

**PLAN DE CONTINUIDAD DEL NEGOCIO**

**OFICINA DE SEGURIDAD DE LA INFORMACIÓN**

**SIGCMA**

Versión 1.

Agosto 2022

**Historial del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Fecha | Comentarios | Por |
| 1 | 28-07-2022 | Versión Inicial | GPET |
| 2 | 29-09-2022 | Modificaciones en los objetivos y el alcance | GPET |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Revisión | Fecha | Comentarios | Por |
| 1 | 15-06-2022 | Versión Inicial | GPET |
| 2 | 20-06-2022 | Revisión de Calidad | GPET |
| 3 | 31-08-2022 | Revisión derivada del proceso de auditoría interna | GPET |
|  |  |  |  |
|  |  |  |  |

**TABLA DE CONTENIDO**

[1 INTRODUCCIÓN 5](#_Toc110442980)

[2 OBJETIVO 5](#_Toc110442981)

[2.1 Objetivo General 5](#_Toc110442982)

[2.2 Objetivos Específicos 5](#_Toc110442983)

[3 ALCANCE 6](#_Toc110442984)

[4 GLOSARIO 8](#_Toc110442985)

[5 ESCENARIOS DE DESASTRE 9](#_Toc110442986)

[6 ESTRATEGIAS DE CONTINUIDAD Y RECUPERACIÓN 10](#_Toc110442987)

[7 SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS REQUERIDOS 12](#_Toc110442988)

[8 PROVEEDORES CRÍTICOS PARA LA OPERACIÓN 15](#_Toc110442989)

[9 PREMISAS DEL PLAN 16](#_Toc110442990)

[10 POLÍTICA DE CONTINUIDAD DE NEGOCIO 17](#_Toc110442991)

[11 GOBIERNO DE LA CONTINUIDAD DEL NEGOCIO Y ARBOL DE LLAMADAS 17](#_Toc110442992)

[12 FASES DEL PLAN DE CONTINUIDAD DE NEGOCIO DE LA OSI 21](#_Toc110442993)

[12.1 Fase preventiva 22](#_Toc110442994)

[12.2 Fase de recuperación 26](#_Toc110442995)

[12.3 Fase de restauración 30](#_Toc110442996)

[13 INDICADORES DEL PLAN DE CONTINUIDAD DE NEGOCIO 31](#_Toc110442997)

[14 PLAN DE CAPACITACIÓN EN CONTINUIDAD DE NEGOCIO 31](#_Toc110442998)

[15 MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO 32](#_Toc110442999)

[16 REVISIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO 33](#_Toc110443000)

**Índice de Tablas**

[Tabla 1. Escenarios de Desastre 10](#_Toc110443001)

[Tabla 2.Consecuencias y afectaciones 10](#_Toc110443002)

[Tabla 3. Estrategia de Continuidad y Recuperación 12](#_Toc110443003)

[Tabla 4. Recursos Requeridos por tiempo de recuperación 15](#_Toc110443004)

[Tabla 5. Proveedores de Bienes y Servicios Críticos 16](#_Toc110443005)

[Tabla 6. Acciones Preventivas 23](#_Toc110443006)

[Tabla 7. Activación y Notificación 28](#_Toc110443007)

[Tabla 8. Alistamiento y Retorno a la Normalidad 31](#_Toc110443008)

[Tabla 9. Indicadores del Plan de Continuidad de Negocio 31](#_Toc110443009)

[Tabla 10. Plan de Capacitación 32](#_Toc110443010)

**Índice de Ilustraciones**

[Ilustración 1. Alcance referido a Corporaciones, Unidades y Seccionales. 7](#_Toc110443011)

[Ilustración 2. Alcance referido al recurso humano. 8](#_Toc110443012)

[Ilustración 3. Gobierno del PCN de la OSI. 17](#_Toc110443013)

[Ilustración 4. Árbol de llamadas. 21](#_Toc110443014)

[Ilustración 5. Fases del PCN. 22](#_Toc110443015)

# INTRODUCCIÓN

El objetivo de este Plan de Continuidad de Negocio, para la Oficina de Seguridad de la Información de la Rama Judicial, es el de documentar y establecer las acciones necesarias para asegurar la continuidad de su operación, a pesar de la materialización de incidentes que amenacen la normal ejecución de las actividades o el cumplimiento de niveles de servicio acordados.

De forma general, se puede indicar que este Plan de Continuidad del Negocio contemplará la gestión integral de las amenazas, iniciando desde la identificación de la eventual exposición a determinados incidentes, siguiendo con diversas actividades de índole preventivo, detectivo y correctivo, y finalizando con lo requerido para el completo restablecimiento de la operación normal.

Este Plan de Continuidad de Negocio está alineado con el gobierno y estructura de gestión de riesgos de la Rama Judicial, constituyéndose en una garantía para todos los grupos de interés de que, ante imprevistos, se mantendrá un grado aceptable de estabilidad en el cumplimiento de las funciones por parte de la Oficina de Seguridad de la Información. Lo anterior se logrará mediante la debida y oportuna respuesta ante eventos de interrupción, la recuperación de las operaciones y la reanudación de la operación normal.

# OBJETIVO

## Objetivo General

El objetivo general de este Plan de Continuidad de Negocio para la Oficina de Seguridad de la Información (en adelante OSI) de la Rama Judicial es establecer las medidas y/o acciones a ejecutar en caso de materializarse algún incidente que tenga la potencialidad de afectar el normal desarrollo de sus funciones y actividades.

En consecuencia, este documento incluye el detallamiento de los protocolos de respuesta inmediata ante determinado tipo de incidentes y de las acciones para la mitigación de impactos que eventualmente puedan generarse debido al compromiso de la continuidad en la prestación de servicios bajo la responsabilidad de la OSI.

## Objetivos Específicos

* Cumplir con los niveles de servicio acordados, en cumplimiento de los contratos y normas vigentes.
* Proteger la operación de la OSI frente a los impactos que pudieran afectarla producto de eventuales interrupciones presentadas durante el desarrollo de sus actividades.
* Preparar a la OSI con respecto a la implementación y acatamiento de las acciones requeridas para mantener la disponibilidad de sus funciones críticas ante la eventual ocurrencia de interrupciones.
* Asegurar la oportuna restauración de las operaciones afectadas por la materialización de determinados incidentes.
* Optimizar el proceso de toma de decisiones en caso de presentarse alguna situación de desastre que pudiera atentar contra la operación normal de la OSI.
* Promover las acciones que se dirijan hacia la mejora continua en la Continuidad del Negocio de la OSI.

# ALCANCE

Este Plan de Continuidad del Negocio establece los escenarios de interrupción a los que está expuesta la operación de la OSI, además de las estrategias de continuidad identificadas para cada uno de estos. La meta que se persigue con la adopción de las estrategias es disminuir la probabilidad de ocurrencia y/o el impacto que puede originar la eventual materialización de un incidente que atente contra el normal desarrollo de las funciones de la OSI. También, permite establecer cuáles son los servicios tecnológicos y los proveedores que se consideran críticos para llevar a cabo aquellos servicios que deben ser recuperados con la mayor agilidad posible ante la ocurrencia de un incidente o desastre.

En complemento a lo indicado antes, este documento también registra aquellas directrices asociadas con las labores preventivas, de recuperación y restauración que permiten, de forma consecuente (en el mismo orden) implementar mecanismos de defensa ante incidentes y desastres, disminuir las consecuencias de una interrupción y ejecutar acciones para reanudar la operación critica de la OSI a la mayor brevedad posible. Este Plan de Continuidad también describe las acciones requeridas para retornar a la operación normal, luego de superada la situación adversa.

La cobertura de este Plan de Continuidad se extiende a la operación de la OSI que, en términos generales, abarca la prestación de servicios de seguridad de la información y continuidad del negocio para el normal desempeño del Modelo de Seguridad y Privacidad de la Información – MSPI.

A fin de dar claridad con respecto al alcance referido en término de funciones de la OSI que están contempladas en este Plan de Continuidad del Negocio, a continuación, se incluye un detalle de estas:

* Gestionar los Incidentes de Seguridad de la Información (Crítico de la OSI).
* Inteligencia de amenazas (cacería) - SOC (Crítico de la OSI).
* Servicio de vigilancia digital – SOC (Crítico de la OSI).
* Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC
* Coordinar la implementación, mejora y mantenimiento del MSPI
* Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información
* Gestionar las métricas de seguridad de la información
* Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información

Considerando que el Security Operation Center (SOC) es responsable de identificar actividades anómalas que sean sospechosas de ser incidentes o compromisos de seguridad y ciberseguridad, dentro de este Plan de Continuidad del Negocio se considerará al SOC como un proveedor crítico para la OSI.

Mapa

Descripción generada automáticamente

Ilustración 1. Alcance referido a Corporaciones, Unidades y Seccionales.

Al entender que el servicio de la OSI tiene una influencia transversal en todas las Corporaciones, se concluye que este Plan de Continuidad del Negocio tiene en consideración las expectativas del CSJ, las Altas Cortes, las Unidades y las Seccionales de la Rama Judicial, las cuales se relacionan a continuación:

* Consejo Superior de la Judicatura
* Corte Constitucional
* Corte Suprema de Justicia
* Consejo de Estado
* Comisión de Disciplina Judicial
* Dirección Ejecutiva de Administración Judicial
* Grupo de Gestión Proyectos Estratégicos
* Direcciones Seccionales
* Unidad de Control Interno
* SIGCMA
* Grupo de Proyectos Especiales de TI - GEPT
* Unidad Informática - DEAJ
* Centro de Documentación Judicial
* UDAE
* Unidad de Recursos Humanos
* Unidad de Registro Nacional de Abogados
* Escuela Judicial (Rodrigo Lara Bonilla)
* Otros Grupos de Interés

En cuanto al alcance asociado al recurso humano, se puede establecer que este Plan de Continuidad aplicará para la siguiente estructura definida para la OSI:

Diagrama

Descripción generada automáticamente

Ilustración 2. Alcance referido al recurso humano.

# GLOSARIO

A continuación, se refieren algunos de los términos que son frecuentemente utilizados en los documentos asociados con la continuidad del negocio (Marco de referencia: ISO 22301.2017):

* **Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés):** Periodo de tiempo, después de un incidente, en el que: los servicios deben ser reanudados, o en el que los recursos deben ser recuperados.
* **Periodo Máximo Tolerable de Interrupción (MTPD, por sus siglas en inglés):** El tiempo en el que los impactos negativos de una interrupción comenzarían a considerarse inaceptables.
* **Punto Objetivo de Recuperación (RPO, por sus siglas en inglés):** Periodo de tiempo en el cual se debe restaurar la información requerida por un proceso con la finalidad de permitir la reanudación de la operación.
* **Impacto:** Afectación de los objetivos de un proceso o servicio, como resultado de una interrupción.
* **Interrupción:** Incidente, bien sea esperado o no, que causa una alteración negativa y no planeada en la prestación de los servicios, afectando el cumplimiento de los objetivos establecidos.
* **Fuente de Riesgo:** Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar determinado riesgo.
* **Valoración del Riesgo:** Proceso de identificación del riesgo, su análisis y correspondiente evaluación.
* **Apetito de Riesgo:** Grado en el cual una organización está dispuesta a asumir los riesgos.

**Recursos:** Activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (bien sea electrónica o no) que una organización posee, y que deben estar disponibles para usarse cuando sea necesario, a fin de operar para lograr los objetivos trazados.

# ESCENARIOS DE DESASTRE

De acuerdo con el análisis de impacto realizado, se identifican diversas situaciones que pueden derivar en una afectación de la continuidad del negocio de la OSI y que se resumen en la siguiente tabla:

| ESC. | DESCRIPCIÓN | AMENAZAS |
| --- | --- | --- |
| 1 | Modificación no autorizada (accidental o malintencionada) de la información asociada con las configuraciones, las parametrizaciones o los datos requeridos para el debido funcionamiento de las herramientas, soluciones informáticas y/o de la información procesada por estas y que guarda relación directa con la operación de la OSI. | ° Ataques cibernéticos. ° Errores u omisiones durante el mantenimiento de las soluciones tecnológicas. (p.e. apagado de máquinas) ° Errores u omisiones durante el uso de las soluciones tecnológicas. ° Fallas tecnológicas. ° Actos malintencionados. ° Hacer configuraciones no adecuadas o que modifiquen las configuraciones oficiales. ° Errores en el control de versiones. |
| 2 | Indisponibilidad del Datacenter de nube privada de la Rama Judicial que puede originarse por destrucción, daño o falla severa de esta infraestructura tecnológica que es requerida para el funcionamiento de la OSI. (En este escenario la OSI quedaría inhabilitada para utilizar las herramientas para la gestión de incidentes de SI, la inteligencia de amenazas y la vigilancia digital). | ° Ataques cibernéticos. ° Errores u omisiones durante el mantenimiento de las instalaciones y/o infraestructura tecnológica. ° Eventos fortuitos como incendios, inundaciones, alteraciones en el suministro del fluido eléctrico, actos terroristas, entre otros. ° Desastres naturales (por ejemplo, terremoto). ° Configuraciones no adecuadas. ° Errores en el control de versiones. |
| 3 | Fallas en conectividad que puede originarse por la destrucción, daño o falla severa de la infraestructura de telecomunicaciones implementada para la interacción entre los sistemas y personal requerido para la operación de la OSI. (En este escenario la OSI quedaría inhabilitada para utilizar las herramientas para la gestión de incidentes de SI, la inteligencia de amenazas y la vigilancia digital). | ° Ataques cibernéticos. ° Errores u omisiones durante el mantenimiento de las instalaciones y/o infraestructura tecnológica. ° Eventos fortuitos como incendios, inundaciones, alteraciones en el suministro del fluido eléctrico, actos terroristas, entre otros. ° Desastres naturales (por ejemplo, terremoto). ° Configuraciones no adecuadas. |
| 4 | No disponibilidad del servicio a cargo de proveedores o aliados clave para la operación de la OSI. (Proveedor SOC). | ° No disponibilidad de personal suficiente y competente.  ° Dificultades presupuestales para cumplir con las obligaciones. ° No disponibilidad de infraestructura tecnológica requerida. ° Pandemias o emergencias sanitarias. ° Disturbios civiles. ° Desastres naturales. |
| 5 | Destrucción, daño o falla severa de los equipos de cómputo de la OSI o del SOC, de los sistemas de almacenamiento de información y/o de los servicios de internet requeridos para prestar los servicios (Se trata de recursos ubicados fuera del centro de procesamiento de datos de la rama judicial). | ° No disponibilidad de equipos, soluciones y/o servicios tecnológicos requeridos. ° Ataques cibernéticos. ° Errores u omisiones durante el mantenimiento de las instalaciones y/o infraestructura tecnológica. ° Eventos fortuitos como incendios, inundaciones, alteraciones en el suministro del fluido eléctrico, actos terroristas, entre otros. ° Desastres naturales (por ejemplo, terremoto). ° Configuraciones no adecuadas. ° Errores en el control de versiones. |
| 6 | Ausencia o no disponibilidad del personal clave requerido para la operación de la OSI. | ° Dificultades presupuestales para contratar y asignar a la cantidad suficiente de personas competentes requeridas para la operación de la OSI. ° Pandemias o emergencias sanitarias. ° Disturbios civiles. ° Desastres naturales. |

**Tabla 1. Escenarios de Desastre**

Estos escenarios de riesgo generan las consecuencias y afectaciones que se relacionan a continuación:

|  |  |
| --- | --- |
| **PRINCIPALES CONSECUENCIAS** | **SERVICIOS AFECTADOS** |
| ° Usar y/o generar información imprecisa o inexacta. ° Afectación del proceso de toma de decisiones respecto de la Seguridad de la Información de la Rama Judicial. ° Suspensión de actividades clave de la OSI. ° Incumplimiento de obligaciones legales y contractuales por parte de la OSI. ° Incremento en la exposición a la explotación de vulnerabilidades de seguridad de la información de la Rama Judicial. ° Afectación reputacional de la OSI en particular y de la Rama Judicial en general. | • Gestionar los Incidentes de Seguridad de la Información (Crítico de la OSI). • Inteligencia de amenazas (cacería) -SOC (Crítico de la OSI). • Servicio de vigilancia digital – SOC (Crítico de la OSI). • Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC • Coordinar la implementación, mejora y mantenimiento del MSPI • Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información • Gestionar las métricas de seguridad de la información • Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |

Tabla 2.Consecuencias y afectaciones

# ESTRATEGIAS DE CONTINUIDAD Y RECUPERACIÓN

Las estrategias de continuidad son entendidas como un conjunto de procesos enfocados a prevenir y mitigar los impactos que pueden originar los escenarios de desastre identificados. A continuación, se describen estas estrategias de continuidad y recuperación:

| ESC. | ESCENARIO | NOMBRE DE LA ESTRATEGIA | DESCRIPCIÓN |
| --- | --- | --- | --- |
| 1 | Modificación no autorizada (accidental o malintencionada) de la información asociada con las configuraciones, las parametrizaciones o los datos requeridos para el debido funcionamiento de las herramientas, soluciones informáticas y/o de la información procesada por estas y que guarda relación directa con la operación de la OSI. | Implementar y mantener operativo un esquema de replicación automática y sincrónica de las soluciones informáticas y su información clave relacionada. | ° Implementar un esquema de generación de copias de respaldo de las soluciones informáticas (incluyendo su configuración y parametrización) así como de la información requerida, para mantener las versiones previas que puedan ser restauradas cuando se detecte pudo presentarse una adulteración o modificación no autorizada de las mismas. De preferencia, este esquema de generación de copias de respaldo debe apoyarse en sistemas de almacenamiento basados en computación en nube y debe ser tan frecuente como lo definan los RPO correspondientes.  ° Revisar la velocidad de consolidación de los logs para asegurar la óptima y oportuna prestación de los servicios. Una alternativa consiste en disponer de máquinas de consolidación en otro datacenter diferente al de nube privada de la Rama Judicial y redireccionar el acceso de las herramientas para que lleguen al consolidador a través de internet. Otra alternativa puede ser mediante la implementación de una máquina física y 2 máquinas virtuales en el datacenter del CAN, de tal forma que se pueda asegurar la consolidación.  ° Reducir al máximo la intervención humana para la generación y almacenamiento de las copias de respaldo, a fin de prevenir la ocurrencia de errores u omisiones, así como mitigando el deterioro de medios físicos. ° Un esquema automático también contribuye con los objetivos en cuanto a la rapidez y confiabilidad del respaldo. |
| 2 | Indisponibilidad del Datacenter de nube privada de la Rama Judicial que puede originarse por destrucción, daño o falla severa de esta infraestructura tecnológica que es requerida para el funcionamiento de la OSI. | Implementar la infraestructura tecnológica de respaldo requerida por la OSI en una ubicación que se encuentre suficientemente distante del centro de procesamiento de datos principal. | ° Asegurar que la infraestructura tecnológica que soporta la ejecución de los procesos clave a cargo de la OSI esté respaldada en instalaciones que queden distantes del Centro de Procesamiento de Datos Principal con la finalidad de prevenir que, ante desastres mayores, este esquema también sea afectado y quede inoperante. (Máquinas virtuales con herramientas preinstaladas y preconfiguradas, incluyendo una solución contingente de monitoreo. Los servicios de Vigilancia Digital y Gestión de Incidentes pueden habilitarse desde los recursos en nube, sin embargo, el servicio de cacería de amenazas si depende totalmente del funcionamiento del datacenter de nube privada de la Rama Judicial). Una alternativa de gestión para este escenario consiste en migrar el funcionamiento de la herramienta Rapid7 a la nube, o que se albergue en la infraestructura del tercero que atiende el servicio). ° Es necesario mantener permanente sincronía entre la infraestructura principal y la de respaldo, en lo referente a la funcionalidad, parametrizaciones, conexiones, usuarios, seguridad y demás, a fin de asegurar una ágil transición entre ellas. ° Esta estrategia también implica la implementación de un esquema de replicación de información, la cual se aborda en la estrategia 4. |
| 3 | Fallas en conectividad que puede originarse por la destrucción, daño o falla severa de la infraestructura de telecomunicaciones implementada para la interacción entre los sistemas y personal requerido para la operación de la OSI. | Implementar y mantener permanentemente funcional la infraestructura de telecomunicaciones redundante (canales, dispositivos y servicios asociadas con la OSI), utilizando proveedores diferentes a los principales. | ° Asegurar que se encuentre disponible y operativa una infraestructura de telecomunicaciones redundante que pueda ser utilizada en caso de interrupciones o fallas en los servicios y/o equipos principales.  ° Por supuesto, requiere que los proveedores de los servicios y/o infraestructura redundante de comunicaciones sean diferentes a los que apoyan la operación cotidiana de la OSI.  ° Es importante que la conmutación entre el esquema principal y alterno sea automática. A fin de lograr eficiencias, existe la alternativa que se establezca un esquema de balanceo de cargas para que alternen en caso de latencias y/o interrupciones de alguno de ellos. ° En caso de, por alguna circunstancia, no se pueda disponer de algún proveedor redundante, se asegurará que en la contratación y ANS con los proveedores principales quede el compromiso de disponer de canales sobre infraestructuras físicas diferentes, minimizando el riesgo de caída simultánea del canal principal y del secundario . |
| 4 | No disponibilidad del servicio a cargo de proveedores o aliados clave para la operación de la OSI. (Proveedor SOC). | Establecer un esquema de supervisión rigurosa y permanente a los proveedores o aliados clave a fin de tomar decisiones oportunas en caso de identificarse alguna amenaza contra la continuidad de la prestación del servicio. | ° Establecer con los proveedores y aliados unos Acuerdos de Niveles de Servicio claros y precisos que sean medidos de manera permanente a fin de establecer oportunamente cualquier desviación. ° Exigir al tercero la documentación y evidencias de la debida actualización y prueba de los esquemas de contingencia y de continuidad de operaciones (PCN) a cargo de los proveedores y aliados clave, para verificar que estén alineados con los requisitos establecidos. ° Planear y ejecutar simulacros integrarles que permitan verificar la efectividad de los esquemas de contingencia y continuidad de los terceros y, en caso de que aplique, supervisar la oportuna ejecución de los planes de acción que se hayan definido en caso de identificarse situaciones a corregir. |
| 5 | Destrucción, daño o falla severa de los equipos de cómputo, de almacenamiento de información y/o servicios de internet requeridos por el personal de la OSI para prestar los servicios (Se trata de recursos ubicados fuera del centro de procesamiento de datos de la rama judicial). | Establecer un esquema de redundancia de recursos tecnológicos y servicios alternos que permitan mantener la operación de las funciones clave de la OSI a pesar de indisponibilidad de los recursos y/o servicios principales. | Implementar y probar un modelo de operación con recursos redundantes o alternos por parte del personal clave (estratégico o especializado) de la OSI, con la finalidad de asegurar que puedan continuar desarrollando sus funciones a pesar de la ocurrencia de situaciones que afecten los recursos o servicios principales que usualmente utilizan. Es necesario que este modelo garantice lo siguiente: ° Protección contra la obsolescencia en equipos portátiles y de escritorio. ° Protección física de activos informáticos y de la información. ° Facilidad en la administración de licenciamiento de soluciones. (La suite de office funciona desde la nube).  ° Facilidad de ejecución de tareas desde equipos redundantes que únicamente requieran una conexión a internet, desde cualquier lugar geográfico.  ° Especificaciones mínimas para los equipos de cómputo que requieren para conectarse a las soluciones tecnológicas correspondientes. |
| 6 | Ausencia o no disponibilidad del personal clave requerido para la operación de la OSI. | Diseñar e implementar un esquema de entrenamiento, rotación, suplencia y sucesión para el personal clave de la OSI. | ° Implementar esquemas que promuevan el entrenamiento y la rotación de personal clave de la OSI a fin de ampliar la disponibilidad de personal competente que esté plenamente habilitado para ejecutar actividades estratégicas y especializadas de la OSI en caso de ausencia de las personas principales. ° Definir y ejecutar esquemas de suplencia y sucesión con la finalidad de asignar rápidamente nuevos roles cuando se presenten situaciones de crisis que afecten la disponibilidad de personal principal. |

Tabla 3. Estrategia de Continuidad y Recuperación

# SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS REQUERIDOS

Los recursos de software necesarios para la operación de la OSI, y que se requieren habilitar como parte del desarrollo de las estrategias de continuidad antes referidas son los siguientes:

* Acceso a las plataformas afectadas.
* Correo electrónico.
* Herramientas de diseño.
* Microsoft Teams.
* Ofimática.
* Rapid7
* Sharepoint.
* SIEM.
* Software de mesa de servicios.
* Solarwinds y WSUS (Wsus es provisto por la Rama Judicial)

De forma complementaria, teniendo en cuenta que se necesitan determinados equipos, tecnologías y suministros para la prestación de servicios por parte de la OSI, abajo se relacionan aquellos que se requieren con prioridad para el normal desarrollo de sus funciones. Estos recursos también son contemplados dentro de las estrategias de continuidad referidos antes y que guardan relación con aspectos de telecomunicaciones e infraestructura:

* Canal de internet.
* Línea SOC.
* Línea de la oficina.
* Computadores personales.

Para mayor claridad, a continuación, se describen los servicios que demandan cada uno de estos recursos, así como la prioridad con la cual se deben disponer para evitar una afectación severa a la continuidad de la operación ante diferentes situaciones de desastre y/o eventos indeseables:

| **Recurso / Servicio** | **1 día** | **3 días** | **14 días** | **60 días** |
| --- | --- | --- | --- | --- |
| **Acceso a las plataformas afectadas.** |  |  |  |  |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Canal de internet.** |  |  |  |  |
| Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información |  | 1 |  |  |
| Coordinar la implementación, mejora y mantenimiento del MSPI |  |  | 1 |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Computador.** |  |  |  |  |
| Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información |  | 1 |  |  |
| Coordinar la implementación, mejora y mantenimiento del MSPI |  |  | 1 |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Correo electrónico.** |  |  |  |  |
| Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información |  | 1 |  |  |
| Coordinar la implementación, mejora y mantenimiento del MSPI |  |  | 1 |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Herramientas de diseño.** |  |  |  |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| **Línea de la oficina** |  |  |  |  |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| **Línea SOC** |  |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Microsoft Teams.** |  |  |  |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| **Ofimática.** |  |  |  |  |
| Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información |  | 1 |  |  |
| Coordinar la implementación, mejora y mantenimiento del MSPI |  |  | 1 |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Rapid7** |  |  |  |  |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Sharepoint.** |  |  |  |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| **SIEM.** |  |  |  |  |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Software de mesa de servicios.** |  |  |  |  |
| Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información |  | 1 |  |  |
| Coordinar la implementación, mejora y mantenimiento del MSPI |  |  | 1 |  |
| Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información |  |  | 1 |  |
| Gestionar las métricas de seguridad de la información |  |  |  | 1 |
| Gestionar los Incidentes de Seguridad de la Información | 1 |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |
| Servicio de vigilancia digital - SOC | 1 |  |  |  |
| **Solarwinds y WSUSE** |  |  |  |  |
| Inteligencia de amenazas (cacería) -SOC | 1 |  |  |  |
| Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC |  |  | 1 |  |

Tabla 4. Recursos Requeridos por tiempo de recuperación

# PROVEEDORES CRÍTICOS PARA LA OPERACIÓN

En complemento a lo indicado en el numeral anterior, para el desarrollo de los servicios a cargo de la OSI se requiere de la prestación de servicios por parte de los proveedores mencionados en la tabla de abajo. Es importante resaltar que, en caso de presentarse una interrupción en la operación de estos proveedores, se vería afectada la normal operación de la OSI.

| **TERCERO** | **SERVICIO** |
| --- | --- |
| ° SOC - Monitoreo, detección, contención y respuesta a incidentes de seguridad, identificación e investigación de posibles eventos de ciberseguridad, gestión de vulnerabilidades y generación de nuevos casos de uso. | ° Gestionar los Incidentes de Seguridad de la Información.  ° Inteligencia de amenazas (cacería) -SOC.  ° Servicio de vigilancia digital – SOC.  ° Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información.  ° Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC.  ° Gestionar las métricas de seguridad de la información. |
| ° Proveedores de infraestructura On Premise de la Rama Judicial, albergada en el centro de procesamiento de datos principal, en dónde se encuentran instaladas las herramientas requeridas para el cumplimiento de funciones a cargo de la OSI. | ° Gestionar los Incidentes de Seguridad de la Información.  ° Inteligencia de amenazas (cacería) -SOC.  ° Servicio de vigilancia digital – SOC.  ° Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información.  ° Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC.  ° Gestionar las métricas de seguridad de la información. |
| ° Proveedores de infraestructura en nube de la Rama Judicial en dónde se encuentran instaladas las herramientas requeridas para el cumplimiento de funciones a cargo de la OSI. | ° Gestionar los Incidentes de Seguridad de la Información.  ° Inteligencia de amenazas (cacería) -SOC.  ° Servicio de vigilancia digital – SOC.  ° Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información.  ° Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC.  ° Gestionar las métricas de seguridad de la información. |
| ° Proveedores de infraestructura tecnológica y soluciones requeridas para la interconectividad en las dependencias y soluciones tecnológicas de la Rama Judicial, las cuales son necesarias para el cumplimiento de funciones a cargo de la OSI. | ° Gestionar los Incidentes de Seguridad de la Información.  ° Inteligencia de amenazas (cacería) -SOC.  ° Servicio de vigilancia digital – SOC.  ° Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información.  ° Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC.  ° Gestionar las métricas de seguridad de la información. |
| ° Proveedores de infraestructura tecnológica (hardware y software de procesamiento y de telecomunicaciones) que se encuentra albergada por fuera del centro de procesamiento de datos principal Rama Judicial requerida para el cumplimiento de funciones a cargo de la OSI. Se incluyen proveedores propios de la OSI que permiten la ejecución de actividades por parte de su personal, quienes laboran de manera remota. | ° Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información.  ° Gestionar las métricas de seguridad de la información.  ° Coordinar la implementación, mejora y mantenimiento del MSPI.  ° Desarrollar estrategias de sensibilización y concientización en seguridad y privacidad de la información. |

Tabla 5. Proveedores de Bienes y Servicios Críticos

# PREMISAS DEL PLAN

Como contexto general, es importante considerar que, tomando en consideración las definiciones entregadas por la Rama Judicial, abajo se relaciona brevemente la secuencia de recuperación que tienen presupuestada en caso de incidentes de interrupción que afecten a la entidad. Se resalta que, en esta secuencia, los servicios de seguridad se encuentran con una prioridad intermedia:

* Datacenters (Incluyendo fluido eléctrico y conectividad).
* Seguridad perimetral.
* **Seguridad informática.**
* Repositorios de información.
* Aplicaciones.

Otras premisas de importancia para este plan son:

* El modelo de operación de la OSI se fundamente, en su gran mayoría, en el debido funcionamiento de soluciones y/o herramientas digitales o electrónicas.
* El personal vinculado a la OSI labora bajo un esquema remota o desde casa.
* Las funciones a cargo de la OSI tienen una dependencia importante de determinados proveedores y aliados, en particular el SOC.
* La mayor parte de la infraestructura tecnológica requerida para la operación de la OSI funciona en un esquema hibrido entre On Premise y computación en nube.
* Este plan de continuidad del negocio de la OSI acoge los componentes del plan de continuidad del negocio de la Rama Judicial (). Por lo tanto, el presente documento contempla las fases (preventiva, recuperación, restauración) enmarcadas en la operación de los servicios que presta la OSI y los recursos (humano, tecnológico, físicos, información) necesarios para el respectivo cumplimiento. En otras palabras, este plan de continuidad del negocio de la OSI se alinea con la gestión de crisis, recuperación tecnológica y manejo de emergencias de la Rama Judicial.

# POLÍTICA DE CONTINUIDAD DE NEGOCIO

La política del Plan de Continuidad de Negocio de la OSI es exactamente igual a la política del Plan de Continuidad de Negocio de la Rama Judicial, la cual se encuentra en la documentación correspondiente al contrato 170.

# GOBIERNO DE LA CONTINUIDAD DEL NEGOCIO Y ARBOL DE LLAMADAS

En lo que hace referencia a la gestión y mejoramiento continuo de este Plan de Continuidad del Negocio de la OSI, así como lo concerniente a la toma de decisiones ante la ocurrencia de eventos, se ha establecido un esquema de gobierno que se refleja en la siguiente gráfica, haciendo énfasis en que este operará en completa coordinación y articulación con el DRP de Rama Judicial:

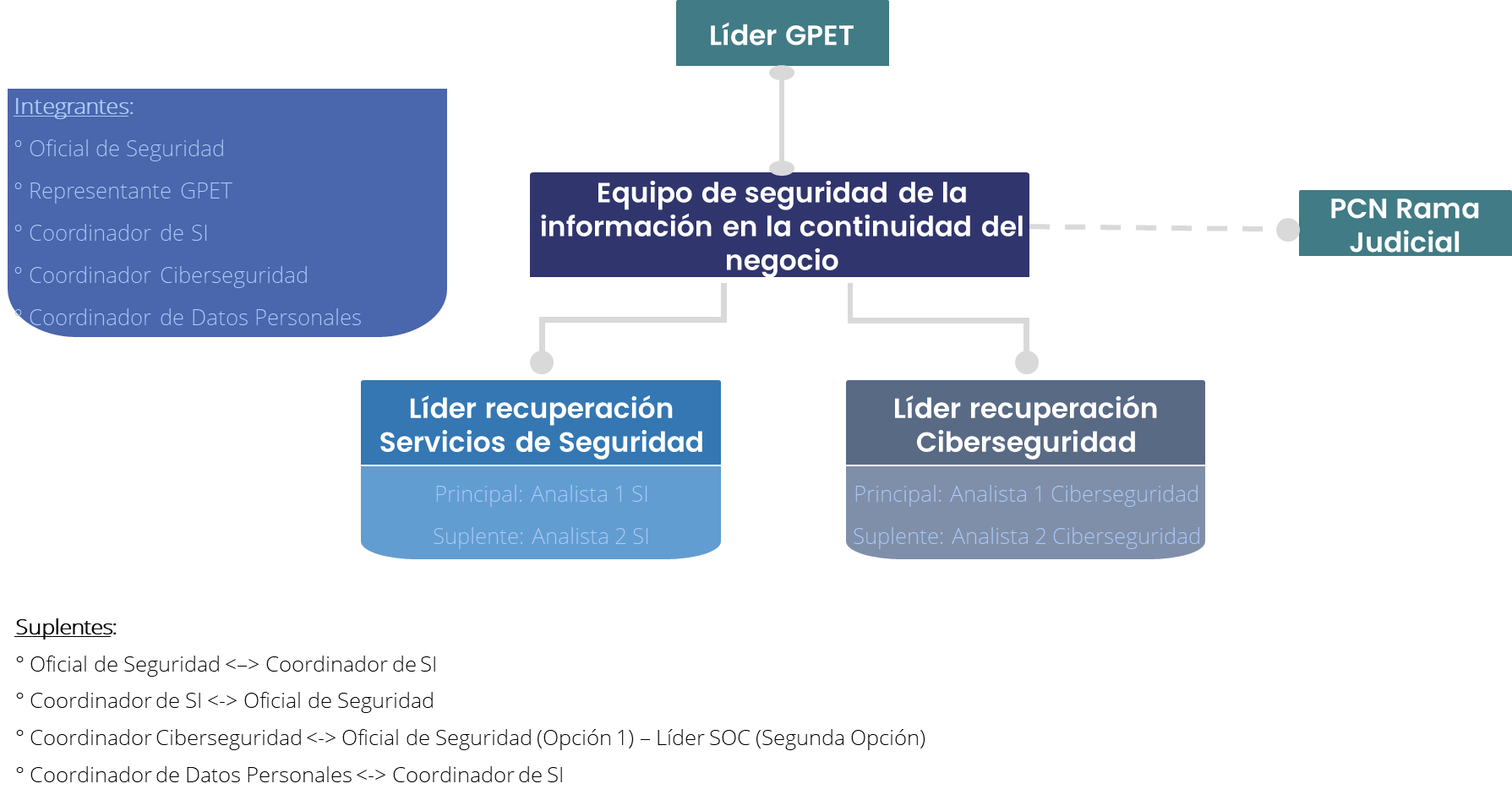


Ilustración 3. Gobierno del PCN de la OSI.

A continuación, se relacionan los roles y responsabilidades asociados con este esquema de gobierno, resaltando que se enmarcan en la atención de situaciones propias de la OSI que puedan afectar única y exclusivamente la normal prestación de sus servicios. Es importante tener en consideración que la Rama Judicial ha establecido unos escenarios de continuidad ante afectaciones de su propia infraestructura que, de manera simultánea, pueden incidir en la normal operación de la OSI. Cuando ocurran este tipo de situaciones, el esquema de gobierno del PCN de la OSI se mantendrá atento, a la espera de la evolución y tratamiento que le den las instancias pertinentes de la Rama Judicial. El accionar del gobierno del PCN de la OSI será orquestado con la Rama Judicial ante situaciones que implican afectación mutua ante la materialización de determinado escenario de desastre o emergencia.

**Equipo de la seguridad de la información en la continuidad del negocio (Equipo SICN)**

* Evaluar y aprobar los comunicados formales para el manejo de incidentes de interrupción que puedan afectar la operación de la OSI, de cara al GPET de la Rama Judicial.
* Definir y asignar recursos que sean necesarios para gestionar los incidentes de interrupción presentados en la OSI.
* Definir, orquestar y participar en los ejercicios y simulacros del Plan de Continuidad de Negocio de la OSI, en conjunto con el GPET de la Rama Judicial.
* Convocar al personal de la OSI ante las situaciones de interrupción que así lo ameriten.
* Tomar la decisión de activar el plan de continuidad de negocio de la OSI.
* Declarar el fin de las contingencias y retorno a la normalidad de la operación de la OSI cuando se obtengan las condiciones esperadas.
* Gestionar el presupuesto requerido para la sostenibilidad del PCN de la OSI.
* Asegurar la generación y custodia de los registros correspondientes a las sesiones del Equipo SICN, así como de los ejercicios de prueba realizados.

**Líder de Recuperación de Servicios de Seguridad.**

* Gestionar la revisión anual de los protocolos para la recuperación de los servicios de seguridad de la información y protección de datos personales a cargo de la OSI, así como para la gestión de emergencias que puedan afectar el cumplimiento de cara a la Rama Judicial.
* Atender las revisiones del GPET de la Rama Judicial en materia de continuidad de operación de la OSI, en lo referente a los servicios de seguridad de la información y protección de datos personales que la oficina tiene directamente a su cargo.
* Gestionar el plan de sensibilización, entrenamiento y capacitación en Continuidad de Negocio para el personal de la OSI, incluyendo el modelo de gobierno, la política y las responsabilidades referidas en el presente plan definido para la OSI.
* Asegurar la debida actualización del análisis de impacto al negocio BIA para prestación de servicios a cargo de la OSI, en conjunto con el personal pertinente del GPET de la Rama Judicial.
* Comunicar al personal de la OSI las decisiones del Equipo SICN en cuanto a activar el plan de continuidad de negocio en los frentes de seguridad de la información y protección de datos personales que son prestados por la OSI.
* Mantener actualizados los datos de contacto del personal de la OSI.
* Coordinar la realización de simulacros del plan de continuidad del negocio de la OSI, en los frentes de seguridad de la información y protección de datos personales a su cargo, en conjunto con el personal pertinente del GPET de la Rama Judicial, en caso de ser necesario.

**Líder de Recuperación de Ciberseguridad**

* Gestionar la revisión anual de los procedimientos establecidos al interior de la OSI para la recuperación de desastres que afecten la prestación de sus servicios específicos de ciberseguridad que se encuentran a cargo de la OSI.
* Atender las revisiones de la Rama Judicial en materia de continuidad de operación de la OSI ante amenazas que atenten contra la prestación del servicio de ciberseguridad que está a cargo de esta oficina.
* Gestionar la presentación, ante el personal pertinente de la Rama Judicial, del esquema de recuperación de los servicios de ciberseguridad prestados por la OSI, cuando se presenten incidentes que originen interrupciones.
* Gestionar la capacitación al personal de la OSI en lo referente a la continuidad del negocio de la OSI en lo que concierne a la prestación de los servicios de ciberseguridad a su cargo.
* Contribuir con las actividades de análisis de impacto al negocio BIA y en los análisis de riesgos propios de la OSI, que pueda adelantar la Rama Judicial, focalizado en aquellos escenarios que puedan originar afectaciones a la normal prestación del servicio de ciberseguridad por parte de la OSI.
* Dirigir la secuencia de recuperación del servicio de ciberseguridad por parte de la OSI, en caso de la ocurrencia de incidentes de interrupción que lo afecten.
* Comunicar al personal de la OSI las decisiones del Equipo SICN en cuanto a activar el plan de continuidad de negocio en el frente de ciberseguridad prestado por la oficina.
* Coordinar la realización de simulacros del plan de continuidad del negocio de la OSI para el frente de los servicios de ciberseguridad a su cargo, en sincronía con el personal pertinente de la Rama Judicial.

**Personal de la OSI**

* Asistir a las jornadas de sensibilización y capacitación internas a la oficina y que estén vinculadas a este Plan de Continuidad de Negocio de la OSI.
* Reportar, de manera inmediata, a los líderes de recuperación de la OSI, aquellos incidentes o eventos de interrupción que identifiquen durante la prestación de los servicios a la Rama Judicial.
* Atender las instrucciones y decisiones emanadas desde el Equipo SICN de la OSI.
* Apoyar los ejercicios de análisis de impacto al negocio BIA y análisis de riesgos concernientes a los servicios a cargo de la OSI.
* Participar en las pruebas asociadas con este Plan de Continuidad del Negocio de la OSI, siempre y cuando sean convocados o autorizados por el Equipo SICN o los Líderes de Recuperación de la OSI mencionados antes.

**Manejo de suplencias o respaldo ante indisponibilidad de personal.**

* Oficial de Seguridad <- Recurso espejo con –> Coordinador de SI
* Coordinador de SI <- Recurso espejo con –> Oficial de Seguridad
* Coord. Ciberseguridad <- Respaldo 1-> Oficial de Seguridad
* Coord. Ciberseguridad <- Respaldo 2-> Líder SOC
* Coord. Datos Personales <- Respaldo -> Coordinador de SI

En cuanto al establecimiento y manejo de las suplencias, a continuación, se presentan las situaciones en las que se activarán:

* Cuando la integridad física del personal principal este comprometida por el evento de interrupción materializado.
* Cuando no se pueda localizar al personal principal en un plazo de tiempo razonable (1 hora) de acuerdo con el nivel de criticidad del incidente de interrupción.
* Cuando sea convocado en las pruebas y ejercicios del plan de continuidad de negocio. Nota: Las personas definidas como suplentes hacen parte del plan de continuidad de negocio por lo tanto deberán ser capacitadas de forma idéntica a los principales.

Para notificar la activación del Plan de Continuidad de Negocio de la OSI, y dar inicio al control del avance de éste, se define el “árbol de llamadas”, de tal manera que cada responsable tan solo se encargue, como máximo, de realizar y controlar el contacto con dos personas hacia abajo y un único punto de reporte hacia arriba.

De esta forma se pueden segregar las funciones de liderazgo, supervisión, gestión y ejecución técnica, y, a su vez, dejar plasmada la estructura de comunicaciones a desarrollar en el marco del Árbol de llamadas.

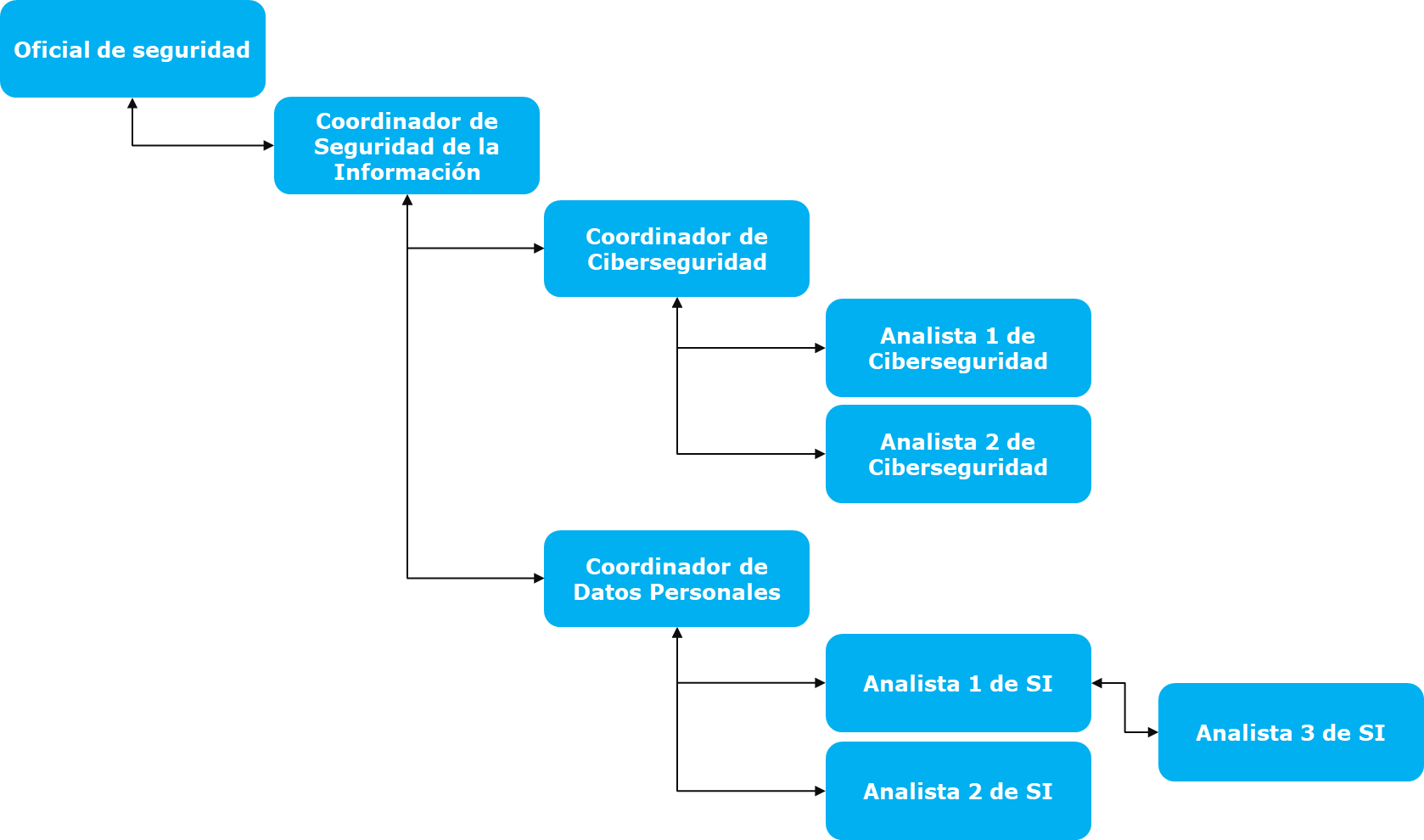


Ilustración 4. Árbol de llamadas.

# FASES DEL PLAN DE CONTINUIDAD DE NEGOCIO DE LA OSI

El Plan de Continuidad de Negocio de la OSI se desarrolló para la recuperación de sus operaciones, teniendo en cuenta aquellos recursos necesarios para su funcionamiento, como lo son los recursos humanos, de información, tecnológicos, instalaciones y protocolo de comunicaciones. En detalle se puede indicar:

* **Recuperación de las Operaciones**: Este aspecto tiene como fin recuperar las operaciones que le permiten prestar los servicios a la OSI. Entre sus prioridades se encuentra la recuperación de la funcionalidad de las herramientas tecnológicas requeridas para realizar las actividades, así como la información que se convierte en insumo para los diferentes frentes de trabajo.
* **Protocolo de comunicación**: El objetivo es mantener la buena coordinación entre la OSI y el GPET de la Rama Judicial a fin de satisfacer los requerimientos, entre ellos, los de la comunidad en general. Este protocolo también operará atendiendo las exigencias de los entes de vigilancia y control que correspondan. Ante situaciones que interrumpan la operación de la OSI, el Equipo SICN las tratará de manera oportuna, atendiendo las directrices y lineamientos acordados con la Rama Judicial.
* **Suplencia de personal**: Este aspecto se enfoca en asegurar que la OSI continúe atendiendo los servicios pactados con la Rama Judicial, disponiendo de personal suficiente, que continúe laborando desde las instalaciones correspondientes, a pesar de la ocurrencia de situaciones adversas. Esto implica que, ante la indisponibilidad de algunas personas, entrarán a operar esquemas de suplencias predefinidos.

De forma general, se considera que la administración del Plan de Continuidad de Negocio se concentra en tres (3) fases, dependiendo del momento de acción frente a la materialización de un escenario adverso:

* Antes
* Durante
* Después

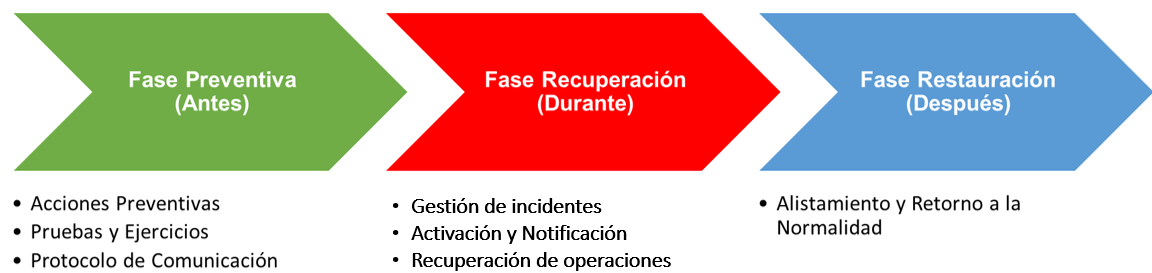


Ilustración 5. Fases del PCN.

NOTA: Teniendo en cuenta que la OSI tiene la característica de ser considerado como un proceso más de la Rama Judicial, se entiende que la OSI acogerá aquellos componentes de emergencias y de recuperación tecnológica establecidos por la Rama Judicial en su propio plan de continuidad del negocio.

## Fase preventiva

En esta fase permite asegurar una comprensión clara y actualizada de los servicios a cargo de la OSI y sus requerimientos frente a la gestión de la continuidad del negocio. Este contexto permite planear y desarrollar los mecanismos de prevención frente a la ocurrencia de incidentes o desastres, así como estrategias para mitigar los impactos en caso de que se materialicen.

* Acciones Preventivas

**Objetivo:** Reducir la probabilidad de ocurrencia de los riesgos y preparar a la OSI para mitigar los impactos que puede sufrir la prestación de sus servicios ante eventuales desastres que llegaran a presentarse.

**Alcance:** Todos los servicios a cargo de la OSI.

**Responsables:** Líder de Recuperación de Servicios de Seguridad y Líder de Recuperación de Ciberseguridad.

A continuación, se describen las actividades que se deben ejecutar, de manera periódica, para garantizar la existencia, cumplimiento y efectividad de los controles preventivos asociados con esta fase del Plan de Continuidad de Negocio.

| **ACTIVIDAD** | **PERIODICIDAD** |
| --- | --- |
| Asegurar que el personal de la OSI disponga de los recursos necesarios para que puedan ejercer sus funciones desde las instalaciones que correspondan. | Semestral |
| Monitorear la disponibilidad, óptimo funcionamiento y correcto uso de los recursos entregados al personal de la OSI para realicen sus actividades, especificando su ubicación y condiciones de los espacios correspondientes: Energía eléctrica (Incluyendo equipos de respaldo, como UPS, en caso de que aplique), Telecomunicaciones (servicio de internet), kits de emergencia, entre otros. | Programado |
| Mantener actualizada la matriz de proveedores críticos de T.I. y de operación. | Anual |
| Mantener permanentemente actualizada la base de datos básicos y detallados del personal de la OSI. | Permanente |
| Asegurar que se disponga de personal debidamente preparado para suplir a otros en el desarrollo de sus funciones en caso de ausencias, de tal forma que se pueda vincular de forma urgente en caso de requerirse. | Permanente |
| Mantener un programa de capacitación al personal de la OSI que incluya asuntos relacionados con la Continuidad del Negocio de la OSI. | Anual |
| Asegurar que el personal de la OSI esté debidamente cubierto por los esquemas de Seguridad Social correspondientes. | Mensual |
| Asegurar que se realice el debido mantenimiento preventivo de la infraestructura tecnológica requerida para el cumplimiento de los servicios por parte del personal de la OSI. | Anual |
| Mantener un inventario de la infraestructura tecnológica disponible para el personal de la OSI. | Semestral |
| Asegurar que permanezcan vigentes los contratos con aquellos proveedores de servicios catalogados como claves para el funcionamiento de la OSI, por ejemplo, el SOC. | Continuo |
| Mantener debidamente actualizado el directorio de proveedores de la infraestructura y servicios requeridos para el funcionamiento de la OSI, incluyendo contactos de proveedores alternos similares que puedan servir de respaldo en caso de requerirse. | Continuo |
| Realizar pruebas al PCN de la OSI, incluyendo las estrategias asociadas con la Tecnología, Personas y Operaciones. | Programadas |
| Socializar el modelo de gobierno y la política de continuidad de negocio de la OSI con el personal de la Oficina para promover su adopción general. | Programado |
| Coordinar la revisión anual del Plan de Continuidad del Negocio de la OSI por parte del Equipo SICN. | Anual |
| Asegurar la actualización del Plan de Continuidad de Negocio de la OSI, cuando sea requerido. | Programado |
| Coordinar reuniones de seguimiento al Plan de Continuidad de Negocio de la OSI, para verificar cumplimiento de las actividades preventivas. | Programada |

Tabla 6. Acciones Preventivas

* Pruebas y Ejercicios

**Objetivo**: Verificar la efectividad de los planes diseñados y medir la capacidad de respuesta de la OSI ante un escenario de riesgo predefinido.

**Alcance**: Servicios definidos en el plan de pruebas.

**Responsables**: Líder de Recuperación de Servicios de Seguridad y Líder de Recuperación Ciberseguridad.

El plan de pruebas consta de cinco etapas: preparación, ejecución, actividades post prueba, evaluación y mejoramiento.

1. **Preparación**

En esta etapa contempla la ejecución de las actividades necesarias para construir el escenario a simular a durante de la prueba. Incluye la coordinación con los responsables clave de los servicios, quienes informan a sus equipos la fecha de inicio, la duración y las actividades que se ejecutarán durante la prueba. También, se deben comunicar, transmitir y entregar aquellos documentos que contengan los planes detallados, con el propósito de que los participantes adquieran los conocimientos correspondientes. Estas actividades permiten asegurar que todo este previamente preparado antes de que se presente una eventual situación de interrupción.

En complemento a lo antes referido, también se debe establecer un grupo de observadores independientes de la prueba, quienes tienen el rol de analizarla y de aportar la respectiva retroalimentación.

En caso de considerarse necesario, es necesario coordinar esfuerzos con el GPET de la Rama Judicial para preparar pruebas integrales que permitan corroborar la alineación entre el PCN de la Rama Judicial y el PCN de la OSI, para determinados escenarios.

1. **Ejecución**

En esta etapa, se ejecutan las respectivas pruebas, que pueden incluir la corroboración del óptimo funcionamiento de las actividades para acceder y analizar la información, de la aplicación del árbol de llamadas o la coordinación con los proveedores clave, como por ejemplo el proveedor del SOC.

El equipo designado para monitorear las pruebas es responsable de examinar la competencia, agilidad y efectividad del personal a cargo de las actividades. El resultado de esta supervisión permitirá establecer el nivel de preparación de la OSI para responder ante la ocurrencia de determinado escenario de desastre.

La ejecución de las pruebas de continuidad debe llevarse a cabo con una periodicidad mínima de un año, considerando que, con el paso del tiempo, las estrategias planteadas en determinado momento podrían dejar de ser efectivas, mientras que también podrían haberse identificado nuevos riesgos para los cuales se requiere una preparación particular.

Es pertinente resaltar que desde la OSI también se podrían programar las denominadas pruebas de escritorio a fin de comprobar la efectividad de los flujos de trabajo definidos. También puede desarrollar pruebas orientadas exclusivamente a los procesos altamente dependientes de la tecnológica, con el propósito de comprobar si la infraestructura de respaldo funciona correctamente. También es necesario que se programen pruebas para verificar el grado de capacidad de los procesos alternos que tenga la OSI para atender determinados escenarios de desastre.

Para aquellos casos de pruebas integrales con la Rama Judicial, es necesario ejecutar las actividades de acompañamiento y articulación que permitan corroborar que el funcionamiento es el esperado.

1. **Post Prueba**

Esta etapa consiste en retornar al estado inicial existente antes de la prueba, es decir, “devolver” todos los activos, recursos o procesos a la configuración, características y/o especificaciones previas a ésta. Además, se concluye con la evaluación del plan de pruebas ejecutado y con la implementación las mejoras identificadas para dicho plan de pruebas.

1. **Evaluación de Resultados**

En esta etapa, se realiza la recopilación y análisis de los resultados obtenidos producto de la prueba o evaluación de la efectividad del Plan de Continuidad del Negocio. Aquí se elabora un informe detallado de los resultados correspondientes a los escenarios probados. Este informe, al ser presentado ante el Equipo SICN, facilita la toma de decisiones con respecto a la definición y ejecución de acciones de mejora, en caso de requerirse.

Si las pruebas se realizaron en conjunto con la Rama Judicial, en esta etapa se entregarán los insumos requeridos para garantizar que los resultados incluyan lo pertinente a lo verificado en el alcance de la OSI.

1. **Aplicación de Mejoras**

En esta última etapa, el personal de la OSI ejecuta los planes de acción de forma efectiva y oportuna. De cualquier forma, se debe gestionar la actualización de este plan de continuidad de la OSI, cuando así se amerite, a fin de mantener el mejoramiento continuo y asegurar la efectividad de este.

* Protocolo de Comunicación

**Objetivo:** Implementar una guía de coordinación y comunicación a ser acogida en el caso de la materialización de eventos que interrumpan el normal funcionamiento de la OSI y que puedan llegar a afectar sus operaciones y la imagen reputacional ante la Rama Judicial. Considerando la interdependencia entre la OSI y la Rama Judicial, es necesario que este protocolo incluya lo pertinente a los esquemas de reporte hacia el GPET.

**Alcance:** Este documento está dirigido específicamente al Equipo SICN, considerando que es la instancia de gobierno responsable de tomar decisiones frente al reconocimiento de una situación adversa que atenta contra la continuidad del negocio de la OSI y determinar los detalles referentes al reporte y coordinación con el GPET de la Rama Judicial.

**Responsables:** Miembros del Equipo SICN.

El protocolo para la comunicación interna y externa está enfocado para promover la generación de respuestas rápidas y planificadas ante situaciones adversas graves. En esencia, permite reflejar la responsabilidad, transparencia, funcionamiento organizado y solidez de la OSI ante dichas situaciones. Lo anterior, considerando que la Rama Judicial demandará información puntual y directa de parte de la OSI ante estos escenarios, razón por la cual se debe asegurar que dispongan de fuentes de información confiables, evitando que reciban reportes no oficiales o formales.

El protocolo de comunicaciones señala las pautas a ser observadas por el Equipo SICN ante la ocurrencia de eventos que se puedan presentar y requieran de su actuación. En consecuencia, es necesario evitar que cualquier colaborador de la OSI, que no esté debidamente designado por el Equipo SICN, tome iniciativas individuales de comunicar detalles de la situación y su manejo ante la Rama Judicial en casos de crisis. Como lineamiento detallado al respecto, se indica que los integrantes del Equipo SICN son quienes actuarán como voceros autorizados ante la Rama Judicial.

## Fase de recuperación

En esta fase se tienen definidos, entre otros, los siguientes objetivos:

* Contención de los daños que pudo haber originado el desastre materializado.
* Evaluación de los daños ocasionados por el mismo.
* Ejecución de planes de acción para recuperar los servicios a cargo de la OSI mediante la activación de los planes y procedimientos de continuidad de negocio previamente definidos.
* Gestión de Incidentes

**Objetivo:** Dar respuesta a incidentes de tipo tecnológico u operacional; y entregar directrices para la preparación, detección, análisis, contención, erradicación, recuperación y actividades posteriores al evento o incidente.

**Alcance:** Contempla las actividades para la adecuada identificación, reporte, evaluación, tratamiento, cierre y seguimiento de los incidentes que afecten la misión y objetivo de la entidad.

**Responsable:** El personal de la OSI es responsable de identificar y reportar los eventos, mientras que los miembros del Equipo SICN y los líderes de recuperación tendrán a cargo gestiones particulares (como la evaluación, tratamiento, cierre y seguimiento) dependiendo del tipo de incidente materializado.

Considerando que la OSI tiene una estructura limitada, la gestión de incidentes se fundamenta en la oportunidad de la comunicación por parte de los coordinadores o de los líderes de recuperación ante cualquier situación que pueda atentar contra la continuidad en la prestación de sus servicios o cumplimiento de los servicios pactados con la Rama Judicial. A su vez, cualquiera de los miembros del Equipo SICN o alguno de los Líderes de Recuperación, realizará un análisis inicial y ágil, a fin de determinar el impacto que puede originar la situación presentada, así como la complejidad de esta. Sobre la base de este análisis se determinará si es necesario alertar a todo el Equipo SICN, ante lo cual procede de conformidad. En caso de necesitarse intervención del Equipo SICN, este tomará decisiones del manejo del incidente y con respecto a la interacción con el GPET de la Rama Judicial. Conjuntamente, se definirá si se activa alguna estrategia de contingencia y se orquestan los esfuerzos del caso, tanto al interior de la OSI, así como de cara a las partes interesadas o relacionados.

* Evaluación de Daños

**Objetivo:** Cuantificar los daños a los servicios a cargo de la OSI o la infraestructura, como resultado de un evento. Es importante realizar una oportuna evaluación de daños debido a su relación directa con las acciones de respuesta.

**Alcance:** Rendir informe de los daños causados y priorización de restauración.

**Responsable:** Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad.

La evaluación de daños se refiere a informar qué sucedió, cuándo, dónde, cómo, servicios afectados, daños causados y priorización de restauración. Estas son las razones por las cuales se debe efectuar una cuidadosa evaluación:

* Proveer información sobre la situación de emergencia o desastre.
* Facilitar una efectiva toma de decisiones.
* Proveer información precisa.

Durante esta etapa se deben tener presentes los siguientes aspectos que ayudaran a precisar el nivel de daño a los servicios/activos a cargo de la OSI.

* Intervención de terceros especializados para la valorar los daños.
* Inspección de todas las operaciones afectadas teniendo en cuenta: 1) Infraestructura tecnológica, 2) Datos, información, contenidos y/o archivos esenciales (archivos, documentos, discos duros, instaladores, etc.) y 3) datos en otros soportes (datos en estaciones de trabajo, etc.).
* Tiempos de reparación de infraestructura tecnológica.
* Activación y Notificación

**Objetivo:** Aplicar un efectivo flujo de la información que derive en la movilización de recursos para responder ante determinado evento que origine la activación del Plan de Continuidad de Negocio de la OSI.

**Alcance:** Contempla las actividades comprendidas desde la toma de la decisión para activar el Plan de Continuidad de Negocio de la OSI, hasta la notificación al GPET de la Rama Judicial sobre lo ocurrido, si es necesario.

**Responsable:** El Equipo SICN es el responsable de la toma de decisiones frente a la activación del Plan de Continuidad de Negocio de la OSI y, así mismo, determinar el responsable de efectuar las notificaciones que correspondan.

Se debe tener presente la estructura definida en el árbol de llamadas durante esta etapa de activación y notificación. A continuación, se describen las actividades a ejecutar.

| **No.** | **RESPONSABLE** | **ACTIVIDAD** |
| --- | --- | --- |
| **1** | Líder de Recuperación de Servicios de Seguridad o Líder de Recuperación de Ciberseguridad | Avisa a los miembros del Equipo SICN, de manera inmediata, el máximo detalle posible del evento ocurrido. |
| **2** | Equipo SICN | Una vez informado del incidente, procederá a evaluar la situación. |
| Evaluará si es necesario reportar ante el GPET de la Rama Judicial. |
| De ser necesario activar el Plan de Continuidad de Negocio de la OSI, inicia la aplicación del árbol de llamadas. |
| Busca soluciones para gestionar el incidente materializado. |

Tabla 7. Activación y Notificación

* Recuperación de Sistemas de Información y Servicios de Tecnología

**Objetivo:** Garantizar la disponibilidad de los sistemas de información y de los servicios tecnológicos clave para el desarrollo de las operaciones, así como minimizar el daño e impacto que pueda originar la materialización de un incidente en los servicios pactados con la Rama Judicial.

**Alcance:** Aplica a aquellos servicios definidos dentro del alcance de este Plan de Continuidad del Negocio de la OSI.

**Responsables:** Líder de Recuperación de Servicios de Seguridad y Líder de Recuperación de Ciberseguridad.

Ante la ocurrencia de un incidente tecnológico que origine la interrupción en la prestación de los servicios de cara a la Rama Judicial, es necesario decidir sobre la activación o uso de infraestructura de respaldo por parte del equipo de la OSI, a fin de que pueda cumplir con los acuerdos establecidos.

Por supuesto, si la situación presentada es que se encuentra inhabilitado el centro de procesamiento principal de la Rama Judicial, en el cual están albergados los sistemas de información y herramientas necesarias para la prestación del servicio por parte de la OSI, será necesario que, en coordinación con el GPET, se establezcan los requisitos para activar los servicios tecnológicos requeridos en otros entornos, según lo definido en el PCN de la Rama Judicial. En este escenario, es importante corroborar la sincronía de versiones de los sistemas de información y herramientas entre los entornos principal y alterno. Además de hacer esta comprobación en cuanto a la funcionalidad, también debe asegurarse la correcta parametrización de las aplicaciones, los redireccionamientos de conexiones, la habilitación de usuarios requeridos, la activación de seguridades requeridas, entre otras cosas.

En seguida, es necesario probar la funcionalidad de la infraestructura de telecomunicaciones requeridas por la OSI, con la finalidad de determinar cuáles continúan igual y cuáles deben ser redireccionadas.

Considerando que el SOC es un proveedor clave de la OSI, es necesario garantizar que este tercero quede completamente habilitado con los accesos y herramientas requeridas para continuar con sus actividades, y que su interconexión con la infraestructura de la Rama Judicial funciona de forma correcta. A continuación, será necesario confirmar que el esquema de replicación de información haya permanecido funcional hasta antes del incidente. Por supuesto, en caso de que la Rama Judicial disponga de esquemas de replicación automática y sincrónica de la información requerida para la normal operación de la OSI, el inicio de operaciones en condiciones de contingencia será muy ágil.

En caso de que el incidente haya podido afectar los recursos y/o servicios tecnológicos asignados al personal de la OSI, considerando la flexibilidad de las especificaciones requeridas para el óptimo funcionamiento de este esquema, tan solo será necesario comprobar que los equipos queden debidamente enlazados y protegidos con los agentes de seguridad requeridos. La estabilidad de las conexiones a los servicios del proveedor de internet será clave para retomar las operaciones sobre la base de la información disponible en la nube.

* Recuperación de los Servicios

**Objetivo:** Dar continuidad a la prestación de los servicios pactados con la Rama Judicial.

**Alcance:** Inicia con la decisión de activar el plan de continuidad de negocio de la OSI y llega hasta ejecución de actividades con esquemas alternos.

**Responsable:** Líder de Recuperación de Servicio de Seguridad y Lídere de Recuperación de Ciberseguridad.

De acuerdo con lo definido, a continuación, se establece el orden en el cual se deben restaurar los servicios a cargo de la OSI.

* Gestionar los Incidentes de Seguridad de la Información (Crítico de la OSI).
* Inteligencia de amenazas (cacería) -SOC (Crítico de la OSI).
* Servicio de vigilancia digital – SOC (Crítico de la OSI).
* Realizar análisis de amenazas, vulnerabilidades y mitigación -SOC
* Asegurar el cumplimiento de políticas y procedimientos de seguridad de la información
* Gestionar las métricas de seguridad de la información

## Fase de restauración

Esta última fase comprende los pasos necesarios para el restablecimiento de la prestación de los servicios al estado que se encontraban antes de la materialización del incidente.

* Retorno a la Normalidad

**Objetivo:** Define las actividades para retornar a la normalidad, lo que implica volver a activar el normal funcionamiento de la infraestructura y recursos de la OSI, y desactivar el uso de tecnologías, actividades o estructuras de respaldo que operaron a partir de la activación de los esquemas de crisis.

**Alcance:** Implica la ejecución de diversas actividades para retornar a la normalidad, las cuales son particulares para cada uno de los servicios a cargo de la OSI.

**Responsables:** Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad.

En paralelo a esta fase de recuperación, también debe ejecutarse la desactivación del plan de continuidad de negocio de la OSI (fin de la contingencia). A continuación, se incluye un detalle de algunos aspectos clave para retornar a la normalidad:

| **No.** | **ACTIVIDAD** | **RESPONSABLE** |
| --- | --- | --- |
| 1 | Notificar el estado de “FIN DE INDIDENTE O DESASTRE” a todos los procesos. | - Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. |
| 2 | Confirmar oficialmente el retorno de la operación a la normalidad a todo el personal de la OSI y al GPET de la Rama Judicial. | - Integrantes del Equipo SICN |
| 3 | Coordinar la desactivación de los procesos alterno o remotos de operación. | - Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. |
| 4 | Solicitar la realización de las sesiones de análisis de lecciones aprendidas- análisis de acciones correctivas y preventivas de la interrupción experimentada. | - Integrantes del Equipo SICN. |
| - Líder de Recuperación de Servicios de Seguridad |
| - Líder de Recuperación de Ciberseguridad |
| 5 | - Realizar ajuste en los métodos utilizados. - Solicitar la actualización de los planes y de la documentación de soporte. | - Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. |

Tabla 8. Alistamiento y Retorno a la Normalidad

# INDICADORES DEL PLAN DE CONTINUIDAD DE NEGOCIO

La OSI evalúa el funcionamiento de sus planes de continuidad de negocio y la eficacia en el cumplimiento de metas, a través de los siguientes indicadores que se medirán anualmente:

| **NOMBRE DEL INDICADOR** | **RESPONSABLE** | **FORMULA** | **META** |
| --- | --- | --- | --- |
| % Revisiones al PCN | Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. | (# Revisiones realizadas) \*100  # Revisiones programadas | * 80% |
| % Actualización al PCN | Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. | (# Actualizaciones realizadas) \* 100  # Actualizaciones programadas | * 80% |
| % Cumplimiento de pruebas y ejercicios | Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. | (# Pruebas realizadas) \*100  # Pruebas programadas | * 80% |
| % Cobertura de capacitación | Líder de Recuperación de Servicios de Seguridad / Líder de Recuperación de Ciberseguridad. | (# colaboradores capacitados) \*100  # colaboradores seleccionados para capacitación | * 80% |

Tabla 9. Indicadores del Plan de Continuidad de Negocio

# PLAN DE CAPACITACIÓN EN CONTINUIDAD DE NEGOCIO

Los líderes de Recuperación de Servicios de Seguridad y de Recuperación de Ciberseguridad, así como los integrantes del Equipo SICN, definirán un plan de socialización y capacitación de los aspectos referentes a la continuidad del negocio de la OSI que se refieren en la siguiente tabla:

| **TEMA** | **OBJETIVO** | **PERIODICIDAD** | **MEDIO DE DIVULGACIÓN** |
| --- | --- | --- | --- |
| Gobierno de continuidad de negocio de la OSI | Divulgar la estructura y conformación de los equipos de recuperación y continuidad de la OSI | Anual | Intranet – virtual |
| Manejo de crisis en la OSI | Fortalecer la capacidad de respuesta a situaciones de crisis en la OSI | Anual | Intranet – virtual |
| Gestión de incidentes en la OSI | Mejorar la capacidad de detección y contención de incidentes en la OSI | Semestral | Intranet – virtual |

**Tabla 10. Plan de Capacitación**

Se tienen definidas capacitaciones internas de la OSI, capacitaciones internas para el SOC y también capacitaciones promovidas por la Rama Judicial, en las cuales deberá participar el personal de la OSI y del SOC, cuando así se determine.

# MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO

El proceso de mantenimiento se divide en las siguientes actividades de carácter periódico.

* Confirmar la vigencia o ajuste de los componentes del PCN de la OSI, incluyendo los cambios que correspondan en la documentación. Ejecutar socializaciones actualizadas a todo el personal de la OSI y capacitar a las personas que ejercen roles identificados como clave en caso de desastres que afecten a la OSI.
* Probar y verificar los procedimientos y soluciones técnicas que entran a ejecutarse o a operar en casos de crisis o materialización de eventos que interrumpen el funcionamiento de la infraestructura necesaria para la prestación de los servicios a cargo de la OSI.
* Probar y verificar los procedimientos de recuperación de servicios de la OSI.

Se ejerce una vigilancia permanente para asegurar que el Plan de Continuidad del Negocio de la OSI se encuentre debidamente actualizado, considerando la dinámica de los servicios a cargo de esta Oficina. El Plan de Continuidad de Negocio de la OSI será sometido a evaluaciones periódicas, originando los ajustes a que haya lugar. Con una frecuencia anual se debe verificar la estructura asociada con los aspectos de Continuidad del Negocio de la OSI; de este modo se buscará asegurar que se realice la debida actualización acorde con los cambios que se hayan producido en cualquiera de los siguientes aspectos:

* Requerimientos legales y/o de la Rama Judicial en cuanto a asuntos que guarden relación directa con los servicios a cargo de la OSI.
* Nuevos servicios acordados con la Rama Judicial.
* Nuevo hardware, plataformas, aplicativos, herramientas u otros cambios de tecnología asociada con los servicios a cargo de la OSI, entre las cuales pueden existir cambios promovidos desde el DRP de la Rama Judicial.
* Cambios en la estructura organizacional de la Rama Judicial que se relaciona con los servicios a cargo de la OSI
* Cambios en las conexiones de telecomunicaciones correspondientes a la operación de la OSI.
* Cambio de proveedores críticos (por ejemplo, en el SOC).
* Cambios en la estructura de personal de la OSI.
* Transferencia de funciones.
* Resultados de las pruebas del Plan de Continuidad de Negocio de la OSI.
* Dinámica de riesgos.
* Novedades en el PCN de la Rama Judicial.

# REVISIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO

Se mantendrá vigente un proceso de revisión imparcial del Plan de Continuidad del Negocio de la OSI que tendrá como objetivo el de verificar si este cumple con las necesidades de la Oficina y su conformidad con los requerimientos específicos definidos por la Rama Judicial, requerimientos legales y/o estándares internacionales.

Este proceso de revisión tendrá como alcance la ejecución de las siguientes actividades:

* En conjunto con la Rama Judicial, revisar la actualización del análisis de impacto al negocio (BIA).
* Asegurar la debida implementación de las estrategias de mitigación de riesgos.
* Revisar el plan de pruebas y los resultados de éstas.
* Revisar el mantenimiento del Plan de Continuidad de Negocio de la OSI.
* Revisar los procesos y documentos de sensibilización y capacitación.
* Entrevistar a los líderes de Recuperación de Servicios de Seguridad y de Recuperación de Ciberseguridad para confirmar que comprenden su rol y actividades a su cargo dentro del PCN de la OSI.
* Revisar documentación diligenciada o a diligenciar antes, durante y después de un desastre.
* Verificar la efectividad de las herramientas e instrumentos que apoyan el PCN de la OSI.

En consecuencia, se generarán las recomendaciones al PCN que se consideren necesarias, las cuales se registrarán en un informe de revisión. Finalmente, se establecerá un esquema de seguimiento al avance en la atención a las recomendaciones surgidas producto de la revisión, cuyos resultados se presentarán de forma periódica ante las instancias de gobierno que correspondan.