revisar disponibilidad de los ambientes de desarrollo y	Líder de Sistemas de Información

Proceso	Subproceso	Actividad	Responsable
		pruebas, en caso de ser necesario. 5. Informar al Líder de Contingencia.	

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 y Tecnológicas

Una vez se restablezca el funcionamiento del SERVICIOS EN LA NUBE principal deben ejecutar las siguientes actividades:

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Proveedor NUBE	1. Informar a líder de sistemas sobre la solución del evento. 2. Comunicar al líder de seguridad de la información las lecciones aprendidas del evento	Líder proveedor NUBE
Gestión de Tecnología de la Información y las Comunicaciones	Coordinación de Innovación, desarrollo y arquitectura de Aplicaciones.	1. Reportar a mesa de ayuda sobre el cierre del evento. 2. Informar a líder de Contingencia sobre retorno a la normalidad 3. Informar a líder de Seguridad de la Información sobre retorno a la normalidad. 4. Comunicar al líder de seguridad de la información las lecciones aprendidas del evento.	Lider de Sistemas
Gestión de Tecnología de la Información y las Comunicaciones	Director de Tecnología de la Información y las Comunicaciones	1. Comunicar a la alta dirección la finalización de la contingencia. 2. Informar a líderes de Infraestructura y de sistemas de Información sobre retorno a la normalidad.	Lider de Contingencia

Proceso	Subproceso	Actividad	Responsable
Gestión de Tecnología de la Información y las Comunicaciones	Coordinador de Seguridad e Informática Forense	1. Comunicar al líder de seguridad de la información las lecciones aprendidas del evento. 2. Verificar monitoreo de componentes tecnológicos de la plataforma de servicios en la nube.	Lider de Seguridad perimetral
Oficina Asesora de Planeación	Oficial de Seguridad de la Información	1. Comunicar a jefe Oficina asesora de Planeación sobre retorno a la normalidad. 2. Consolidar lecciones aprendidas y entregarlas para registro al líder de seguridad perimetral.	Lider Seguridad de la Información
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. 3. Comunicar al líder de seguridad de la información las lecciones aprendidas del evento	Coordinador de mesa de ayuda

5.3 Actividades de cierre del evento de contingencia.

Una vez se restablezca el servicio de las aplicaciones en la nube, el líder de Contingencia debe ejecutar las siguientes actividades:

Actividad
a. Informar a la alta dirección o a quien esta designe: • La fecha del retorno a operación normal. • Las consideraciones especiales por aplicar en el proceso de retorno. • Emitir informe de cierre del evento. b. 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, así como, las lecciones aprendidas.

6. REGISTROS

- Informe de recuperación del incidente.
- Formato GINT-F-004 Plan, Diseño, Ejecución y Evaluación de pruebas.

7. ANEXOS

- Anexo 1. Directorio Telefónico

8. CONTROL DE CAMBIOS

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	28-06-2024		Creación del documento	Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones

ANEXOS

Anexo 1 Directorio Telefónico (Conmutador: 2201000)

No.	Cargo	Nombre / Correo Electrónico	Rol	Celular / Extensión
1	Director Informática y Desarrollo	Mayra Isabel Gonzalez Nuñez MIGonzalez@SUPERSOCIEDADES.GOV.CO	Director	3000
2	Oficial de Seguridad de la Información	Ivan Alexis Ontibon Rojas 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	Coordinación de 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	Gerente de Proyectos	Marcela Sánchez Sierra marcela.sanchez@nuvu.cc	Proveedor servicios en la nube	3013366239