PLAN DE CONTINUIDAD DE NEGOCIO EN LA SDSCJ.

PROCESO DE CONTINUIDAD DEL NEGOCIO

Secretaria Distrital de Seguridad Convivencia y Justicia.

Tabla de Contenido

Índice de Tablas

Índice de Ilustraciones

1. Introducción

El Plan de Continuidad de Negocio de la Secretaría Distrital de Seguridad, Convivencia y Justicia establece el marco institucional para garantizar la continuidad de los servicios, procesos y funciones de la entidad ante escenarios de interrupción que puedan afectar su operación.

Este plan tiene como propósito definir los lineamientos, estructuras y acciones necesarias para que la entidad pueda responder, mantener y recuperar la prestación de sus servicios en condiciones de afectación, asegurando la protección de la misión institucional, la atención a la ciudadanía y la estabilidad de la operación.

El Plan de Continuidad de Negocio se aplica a todos los procesos institucionales y a la totalidad de los equipamientos de la Secretaría, incluyendo centros de comando, sedes administrativas, casas de justicia, centros de reclusión, centros de atención social y los demás equipamientos que hagan parte de la operación institucional y sean incorporados formalmente en los análisis, caracterizaciones o instrumentos de continuidad aplicables.

Este documento constituye el instrumento institucional que orienta la preparación, respuesta y recuperación ante interrupciones, y se articula con los demás componentes del Modelo Integrado de Planeación y Gestión, en particular con la gestión de riesgos, la planeación institucional y los mecanismos de control interno.

2. Glosario

Activo: Datos y conocimiento que tiene valor para la Entidad.

Análisis de riesgo: Proceso mediante el cual se comprende la naturaleza de un riesgo, se estima su probabilidad e impacto, y se determina su nivel para apoyar la toma de decisiones sobre su tratamiento, aceptación o seguimiento en la SDSCJ.

BACKUP: Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.

BIA – Business Impact Analysis (Análisis de Impacto al Negocio): El proceso de análisis de las actividades y el efecto que una interrupción del negocio podría tener sobre ellas.

C4: Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá**.**

CAO - Centro Alterno de Operaciones. Instalaciones físicas de respaldo que tiene una organización para movilizar los miembros de los equipos de recuperación de los procesos críticos una vez se active el plan de continuidad del negocio.

Comité de Crisis: Órgano decisorio para la gestión unificada de una situación de crisis. Su principal cometido es acelerar el proceso de toma de decisiones para solventar incidencias y/o crisis definiendo las prioridades, estableciendo la estrategia y la táctica a seguir.

Contingencia: Hecho o problema que se presenta de forma imprevista y que interrumpe la operación normal de una organización.

Control: Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Datos: Corresponde a los elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la SDSCJ.

Disponibilidad: Propiedad de que la información, los sistemas, recursos o servicios estén accesibles y utilizables cuando sean requeridos por usuarios, procesos o partes autorizadas.

DRP (Disaster Recovery Plan): Conjunto de procedimientos para restaurar rápidamente los sistemas de tecnología después de un incidente grave (fallas de servidores, ciberataques, caídas de red).

Emergencia: Situación de peligro o desastre que requiera una acción inmediata.

Escenario de interrupción: Conjunto predefinido de condiciones que describe una afectación sobre procesos, servicios, sedes, sistemas, personal o recursos críticos de la SDSCJ, con el propósito de orientar la respuesta, continuidad, recuperación y retorno a la normalidad. Cuando el evento tenga origen natural, socio-natural o tecnológico de alto impacto, podrá relacionarse con escenarios de desastre.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento Disruptivo: Situación, incidente o condición que interrumpe total o parcialmente la operación normal de la SDSCJ, afectando la prestación de servicios, la disponibilidad de recursos críticos, la atención a la ciudadanía o la continuidad de los procesos institucionales.

Gestión del riesgo: En términos generales la gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodología a riesgos particulares.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

MTPD (Máximum Tolerable Period of Disruption): Periodo Máximo Tolerable de Interrupción. El tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto / servicio o realizando una actividad, se tornen inaceptables.

Plan de continuidad del negocio (BCP): Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de la entidad generando un impacto mínimo o nulo ante una contingencia.

Plan de Recuperación de Desastres (DRP): Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos.

Plataformas misionales: Son los sistemas tecnológicos que sostienen directamente la misión de la SDSCJ.

Riesgo: Probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos para la Entidad.

RPO (Recovery Point Objective): Cantidad máxima de información que se puede perder, medida en tiempo. Ejemplo: un RPO de 1 hora significa que solo se pueden perder como máximo los datos de la última hora.

RTO (Recovery Time Objective): Tiempo de Recuperación Objetivo. Periodo de tiempo después de un incidente en el que el producto o servicio debe ser reanudado, o la actividad debe reanudarse o los recursos deben ser recuperados.

SDSCJ: Secretaría Distrital de Seguridad, Convivencia y Justicia.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como, autenticidad, trazabilidad, no repudio y fiabilidad.

Servicios Tecnológicos: Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.

Sistema de Gestión de Continuidad del Negocio: Parte del sistema de gestión institucional orientada a establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la continuidad de negocio en la SDSCJ, con base en el análisis de impactos, riesgos, escenarios, estrategias, pruebas y acciones de mejora.

Vulnerabilidad: Debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: deficiente control de accesos, poco control de versiones de software, entre otros.

3. Políticas de Gestión de Continuidad del Negocio - GCN

La Secretaría Distrital de Seguridad, Convivencia y Justicia adopta la Gestión de Continuidad de Negocio como un componente estratégico del Modelo Integrado de Planeación y Gestión, orientado a garantizar la continuidad de sus servicios, procesos y funciones ante escenarios de interrupción que puedan afectar la operación institucional.

La política de continuidad de negocio establece los principios y lineamientos generales bajo los cuales la entidad identifica, analiza, prepara, responde y recupera su capacidad operativa, asegurando la prestación de los servicios a la ciudadanía y el cumplimiento de su misión institucional.

Las políticas definidas en el presente capítulo son de aplicación transversal a todos los procesos y equipamientos de la entidad, y orientan la implementación del Plan de Continuidad de Negocio, así como la articulación con los planes subsidiarios que puedan desarrollarse a nivel de proceso

Políticas para la gestión de continuidad de negocio en la SDSCJ:

- Las actividades de continuidad de negocio se alinean con la norma ISO 22301 como directriz principal. **Por tanto, aquellos responsables directos de la documentación deben contar con conocimientos certificados en esta norma**.
- La SDSCJ mantendrá un sistema operativo, documentado, funcional y probado para asegurar la continuidad de negocio.
- Se debe implementar un proceso de mejoramiento continuo que realice revisiones periódicas de acuerdo con las estrategias definidas o tras cambios significativos en la Entidad.
- Se debe garantizar la comunicación efectiva interna y externa, especialmente ante incidentes.
- La gestión de continuidad de negocio deberá proteger a las partes interesadas, los recursos institucionales, la información crítica, la prestación de servicios y la reputación de la SDSCJ.
- Las actividades de continuidad de negocio deben ser difundidas a todos los niveles mediante el SIG del MIPG.

En particular, las políticas definidas para la gestión de continuidad de negocio (GCN) se relacionan con las siguientes políticas institucionales:

- La política de gestión del riesgo, al complementar su enfoque con medidas específicas para asegurar la continuidad operativa.
- La política de seguridad de la información, al considerar la recuperación de datos y sistemas ante fallos tecnológicos o ciberataques.
- La política de atención al ciudadano, al garantizar la prestación de servicios esenciales ante eventos disruptivos.
- La política de mejora continua, al integrar mecanismos de revisión posterior, análisis de lecciones aprendidas y actualización del plan.
- La política de gestión documental, para asegurar el resguardo de información crítica que respalde la toma de decisiones y la operación institucional.

Esta integración permite que la gestión de continuidad de negocio GCN no se conciba como un sistema aislado, sino como un componente transversal a la gestión pública y a los objetivos misionales de la Secretaría.

4. Objetivos del plan

El objetivo general del Plan de Continuidad del Negocio es establecer las medidas y acciones que debe aplicar la SDSCJ ante eventos no planificados que afecten la operación normal de sus procesos, con el fin de orientar la respuesta, mitigar los impactos y mantener o recuperar la prestación de los servicios críticos. Los objetivos específicos son:

- Proteger la integridad de los colaboradores de la SDSCJ.
- Preparar a la organización en las acciones necesarias para mantener la disponibilidad de los servicios críticos ante la ocurrencia de interrupciones significativas.
- Complementar la gestión de riesgos institucional mediante acciones orientadas a reducir el impacto de interrupciones que afecten los servicios críticos.
- Incrementar la oportunidad en la restauración de las operaciones afectadas por algún evento.
- Cumplir los requisitos normativos, técnicos y contractuales aplicables a la continuidad de negocio de la SDSCJ.
- Reducir los impactos operativos, financieros, reputacionales y de servicio derivados de interrupciones significativas.
- Facilitar la toma de decisiones durante una situación de interrupción o crisis.
- Promover acciones de mejora que fortalezcan la preparación, respuesta y recuperación de la SDSCJ frente a interrupciones.
- Asignar roles y responsabilidades a los equipos responsables de continuidad, y orientar su actuación durante la respuesta, recuperación y retorno a la normalidad.
- Coordinar las acciones de los equipos internos, actores externos y proveedores críticos para mantener y recuperar la operación.

5. Alcance

El Sistema de Gestión de Continuidad del Negocio (SGCN) de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) se aplica a los procesos estratégicos, misionales, de apoyo y de evaluación y control definidos en el marco del Modelo Integrado de Planeación y Gestión (MIPG). La priorización de acciones, estrategias y recursos se orienta principalmente a los procesos, servicios y actividades identificados como críticos mediante el Análisis de Impacto al Negocio (BIA).

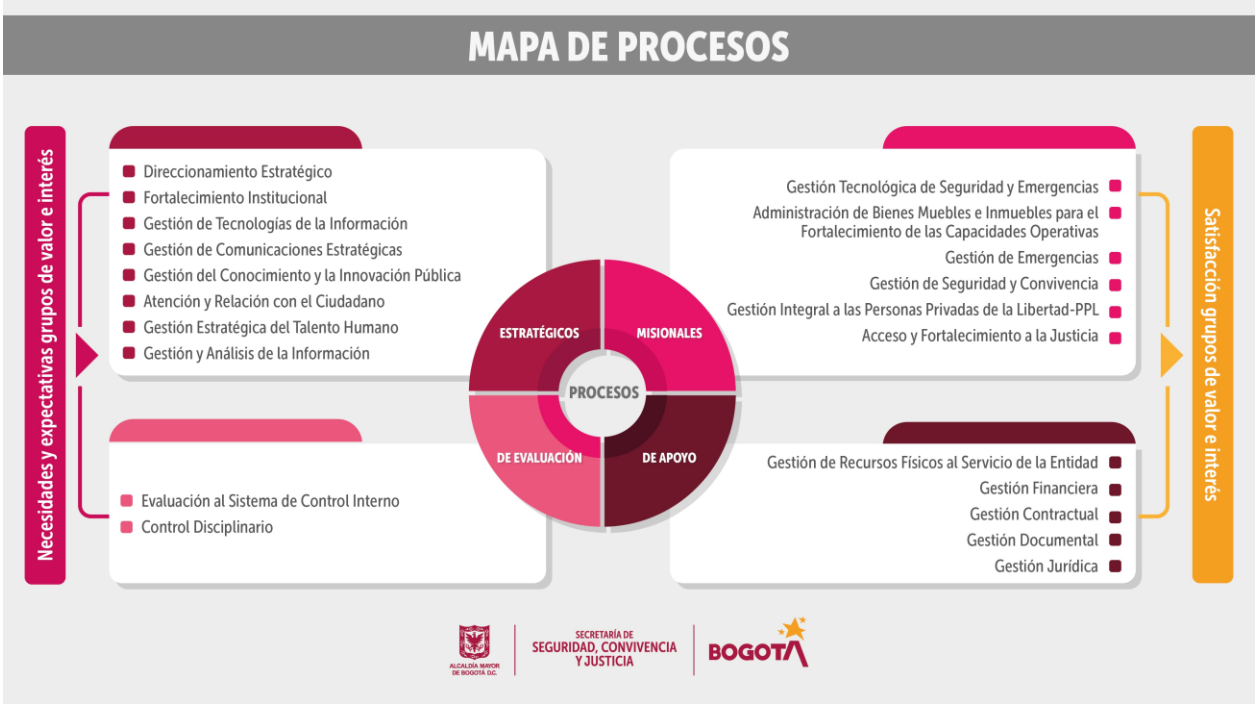

Ilustración 1 - Cadena de valor de la SDSCJ. Fuente: SDSCJ

Aplica a las dependencias, sedes, equipamientos, unidades móviles y puntos de atención en los que la SDSCJ desarrolla procesos, presta servicios o ejecuta actividades críticas.

Abarca a líderes de proceso, Oficina Asesora de Planeación, Dirección de Tecnologías y Sistemas de la Información, Talento Humano, Jurídica, Comunicaciones Estratégicas y demás dependencias o equipos que tengan responsabilidades en la preparación, respuesta, recuperación o mejora de la continuidad de negocio.

No obstante, el sistema excluye procesos de bajo impacto no priorizados, dependencias externas no controlables directamente, servicios compartidos del Distrito sin cobertura por la gestión de continuidad de negocio - GCN específica, y eventos catastróficos de escala mayor no previstos en los escenarios de planificación actual.

El SGCN se implementa con los recursos institucionales disponibles. Las estrategias que requieran inversiones adicionales deberán gestionarse mediante los instrumentos de planeación, presupuesto, contratación o fortalecimiento institucional que correspondan.

El alcance se revisará anualmente o cuando se presenten cambios significativos en el entorno interno o externo de la Entidad.

5.1. Elementos internos relevantes para la continuidad de negocio

Los siguientes elementos internos deben considerarse para planificar, activar y mantener la continuidad de los procesos y servicios críticos de la SDSCJ.

Elemento	Descripción en SDSCJ
Estructura organizacional	La SDSCJ opera mediante procesos estratégicos, misionales, de apoyo y de evaluación y control. La continuidad requiere coordinación entre líderes de proceso, dependencias de apoyo y equipos responsables de recuperación.
Recursos humanos críticos	Personal clave para operar, coordinar, tomar decisiones, atender ciudadanía, administrar infraestructura, gestionar información y recuperar servicios. Su indisponibilidad puede afectar la continuidad.
Infraestructura y tecnología	Dependencia de sedes, equipamientos, redes, sistemas de información, plataformas de monitoreo, comunicaciones, energía y servicios tecnológicos. Su afectación puede limitar la prestación de servicios críticos.
Procesos, servicios y actividades críticas priorizadas en el BIA	El BIA identifica procesos, servicios y actividades críticas, así como dependencias, impactos y tiempos de recuperación que orientan la priorización de la respuesta.
Cultura organizacional	Nivel de conocimiento, preparación y apropiación de los equipos frente a continuidad, gestión del riesgo, protocolos, pruebas y simulacros.
Gestión documental e información	Disponibilidad de información, registros vitales y documentos necesarios para operar, responder, recuperar servicios y soportar decisiones durante una interrupción.
Presupuesto y recursos asignados	Disponibilidad de recursos para implementar, mantener, probar y mejorar las estrategias de continuidad, así como para gestionar necesidades adicionales cuando se requiera.
Coordinación interna	Coordinación con dependencias de apoyo como OAP, Tecnologías, Talento Humano, Jurídica, Recursos Físicos, Gestión Documental, Comunicaciones Estratégicas y demás áreas requeridas según el escenario.

Tabla 1. Elementos internos relevantes para la Continuidad de Negocio. Fuente: SDSCJ

5.2. Elementos externos relevantes para la continuidad de negocio

Elemento	Descripción en SDSCJ
Normatividad distrital y nacional	Requisitos normativos y lineamientos distritales o nacionales aplicables a gestión pública, riesgos, transparencia, información, atención ciudadana y continuidad operativa.
Entidades externas y autoridades	Coordinación con Policía, Fiscalía, Secretaría de Gobierno, entidades distritales, nacionales y demás autoridades que inciden en la operación o respuesta de la SDSCJ.
Ciudadanía y grupos de valor	Expectativas de continuidad, oportunidad, información y confianza frente a servicios relacionados con seguridad, convivencia, justicia, emergencias y atención institucional.
Eventos naturales, sociales o tecnológicos	Situaciones como sismos, inundaciones, incendios, bloqueos, protestas, fallas de servicios públicos, apagones o eventos tecnológicos que pueden afectar sedes, equipamientos o servicios.
Amenazas de ciberseguridad	Ataques, pérdida de datos, secuestro de información, indisponibilidad de plataformas o afectación de servicios tecnológicos que soportan la operación institucional.
Medios de comunicación y reputación	Exposición pública ante interrupciones, fallas de servicio o manejo inadecuado de la comunicación durante eventos de crisis.
Proveedores críticos	Dependencia de proveedores de conectividad, servicios tecnológicos, mantenimiento, infraestructura, servicios públicos, logística u otros bienes y servicios necesarios para la continuidad.
Contexto político-administrativo	Cambios en prioridades institucionales, estructura, lineamientos o disponibilidad de recursos pueden incidir en la ejecución y sostenibilidad de estrategias de continuidad.

Tabla 2. Elementos externos relevantes para la Continuidad de Negocio. Fuente: SDSCJ

6. Documentos de referencia

Los documentos y referencias aplicadas para la elaboración de este plan de continuidad de negocio son:

Referencia	Descripción del documento
NTC ISO-22301:2019 Norma internacional de Gestión de Continuidad de Negocio.	Norma internacional que establece los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, la prueba, el mantenimiento de una Gestión de Continuidad del Negocio - GCN.
Norma Internacional de Gestión de seguridad de la información ISO 27001:2022	Este documento especifica los requisitos para estableces, implementar, mantener y de forma continua mejorar una Gestión de Seguridad de la Información. El documento también incluye requisitos para la evaluación y tratamiento de riesgos de seguridad de la información. Incluye controles relacionados con Seguridad de la Información dentro de los que se encuentran los referentes a continuidad de negocio.
Guía para la preparación de las TIC para la continuidad del negocio, del 15 diciembre del 2010 de MINTIC.	Guía del Ministerio de Tecnologías de la información y las comunicaciones define un modelo de operación de Continuidad de Negocio y Privacidad de la Información.
Guía para realizar el Análisis de Impacto de Negocios BIA, del 12 de mayo de 2015 de MINTIC.	Guía del Ministerio de Tecnologías de la información y las comunicaciones define una serie de pasos para realizar y análisis el BIA.

Tabla 3. Referencias técnicas de Continuidad de Negocio. Fuente: SDSCJ

7. Requisitos legales y reglamentarios

El Sistema de Gestión de Continuidad del Negocio (SGCN) de la Secretaría Distrital de Convivencia, Seguridad y Justicia (SDSCJ) se fundamenta en un marco normativo compuesto por disposiciones nacionales, distritales y técnicas, que exigen garantizar la operación continua de los servicios públicos misionales y de apoyo.

Estos requisitos han sido integrados en la política, el alcance, los análisis de impacto y riesgo, y la definición de estrategias operativas del presente Plan de Continuidad del Negocio.

Norma o disposición	Aplicación para la SDSCJ
Decreto 612 de 2018 – MIPG	Establece la gestión del riesgo y la continuidad como componentes obligatorios del modelo de gestión pública. Debe incorporarse en la planeación institucional y en los procesos estratégicos.
Ley 87 de 1993 – Sistema de Control Interno	Obliga a tener planes de contingencia y mecanismos que aseguren la operación continua de la entidad. Es base para el control posterior y auditorías internas.
Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública	La continuidad de los servicios también implica mantener la disponibilidad de información y sistemas de atención en emergencias.
Ley 594 de 2000 – Ley General de Archivos	Establece medidas para la conservación y recuperación de documentos en caso de emergencia. Afecta directamente al sistema de información institucional.
Ley 1341 de 2009 – Régimen TIC	Impone lineamientos sobre continuidad operativa de servicios TIC públicos. Reforzada por la Guía MINTIC 150506.
Documento Técnico Plan de Continuidad del Negocio – Función Pública (versión mayo 2019)	No es norma legal, pero es una **referencia técnica obligada** para entidades públicas. Define roles, fases del plan y estructura mínima esperada.
Decreto Distrital 591 de 2018	Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG en las entidades y organismos distritales.
Guías y lineamientos internos del Distrito (MECI – SIG Bogotá)	Exigen mantener operación continua de servicios esenciales. En SDSCJ aplica a procesos como atención ciudadana, conciliación, seguridad y convivencia.

Tabla 4. Requisitos legales relacionados con Continuidad de Negocio. Fuente: SDSCJ

Ver Normas asociados del documento en https://portalmipg.scj.gov.co

8. Partes interesadas y sus requisitos

Como parte de la comprensión de su contexto, la Secretaría Distrital de Convivencia, Seguridad y Justicia ha identificado a las partes interesadas relevantes que pueden afectar o ser afectadas por el Sistema de Gestión de Continuidad del Negocio (SGCN). Estas partes interesadas incluyen tanto actores internos (como líderes de proceso, áreas de apoyo y la alta dirección), como externos (ciudadanía, otras entidades distritales, entes nacionales y proveedores).

Cada parte interesada tiene necesidades y expectativas específicas relacionadas con la continuidad de los servicios críticos de la Entidad, especialmente en situaciones de emergencia, disrupción o crisis.

La identificación y evaluación periódica de estas partes interesadas permitirá mantener actualizado el sistema y garantizar su pertinencia frente a las obligaciones legales, sociales y misionales de la SDSCJ.

Parte interesada	Rol / interés en el GCN
Ciudadanía y comunidad en general	Usuarios finales de servicios de justicia, seguridad y convivencia
Alta Dirección de la SDSCJ	Responsable del liderazgo, priorización y recursos del SGCN
Líderes de proceso	Dueños de los procesos críticos institucionales
Oficina de Planeación	Responsable de articular políticas, planes, indicadores y seguimiento
Oficina de Tecnologías de la Información	Encargada de plataformas, comunicaciones, seguridad y respaldo digital
Talento Humano	Responsable de personal clave, bienestar y continuidad operativa
Oficina Jurídica y Control Interno	Revisión normativa y aseguramiento de cumplimiento
Secretarías distritales aliadas (Gobierno, Seguridad, Salud, Mujer, Educación)	Actores interinstitucionales con coordinación operativa
Policía Nacional y Fiscalía	Entidades aliadas para la seguridad y la respuesta a incidentes
Función Pública y MINTIC	Entidades que emiten lineamientos técnicos y normativos
Proveedores de servicios tecnológicos y logísticos	Apoyo externo para operación TIC, suministros, conectividad, mantenimiento
Medios de comunicación y opinión pública	Interlocutores de la percepción social e institucional

Tabla 5. Partes interesadas identificadas por la SDSCJ

9. Herramientas para el desarrollo del Plan de Continuidad de Negocio

9.1. Análisis de Impacto al Negocio (BIA)

9.1.1. Propósito del BIA en la SCJ

El Análisis de Impacto al Negocio (BIA) constituye el instrumento central del Sistema de Gestión de Continuidad de Negocio de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ). Su propósito es identificar los procesos institucionales cuya interrupción tendría un efecto crítico en la misión, los servicios al ciudadano o el cumplimiento de las funciones legales de la entidad, evaluando el impacto operativo, reputacional, tecnológico y económico que podría derivarse de dicha interrupción.

El BIA es el insumo institucional que permite identificar procesos, servicios, recursos y dependencias críticas para orientar escenarios, estrategias y prioridades de continuidad. La metodología, parámetros, responsables y modelo de actualización del BIA se desarrollan en la Guía G-DE-06

Los resultados del BIA sirven como insumo para:

- Los Planes de Continuidad por Proceso, en los cuales se documentan los escenarios de interrupción, los recursos mínimos requeridos y los procedimientos de recuperación.
- El Plan Institucional de Continuidad, que consolida la priorización general de procesos críticos y orienta la planificación de estrategias transversales (Centro Alterno de Operaciones – CAO, Plan de Recuperación ante Desastres – DRP, teletrabajo, coordinación interinstitucional, entre otras).

9.1.2. Resultados BIA utilizados para seleccionar escenarios de interrupción

Con base en los resultados consolidados del BIA, la SDSCJ identifica las dependencias críticas que sustentan la selección de los escenarios institucionales de interrupción.:

Dependencia de infraestructura física – Escenario: Interrupción por afectación de infraestructura o equipamiento.

El BIA evidencia alta dependencia de infraestructura física y equipamientos institucionales para la prestación de servicios críticos. Esta condición justifica mantener un escenario de interrupción por afectación de infraestructura o equipamiento.

Variable	Valor consolidado	Fuente BIA
Pérdida de sede o infraestructura	62 % de procesos dependientes de infraestructura física	(**BIA – Hoja "Procesos Misionales"**) -Dependencias críticas
Estrategias de respaldo o CAO disponible	35 % de procesos con sede alterna identificada	(**BIA – Hoja "Estrategias y Respaldos"**) – Estrategias de respaldo
Impacto operativo por pérdida de sede	Promedio 4.6 (escala 1–5)	(**BIA – Hoja "Evaluación de Impactos"**) - Criterio de impacto operativo

Tabla 6 - Dependencia de infraestructura física - Evaluación BIA - Fuente SDSCJ

Dependencia tecnológica – Escenario: Indisponibilidad total de plataformas TIC (ciberataque o falla extendida)

El BIA evidencia dependencia alta de plataformas TIC, sistemas de información y servicios tecnológicos que soportan procesos misionales y de apoyo. Esta condición justifica mantener un escenario de indisponibilidad total de plataformas TIC.

Variable	% Procesos Afectados	Promedio RPO (h)	Observación técnica
Dependencia de aplicativos críticos (**BIA – Hoja "Dependencias TIC"**)	78 %	4	Mayor impacto en NUSE 123, Orfeo y sistemas de justicia.
Requisito de respaldo redundante / DRP (**BIA – Hoja "Estrategias y Respaldos TIC"**)	55 %	–	Identificada en bases de datos y servidores locales.
Impacto económico por interrupción TIC (**BIA – Hoja "Evaluación de Impactos"**)	4.2 (escala 1–5)	–	Afectación transversal a operaciones misionales y de apoyo.

Tabla 7 - Dependencia tecnológica - Evaluación BIA - Fuente SDSCJ

Dependencia de personal clave – Escenario: Ausencia masiva de personal clave

El BIA evidencia dependencia de personal clave y necesidad de sustitutos para funciones críticas. Esta condición justifica mantener un escenario de ausencia masiva de personal clave.

Variable	% Procesos Afectados	Nivel de Impacto (1–5)	Tolerancia (días)
Procesos con ≤ 5 personas en función crítica (**BIA – Hoja "Talento Humano"**)	46 %	4.5	≤ 2
Existencia de sustituto operativo designado (**BIA – Hoja "Talento Humano"**)	28 %	–	–
Dependencia de personal especializado (**BIA – Hoja "Evaluación de Impactos"**)	32 %	4.7	≤ 1

Tabla 8 - Dependencia de personal clave - Evaluación BIA - Fuente SDSCJ

Dependencia de servicios de soporte – Escenario: Interrupción por afectación de servicios de soporte

El BIA evidencia dependencia de servicios de soporte internos y externos, incluyendo energía, conectividad, mantenimiento, logística, salud, alimentación, seguridad y proveedores críticos. Esta condición justifica mantener un escenario de interrupción por afectación de servicios de soporte.

Variable	Valor consolidado	Fuente BIA
Procesos con proveedores internos críticos con importancia alta o muy importante	21 de 21 procesos institucionales	BIA – Hoja "06 Proveedores_internos" – Campo "Importancia"
Procesos con proveedores externos críticos con importancia alta o muy importante	19 de 21 procesos institucionales	BIA – Hoja "05 Proveedores_externos" – Campo "Importancia"
Procesos con dependencias asociadas a energía, conectividad, telecomunicaciones o red	11 de 21 procesos institucionales	BIA – Hojas "05 Proveedores_externos", "06 Proveedores_internos" y "09 Sistemas_informacion"
Procesos con dependencias asociadas a logística, mantenimiento, transporte, seguridad, alimentación, salud o soporte operativo	10 de 21 procesos institucionales	BIA – Hojas "05 Proveedores_externos" y "06 Proveedores_internos"
Procesos con impactos de interrupción valorados en nivel 3 o superior	6 de 21 procesos institucionales	BIA – Hoja "11 Impactos interrrupcion"

Tabla 9 - Dependencia de servicios de soporte – Evaluación BIA – Fuente SDSCJ

Escenarios de interrupción priorizados a partir del BIA

La correlación de los criterios de impacto evaluados en el BIA permite identificar los escenarios de interrupción que representan las condiciones más críticas para la SDSCJ:

Escenario de interrupción	Criterio BIA predominante	Procesos afectados (alta criticidad)	Justificación técnica
Interrupción por afectación de infraestructura o equipamiento.	Impacto operativo y logístico	6 de 6 misionales	Dependencia física directa y baja redundancia de espacios alternos.
Indisponibilidad total de plataformas TIC (ciberataque o falla extendida).	Impacto tecnológico y económico	14 de 21 procesos totales	Alta dependencia TIC y requisito de redundancia o DRP activo.
Ausencia masiva de personal clave.	Impacto operativo y legal	7 de 21 procesos totales	Dependencia de personal especializado y requisito de sustituto designado.
Interrupción por afectación de servicios de soporte.	Impacto operativo, tecnológico y logístico	21 de 21 procesos institucionales	Dependencia transversal de servicios de soporte como energía, conectividad, mantenimiento, logística y proveedores críticos

Tabla 10 - Escenarios de interrupción priorizados a partir del BIA - Fuente SDSCJ

9.2. Análisis de Riesgos de Continuidad de Negocio (RA)

9.2.1. Contexto y Enfoque Metodológico

El Análisis de Riesgos de Continuidad de Negocio (RA) es un componente esencial que identifica las amenazas potenciales que podrían materializarse, afectando la capacidad de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) para cumplir con los Tiempos Objetivos de Recuperación (RTO) y los Puntos Objetivos de Recuperación (RPO) definidos en el Análisis de Impacto al Negocio (BIA).

La gestión de riesgos de CN en la SDSCJ se integra directamente con el Sistema de Gestión de Riesgos Institucional, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG). La SDSCJ utiliza la Matriz Institucional de Riesgos, formato F-FI-1382 en su versión vigente, como herramienta oficial para la identificación, valoración, tratamiento y seguimiento de los riesgos que pueden afectar la continuidad.

Definición Operativa del Riesgo de Continuidad:

Un riesgo es considerado de continuidad cuando, al materializarse, interrumpe la prestación de servicios esenciales al ciudadano o compromete la capacidad operativa o de soporte institucional por un periodo inaceptable, afectando el cumplimiento de los tiempos definidos en el BIA.

La identificación de estos riesgos constituye un insumo fundamental para la definición de los escenarios de interrupción establecidos en el presente plan.

9.2.2. Identificación institucional de riesgos que afectan la continuidad

La identificación de riesgos en la SDSCJ se realiza de manera estructurada por cada proceso, siguiendo las directrices del procedimiento o modelo de gestión de riesgos de la SDSCJ. Esta identificación se clasifica según las categorías definidas en la metodología institucional de riesgos, las cuales se presentan de forma referencial en la siguiente ilustración:

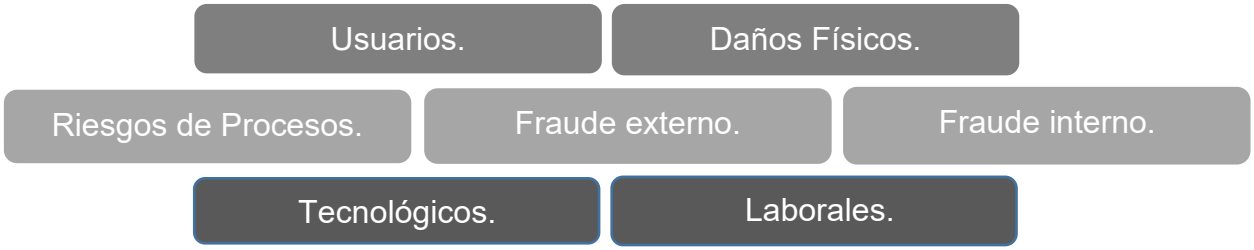

Ilustración 2 - Categoría de riegos. Fuente SDSCJ

Aplicación de la Matriz F-FI-1382

La SDSCJ asegura la trazabilidad del SGCN dentro de la gestión institucional mediante el campo de marcación definido en la Matriz Institucional de Riesgos F-FI-1382: '**¿Afecta la continuidad?**' o el campo equivalente que se encuentre vigente.

Criterio de Marcación: Cada líder de proceso debe marcar 'Sí' cuando el riesgo pueda interrumpir o degradar servicios, actividades, recursos o dependencias críticas identificadas en el BIA. La justificación debe documentarse en el análisis de riesgos del proceso.

Ejemplo Aplicado (Riesgos Tecnológicos):

- La falla en plataformas tecnológicas institucionales se marca como "Sí", dado que compromete la operación de procesos misionales y la prestación de servicios críticos.

9.2.3. Valoración y Priorización bajo el Modelo de Gestión de Riesgos de la SDSCJ

Una vez que los riesgos se marcan que afectan la continuidad del negocio, estos se integran y continúan su ciclo en el Proceso de Gestión de Riesgos institucional, el cual se enmarca en el MIPG y se desarrolla conforme a la Guía de Administración de Riesgos G-FI-04 o el documento interno que la actualice.

El análisis, valoración, tratamiento y monitoreo de los riesgos se realiza conforme a la metodología institucional de administración de riesgos vigente.

Priorización Operativa:

El Plan de Continuidad establece que los riesgos que afectan la continuidad deben priorizarse en su valoración, tratamiento y seguimiento.

9.2.4. Uso Operativo de los Riesgos

Los riesgos identificados se utilizan como insumo para la toma de decisiones, la prevención y la planificación de la continuidad institucional:

1. **Definición de Escenarios de Interrupción:** Los riesgos de mayor impacto y probabilidad constituyen insumos para la definición de los escenarios de interrupción institucional. El BIA identifica las consecuencias de una interrupción; el análisis de riesgos identifica las causas que pueden originarla.
2. **Definición de acciones preventivas:** Las acciones definidas en los planes de tratamiento de riesgos, tales como contratación de proveedores alternos, respaldo de información, mantenimiento de infraestructura y fortalecimiento de capacidades operativas, se articulan con la fase preventiva del Plan de Continuidad de Negocio.
3. **Asignación de responsabilidades y seguimiento**: Cada riesgo que afecta la continuidad se asocia a un responsable dentro del proceso correspondiente, asegurando la implementación de acciones preventivas y correctivas. El seguimiento y actualización de estos riesgos se realiza conforme al ciclo institucional de gestión de riesgos.

4. **Articulación con los planes de continuidad por proceso:** Cuando un proceso no cuente aún con plan específico, el Plan de Continuidad de Negocio institucional orientará la respuesta inicial ante los escenarios de interrupción definidos. No obstante, el Plan de Continuidad de Negocio institucional mantiene su capacidad operativa independiente para orientar la respuesta ante escenarios de interrupción.

9.3. Estrategias de respuesta y recuperación de aplicación en SDSCJ

De manera general las estrategias de recuperación tecnológica y de continuidad del negocio para que la SDSCJ supere una interrupción, pueden verse reflejadas en las siguientes alternativas, pueden usarse más de una por Proceso:

Creación de un Centro Alterno de Operaciones (CAO). Definir modalidad, dimensionamiento, capacidades mínimas, activación/retorno, roles y abastecimiento.		**Respaldo TIC y Plan de Recuperación de Desastres (DRP).** Arquitectura de recuperación por capas (datos, aplicaciones, plataformas, conectividad), RPO/RTO, conmutación y pruebas.
Teletrabajo como mecanismo de contingencia. Modalidades de operación mínima, controles, acceso remoto seguro, escalamiento por turnos y criterios de activación.	**Priorización de procesos y servicios críticos.** Reglas de priorización basadas en BIA (criticidad, RTO/MTPD), niveles de servicio mínimos y colas de atención.	**Coordinación interinstitucional.** Enlaces y protocolos con entidades distritales y nacionales roles, canales y escalamiento.

Ilustración 3 - Alternativas de recuperación. Fuente: adaptación de la norma ISO 22301:2019 Clausulas 8.2 a 8.4.

10. Escenarios de interrupción

10.1. Articulación de escenarios de interrupción

La SDSCJ define sus escenarios de interrupción como condiciones institucionales que pueden afectar la continuidad de los servicios y superar los Tiempos Máximos de Interrupción Tolerable (MTPD) identificados en los BIA por proceso.

La definición de estos escenarios se fundamenta en el análisis conjunto de los resultados del Análisis de Impacto al Negocio (BIA), la gestión institucional de riesgos y las dependencias

críticas identificadas en los procesos institucionales, permitiendo establecer estrategias de continuidad coherentes con las necesidades operativas de la entidad:

1. **Selección de Escenarios de Referencia**: se identifican eventos o condiciones con capacidad de afectar sedes, equipamientos, plataformas, personal o servicios de soporte críticos para la SDSCJ:

Afectación de infraestructura o equipamiento | Indisponibilidad TIC | Afectación de servicios de soporte | Ausencia masiva de personal clave | Indisponibilidad de sedes

2**. Mapeo de Criticidad:** Los escenarios de interrupción se correlacionan con los resultados de los BIA por proceso, priorizando los procesos, servicios o actividades con criticidad alta o muy crítica, y los procesos de apoyo que habilitan la operación institucional.

3**. Vinculación con la Gestión Institucional de Riesgos**: Los escenarios de interrupción se validan frente a los riesgos identificados en la Matriz Institucional de Riesgos F-FI-1382, en su versión vigente, especialmente aquellos que afectan a la continuidad del negocio. Esta correlación permite priorizar estrategias institucionales de prevención, respuesta y recuperación.

4. **Diseño de Estrategias de Respuesta**: Con base en los escenarios definidos, la SDSCJ establece estrategias institucionales orientadas a mantener niveles mínimos aceptables de operación, incluyendo mecanismos de operación alterna, recuperación tecnológica, trabajo remoto, uso de sedes alternas, fortalecimiento logístico y medidas de recuperación operativa.

Con base en el BIA y la gestión institucional de riesgos, la SDSCJ define los escenarios de interrupción institucional con mayor capacidad de afectar la continuidad de los servicios.

Estos escenarios se aplican de manera transversal a los diferentes procesos y equipamientos de la entidad y constituyen la base para la definición de estrategias de continuidad, respuesta y recuperación.

Cuando existan planes de continuidad específicos por proceso, estos desarrollarán el componente operativo aplicable al proceso. Cuando un proceso no cuente aún con plan específico, el presente Plan de Continuidad de Negocio institucional orientará la respuesta inicial ante los escenarios de interrupción definidos.

10.2. Escenario 1: Interrupción por afectación de infraestructura o equipamiento.

Este escenario contempla la afectación total o parcial de uno o varios equipamientos institucionales de la SDSCJ, ocasionando la interrupción de la operación de los procesos y servicios que dependen de dichos espacios físicos.

La afectación puede originarse por daños físicos, fallas estructurales, emergencias, restricciones de acceso, órdenes de cierre o fallas de servicios que impidan el uso seguro o funcional del equipamiento institucional.

A. Aplicación al contexto de la SDSCJ según BIA vigente:

- **Amenazas o factores detonantes asociados**: sismos, incendios, fallas estructurales, inundaciones, bloqueos, restricciones de acceso, órdenes de cierre, emergencias de seguridad o fallas de servicios que impidan el uso del equipamiento.

- Afectación institucional: La indisponibilidad de equipamientos institucionales puede afectar la prestación de servicios misionales, estratégicos, de apoyo y de evaluación, especialmente aquellos cuya operación depende de infraestructura física especializada o atención presencial.

B. Estrategia de Continuidad Escenario 1:

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Afectación total o parcial de sedes, equipamientos o puntos de atención que impida o restrinja la operación normal de servicios de la SDSCJ.	Activación de sedes alternas, operación alterna y Plan de Emergencias.
Desencadenantes	Sismo, incendio, inundación, daño estructural, bloqueo, restricción de acceso, orden de cierre, emergencia de seguridad o falla de servicios que impida el uso del equipamiento.	Declaración de situación de interrupción y activación del CIGD.
Procesos Afectados	Procesos que operan en la sede, equipamiento o punto afectado; procesos de apoyo requeridos para recuperación física, logística, tecnológica, documental, comunicaciones y talento humano.	Priorización de procesos críticos y activación de trabajo alterno.
Dependencias Críticas	La continuidad depende de que la sede, equipamiento o punto de atención afectado cuente con condiciones físicas seguras y funcionales para operar, incluyendo acceso habilitado, áreas utilizables, condiciones locativas mínimas, mobiliario básico, equipos de trabajo disponibles, información crítica accesible y control de ingreso al lugar.	Identificar qué sede, equipamiento, área física o punto de atención quedó afectado; confirmar si existen condiciones seguras para ingreso, permanencia u operación; comunicar la afectación a Recursos Físicos, Tecnología, Gestión Documental, Talento

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
		Humano, Comunicaciones y al líder del proceso impactado, según corresponda; definir si la operación continúa en el mismo lugar, se restringe, se traslada temporalmente o se activa operación alterna; y priorizar la recuperación física de los espacios necesarios.
Acciones Inmediatas	Activación del Plan de Emergencias, evacuación, evaluación de daños, notificación a autoridades y traslado de personal clave. Informar a los responsables internos y activar comunicación institucional según el nivel del evento.	Coordinación institucional y habilitación de operación alterna.
Criterio de Retorno	Validación técnica de condiciones seguras y restablecimiento de servicios mínimos operativos.	Autorización institucional para retorno gradual de la operación.

Tabla 11. Estrategia de continuidad Escenario 1 - Pérdida Catastrófica por daño físico. Fuente: SDSCJ.

Para generar cambios o la creación de nuevos planes subsidiarios o por proceso puede referirse a la guía: 16.1. ANEXO – 1 Guía para Estrategia Centro Alterno de Operaciones (CAO).

10.3. Escenario 2: Indisponibilidad total de plataformas TIC (ciberataque o falla extendida)

Este escenario contempla la indisponibilidad total o parcial de plataformas tecnológicas institucionales críticas, afectando la operación de los procesos y servicios de la SDSCJ. La afectación puede originarse por ciberataques, fallas tecnológicas extendidas, indisponibilidad de infraestructura tecnológica o incidentes de seguridad de la información.

A. Aplicación al contexto de la SDSCJ según BIA vigente:

- Amenazas o factores detonantes: ciberataques, ransomware, malware, denegación de servicio, falla extendida de infraestructura tecnológica, daño en centros de procesamiento o almacenamiento, indisponibilidad de conectividad, afectación de servicios tecnológicos críticos o incidente de seguridad de la información con impacto operativo.

- La indisponibilidad de plataformas tecnológicas institucionales afecta procesos misionales, estratégicos y de apoyo que dependen de sistemas de información, servicios digitales, conectividad y acceso a información institucional.

- El BIA evidencia tiempos reducidos de recuperación para servicios tecnológicos críticos, por lo que este escenario requiere activación prioritaria de recuperación tecnológica y operación alterna.

B. Estrategia de continuidad ante indisponibilidad total de plataformas TIC por ciberataque o falla extendida:

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Indisponibilidad total o parcial de plataformas tecnológicas institucionales causada por ciberataque, falla extendida o afectación de infraestructura tecnológica.	Activar la respuesta técnica de Tecnología, priorizando las plataformas que soportan servicios críticos, y adoptar operación en modo degradado cuando no sea posible recuperar el servicio.
Desencadenantes	Ciberataque, ransomware, malware, falla masiva de infraestructura tecnológica, pérdida de conectividad o indisponibilidad de servicios críticos TIC.	Declaración de situación de interrupción y activación del CIGD. Confirmar el tipo de afectación, contener el incidente cuando aplique, preservar evidencias, restringir accesos comprometidos y escalar la situación según los procedimientos de tecnología y seguridad de la información.
Procesos Afectados	Procesos que dependan de sistemas institucionales, plataformas tecnológicas, conectividad o acceso a información digital.	Identificar servicios críticos afectados, aplicar mecanismos alternos de operación, registrar la información mínima necesaria y reportar afectaciones.
Dependencias Críticas	La continuidad depende de la disponibilidad de plataformas misionales, sistemas de información, bases de datos, autenticación, conectividad, redes, respaldos, servicios tecnológicos, proveedores TIC y soporte especializado de la Dirección de Tecnologías y Sistemas de la Información.	Identificar qué plataforma, servicio, proveedor o componente técnico está afectado; confirmar responsable interno y tercero asociado; comunicar la afectación a Tecnología y a los procesos impactados; escalar al proveedor cuando corresponda; verificar respaldos, conectividad, accesos e integridad de datos; y priorizar la recuperación de los servicios tecnológicos.
Acciones Inmediatas	Aislamiento de sistemas afectados, activación de protocolos de seguridad, restauración de respaldos y notificación a responsables técnicos.	Coordinación técnica y recuperación priorizada de servicios críticos.
Criterio de Retorno	Validación de estabilidad operativa, disponibilidad de servicios críticos y verificación de integridad de la información.	Restablecimiento controlado y monitoreo reforzado de plataformas TIC.

Tabla 12. Estrategia de continuidad Escenario 2 - Indisponibilidad total de plataformas TIC por ciberataque o falla extendida. Fuente: SDSCJ

La activación técnica, conmutación, restauración, validación de respaldos y retorno tecnológico se desarrolla conforme a los procedimientos técnicos vigentes definidos por la Dirección de Tecnologías y Sistemas de la Información.

Cuando existan planes de contingencia o continuidad específicos para plataformas, subsistemas o procesos, estos deberán activarse de manera articulada con el presente escenario institucional, sin duplicar responsabilidades técnicas ni operativas.

Para generar cambios o la creación de nuevos planes subsidiarios o por proceso puede referirse a la guía: 16.2. ANEXO – 2 Estrategia Respaldo TIC y Plan de Recuperación de Desastres

10.4. Escenario 3: Ausencia masiva de personal clave

Este escenario contempla la indisponibilidad masiva de personal clave para la operación institucional, afectando la capacidad de ejecución de los procesos y servicios de la SDSCJ. La afectación puede originarse por emergencias sanitarias, restricciones de movilidad, situaciones administrativas, laborales, de seguridad o cualquier condición que limite la disponibilidad del personal requerido para la operación.

A. Aplicación al contexto de la SDSCJ según BIA vigente:

- Amenazas o factores detonantes: emergencias sanitarias o epidemiológicas, restricciones de movilidad, ausentismo masivo, afectación de turnos, indisponibilidad simultánea de roles clave, vacancias no cubiertas, restricciones de ingreso o situaciones de seguridad que limiten la disponibilidad del personal requerido.

- Afectación Crítica: La indisponibilidad de personal clave identificado en los BIA por proceso afecta la capacidad operativa institucional, especialmente en procesos con funciones especializadas, cobertura mínima o tiempos reducidos de recuperación.

B. Estrategia de Continuidad ante Ausencia masiva de personal clave.

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Indisponibilidad masiva de personal clave que impide sostener la operación normal o mínima de procesos y servicios institucionales críticos.	Los líderes de proceso deben activar la reorganización operativa disponible, priorizando las actividades críticas definidas en el BIA y asignando el personal disponible a las funciones que no pueden suspenderse sin afectar la continuidad institucional.
Desencadenantes	Emergencias sanitarias o epidemiológicas, restricciones de movilidad, ausentismo masivo, afectación de turnos, indisponibilidad	Declaración de situación de interrupción y activación del CIGD. El líder del proceso debe verificar la cobertura real disponible, identificar roles o funciones críticas sin

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
	simultánea de roles clave, vacancias no cubiertas, restricciones de ingreso o situaciones de seguridad.	respaldo y escalar la situación al nivel táctico o estratégico cuando la capacidad del proceso no permita sostener la operación mínima.
Procesos Afectados	Procesos cuya operación depende de cobertura mínima, turnos, atención presencial, operación especializada, coordinación institucional, soporte técnico, gestión documental, atención ciudadana o toma de decisiones críticas.	Cada proceso afectado debe definir qué actividades se mantienen, cuáles se restringen temporalmente y cuáles se reprograman, asegurando trazabilidad de pendientes y continuidad de los servicios priorizados.
Dependencias Críticas	La continuidad depende de la disponibilidad de roles clave, suplencias definidas, redistribución temporal de funciones, coordinación con Gestión Estratégica del Talento Humano, liderazgo del proceso, comunicación interna y condiciones mínimas para trabajo alterno cuando aplique.	Identificar los cargos, roles o funciones críticas afectadas; confirmar personal disponible y posibles suplencias; coordinar con Talento Humano y líderes de proceso la redistribución temporal; comunicar ajustes operativos a los equipos impactados; y escalar necesidades de apoyo cuando no exista capacidad interna suficiente.
Acciones Inmediatas	Confirmación de disponibilidad real de personal, identificación de funciones críticas afectadas, definición de operación mínima, reasignación temporal de funciones, activación de trabajo alterno cuando aplique y comunicación de ajustes operativos.	El líder del proceso debe coordinar la redistribución del personal disponible, mantener seguimiento a la cobertura mínima, controlar pendientes críticos y reportar a la instancia de continuidad correspondiente cuando la ausencia afecte tiempos de recuperación, atención ciudadana o servicios misionales.
Criterio de Retorno	Cobertura mínima estabilizada, roles críticos cubiertos, turnos o funciones normalizados, pendientes críticos controlados y capacidad operativa validada por los líderes de proceso afectados.	El retorno debe realizarse de manera progresiva, normalizando actividades reprogramadas, cerrando pendientes generados durante la contingencia y registrando decisiones, impactos y acciones de mejora para ajustar suplencias o esquemas de respaldo de personal.

Tabla 13. Estrategia de continuidad: Escenario 3 - Ausencia Masiva de Personal Clave. Fuente: SDSCJ

Para generar cambios o la creación de nuevos planes subsidiarios o por proceso puede referirse a la guía: 16.3. ANEXO – 3 Teletrabajo como mecanismo de contingencia

10.5. Escenario 4: Interrupción por afectación de servicios de soporte

Este escenario contempla la afectación de servicios de soporte internos o externos requeridos para la operación de los procesos y equipamientos institucionales de la SDSCJ, generando limitaciones para la continuidad de los servicios aun cuando la infraestructura, las plataformas tecnológicas y el personal clave se encuentren disponibles.

A. Aplicación al contexto de la SDSCJ según BIA vigente:

- **Amenazas o factores detonantes**: Fallas de energía eléctrica, Interrupción de conectividad o telecomunicaciones, Indisponibilidad de servicios logísticos o de transporte, Fallas en servicios de mantenimiento o soporte operativo, Interrupción de servicios de seguridad física o control de acceso, Indisponibilidad de proveedores críticos.
- **Afectación Crítica:**
  La interrupción de servicios de soporte afecta transversalmente la capacidad operativa de los procesos institucionales, especialmente aquellos que dependen de servicios públicos, conectividad, logística, proveedores críticos o servicios de apoyo para mantener la continuidad de la operación.

  El análisis de los BIA por proceso evidencia dependencias recurrentes asociadas a energía, conectividad, soporte operativo y proveedores internos y externos críticos, lo que puede afectar tanto procesos misionales como estratégicos, de apoyo y de evaluación.

B. Estrategia de Continuidad Escenario 4: Interrupción por afectación de servicios de soporte

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Interrupción de servicios de soporte internos o externos que afecta varios procesos, sedes, equipamientos, canales de atención o servicios críticos de la SDSCJ.	El **CIGD** define prioridades institucionales cuando la afectación comprometa la continuidad. Las dependencias responsables gestionan recuperación, alternativas o escalamiento. La **OAP** asesora metodológicamente la aplicación del PCN.
Desencadenantes	Fallas extendidas de energía, conectividad, telecomunicaciones, transporte, logística, mantenimiento, seguridad física, control de acceso, servicios públicos o proveedores críticos.	La dependencia responsable confirma origen, alcance y duración estimada. Los líderes de proceso reportan impactos sobre servicios críticos. El **CIGD** define restricciones, priorización o modo degradado cuando aplique.
Procesos Afectados	Procesos estratégicos, misionales, de apoyo y de evaluación que dependen de los servicios de soporte interrumpidos para sostener actividades críticas definidas en el BIA.	Los líderes de proceso identifican actividades afectadas y aplican los ajustes definidos. Las dependencias responsables priorizan la recuperación de los soportes que habilitan servicios críticos.
Dependencias Críticas	La continuidad depende del servicio de soporte afectado, la dependencia interna responsable, el proveedor externo cuando aplique, las alternativas disponibles y los tiempos de restablecimiento.	Identificar el soporte afectado, responsable interno y proveedor asociado; activar comunicación con la dependencia responsable; escalar al proveedor cuando corresponda; y priorizar el restablecimiento según criticidad BIA.

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Acciones Inmediatas	Confirmar servicios interrumpidos, sedes y procesos afectados, duración estimada, alternativas disponibles y restricciones operativas.	Las dependencias responsables gestionan la recuperación. Los líderes de proceso aplican operación degradada o restricciones. Comunicaciones Estratégicas apoya mensajes internos o externos cuando haya impacto ciudadano o reputacional.
Criterio de Retorno	Servicios de soporte restablecidos o sustituidos de forma estable, procesos críticos operando, restricciones levantadas y afectaciones registradas.	Las dependencias responsables confirman restablecimiento. Los líderes de proceso validan normalización de actividades críticas. El **CIGD** valida el retorno cuando haya tomado decisiones institucionales durante el evento.

Tabla 14 - Estrategia de continuidad Escenario 4 – Interrupción por afectación de servicios de soporte.
Fuente: SDSCJ

Otros anexos para evaluar y referir la creación de escenarios:

16.4. ANEXO – 4 Priorización de procesos y servicios críticos

16.5. ANEXO – 5 Coordinación interinstitucional

16.6. ANEXO - 6 Metodología para la creación de escenarios de interrupción.

11. Gobierno y estructura de continuidad

La estructura de gobierno y continuidad de negocio de la SDSCJ establece los niveles de dirección, coordinación y ejecución requeridos para garantizar la respuesta institucional ante escenarios de interrupción que afecten la prestación de los servicios y la operación de los procesos institucionales.

El modelo de gobierno definido en el presente plan se articula con la estructura organizacional de la entidad y con el Modelo Integrado de Planeación y Gestión (MIPG), permitiendo coordinar la toma de decisiones estratégicas, la gestión operativa y la recuperación de los servicios institucionales.

Esta estructura reemplaza el modelo de "Comité de Crisis" para integrar sus funciones de alta gobernanza en el Comité Institucional de Gestión y Desempeño (CIGD), atendiendo a las directrices institucionales sobre la consolidación de órganos colegiados no obligatorios por mandato legal, garantizando que el CIGD actúe como el máximo órgano de gestión estratégica y toma de decisiones.

Justificación Normativa para la Integración al CIGD

- La observación institucional que promueve la actualización del Comité de Gestión y Desempeño, estableciendo que este sustituirá los demás comités no obligatorios por mandato legal (Resolución 579 de 2023, Artículo 1, Parágrafo 1, conforme a la solicitud), se articula con el marco general del Modelo Integrado de Planeación y Gestión (MIPG).

- Propuesta de Sustitución: Se propone que las funciones de gobernanza estratégica y de manejo de crisis del actual Comité de Crisis sean asumidas por el Comité Institucional de Gestión y Desempeño (CIGD), manteniendo la autoridad para la toma de decisiones estratégicas y la activación del PCN.

El gobierno de continuidad se organiza en tres niveles, asegurando la capacidad de respuesta oportuna: Estratégico (Decisión), Táctico (Coordinación) y Operativo (Ejecución).

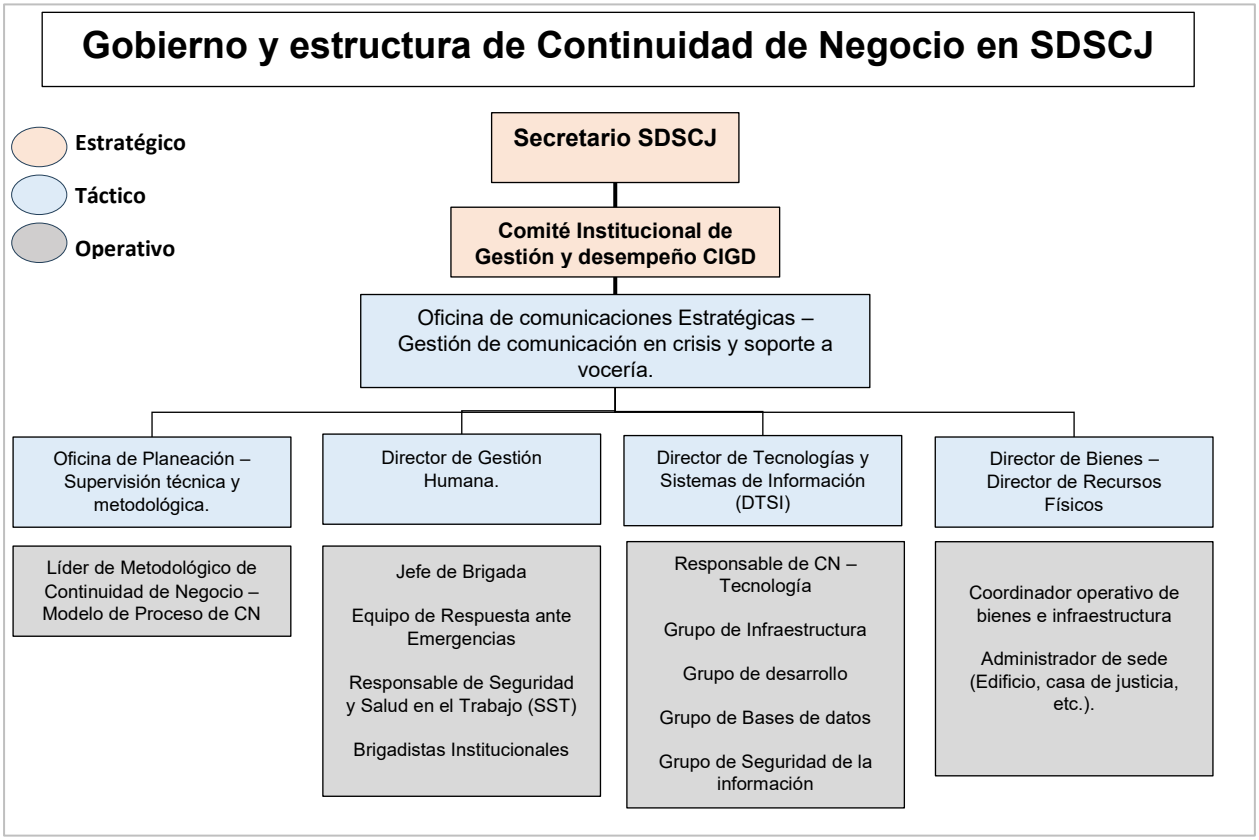

Ilustración 4 - Gobierno y estructura de Continuidad de Negocio. Fuente SDSCJ

11.1. Nivel Estratégico: liderazgo y gobierno de continuidad

El nivel estratégico corresponde a la instancia responsable de direccionar, priorizar y coordinar las decisiones institucionales relacionadas con la continuidad de negocio ante escenarios de interrupción que afecten la operación de la SDSCJ.

En el marco del presente plan, el Comité Institucional de Gestión y Desempeño (CIGD) asume las funciones institucionales de direccionamiento estratégico, priorización y toma de decisiones para la continuidad de la operación institucional.

11.1.1. Comité Institucional de Gestión y Desempeño (CIGD)

El CIGD asume las funciones de gobernanza estratégica y manejo de crisis, y actúa como máxima instancia de decisión cuando la interrupción tiene alcance institucional, supera la capacidad de respuesta ordinaria o compromete servicios críticos de la SDSCJ.

Justificación y Convocatoria en Emergencia: El CIGD será convocado de manera extraordinaria cuando la interrupción tenga impacto institucional, comprometa servicios críticos, requiera priorización de recursos, active decisiones de crisis o supere la capacidad de respuesta de los procesos o dependencias responsables.

Participantes del nivel estratégico: El CIGD en su función de Comité de Crisis, estará compuesto por la Alta Dirección y directivos clave:

- Secretario Distrital de Seguridad, Convivencia y Justicia: Liderazgo, Presidencia del CIGD y rol de Director de Emergencia (Comando Superior durante la Crisis).
- Subsecretarios (Seguridad y Convivencia; Gestión Institucional; Acceso a la Justicia).
- Jefe Oficina Asesora de Planeación.
- Director de Tecnologías y Sistemas de Información.
- Jefe de Comunicaciones Estratégicas.
- Director Centro de Comando, Control, Comunicaciones y Cómputo (C4).
- Jefe de la Oficina Jurídica; Jefe de la Oficina de Control Interno; Subdirector(a) de Gestión del Talento Humano (Invitados permanentes/Miembros según normatividad del CIGD).

Cuando la afectación o el escenario de interrupción comprometa la operación de procesos misionales específicos, los líderes de proceso correspondientes participarán en las sesiones de coordinación y toma de decisiones del CIGD, con el fin de suministrar información operativa, priorizar necesidades de continuidad y apoyar la definición de acciones institucionales de respuesta y recuperación.

Funciones Principales del CIGD (Gobernanza GCN):

- Aprobación y Revisión: Avalar y aprobar la Política de GCN, el Plan de Continuidad Institucional, las estrategias de continuidad (CAO, DRP) y los resultados del Análisis de Impacto al Negocio (BIA).
- Liderazgo y Recursos: Suministrar los recursos necesarios para el desarrollo, mantenimiento y mejora del Plan de Continuidad del Negocio.
- Riesgo: Orientar las decisiones institucionales sobre riesgos que afectan la continuidad, conforme a la política y metodología de administración de riesgos vigente.
- Activación institucional: Declarar la situación de crisis institucional y autorizar lineamientos de continuidad, priorización o modo degradado cuando la interrupción comprometa servicios críticos. La activación técnica del DRP se realizará conforme a los procedimientos de Tecnología, con escalamiento al CIGD cuando tenga impacto institucional.
- Monitoreo: Evaluar el Informe de Madurez del SGCN y el resultado de las pruebas periódicas, promoviendo la mejora continua.

11.1.2. Dirección institucional durante escenarios de interrupción (Secretario Distrital)

El Secretario Distrital, como máxima autoridad de la SDSCJ y presidente del CIGD, orienta las decisiones institucionales de alto impacto durante escenarios de interrupción y ejerce la vocería principal, directamente o mediante delegación, con apoyo de la Oficina de Comunicaciones Estratégicas.:

- **Decisión institucional:** Orientar o autorizar decisiones de alto impacto sobre priorización de servicios, restricciones operativas, comunicación institucional, uso de recursos y activación de estrategias de continuidad cuando el evento supere la gestión ordinaria.
- **Dirección institucional:** Liderar, desde el CIGD, las decisiones estratégicas para sostener o recuperar servicios críticos.
- **Vocería oficial:** Ejercer o delegar la vocería institucional, con apoyo de la Oficina de Comunicaciones Estratégicas para la preparación y difusión de mensajes internos o externos.

11.2. Nivel Táctico: Coordinación y Liderazgo del SGCN

El nivel táctico corresponde a las dependencias responsables de habilitar, coordinar o ejecutar componentes técnicos, logísticos, tecnológicos, humanos, comunicacionales y metodológicos necesarios para la continuidad institucional, de acuerdo con su competencia.

11.2.1. OAP / Líder metodológico de continuidad de negocio

Responsable: Jefe de la Oficina Asesora de Planeación (OAP) o delegado.

Requisito de Competencia: El responsable principal o delegado debe contar con formación, conocimiento o experiencia suficiente en continuidad de negocio e ISO 22301:2019 para orientar metodológicamente la implementación del SGCN.

Funciones Principales:

- Coordinación Metodológica: Orientar metodológicamente la implementación, mantenimiento y mejora del SGCN, y definir lineamientos, formatos, criterios y controles de trazabilidad del modelo de continuidad.
- Gestión del BIA/Riesgos: Facilitar metodológicamente la actualización del BIA, el análisis de riesgos que afectan la continuidad y la trazabilidad con los planes de continuidad, en coordinación con los líderes de proceso y las dependencias responsables.
- Propuesta de Activación: Aportar criterios metodológicos del PCN, BIA, escenarios y estrategias documentadas para apoyar la toma de decisiones del CIGD y de los responsables técnicos durante una interrupción.
- Monitoreo: Consolidar información metodológica, indicadores, resultados de pruebas, avances de implementación y madurez del SGCN para seguimiento del CIGD en condiciones normales o posteriores al evento.

- Pruebas: Coordinar metodológicamente el programa anual de pruebas del PCN, con participación de las dependencias responsables, consolidando resultados, evidencias y lecciones aprendidas.

11.2.2. Dirección de Tecnologías y Sistemas de Información

Responsable: Director de Tecnologías y Sistemas de Información.

Funciones Principales:

- DRP: Gestionar y supervisar la adecuación, implementación, documentación y pruebas del Plan de Recuperación de Desastres (DRP) de TI.
- Activación Tecnológica: Liderar la recuperación de servicios tecnológicos críticos, conectividad, plataformas, respaldos, seguridad de la información y demás componentes TIC requeridos para la operación institucional.
- Soporte: Garantizar el soporte tecnológico necesario para que se pueda cumplir con los objetivos de la misionalidad de la entidad.
- Proveedores TIC: Coordinar el escalamiento y seguimiento con proveedores tecnológicos cuando la recuperación dependa de servicios externos, licenciamiento, infraestructura, conectividad o soporte especializado.

11.2.3. Recursos físicos, bienes e infraestructura

Responsables: Director de Recursos Físicos y Gestión Documental y Director de Bienes para la Seguridad, Convivencia y Acceso a la Justicia, según el tipo de recurso, sede, bien, equipamiento o servicio afectado.

Este rol táctico agrupa las responsabilidades relacionadas con la disponibilidad física, locativa, documental, logística y de bienes requeridos para sostener o recuperar la operación institucional durante un escenario de interrupción. Su participación se activa cuando la continuidad de los procesos, sedes, equipamientos, puntos de atención o servicios críticos dependa de condiciones físicas, recursos materiales, bienes muebles o inmuebles, vehículos, espacios alternos, mantenimiento, administración de inmuebles o recuperación de condiciones mínimas de operación.

- **Recursos Físicos y Gestión Documental - Función Principal:** Este rol táctico agrupa las responsabilidades relacionadas con la disponibilidad física, locativa, documental, logística y de bienes requeridos para sostener o recuperar la operación institucional durante un escenario de interrupción. Su participación se activa cuando la continuidad de los procesos, sedes, equipamientos, puntos de atención o servicios críticos dependa de condiciones físicas, recursos materiales, bienes muebles o inmuebles, vehículos, espacios alternos, mantenimiento, administración de inmuebles o recuperación de condiciones mínimas de operación.

- **Bienes para la Seguridad, Convivencia y Acceso a la Justicia - Función principal**: Verificar la afectación sobre bienes, equipamientos, inmuebles, vehículos o recursos operativos administrados por la Dirección. Coordinar las acciones de mantenimiento, recuperación, reposición, uso alterno o escalamiento contractual con proveedores, supervisores o terceros responsables, cuando estos bienes sean necesarios para sostener servicios críticos o capacidades operativas institucionales.

11.2.4. Gestión Estratégica del Talento Humano

Responsable: Director de Gestión Humana.

Función principal: apoyar la identificación de disponibilidad de personal, suplencias, novedades administrativas, lineamientos de trabajo alterno y medidas relacionadas con capacidad humana requerida para sostener actividades críticas.

11.2.5. Comunicaciones Estratégicas

Responsable: Jefe de la Oficina Asesora de Comunicaciones.

Función principal: preparar, validar y canalizar mensajes internos o externos asociados a la interrupción, de acuerdo con las decisiones del CIGD y la vocería autorizada.

11.3. Nivel Operativo: Ejecución y Recuperación

Este nivel ejecuta las acciones de continuidad, operación degradada, recuperación y retorno a la normalidad. Actúa bajo la conducción de los líderes de proceso y dependencias responsables, y se articula con el CIGD cuando la interrupción alcance nivel institucional.

11.3.1. Líderes de Proceso y Equipos de Recuperación

Los Líderes de Proceso son los responsables directos de asegurar la continuidad de sus funciones críticas.

Responsables: líder del proceso designado en MIPG, líder operativo del proceso y equipo de recuperación definido en el plan específico cuando exista.

Equipo de Recuperación: Compuesto por funcionarios clave nombrados por el Líder del proceso y encargado entre otras actividades de efectuar el BIA.

Funciones Principales:

- Mantenimiento de Planes: Mantener actualizado el BIA, la información de riesgos que afectan la continuidad y el plan de continuidad del proceso, con revisión metodológica de la OAP cuando corresponda.

- Ejecución: Ejecutar las acciones definidas en el plan de su proceso, incluyendo el traslado a un Centro Alterno de Operaciones (CAO), la activación del teletrabajo, o la activación de proveedores alternos.
- Reporte: Reportar al Líder del Proceso, líder operativo y dependencias responsables el avance, dificultades y afectación de tiempos definidos en el BIA. Cuando el evento escale institucionalmente, reportar según el canal definido para el CIGD. La OAP podrá recibir información para trazabilidad metodológica y mejora del PCN.
- Pruebas: Participar activamente en pruebas y simulacros, asegurando que su equipo conozca y practique los procedimientos.

11.4. Modelo de participación de los roles durante la interrupción

Propósito. Establecer la participación de los roles durante la interrupción, la operación en modo degradado, la recuperación y el retorno a la normalidad.

Ilustración 5 - Modelo de participación por roles durante la emergencia. Fuente SDSCJ

12. Fases del Plan de Continuidad del Negocio

La administración del Plan de Continuidad del Negocio se realiza en tres fases, de acuerdo con el momento de la interrupción:

12.1. Fase Preventiva

La fase preventiva comprende el conjunto de acciones orientadas a reducir la probabilidad de interrupción de los procesos institucionales y a fortalecer las capacidades internas de preparación.

12.1.1. ANTES – Fase Preventiva: Capacitación y Sensibilización

La capacitación y sensibilización fortalecen la capacidad de los servidores públicos y contratistas para reconocer su rol, aplicar los canales definidos y actuar de forma coordinada ante escenarios de interrupción.

12.1.1.1. Objetivo de formación y divulgación

El propósito es asegurar que los servidores públicos y contratistas conozcan el PCN, identifiquen su rol y actúen conforme a los lineamientos definidos para su proceso o dependencia. La formación debe orientarse a:

- Difundir los principios de la continuidad de negocio y los pilares definidos en el plan institucional.
- Asegurar que cada funcionario identifique el rol de su proceso en escenarios de crisis.
- Fortalecer la capacidad de respuesta inmediata y coordinada frente a incidentes que interrumpan los servicios críticos de la Secretaría.

12.1.1.2. Capacitaciones periódicas y campañas de sensibilización

La capacitación en continuidad de negocio tendrá periodicidad anual y se complementará con campañas internas de sensibilización. Los contenidos deberán ajustarse al rol de los procesos y podrán divulgarse mediante los canales institucionales definidos por la SDSCJ.

Además, se complementarán con campañas de sensibilización internas que refuercen los mensajes clave del plan de continuidad, como:

- Importancia de proteger los procesos críticos.
- Correcto uso de los canales oficiales de comunicación en crisis.
- Reglas básicas de activación del CAO, DRP y teletrabajo en contingencias.

Estas campañas pueden realizarse a través de correos institucionales, afiches en sedes, cápsulas informativas en la intranet o charlas breves en reuniones de equipo.

12.1.1.3. Inducciones actualizadas con Continuidad de Negocio

La inducción institucional deberá incluir un componente básico de continuidad de negocio, orientado a explicar qué es el PCN, cuáles son los roles principales y cómo reportar o actuar ante una interrupción. Este módulo puede incluir, de manera breve y práctica:

- Qué es el Plan de Continuidad de Negocio institucional.
- Cuáles son los roles principales durante una crisis.
- Cómo debe actuar un funcionario frente a una interrupción (Ejemplo a quién reportar, qué canales usar, dónde consultar información).

Este componente no sustituye las capacitaciones anuales, pero asegura que desde su ingreso los servidores comprendan que la continuidad de negocio es parte de la cultura organizacional.

12.1.1.4. Indicadores de seguimiento y responsables

La evaluación de la capacitación y sensibilización en continuidad debe planearse de forma gradual. Se inicia con los siguientes indicadores de alto nivel y luego se fortalecerán para orientar a posibles mejoras:

- % de servidores capacitados en continuidad de negocio cada año.
- Número de campañas internas ejecutadas anualmente.

La OAP orienta metodológicamente los contenidos de continuidad; la Dirección de Gestión Humana articula su inclusión en procesos de formación o inducción; y los líderes de proceso aseguran la participación de sus equipos cuando sean convocados.

12.1.2. ANTES – Fase Preventiva: Planes de Continuidad por Proceso

El PCN institucional orienta la elaboración de los planes de continuidad por proceso, los cuales desarrollan las acciones específicas para mantener, recuperar o restablecer la operación ante

escenarios de interrupción. La formulación, actualización y aplicación de estos planes corresponde al Líder del Proceso y a su equipo de continuidad, con revisión metodológica de la OAP. Cuando la complejidad, ubicación o criticidad lo requiera, podrán elaborarse planes por área o dependencia, siempre como instrumentos subsidiarios del plan del proceso correspondiente.

12.1.3. ANTES – Fase Preventiva: Plan de pruebas y ejercicios

Las pruebas y ejercicios permiten verificar la aplicabilidad del PCN, la comprensión de roles, la coordinación entre dependencias y la capacidad de recuperación frente a escenarios de interrupción. Su planeación, ejecución, registro y evaluación se desarrollan conforme al Plan de Pruebas del PCN PL-DE-03 y al programa anual de pruebas definido por la SDSCJ.

12.2. Fase de Respuesta

Esta fase tiene por objetivo contener la afectación, evaluar el impacto y activar las acciones necesarias para mantener, recuperar o restablecer los procesos y servicios críticos de la SDSCJ.

12.2.1. DURANTE – Fase de Respuesta: Plan de gestión del riesgo de desastres

El Plan de Gestión del Riesgo de Desastres y los protocolos de emergencia aplicables orientan la protección de personas, la respuesta inicial y la coordinación frente a eventos de origen natural, socio-natural, tecnológico o humano no intencional. El PCN se articula con estos instrumentos para definir la continuidad, operación alterna, recuperación y retorno a la normalidad, una vez controlada la condición inicial de emergencia.

12.2.2. DURANTE – Fase de Respuesta: Plan de Evaluación de Daños

Objetivo: identificar el alcance de la afectación sobre personas, sedes, equipamientos, plataformas, información, proveedores, servicios de soporte y procesos críticos, para definir la activación o continuidad de las acciones del PCN.

Actividad	Responsable principal	Evidencia mínima
Verificar el alcance de la afectación sobre personas, sedes, plataformas, información, proveedores, servicios de soporte y procesos críticos.	Dependencia responsable según el tipo de afectación, con reporte al Líder del Proceso y al CIGD cuando el evento tenga alcance institucional.	Reporte inicial de afectación, registro de decisiones y soportes técnicos o administrativos disponibles.

Tabla 15. Ejemplo Fase de Respuesta – Evaluación inicial de afectación. Fuente SDSCJ

12.2.3. DURANTE – Fase de Respuesta: Plan de activación y notificación

Objetivo: determinar el flujo de la información para activar la movilización de recursos para la respuesta ante algún evento que active el Plan de Continuidad del Negocio.

La activación del PCN institucional corresponde al CIGD cuando la interrupción tenga alcance institucional o supere la capacidad ordinaria de los procesos. Los planes por proceso podrán activarse por el Líder del Proceso, conforme a sus criterios internos de escalamiento y notificación.

12.2.4. DURANTE – Fase de Respuesta: Comunicación en crisis

La comunicación en crisis dentro de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) tiene como objetivo asegurar que la información fluya de manera rápida, clara y verificable, tanto hacia el interior de la entidad como hacia la ciudadanía y los actores externos clave, evitando rumores, duplicidad de mensajes o vacíos de información.

La comunicación en crisis dentro de la SDSCJ se fundamenta en tres pilares:

Uso disciplinado de los **canales institucionales**	**Voceros definidos** según el nivel de crisis	**Lineamientos de transparencia** que garanticen confianza ciudadana

De esta manera, se asegura que la Secretaría pueda mantener la continuidad de sus procesos y preservar su legitimidad frente a la ciudadanía en escenarios de emergencia.

12.2.4.1. Lineamientos de transparencia

La SDSCJ, como entidad pública, está obligada a mantener altos estándares de transparencia en el manejo de la información en crisis. Para ello se establecen los siguientes lineamientos:

Oportunidad

Los mensajes iniciales deben **emitirse dentro de la primera hora de ocurrido el evento,** incluso si aún no se tiene un balance definitivo.

Claridad

La información debe ser **comprensible para la ciudadanía,** evitando tecnicismos excesivos.

Veracidad

Solo se divulgarán **datos confirmados por el Comité de Crisis;** no deben emitirse especulaciones.

Periodicidad

Mientras dure la contingencia, deben emitirse actualizaciones regulares (cada 2–3 horas para incidentes mayores, al cierre de la jornada en eventos menores).

Accesibilidad

Toda la información publicada en web y redes debe permanecer disponible para consulta posterior, como parte del principio de rendición de cuentas.

12.2.4.2. Mecanismos de comunicación interna y externa

En situaciones de crisis o interrupciones de servicios críticos, la SDSCJ debe utilizar de forma prioritaria los canales institucionales ya establecidos:

- **Internos:** correos electrónicos oficiales, intranet de la entidad, circulares internas y mensajería segura entre áreas críticas (incluyendo grupos cerrados de coordinación para emergencias). Estos mecanismos garantizan que los líderes de proceso y sus equipos reciban instrucciones claras y oportunas.

- **Externos:** página web institucional (www.scj.gov.co), comunicados oficiales en redes sociales (X/Twitter y Facebook de la Secretaría), boletines de prensa y ruedas de medios coordinadas por la Oficina de Comunicaciones Estratégicas. Estos canales son los que la ciudadanía reconoce como fuentes legítimas de información y deben ser usados para todo anuncio en crisis.

12.2.4.3. Voceros autorizados

El esquema de vocerías en crisis se organiza por niveles:

- **Nivel estratégico:** El Secretario Distrital de Seguridad, Convivencia y Justicia es el vocero principal de la entidad y el responsable de emitir mensajes oficiales en casos de crisis institucionales de gran magnitud (Ejemplo sismos que afecten la sede central, ataques al sistema 123, indisponibilidad general de servicios).
- **Nivel táctico:** Los Subsecretarios y Directores actúan como voceros técnicos de acuerdo con el tipo de crisis. **Por ejemplo**, el Director del C4 comunica medidas relacionadas con emergencias y operación del 123, el Director de Tecnologías y Sistemas de Información explica incidentes tecnológicos, y el Jefe de Recursos Físicos aborda problemas logísticos.
- **Nivel operativo:** Los coordinadores de procesos críticos pueden brindar información puntual a equipos internos y al Líder de Continuidad, pero no son voceros externos. En todos los casos, deben canalizar sus reportes hacia el CIGD y la Oficina de Comunicaciones.

Este esquema se alinea con la práctica actual de la Secretaría, en la que el Secretario es el vocero por defecto, salvo delegación expresa en un Subsecretario o Director específico según la naturaleza del evento.

12.2.4.4. Coordinación con medios

Toda comunicación con medios debe estar centralizada en la **Oficina de Comunicaciones Estratégicas**, que actúa como enlace único para preparar comunicados, atender entrevistas y garantizar la coherencia de los mensajes. Esta oficina se coordina directamente con el CIGD para autorizar la publicación de información, de manera que se mantenga consistencia entre lo que se informa al interior y lo que se comunica al público. La prioridad es ofrecer mensajes únicos, claros y verificables que generen confianza en la ciudadanía y eviten contradicciones.

12.2.5. DURANTE – Fase de Respuesta: Recuperación en sitio y en CAO

Describe cómo el proceso se restablece en su ubicación habitual si es posible, o cómo traslada su operación al Centro Alterno de Operaciones (CAO).

La recuperación puede realizarse en el sitio habitual, en un espacio alterno, mediante operación remota o a través del CAO, según el escenario, criticidad del servicio y disponibilidad de recursos.

Actividad	Responsable principal	Evidencia mínima
Definir si la recuperación se realiza en el sitio habitual, en sede alterna, mediante trabajo remoto, con apoyo de CAO o a través de recursos temporales.	CIGD cuando el evento sea institucional; Líder del Proceso cuando la afectación sea del proceso; dependencias técnicas según el recurso afectado.	Acta, reporte o registro de activación de estrategia de recuperación, con responsable, alcance y condición de operación.

Tabla 16. Ejemplo Fase de Respuesta - Recuperación en sitio, alterna o CAO. Fuente: SDSCJ

12.2.6. DURANTE – Fase de Respuesta: Plan De Recuperación De Desastres Tecnológicos - DRP

El DRP define las acciones técnicas para recuperar servicios tecnológicos críticos, respaldos, conectividad, plataformas e información dentro de los tiempos definidos en el BIA. Su ejecución corresponde a la Dirección de Tecnologías y Sistemas de Información, conforme a los procedimientos técnicos vigentes y al Anexo 2 del presente plan.

12.3. Fase de restauración

12.3.1. DESPUES – Fase de restauración: Retorno a la normalidad

Objetivo: definir las condiciones para retornar progresivamente a la operación normal, una vez se verifique la estabilidad de los recursos, sedes, plataformas, personal, proveedores o servicios de soporte afectados. Implica las actividades de regreso a la normalidad de los procesos críticos de la entidad.

Actividad	Responsable principal	Evidencia mínima
Validar que los recursos, servicios, plataformas, sedes o capacidades afectadas se encuentren estables para retornar progresivamente a la operación normal.	Responsable técnico o dependencia competente, con validación del Líder del Proceso y del CIGD cuando haya sido activado.	Registro de autorización de retorno, verificación de estabilidad y cierre de restricciones operativas.

Tabla 17. Ejemplo Fase de Restauración - Retorno a la normalidad. Fuente SDSCJ.

12.3.2. DESPUES – Fase de restauración: Fase de restauración: cierre de operación temporal

Objetivo: definir las acciones para cerrar la operación temporal, alterna o degradada, una vez se autorice el retorno a la operación normal.

Actividad	Responsable principal	Evidencia mínima
Cerrar la operación temporal, alterna o degradada, asegurando regularización de registros, control de pendientes y disponibilidad futura de los recursos de contingencia.	Líder del Proceso y dependencia responsable del recurso utilizado en contingencia.	Registro de cierre, pendientes regularizados y relación de recursos utilizados o liberados.

Tabla 18. Ejemplo Fase de Restauración – Cierre de operación temporal. Fuente SDSCJ

12.3.3. DESPUES – Fase de restauración: Lecciones aprendidas y acciones de mejora

Proceso de evaluación posterior al evento para identificar qué funcionó, qué falló y qué debe mejorarse en los planes.

En esta etapa se documentan los resultados del evento, las decisiones adoptadas, las brechas identificadas y las acciones de mejora requeridas.

Actividad	Responsable principal	Evidencia mínima
Evaluar el evento, identificar brechas, documentar lecciones aprendidas y definir acciones de mejora sobre el PCN, planes por proceso, estrategias, roles o recursos.	Líder del Proceso, dependencias participantes y OAP como asesor metodológico.	Informe o acta de evaluación, matriz de acciones de mejora y responsables definidos.

Tabla 19. Ejemplo Fase de Restauración - Lecciones aprendidas y acciones de mejora. Fuente SDSCJ

12.3.4. DESPUES – Fase de restauración: Actualización del Plan de Continuidad

Las actualizaciones derivadas de incidentes, pruebas, simulacros o cambios relevantes deberán gestionarse conforme al capítulo 13. Mantenimiento y actualización del plan.

13. Mantenimiento y actualización del plan

Este capítulo define la periodicidad, responsables, condiciones y trazabilidad para mantener actualizado el PCN institucional y los planes de continuidad por proceso, en coherencia con el BIA, la matriz de riesgos, el DRP y las estrategias de continuidad aplicables.

13.1. Periodicidad y criterios de evaluación

Tipo de revisión	Cuándo aplica	Alcance mínimo
Actualización bienal obligatoria	Cada dos años, en sincronía con el ciclo del BIA.	Revisar PCN institucional, planes por proceso, RTO, RPO, MTPD, escenarios, estrategias, responsables, evidencias y documentos relacionados.
Revisión extraordinaria	Cuando se presenten cambios normativos, organizacionales, tecnológicos, físicos, de riesgos, proveedores, servicios críticos o estructura institucional.	Ajustar los apartes afectados y verificar coherencia con BIA, matriz de riesgos, DRP, estrategias de continuidad y planes por proceso.
Revisión posincidente, posprueba o possimulacro	Después de incidentes relevantes, pruebas, ejercicios o simulacros que evidencien brechas.	Incorporar lecciones aprendidas, acciones de mejora, ajustes de roles, tiempos, dependencias críticas, comunicación, recuperación o retorno.
Publicación de cambios	Una vez aprobado el ajuste conforme al procedimiento documental vigente.	Publicar preferiblemente cambios menores dentro de los 15 días hábiles siguientes a su aprobación y cambios mayores dentro de los 30 días hábiles siguientes, conforme al procedimiento de control documental.

Tabla 20 - Periodicidad y criterios de actualización PCN. Fuente: SDSCJ.

13.2. Responsabilidades de mantenimiento y actualización

Rol	Responsabilidad principal
CIGD	Aprobar cambios estratégicos o de alto impacto relacionados con priorización institucional, recursos, políticas, escenarios críticos o entrada en vigor de ajustes relevantes.
OAP / Líder metodológico de continuidad	Orientar metodológicamente el ciclo de actualización, verificar coherencia documental, apoyar la trazabilidad del modelo y gestionar la publicación/control de versiones del PCN institucional cuando corresponda.
Líderes de proceso	Identificar necesidades de actualización, actualizar la información del plan de continuidad de su proceso, aportar evidencias, validar cambios y socializarlos con sus equipos.
Líderes operativos de proceso	Apoyar la actualización documental, trazabilidad, recopilación de evidencias, control de pendientes y articulación con el equipo del proceso.
Dependencias técnicas o de apoyo	Actualizar la información bajo su competencia cuando el cambio afecte tecnología, sedes, bienes, recursos físicos, talento humano, comunicaciones, proveedores, gestión documental o servicios de soporte.
Oficina de Comunicaciones Estratégicas	Apoyar la actualización de lineamientos de comunicación, vocería, mensajes internos o externos cuando los cambios afecten la atención ciudadana, reputación o comunicaciones institucionales.

Tabla 21 - Responsabilidades de mantenimiento y actualización PCN. Fuente SDSCJ.

13.3. Condiciones para actualización y procedimiento

13.3.1. Detonantes y documentos para revisar

Detonante de actualización	Documentos o componentes para revisar
Cambios estratégicos, normativos o de política institucional	PCN institucional, alcance, roles, requisitos legales, partes interesadas y políticas de continuidad.
Cambios en procesos, servicios o estructura organizacional	Planes por proceso, BIA, matriz de riesgos, roles, responsables, dependencias críticas y escenarios aplicables.
Cambios en riesgos o materialización de amenazas	Matriz institucional de riesgos, escenarios de interrupción, controles, estrategias de continuidad y acciones de mejora.
Cambios en sedes, equipamientos o infraestructura física	Escenarios de infraestructura, estrategias de recuperación, CAO, recursos físicos, responsables y planes por proceso afectados.
Cambios tecnológicos o de seguridad de la información	DRP, RTO, RPO, plataformas críticas, respaldos, conectividad, procedimientos técnicos y planes de continuidad asociados.
Cambios en proveedores, contratos, convenios o servicios tercerizados	Dependencias críticas, estrategias alternas, contactos, acuerdos de servicio, tiempos de respuesta y planes por proceso.
Resultados de incidentes, pruebas, simulacros, auditorías o revisiones	Lecciones aprendidas, acciones de mejora, indicadores, roles, comunicación, evidencias, planes y anexos aplicables.

Tabla 22 - Detonantes y documentos a revisar cambio en PCN. Fuente SDSCJ.

13.3.2. Procedimiento de actualización

Paso	Actividad	Responsable principal	Evidencia mínima
Detección	Identificar el cambio, hallazgo, incidente, prueba o condición que requiere actualización.	Líder del Proceso, dependencia responsable u OAP según origen del cambio.	Solicitud, reporte, acta, informe, hallazgo o registro del evento.
Evaluación	Determinar impacto sobre PCN, BIA, riesgos, DRP, escenarios, responsables, evidencias o planes por proceso.	Líder del Proceso o dependencia responsable; OAP revisa coherencia metodológica.	Análisis de impacto documental o registro de revisión.
Actualización	Ajustar el documento, anexo, plan, matriz o registro afectado.	Responsable del documento o componente afectado.	Versión ajustada y control de cambios.
Validación	Revisar coherencia técnica, metodológica y documental del ajuste.	Líder del Proceso, dependencia técnica y OAP, según corresponda.	Registro de revisión, validación o aprobación.
Aprobación	Aprobar el cambio conforme al nivel de impacto y al procedimiento documental vigente.	Líder del Proceso, CIGD o instancia competente, según el tipo de cambio.	Acta, aprobación en sistema documental o soporte equivalente.
Publicación y socialización	Publicar la versión vigente y comunicar el cambio a los roles impactados.	Responsable documental, OAP o líder del proceso según corresponda.	Publicación en repositorio, comunicación, acta o lista de asistencia.
Seguimiento	Verificar implementación de acciones de mejora o cambios derivados.	Líder del Proceso, dependencia responsable y OAP para trazabilidad metodológica.	Matriz de acciones, seguimiento o informe de cierre.

Tabla 23 - Procedimiento de actualización del PCN. Fuente SDSCJ

13.3.3. Dónde debe reflejarse cada actualización (trazabilidad)

Toda actualización aprobada se refleja en:

- Plan de Continuidad del Proceso y en el Plan Institucional de CN.
- BIA del proceso (si cambian criticidad o tiempos).
- Matriz de riesgos institucional (marcación de continuidad y controles).
- DRP y catálogos TIC (si cambian RTO/RPO o arquitectura).

- Diseño/Inventario del CAO (puestos, conectividad, energía) y teletrabajo (perfiles de acceso).
- Micrositio/Repositorio institucional (versión publicada y control de cambios).
- Agenda de pruebas/simulacros (si el cambio requiere validación específica).

14. Indicadores del Plan de Continuidad del Negocio

El seguimiento al Sistema de Gestión de Continuidad de Negocio (SGCN) de la SDSCJ requiere indicadores claros que permitan medir su eficacia y asegurar la mejora continua. Estos indicadores se diseñan bajo criterios SMART (específicos, medibles, alcanzables, relevantes y con periodicidad definida) y deben integrarse progresivamente al tablero institucional de control dentro del MIPG/SIG una vez se consoliden todos los componentes documentales y operativos.

Indicador (KPI)	Definición / Objetivo	Fórmula de cálculo	Periodicidad	Responsable
Éxito en pruebas de continuidad	Mide el porcentaje de pruebas/simulacros ejecutados con resultados satisfactorios.	(N° de pruebas exitosas ÷ N° total de pruebas realizadas) × 100	Anual	OAP y CIGD
Cobertura de capacitación en continuidad	Proporción de servidores capacitados frente al total de la entidad.	(N° de servidores capacitados ÷ N° total de servidores) × 100	Anual	OAP y Talento Humano
Planes de continuidad actualizados	Mide el avance en actualización de planes de proceso.	(N° de planes actualizados ÷ N° total de procesos) × 100	Bienal (con ciclo BIA)	Líderes de proceso y OAP
Actualización de BIA	Evalúa la actualización bienal del análisis de impacto.	(N° de procesos con BIA actualizado ÷ N° total de procesos) × 100	Bienal	OAP y Líder de Continuidad

Tabla 24. Tabla de Indicadores de Desempeño - Continuidad de Negocio. Fuente SDSCJ

Consideraciones metodológicas

- Estos indicadores deben aplicarse gradualmente: en 2025 solo se consolidarán como parte del diseño documental, y a partir de 2026 se medirán con las primeras pruebas y simulacros institucionales.
- La OAP y el Líder de Continuidad serán los responsables de consolidar los resultados institucionales.
- La Oficina de Comunicaciones Estratégicas apoyará en los indicadores vinculados a simulacros con interacción ciudadana.
- Los resultados deben integrarse en el tablero institucional de gestión (MIPG/SIG) para fortalecer la trazabilidad y el control en auditorías internas y externas.

15. Auditoría y mejora continua de continuidad de negocio

La auditoría y la mejora continua son elementos esenciales para garantizar que los planes de continuidad de negocio en la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) se mantengan vigentes, eficaces y alineados con la realidad institucional. La verificación periódica de los planes por proceso y la incorporación de hallazgos en acciones de mejora fortalecen la capacidad de respuesta de la entidad frente a eventos disruptivos.

15.1. Auditoría interna de los planes de continuidad por proceso

Una vez los planes de continuidad de cada proceso estén documentados y aprobados, se incorporarán de manera progresiva en las auditorías internas del Sistema Integrado de Gestión, orientadas por la Oficina de Control Interno. Estas auditorías deben abarcar la totalidad de los planes por proceso, verificando que cumplan con la metodología definida por la entidad y que mantengan coherencia con los análisis de impacto al negocio (BIA) y las matrices de riesgos institucionales.

Durante la fase inicial de implementación (2025), y mientras no entren a formar parte de las auditorías de calidad formales, el cumplimiento y avance de los planes será verificado directamente por la Oficina Asesora de Planeación (OAP) y el Líder de Continuidad de Negocio. Estos órganos tendrán la tarea de revisar que los líderes de proceso documenten, socialicen y actualicen sus planes en el micrositio institucional de continuidad, antes de someterlos a evaluaciones externas.

15.2. Responsables y funciones

Líderes de Proceso: mantener actualizado el plan de continuidad de su proceso, conservar evidencias de pruebas y simulacros, y atender los hallazgos que se deriven de auditorías o revisiones internas.

Líder de Continuidad de Negocio: consolidar la información de verificación de los procesos, dar seguimiento a los hallazgos iniciales y presentar reportes de cumplimiento a la OAP y al CIGD.

Oficina Asesora de Planeación (OAP): coordinar la revisión metodológica de los planes de proceso, validar que se ajusten a los lineamientos institucionales y emitir informes periódicos de cumplimiento.

Oficina de Control Interno: una vez documentados y estabilizados los planes, incluirlos en las auditorías de calidad del Sistema Integrado de Gestión, garantizando independencia en la revisión y emitiendo recomendaciones de mejora.

15.3. Acciones correctivas y mejora continua

Los hallazgos derivados de las auditorías, tanto las realizadas inicialmente por la OAP y el Líder de Continuidad como las posteriores por Control Interno, deberán consolidarse en un Plan de Mejora de Continuidad de Negocio. Dicho plan debe incluir:

- Las no conformidades detectadas o debilidades en los planes de proceso.
- Las acciones correctivas propuestas, responsables y plazos de ejecución.
- El seguimiento a la implementación de dichas acciones y su verificación en pruebas posteriores.

Este ciclo asegura que la continuidad de negocio en la SDSCJ no se limite a la elaboración documental de los planes, sino que se convierta en un proceso vivo, en permanente revisión y perfeccionamiento.

Elaboró: Miguel Angel Barbosa Robayo – Profesional OAP

Revisó: Julián Pontón - Jefe OAP

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co

16. Anexos

16.1. ANEXO – 1 Guía para Estrategia Centro Alterno de Operaciones (CAO)

Objetivo

Establecer una guía institucional para seleccionar, dimensionar, operar y mantener el CAO que asegure la prestación mínima de los procesos con prioridad BIA y los servicios críticos de la Secretaría, cuando una sede o sus capacidades TIC estén degradadas o indisponibles.

Principios

- Proporcionalidad: el CAO se dimensiona según criticidad y RTO de los procesos (no es una réplica de la operación completa).
- Diversificación: evitar puntos únicos de falla (sitio, red, energía, personal).
- Escalonamiento: combinar CAO físico con teletrabajo controlado para absorber picos de demanda.
- Practicidad: activar el CAO o espacio alterno dentro del tiempo definido para el escenario, a partir de la decisión del CIGD cuando el evento sea institucional, o del responsable competente cuando se trate de una activación operativa por proceso.

Pasos metodológicos (aplicables a cualquier sede)

Paso A **Identificar funciones críticas por sede**

- Identificar los procesos y actividades que operan en la sede, equipamiento o punto afectado, incluyendo procesos misionales, estratégicos, de apoyo y de evaluación cuando aplique.
- Marcar dependencias TIC y de servicios (energía, datos, telefonía).
- Señalar recursos físicos clave (puestos, salas, equipos especiales).
- Interpretación sencilla: Este paso permite definir qué actividades, roles, recursos e información mínima deben trasladarse, habilitarse o mantenerse para sostener la operación crítica.

Paso B **Seleccionar el modelo de CAO**

- **CAO único (sede alterna fija):** Se refiere a la designación de un lugar específico y permanente como centro alterno para trasladar la operación de los procesos críticos en caso de indisponibilidad de la sede principal. La ventaja es la simplicidad en la preparación y en las pruebas, pues todo se concentra en un mismo punto. Su limitación está en que, si el evento afecta también esa sede, no hay alternativa inmediata de respaldo.
- **CAO multi-sede (dos o más sedes alternas balanceadas):** Este modelo distribuye la operación en dos o más sedes de respaldo. En caso de falla en una, otra puede asumir la continuidad de forma parcial o total. Se usa cuando la entidad tiene varias sedes

disponibles (como la sede central, el C4 y algunas Casas de Justicia) y puede balancear allí la operación crítica. Permite redundancia, aunque exige mayor coordinación logística y tecnológica.

- **CAO virtual (telecentros distribuidos y acceso remoto seguro):** Se basa en que los funcionarios puedan conectarse desde telecentros u oficinas remotas con acceso seguro a los sistemas institucionales. Generalmente incluye el uso de VPN, escritorios virtuales y autenticación multifactor. Este esquema disminuye costos físicos, pero depende fuertemente de la estabilidad de la infraestructura TIC y de la ciberseguridad. Cuando el modelo incluya operación remota o teletrabajo, deberá articularse con el Anexo 3. Teletrabajo como mecanismo de contingencia y con los controles de acceso seguro definidos por Tecnología.
- **CAO híbrido (combinación física y virtual):** Integra puestos de trabajo en un sitio físico alterno con esquemas de teletrabajo seguro. Por ejemplo, los roles críticos que requieren interacción presencial se trasladan a la sede alterna, mientras que funciones de análisis o gestión documental se continúan de forma remota. Ofrece mayor flexibilidad y optimización de recursos.

Criterios que se deben tener en cuenta al momento de comparar las alternativas: tiempo de alistamiento, costo, disponibilidad de TIC y energía, cercanía a equipos, riesgos del entorno, rutas de acceso.

Paso C **Dimensionar capacidad mínima**

- Puestos críticos: cubrir 100% de roles con RTO ≤ 4 h y ≥ 50% con RTO 5–24 horas.
- Turnos: definir 2×8 h o 3×6 h según pico; un suplente por rol crítico.
- Conectividad y energía: doble enlace y UPS, planta con autonomía ≥ 8 h.
- Seguridad física y acceso: control de ingreso, CCTV, listas de habilitados.

Paso D **Definir activación y retorno**

- **Disparadores**: sismo/incendio/indisponibilidad de sede, ciberataque o caída de plataforma crítica, orden de autoridad.
- **Activación**: CIGD; notificación a equipos; alistamiento CAO más o menos 2 h.
- **Operación en modo degradado**: Implica priorizar solo los procesos y servicios más críticos, reduciendo la cobertura normal. Se utilizan colas de atención, servicios mínimos presenciales y canales alternativos (ejemplo: atención telefónica o en línea en lugar de presencial). La idea es mantener la operación esencial mientras se restablecen las condiciones normales.
- **Retorno**: verificación técnica/estructural; cierre de turnos; lecciones aprendidas.

Paso E **Integraciones**

- **Con DRP (TIC):** Significa que, cuando ocurre una falla tecnológica grave, los sistemas de la entidad (bases de datos, aplicaciones, videovigilancia, etc.) se trasladan automáticamente o de forma planificada a un centro de respaldo. Esto asegura que la información se pierda solo hasta un punto aceptable (RPO) y que el servicio se recupere en el tiempo máximo establecido (RTO). En la práctica, es como encender un "segundo servidor" que ya tiene los datos listos para seguir trabajando.
- **Con teletrabajo**: El teletrabajo se usa para que algunas funciones que no requieren presencia física se realicen desde casa u oficinas remotas. Esto permite que en el Centro Alterno de Operaciones (CAO) solo estén las personas indispensables, reduciendo la congestión y asegurando que los recursos limitados del CAO se destinen a los procesos más críticos.
- **Con logística (transporte, inventarios, periféricos, credenciales):** La logística garantiza que las personas y los recursos lleguen al CAO y funcionen correctamente. Incluye transporte para mover al personal, inventarios de equipos y suministros básicos (computadores, papelería, radios), periféricos listos para uso inmediato y credenciales de acceso para que los funcionarios puedan trabajar sin retrasos. Sin este apoyo, aun con tecnología disponible, el CAO no podría operar en condiciones reales.

Indicadores de seguimiento

Tiempo de alistamiento del CAO (minutos): Mide cuánto tiempo pasa entre que se ordena activar el Centro Alterno de Operaciones y el momento en que está listo para funcionar. Se calcula registrando la hora de la orden y la hora en que el CAO queda operativo.

% de puestos críticos disponibles vs. Requeridos: Compara la cantidad de puestos de trabajo que realmente están habilitados en el CAO con la cantidad que deberían estar listos según el BIA (procesos con RTO corto).

Cumplimiento de RTO en simulacros: Verifica si los procesos críticos logran restablecerse dentro del tiempo máximo de recuperación definido en el BIA (RTO). Se mide en pruebas o simulacros, comparando el tiempo real de recuperación con el tiempo objetivo.

Incidentes de conectividad/energía por trimestre: Cuenta cuántas veces, en un periodo de tres meses, el CAO tuvo fallas de internet, red o energía que afectaron su funcionamiento. Es un indicador de estabilidad de la infraestructura.

Ejemplos de aplicación de estrategia CAO por sedes (con valores simulados).

Sede Central – Ejemplo de Estrategia CAO

- Objetivo del CAO: sostener coordinación misional y soporte operativo (jurídico, documental, logística, analítica).
- Modelo recomendado: híbrido (sede alterna física y teletrabajo para áreas de apoyo).
- Con este diseño, si la sede central se cierra o sufre fallas, un núcleo esencial del personal trabaja en el CAO físico y el resto remoto; los servicios clave siguen disponibles mientras TIC aplica el DRP.

Característica	Descripción (como se planea aplicar en el CAO)
Capacidad de puestos	30 puestos críticos (RTO ≤ 4 h), 12 de apoyo (RTO 5–24 h)
Turnos	2×8 h (día/noche) con 1 suplente por rol crítico
Conectividad	2 enlaces (primario 500 Mbps / respaldo 200 Mbps) con QoS para 123, videovigilancia, correo
Energía	UPS por rack y por puesto (≥ 30 min), planta 20 kVA (≥ 8 h reabastecible)
Seguridad	Control de acceso por listas; CCTV; registro de ingreso por turnos
Integración TIC	Autenticación federada; acceso a SI; VPN priorizada; telefonía softphone de contingencia
Logística	Inventario mínimo (periféricos, EPP, radios, SIM de datos, papelería); contratos de transporte

C4 – Centro de Comando, Control, Comunicaciones y Cómputo. Ejemplo estrategia CAO

- Rol operativo: nodo 24/7 para atención y coordinación de emergencias (videovigilancia, radiocomunicaciones, NUSE 123).
- Objetivo del CAO: mantener operación mínima del ecosistema 123/videovigilancia ante interrupciones tecnológicas o de infraestructura.
- Por su misión, el C4 requiere un CAO técnico con conmutación rápida hacia plataformas espejo y operación mínima 24/7 aún en modo degradado.

Aspecto	Parámetro orientador
Capacidad de puestos	16 operadores (videowalls/analistas), 4 coordinadores
Turnos	3×6 h para continuidad 24/7 (pico nocturno/fin de semana)
Conectividad	Red metropolitana redundante; rutas alternativas a datacenter; priorización de tráfico de video y voz
Energía	UPS centralizada, planta con autonomía ≥ 12 h; mantenimiento preventivo calendarizado
Integración TIC	Conmutación a plataforma espejo; RPO ≤ 1 h; telefonía de contingencia y canales alternos
Seguridad	Control reforzado de acceso; restricción de dispositivos; procedimientos de sala
Logística	Mapa de consolas críticas; inventario de repuestos; soporte onsite de proveedores clave

Casas de Justicia. Ejemplo estrategia CAO.

- Rol operativo: atención al ciudadano (recepción, mediación, conciliación, cursos y orientación).

- Objetivo del CAO: continuidad de atención básica usando sub-CAO local (otra Casa de Justicia) o CAO virtual (citas remotas, turnos priorizados).
- Al interconectar Casas de Justicia o habilitar atención remota, se evita suspender servicios al ciudadano ante cierres puntuales.

Configuración	Cuando usarla	Elementos mínimos
Sub-CAO local (Casa A respalda Casa B)	Indisponibilidad temporal por daños/orden de autoridad	4 puestos de atención; VPN; 2 líneas de orientación; agenda compartida
Virtual (atención remota)	Bloqueos viales/protestas; eventos masivos	2 agentes en sitio seguro, 4 remotos; canales digitales; priorización de casos
Híbrido	Demanda alta en eventos/brotes	3 puestos locales, 3 remotos; colas unificadas; guías de derivación

Activación/retorno del CAO (Ejemplo de validaciones antes de ordenar el regreso a operación normal – aplica para cualquier sede mencionada)

Disparador	Umbral	Quién activa	Primeras acciones	Retorno
Indisponibilidad de sede	Orden autoridad/daño crítico	CIGD	Notificar equipos, movilizar, alistar, validar conectividad, confirmar roles	Sede verificada y estable
Caída plataforma crítica	> 30–60 min con impacto	CIGD / TIC	Conmutar (DRP), abrir CAO parcial, informar, monitorear	Estabilidad ≥ 24 h

Nota general: se citan sedes oficiales de la SDSCJ para contextualizar la metodología: sede central en Torre 7; C4 como centro de comando; y Casas de Justicia (Bosa, Ciudad Bolívar, Chapinero, Fontibón, entre otras) como puntos de servicio al ciudadano.

16.2. ANEXO – 2 Estrategia Respaldo TIC y DRP

Objetivo

Definir cómo asegurar que los sistemas tecnológicos críticos de la Secretaría se recuperen rápidamente después de una interrupción, incidente tecnológico, ciberataque, falla extendida o desastre que afecte servicios tecnológicos críticos.

Paso A **Identificación de plataformas, sistemas y servicios TIC críticos**

Se listan los sistemas tecnológicos que soportan los procesos de criticidad Muy Alta o Alta según el BIA.

Sistema crítico	Proceso soportado	RTO (h)	RPO	Observación
NUSE 123	Gestión de Emergencias	4	1 h	Interrupción >4 h afecta directamente la atención de emergencias.

Videovigilancia	Gestión de Emergencias / C4	4	2 h	Permite monitoreo en tiempo real; debe mantener mínimo 70% de cámaras activas.
Radiocomunicaciones	Gestión de Emergencias	2	0 h (sin pérdida)	Comunicación inmediata con cuerpos de seguridad; no admite pérdida de datos.

Paso B **Definir estrategias de respaldo**

Para cada sistema crítico se establecen mecanismos de continuidad:

Copias de seguridad (backups)

Se hacen de manera automática con periodicidad según el RPO.

Plataformas espejo

Centros de datos alternos que tienen una copia en tiempo real del sistema.

Conmutación automática o manual

Paso del sistema principal al alterno en caso de falla.

Servicios en la nube (cuando aplique)

Uso de proveedores externos con alta disponibilidad.

Sistema	Estrategia de respaldo	Explicación para no especialistas
NUSE 123	Plataforma espejo en datacenter alterno y backups cada hora	Si el servidor principal se cae, otro servidor ya configurado toma el control y sigue recibiendo llamadas.
Videovigilancia	Redundancia de almacenamiento (RAID) y replicación parcial en nube	Los videos se guardan en discos duplicados; si uno falla, el otro mantiene la información.
Radiocomunicaciones	Conmutación a red alterna de frecuencia y respaldo eléctrico	Si la red principal cae, se usa otra frecuencia y equipos de radio alimentados por planta eléctrica.

Paso C **Establecer roles y responsabilidades**

- Oficina de Tecnologías de la Información: Diseña, mantiene y prueba el DRP.
- C4 – Operaciones: Valida que sistemas de emergencia (123, videovigilancia, radio) funcionen en contingencia.
- Oficina Asesora de Planeación: Supervisa que los RTO/RPO definidos se cumplan.
- CIGD: Ordena activación del DRP y seguimiento en emergencias.

Paso D **Activación y retorno**

- **Activación**: Activación: ocurre cuando un sistema crítico supera su RTO de falla o cuando el impacto es inmediato. La activación técnica del DRP corresponde a la Dirección de Tecnologías y Sistemas de Información; el CIGD interviene cuando la afectación tecnológica comprometa la continuidad institucional, servicios críticos o decisiones de priorización.
- **Retorno**: se realiza cuando el sistema principal está estable y validado; se migran los datos procesados en el alterno para mantener consistencia.

Paso E **Pruebas y simulacros**

El DRP se prueba conforme al Plan de Pruebas del PCN PL-DE-03, al Programa anual de pruebas del PCN y a los procedimientos técnicos definidos por la Dirección de Tecnologías y Sistemas de Información.

Indicadores de seguimiento

Indicador	Cómo se mide	Fuente de información	Interpretación
% de cumplimiento de RTO/RPO en simulacros	(N° de sistemas que cumplieron ÷ N° simulados) × 100	Informes de pruebas DRP	Indica si los tiempos planeados son realistas.
Tiempo de conmutación promedio (minutos)	Promedio entre orden y activación efectiva del alterno	Bitácoras de TIC	Evalúa rapidez de respuesta del DRP.
% de éxito en restauración de datos	(N° de restauraciones exitosas ÷ N° intentos) × 100	Registros de backup y pruebas	Mide confiabilidad de copias de seguridad.

16.3. ANEXO – 3 Teletrabajo como mecanismo de contingencia

El teletrabajo, entendido como la posibilidad de que los funcionarios realicen sus funciones desde casa u otro lugar diferente a la sede institucional con acceso seguro a los sistemas, es una de las estrategias más prácticas para asegurar continuidad en la SDSCJ cuando las instalaciones físicas o el transporte se ven afectados. No sustituye al Centro Alterno de Operaciones (CAO), pero lo complementa al liberar espacio y reducir la presión sobre los recursos presenciales.

Pasos metodológicos

- **Identificación de roles teletrabajables**
  Cada proceso debe señalar qué funciones pueden ejecutarse sin presencia física. Ejemplo: análisis jurídico, gestión documental digital, reportes estadísticos.
- **Definir accesos seguros**

El teletrabajo requiere VPN (red privada virtual) o escritorios virtuales que permitan conectarse de forma cifrada a los sistemas de la Secretaría, evitando riesgos de ciberseguridad.

- **Asignar equipos y credenciales**
  Los funcionarios deben contar con computador portátil institucional, acceso a correo, aplicaciones misionales o de apoyo, y credenciales de autenticación reforzada (por ejemplo, doble factor de seguridad).
- **Integración con el CAO y DRP**
  Cuando se activa el CAO, algunos roles se trasladan físicamente; los teletrabajables permanecen remotos. Esto asegura que los puestos críticos en el CAO se reserven para procesos con RTO ≤ 4 horas (ejemplo: operadores del 123 o C4).

Proceso	Rol	Teletrabajable (Sí/No)	Justificación
Gestión de Emergencias	Operador del 123	No	Requiere consola en sitio o en CAO para atención directa de llamadas.
Gestión Jurídica	Abogado revisor de tutelas	Sí	Accede a expedientes digitales y puede tramitar documentos por medios electrónicos.
Gestión Documental	Radicación digital	Sí	Puede ejecutarse en plataforma de gestión documental vía VPN.
Recursos Físicos	Coordinador de transporte	No	Necesita gestionar logística en campo y coordinar proveedores directamente.

Indicadores de seguimiento

Indicador	Cómo se mide	Interpretación
% de roles identificados como teletrabajables	(N° de roles teletrabajables ÷ total de roles del proceso) × 100	Indica el nivel de flexibilidad del proceso frente a contingencias.
Disponibilidad de accesos VPN activos	N° de accesos VPN asignados ÷ N° de roles teletrabajables	Permite validar que el personal pueda conectarse en caso de emergencia.

El teletrabajo en la SDSCJ debe entenderse como una estrategia complementaria, que aumenta la capacidad de respuesta en emergencias y evita suspender funciones administrativas o de apoyo. Su éxito depende de una adecuada identificación de roles, de la provisión de accesos seguros y de la integración con las otras estrategias (CAO y DRP).

16.4. ANEXO – 4 Priorización de procesos y servicios críticos

Los criterios, parámetros y escalas de valoración del BIA se encuentran definidos en la Guía G-DE-06 y en el Formato F-DE-1498. El PCN utiliza los resultados consolidados para priorizar procesos, servicios y estrategias de continuidad.

Pasos metodológicos

- **Clasificar procesos por criticidad**

Usar los resultados del BIA para ordenar los procesos en Muy Alta, Alta, Media o Baja criticidad.

- Muy Alta: RTO ≤ 4 h, sin tolerancia a interrupciones (Ejemplo recepción de llamadas 123, videovigilancia).
- Alta: RTO entre 4 y 8 h, debe recuperarse el mismo día (Ejemplo gestión de transporte de PPL).
- Media: RTO hasta 24 h, puede recuperarse en la misma jornada o al día siguiente.
- Baja: puede suspenderse temporalmente sin afectar de forma grave la misión (Ejemplo recorridos territoriales).

- **Definir niveles de servicio mínimos aceptables**
  Se establece la operación mínima que cada proceso debe mantener en contingencia. Ejemplo: que el 123 atienda el 70% de llamadas o que la videovigilancia funcione al menos con la mitad de las cámaras.
- **Asignar recursos prioritarios**
  Los recursos limitados (puestos en el CAO, accesos a TIC, transporte, insumos) se distribuyen primero a los procesos de Muy Alta y Alta criticidad.
- **Validar interdependencias**
  Algunos procesos de apoyo deben priorizarse porque habilitan a los misionales. Ejemplo: sin transporte de Recursos Físicos, no se pueden mover equipos a CAO; sin TIC, no funciona el 123.

Proceso	Criticidad (BIA)	RTO	Servicio mínimo aceptable en contingencia	Recursos prioritarios asignados
Gestión de Emergencias – NUSE 123	Muy Alta (29 puntos)	4 h	Atender ≥70% de llamadas de emergencia	Consolas en CAO, servidores espejo, operadores en turnos 24/7
Gestión de Recursos Físicos (traslado de PPL)	Alta (18 puntos)	8 h	Garantizar mínimo 50% de traslados programados	Vehículos de respaldo, contratos alternos de transporte
Gestión Jurídica	Media (14 puntos)	24 h	Radicar digitalmente expedientes urgentes	Acceso remoto (VPN), abogados en teletrabajo
Gestión de Comunicaciones Estratégicas	Baja (≤10 puntos)	>24 h	Reprogramar actividades no urgentes	Comunicación posterior

Indicadores de seguimiento

Indicador	Cómo se mide	Interpretación
% de procesos críticos con plan de continuidad específico	(N° de procesos Muy Alta/Alta con plan validado ÷ total de críticos) × 100	Verifica que todos los procesos prioritarios tengan plan propio.
Cumplimiento de niveles de servicio mínimos en simulacros	N° de servicios que alcanzan su meta mínima ÷ N° simulados	Evalúa si los servicios críticos pueden sostenerse aun en contingencia.

Tiempo promedio de recuperación por nivel de criticidad	Tiempo real de restablecimiento ÷ procesos por nivel	Permite comparar RTO planeado con el obtenido en pruebas.

La priorización garantiza que, en escenarios de interrupción, los recursos se concentren en lo esencial: procesos que protegen la vida, la seguridad ciudadana y el acceso a la justicia. Con base en el BIA 2024, los procesos de Gestión de Emergencias (123, videovigilancia, radio) deben ocupar el primer lugar en la estrategia de continuidad, seguidos por los procesos de apoyo que los habilitan. El éxito de esta estrategia depende de mantener actualizados los criterios de criticidad y de probar regularmente si los niveles mínimos de servicio se cumplen en la práctica.

16.4.1. Alcance y cobertura institucional

El Análisis de Impacto al Negocio (BIA) de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) abarca la totalidad de los procesos definidos en el Mapa de Procesos Institucional, incluyendo los procesos misionales, estratégicos, de apoyo y de evaluación y control, junto con todas las dependencias y sedes que los desarrollan.

El BIA tiene un alcance transversal y por proceso, en el que cada líder institucional identifica:

- Las actividades esenciales de su proceso y su dependencia con otros procesos internos o externos.
- Los recursos humanos, tecnológicos, logísticos y financieros mínimos requeridos para mantener la continuidad.
- Las interdependencias y relaciones críticas con proveedores, contratistas o entidades aliadas.
- Los impactos esperados ante una interrupción prolongada, expresados en términos de operación, reputación, servicio al ciudadano y cumplimiento de obligaciones legales.

La Oficina Asesora de Planeación (OAP) coordina metodológicamente el BIA y consolida sus resultados con los líderes de proceso, para articularlos con la gestión de riesgos, las estrategias de continuidad y la recuperación tecnológica.

16.4.2. Criterios e indicadores aplicados en la SCJ

El Análisis de Impacto al Negocio (BIA) de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) se fundamenta en criterios de valoración formulados y aprobados por la Oficina Asesora de Planeación (OAP), validados con los líderes de proceso, y aplicados de manera uniforme en todos los procesos del Mapa Institucional.

Estos criterios, alineados con la Metodología de Gestión del BIA institucional, permiten cuantificar los impactos que tendría la interrupción de un proceso, considerando sus efectos en la operación, la legalidad, la reputación y el uso de recursos tecnológicos y financieros.

a. Dimensiones institucionales de impacto

El modelo adoptado por la SCJ agrupa los impactos en tres dimensiones principales, cada una con criterios de medición y variables asociadas.

Dimensión de impacto	Criterios de valoración aplicados	Variables medibles en plantilla BIA
1. Impacto Operativo y de Servicio	• Grado de afectación a la atención al ciudadano o a la prestación de servicios críticos (línea 123, Casas de Justicia, CAV, gestión de emergencias). • Interrupción de funciones esenciales o pérdida de capacidad operativa. • Volumen de usuarios o dependencias impactadas.	• % de servicios o sedes afectados. • Tiempo de inoperatividad estimado frente al RTO definido. • Nº de procesos dependientes afectados.
2. Impacto Legal y Reputacional	• Incumplimiento de normas, sentencias o compromisos legales. • Riesgo de sanción o requerimiento por entes de control. • Deterioro de imagen institucional o pérdida de confianza ciudadana.	• Nº de obligaciones legales afectadas. • Nº de sanciones o requerimientos derivados de incidentes. • Evaluación de reputación (escala 1–5).
3. Impacto Económico y Tecnológico	• Pérdidas financieras o sobrecostos operativos. • Dependencia de infraestructura tecnológica (C4, SIGA, NUSE, aplicativos internos). • Pérdida de datos o indisponibilidad de sistemas.	• Valor estimado de pérdida diaria (COP). • % de procesos con alta dependencia TIC. • Tiempo medio de recuperación del sistema (RTO tecnológico).

b. Escala de valoración institucional

La escala de valoración definida por la SCJ se aplica de manera uniforme en todos los procesos.

Cada criterio es calificado en una escala del 1 al 5, de acuerdo con la severidad del impacto y los umbrales establecidos en la metodología del BIA institucional:

Nivel	Descripción	Efecto esperado en la continuidad institucional
1 – Bajo	Afectación mínima. El proceso continúa con medios alternos o manuales.	Operación sin impacto en el ciudadano ni en la misión.
2 – Moderado	Interrupción parcial o diferida.	Impacto leve en eficiencia operativa.
3 – Alto	Afectación de funciones relevantes o retraso en servicios.	Requiere acciones de contingencia internas.
4 – Muy Alto	Interrupción de servicios esenciales o atención al ciudadano.	Compromete temporalmente la misión institucional.
5 – Crítico	Suspensión total del proceso o de servicios públicos esenciales.	Afecta la seguridad, la convivencia o el acceso a la justicia.

Cada líder de proceso diligencia la valoración dentro de la plantilla institucional del BIA, asignando puntajes para las tres dimensiones.

16.5. ANEXO – 5 Coordinación interinstitucional

La coordinación interinstitucional significa que, en situaciones de emergencia, la SDSCJ no actúa sola: debe trabajar de manera articulada con otras entidades del Distrito y del orden nacional para sostener la continuidad de los servicios críticos. Esta integración es clave porque los incidentes que afectan la seguridad y la justicia en Bogotá suelen involucrar varios actores al mismo tiempo (Ejemplo IDIGER en emergencias naturales, Policía en orden público, Fiscalía en judicialización).

Pasos metodológicos

- **Identificar actores clave**
  Se listan las entidades con las que la SDSCJ debe coordinarse en escenarios de continuidad:
  - IDIGER: emergencias por sismos, inundaciones, incendios, etc.
  - Policía Metropolitana y Bomberos: atención de incidentes de seguridad y rescates.
  - Fiscalía General de la Nación: coordinación judicial en caso de delitos o investigaciones en curso.
  - Secretaría de Salud: atención de víctimas y emergencias médicas.
  - Proveedores estratégicos (ETB, Oracle, Microsoft, etc.): soporte de TIC para mantener plataformas misionales.
- **Definir protocolos de comunicación**
  Se establecen canales y responsables de contacto directo. Para no especialistas, esto significa tener claro a quién llamar primero y por qué medio (teléfono directo, radio, correo oficial, sala de crisis).
- **Asignar roles y vocerías**
  La SDSCJ debe definir quién comunica hacia afuera (ejemplo Jefe de OAP, CIGD) y quién mantiene la relación técnica con cada entidad (ejemplo TIC con proveedores de red, Seguridad con Policía).
- **Realizar ejercicios conjuntos**
  Simulacros integrados con IDIGER, Policía y otras entidades, para validar que la comunicación y la acción se den en los tiempos adecuados.

Escenario	Entidad coordinadora	Rol de la SDSCJ	Rol de la otra entidad
Sismo que afecta sede central	IDIGER	Activa CAO, mantiene atención de procesos críticos	Declara nivel de emergencia, coordina evacuaciones y evaluación de edificios
Ciberataque al NUSE 123	MinTIC – CSIRT nacional	Coordina con TIC para activar DRP	Brinda apoyo técnico y alerta sobre ataques similares en otras entidades
Protesta social con bloqueos	Policía Metropolitana	Coordina atención en Casas de Justicia y comunicación con ciudadanía	Garantiza seguridad de funcionarios y acceso controlado a instalaciones
Incendio en una Casa de Justicia	Bomberos de Bogotá	Notifica y activa sub-CAO en otra Casa de Justicia	Atiende emergencia, asegura infraestructura, reporta condiciones de retorno

16.6. ANEXO - 6 Metodología para la creación de escenarios de interrupción.

Paso 1. Seleccionar los escenarios de referencia (contextualizados a Bogotá)

Identifique, con base en fuentes oficiales, los escenarios más probables y de mayor impacto para la ciudad y la entidad. En Bogotá, la autoridad técnica (IDIGER) prioriza, entre otros: sismo, inundaciones/avenidas torrenciales, movimientos en masa, incendios (estructurales y forestales), aglomeraciones de público/eventos masivos; compleméntelos con fallas tecnológicas y ciberataques, fallas de servicios públicos (energía/telecomunicaciones), protestas sociales y bloqueos, e indisponibilidad de sedes.

Escenario	Cuando mencionarlo (criterio operativo)	Ejemplos de activación	Procesos típicamente afectados
Sismo	Evento ≥ intensidad percibida que comprometa estructura/operación o por instrucción de autoridad	Daños en sede; evacuación; restricción de ingreso	Misionales y de apoyo (según sede afectada)
Inundación / Avenidas torrenciales	Alertas y afectación de acceso a sedes/CAO	Vías anegadas; acceso restringido a C4/CAO	Misionales (C4) y apoyo (logística)
Incendio (estructural/forestal)	Afectación directa en sede o perímetro crítico	Evacuación; pérdida de equipos/archivos	Misionales (si es C4) y apoyo (bodegas)
Movimientos en masa	Riesgo o evento que bloquee accesos críticos	Talud inestable; cierre de vías	Apoyo (transporte) y misionales (demoras de respuesta)
Aglomeraciones / Protestas / Bloqueos	Orden público limita movilidad/operación	Bloqueos a sedes; marchas masivas	Misionales (atención) y apoyo (movilización)
Fallas tecnológicas	Caída prolongada de plataformas claves	Indisponibilidad NUSE 123, videovigilancia	Misionales (Gestión de Emergencias)
Ciberataques	Ransomware/DDoS/filtración con impacto operativo	Encriptación de servidores; DDoS al 123	Misionales y TIC (DRP)
Fallas de servicios públicos	Corte prolongado de energía/datos	Apagón en sede; caída de red metropolitana	Transversal (CAO/DRP)
Indisponibilidad de sedes	Cierre total/parcial por riesgo u orden oficial	Cierre edificio; reubicación temporal	Apoyo (Recursos Físicos) y todos los críticos

Esta tabla guía cuándo traer cada escenario a la conversación de continuidad. La prioridad real debe alinearse con impactos del BIA y con la disponibilidad de estrategias (CAO, DRP, teletrabajo, proveedores alternos detalladas más adelante).

Paso 2. Perfilar cada escenario

Para cada escenario priorizado, se elaborar una ficha como la siguiente, que permite generar informes:

Campo	Descripción / Valores esperados
Escenario	Nombre (Ejemplo, “Sismo con indisponibilidad de sede principal”)
Desencadenantes (umbrales)	Ejemplos: orden de autoridad; caída de plataforma crítica ≥ N horas; daño estructural; bloqueo de accesos
Procesos afectados	Vincule procesos priorizados por BIA (crítico/alto/medio/bajo)
Dependencias TIC	Sistemas/servicios afectados (NUSE 123, videovigilancia, correo, conectividad)
Severidad (Alta/Media/Baja)	Cualitativa; relacione con MTPD de procesos críticos
Estrategias de continuidad	CAO, DRP, trabajo remoto, rutas alternas, proveedores alternos
Criterios de activación	Quién activa (CIGD), cuándo y cómo se notifica
Criterios de retorno	Condiciones para desactivar contingencia y volver a operación normal

Paso 3. Mapear procesos priorizados (BIA) a escenarios

Cruzar cada escenario con los procesos priorizados en el BIA, indicando grado de afectación.

Proceso	Afectación por escenario (Alta/Media/Baja)	Notas operativas
Gestión de Emergencias (misional)	Alta (sismo; ciberataque)	Requiere CAO/DRP para NUSE 123 y videovigilancia
Gestión de Recursos Físicos (apoyo)	Media-Alta (sismo; bloqueos)	Moviliza personal/equipos; rutas y proveedores alternos

Este mapeo convierte el BIA en decisiones de contingencia: procesos con RTO corto y MTPD ajustado deben tener estrategias inmediatas.

Paso 4. Vincular estrategias y criterios de activación

Para cada escenario, definir qué se activa, quién y en qué orden (sin duplicar el proceso institucional: aquí solo se referencia).

Escenario	Estrategias asociadas	Activación (rol)	Comunicación
Sismo	CAO, alternancia de sede, copias frías, rutas alternas	CIGD / Jefe OAP	Interna (equipos) / Externa (IDIGER/medios si aplica)
Ciberataque	DRP, segmentación/redes, restauración respaldos, bypass 123	CIGD / TIC	CSIRT/entes de control; mensajes al ciudadano

Los siguientes son ejemplos reales de uso del método (no reemplazan los planes específicos que se generen por cada proceso, deben usarse solo como ilustración).

Campo	Contenido (ejemplo aplicado 2024)
Escenario	Sismo que obliga cierre preventivo de sede (evaluación estructural)
Desencadenantes	Evento sísmico; instrucción de autoridad; daños visibles; alarma de evacuación

Procesos afectados	Gestión de Recursos Físicos (apoyo clave para reubicación/traslado); impacto indirecto en misionales
Dependencias TIC	Energía, datos; acceso a SIGA e inventarios para reasignación
Severidad	**Media-Alta** (operación continúa si CAO y rutas alternas están disponibles)
Estrategias	Activación **CAO**, contratos de transporte y **reubicación**; priorización de puestos críticos
Activación	CIGD; coordinación con IDIGER (orientaciones de sismo-resistencia/continuidad)
Retorno	Reapertura segura; verificación de puestos críticos; actualización inventarios