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

Este documento consolida la información requerida para activar y poner en funcionamiento el Plan de Continuidad del Negocio de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ.

El objetivo Gestión de Continuidad del Negocio - GCN es identificar amenazas potenciales y sus impactos, para planificar las acciones necesarias que garanticen la continuidad de la prestación de los servicios en los niveles predefinidos como aceptables, desde el momento en que se presente el incidente hasta el restablecimiento a la normalidad de acuerdo con lo indicado en la norma ISO 22301:2019.

El Plan de Continuidad de Negocio, de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, se enfoca en describir los procedimientos, procesos, responsables y herramientas necesarias para dar respuesta a cualquier interrupción causada por una emergencia o evento (fallas técnicas, desastres naturales, fallas humanas, etc.), así como aplicar las herramientas que permitan retornar a las condiciones normales de funcionamiento.

Con el Plan de Continuidad del Negocio se fortalece el gobierno y estructura de gestión de riesgos, ofreciendo mayor seguridad a los ciudadanos, entidades del distrito capital y otros interesados frente a imprevistos, buscando garantizar un adecuado nivel de estabilidad organizativa durante la respuesta a un evento de interrupción, la recuperación de las operaciones o procesos críticos y la reanudación de la operación normal.

2. Glosario

Aceptación del riesgo: Nivel y tipo de riesgo que la organización está dispuesta a asumir (Pérdida que la organización considera tolerable por periodo de tiempo).

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

Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos, positivos y/o negativos, y el impacto de sus consecuencias calificándolas y evaluándolos a fin de determinar la capacidad de la Compañía para su aceptación y manejo. Proceso sistemático para entender la naturaleza del riesgo y deducir el nivel del riesgo.

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**.**

CAD: Computer Aided Dispatch (CAD-por sus siglas en inglés): Policía: Centro Automático de Despacho - (Policía Metropolitana de Bogotá). Se refiere al subsistema de la plataforma

tecnológica del Sistema Integrado de Seguridad y Emergencias, destinado a la gestión de la información de seguridad o emergencias de la ciudad.

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.

Conmutación de servicios: Cambio automático o planificado de un sistema en falla hacia un sistema alterno que ya está listo para operar.

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 sea accesible y utilizable por solicitud de una compañía autorizada.

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 desastre: Un conjunto predefinido de condiciones que describen una interrupción de los procesos del negocio de una organización con el propósito de diseñar los planes y definir las personas que administrarían la respuesta**.**

ETB: Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.

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

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Evento Disruptivo: Se refiere a situaciones, tecnologías o innovaciones que causan una interrupción significativa en una organización.

Gbps: Gigabits por segundo.

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.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

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

MEBOG: Policía Metropolitana de Bogotá.

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.

Operador Tecnológico: es el encargado de brindar el soporte tecnológico necesario para que se pueda cumplir con los objetivos de la misionalidad de las agencias.

PIVOT3: Soluciones de infraestructura hiperconvergentes simples, inteligentes y automatizadas para admitir cualquier carga de trabajo, cualquier iniciativa de centro de datos en cualquier entorno de TI.

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 residual: Nivel restante del riesgo después del tratamiento del riesgo.

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.

SecurOS - ISS: Security Operating System – Intelligent Security Systems, es una plataforma de software avanzada utilizada para la gestión y el análisis de sistemas de videovigilancia y seguridad.

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.

Servicio Ciudadano Digital: Son un conjunto de soluciones tecnológicas y procedimientos que brindan al Estado la capacidad para su transformación digital y lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Se clasifican en SCD base y especiales.

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 global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la Continuidad del Negocio. Parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad de negocio.

Sistema de Información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

Solución Tecnológica: Hace referencia a la articulación de artefactos de hardware y de software que dan respuesta de forma adecuada a una necesidad, en este caso puede ser una necesidad operacional o funcional de un área interesada.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

UAECOBB: Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo. Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

VMS (Video Management Software - por sus siglas en inglés): Software mediante el cual se administra el sistema de videovigilancia.

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*

El Despacho de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) en coherencia con su misión y compromiso con clientes y partes interesadas, gestiona, mantiene y mejora la Continuidad de Negocio de la Entidad, mediante la identificación de estrategias e implementación de planes que permitan salvaguardar la integridad física de las personas, cumplir con la normatividad vigente y mitigar los impactos operacionales y financieros asociados a la interrupción del servicio.

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

- Las actividades de continuidad de negocia 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.
- Se busca proteger a las partes interesadas: personas, recursos institucionales y 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/o acciones a seguir en caso de un evento no planificado que afecte la normal operación de los procesos, detallar las actividades de respuesta inmediata para cada incidente y así mitigar los impactos para la continuidad a la prestación de los servicios críticos de la SDSCJ. 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.
- Hace parte y complemento de la función de mitigar el impacto de los riesgos asociados a interrupciones que afecten los servicios críticos.
- Incrementar la oportunidad en la restauración de las operaciones afectadas por algún evento.
- Cumplir con los requisitos contractuales y contemplados en la normativa vigente.
- Proteger a la SDSCJ de impactos financieros y operativos que pondrían en riesgo la entidad en particular y el gobierno distrital en general.
- Facilitar la toma de decisiones durante una situación de desastre.
- Implementar proyectos de mejora hacia la continuidad del negocio.
- Asignar roles y responsabilidades a cada uno de los funcionarios y proveerle guías para la atención de emergencias y recuperación de los procesos durante y después de los eventos que generan una interrupción en la operación.
- Asegurar la coordinación de las acciones a seguir por parte de los equipos de trabajo, funcionarios, entes externos y proveedores para lograr la continuidad de las operaciones y su recuperación.

5. *Alcance*

El Sistema de Gestión de Continuidad del Negocio (SGCN) de la Secretaría Distrital de Convivencia, Seguridad y Justicia (SDSCJ) se aplica a todos los procesos misionales, de apoyo y estratégicos definidos en el marco del Modelo Integrado de Planeación y Gestión (MIPG), especialmente a aquellos identificados como críticos mediante el Análisis de Impacto al Negocio (BIA).

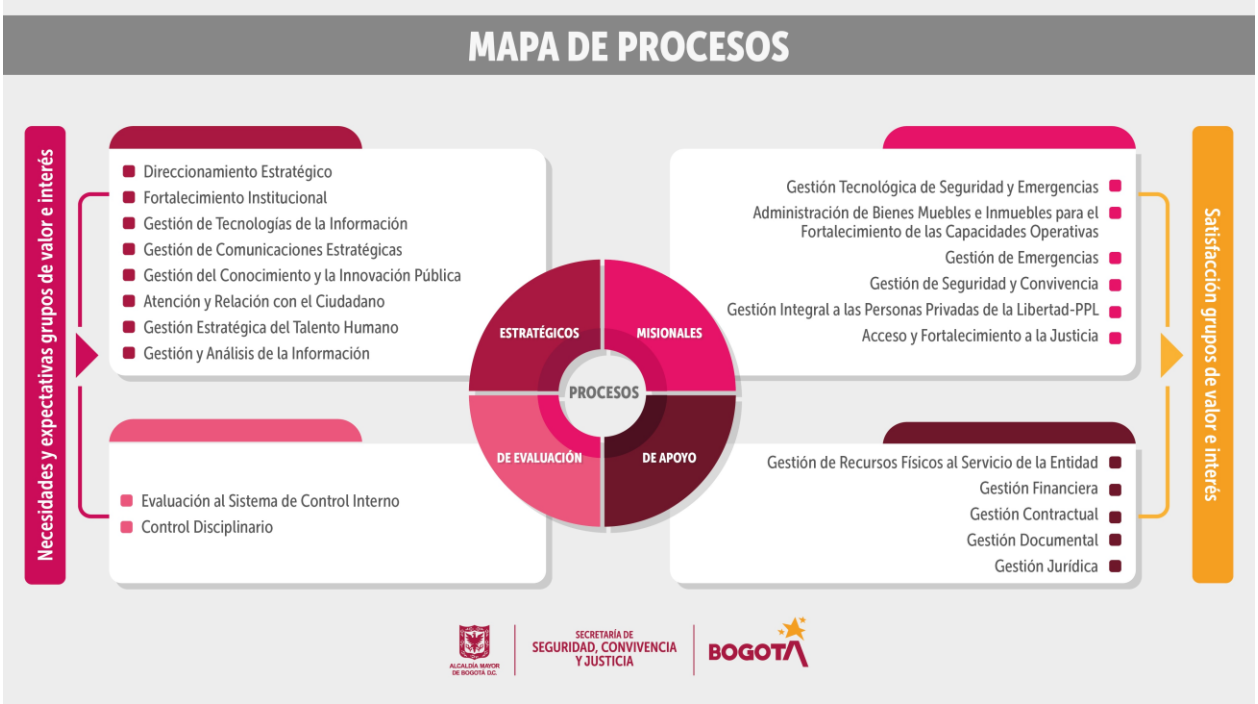


***Ilustración 1** - Cadena de valor de la SDSCJ. Fuente: SDSCJ*

Aplica a todas las áreas de la Entidad, incluyendo oficinas centrales, subsedes, centros móviles y puntos descentralizados de atención, donde se ejecutan funciones críticas.

Abarca a líderes de procesos, Coordinación TIC, Oficina de Planeación, Talento Humano, Jurídica, Comunicaciones, y otros actores definidos en el MIPG.

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 recursos ordinarios. Las estrategias que impliquen grandes inversiones requerirán inclusión en el plan de desarrollo institucional o solicitudes específicas al sector Hacienda.

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

En el marco de la implementación de la Gestión de Continuidad del Negocio (GCN), la Secretaría Distrital de Convivencia, Seguridad y Justicia ha identificado los elementos internos y externos que podrían afectar su capacidad para mantener sus procesos críticos ante incidentes disruptivos.

Este análisis es fundamental para la planificación de estrategias de continuidad, la asignación de recursos, y la activación de protocolos que garanticen la continuidad operativa y la prestación de servicios esenciales.

Elemento	Descripción en SDSCJ
Estructura organizacional	La SDSCJ opera con 21 procesos institucionales, que incluyen áreas como acceso a justicia, seguridad, convivencia, centros de atención, entre otros. La dispersión de funciones puede generar dependencia crítica de ciertas áreas.
Recursos humanos críticos	Personal especializado en mediación, análisis jurídico, administración territorial, TIC. Su ausencia puede afectar la operación ante incidentes.
Infraestructura y tecnología	Dependencia de redes TIC, bases de datos, cámaras, plataformas de monitoreo, sistemas de información y enlaces distritales. Vulnerabilidad ante caídas de red, cortes eléctricos o ciberataques.
Procesos críticos priorizados en el BIA	Los resultados del BIA identifican actividades críticas como respuesta a incidentes de seguridad ciudadana, coordinación con autoridades, atención a población vulnerable.
Cultura organizacional	Nivel actual de conocimiento y madurez frente a gestión del riesgo, uso de protocolos de emergencia, pruebas de simulacros.
Gestión documental e información	Uso del SIG-DOC para información clave. Pérdida o inaccesibilidad de documentos puede comprometer respuestas ante situaciones disruptivas.
Presupuesto y recursos asignados	Limitaciones presupuestales pueden afectar la recuperación de servicios o adquisición de recursos de respaldo.
Alianzas internas	Coordinación con dependencias internas como Planeación, Jurídica, Talento Humano, Tecnologías, Seguridad Interna. Necesarias para activar y mantener planes de continuidad.

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	Aplicación del Decreto 612 de 2018 (MIPG), normativas de Función Pública, y exigencias de transparencia, rendición de cuentas, y continuidad operativa de servicios públicos esenciales.
Dependencia de entidades externas	Coordinación con Policía, Fiscalía, Secretaría de Gobierno, IDIPRON, y otras entidades distritales y nacionales. Disrupciones externas pueden limitar acciones propias.
Expectativas ciudadanas	Alta sensibilidad y presión social ante eventos que afecten la seguridad y convivencia. Fallas en atención pueden impactar confianza pública.
Eventos naturales o sociales	Riesgos como bloqueos, protestas, apagones, sismos o eventos climáticos que afectan la operatividad en sedes o centros móviles.
Amenazas de ciberseguridad	Incremento de ataques a entidades públicas en Colombia. Pérdida de datos, secuestro de información o interrupción de plataformas.
Medios de comunicación y reputación	Riesgos de afectación reputacional ante mala gestión de crisis o fallos de servicio.
Proveedores críticos de TIC y servicios	Dependencia de servicios de conectividad, servidores, sistemas de atención a víctimas, sistemas de monitoreo y plataformas compartidas.
Situación política-administrativa	Cambios en liderazgo distrital pueden afectar continuidad de decisiones o asignación de recursos para contingencia.

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 149 de 2020 – Por el cual se adopta el Modelo MIPG en Bogotá	Establece como obligatoria la inclusión de la continuidad operativa y gestión del riesgo dentro de la planeación estratégica y gestión por procesos.
Decreto Distrital 221 de 2023	Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones.
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 permite determinar los tiempos máximos aceptables de interrupción y recuperación Tiempo Máximo de Interrupción Tolerable (MTPD), Tiempo Objetivo de Recuperación (RTO) y Punto Objetivo de Recuperación (RPO), así como las dependencias de recursos, infraestructura, tecnología y terceros requeridos para reanudar las operaciones esenciales.

En la SDSCJ, el BIA se aplica a nivel de proceso, de conformidad con el mapa de procesos institucional y bajo la coordinación metodológica de la Oficina Asesora de Planeación (OAP). Cada líder de proceso es responsable de suministrar la información necesaria y de validar los resultados correspondientes, garantizando la trazabilidad entre los impactos identificados, los riesgos asociados y las estrategias de continuidad definidas en este Plan.

Los resultados del BIA alimentan directamente:

- 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).

La SDSCJ adopta un modelo **bienal de actualización del BIA**, en coherencia con la revisión integral del Plan de Continuidad de Negocio y del Sistema de Gestión de Riesgos Institucional. No obstante, se contempla su revisión anticipada cuando ocurran cambios significativos en los procesos, en la estructura organizacional, en la infraestructura tecnológica o física, o ante la materialización de eventos que modifiquen la criticidad de los servicios institucionales.

9.1.2. 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 análisis se extiende a la sede central, al Centro de Comando, Control, Comunicaciones y Computo (C4), las Casas de Justicia, los Centros de Atención a Víctimas, la Cárcel Distrital y otros puntos de prestación de servicios o soporte institucional, garantizando una visión completa de la operación de la entidad.

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 el desarrollo metodológico y consolida los resultados, en articulación con los líderes de proceso y con el Líder de Continuidad de Negocio, asegurando que los impactos identificados en el BIA se integren con la gestión de riesgos institucional, las estrategias de continuidad y los planes de recuperación tecnológica.

9.1.3. 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.	• Valor estimado de pérdida diaria (COP). • % de procesos con alta dependencia TIC.

	• Dependencia de infraestructura tecnológica (C4, SIGA, NUSE, aplicativos internos). • Pérdida de datos o indisponibilidad de sistemas.	• Tiempo medio de recuperación del sistema (RTO tecnológico).

Tabla 6. *Dimensiones y criterios de valoración. Fuente: SDSCJ*

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.

Tabla 7*. Escala de valoración de severidad. Fuente: SDSCJ*

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

La criticidad global del proceso se obtiene mediante la media ponderada de los valores asignados, según la siguiente fórmula:

$$\text{índice de Criticidad } IC = \frac{\text{IO}+\text{IL}+\text{IE}}{3}$$

Donde:

- IO: Puntuación de Impacto Operativo y de Servicio
- IL: Puntuación de Impacto Legal y Reputacional
- IE: Puntuación de Impacto Económico y Tecnológico

La criticidad resultante se clasifica institucionalmente en los siguientes rangos:

Valor promedio (IC)	Clasificación	Interpretación para continuidad
4,5 – 5,0	Muy crítico	Requiere plan de continuidad inmediato y estrategias transversales (CAO, DRP).
3,5 – 4,4	Alto	Plan de continuidad específico con recursos y dependencias priorizadas.
2,5 – 3,4	Medio	Se mantiene controlado con respaldo institucional y pruebas regulares.
1,0 – 2,4	Bajo	Seguimiento básico. No requiere estrategias adicionales.

Tabla 8. *Valor de la criticidad. Fuente: SDSCJ*

9.1.4. 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. Los siguientes análisis representan los valores y evaluaciones que permiten a la SDSCJ seleccionar los escenarios de mayor afectación:

Dependencia de infraestructura física – Escenario: Pérdida catastrófica de sede o infraestructura

El 62 % de los procesos misionales reportó dependencia directa de infraestructura física para su operación.

El BIA muestra que la indisponibilidad de una sede genera impacto operativo de nivel 4 o 5 en la mayoría de los procesos evaluados.

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 9 - Dependencia de infraestructura física - Evaluación BIA - Fuente SDSCJ

La baja disponibilidad de espacios alternos y la alta dependencia de sedes operativas justifican la definición del escenario de pérdida catastrófica de infraestructura como una de las condiciones prioritarias de interrupción para la SDSCJ.

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

El 78 % de los procesos analizados reportó dependencia alta (Nivel 4 o 5) de aplicaciones críticas, y el 55 % de esas aplicaciones no cuenta con respaldo redundante o DRP activo.

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 10 - Dependencia tecnológica - Evaluación BIA - Fuente SDSCJ

La amplia exposición tecnológica y los altos niveles requeridos de redundancia sustentan la identificación del escenario de indisponibilidad tecnológica o ciberataque como uno de los riesgos más críticos para la continuidad institucional.

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

El 46 % de los procesos opera con equipos críticos de menos de cinco personas, y solo el 28 % cuenta con sustitutos designados para funciones vitales.

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 11 - Dependencia de personal crítico - Evaluación BIA - Fuente SDSCJ

La concentración de responsabilidades en equipos reducidos y la necesidad de relevo operativo sustentan el escenario de ausencia masiva de personal crítico, derivado de eventos como emergencias sanitarias o restricciones de movilidad.

Selección de escenarios basados en los resultados del BIA

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

Escenario de desastre	Criterio BIA predominante (Hoja fuente)	Procesos afectados (alta criticidad)	Justificación técnica
Pérdida de sede o infraestructura (**BIA – Hoja "Procesos Misionales"**)	Impacto operativo y logístico	6 de 6 misionales	Dependencia física directa y baja redundancia de espacios alternos.
Indisponibilidad tecnológica / ciberataque (**BIA – Hoja "Dependencias TIC"**)	Impacto tecnológico y económico	14 de 21 procesos totales	Alta dependencia TIC y requisito de redundancia o DRP activo.
Ausencia masiva de personal crítico (**BIA – Hoja "Talento Humano"**)	Impacto operativo y legal	7 de 21 procesos totales	Dependencia de personal especializado y requisito de sustituto designado.

Tabla 12 - Selección de escenarios basados en los resultados 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-V3) como la herramienta oficial y única fuente de verdad para la identificación, valoración y tratamiento de los riesgos que afectan 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 (ej. operación del NUSE 123) o compromete la capacidad operativa o de soporte logístico (ej. indisponibilidad del Centro Alterno de Operaciones - CAO) por un periodo inaceptable.

9.2.2. Identificación Institucional de Riesgos de CN

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 en siete grandes categorías institucionales:

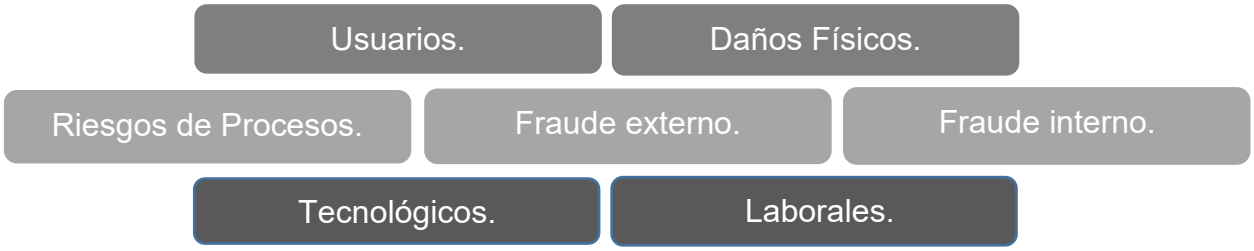


Ilustración 2 - Categoría de riegos. Fuente SDSCJ

Aplicación de la Matriz F-FI-1382-V3

La SDSCJ asegura la trazabilidad del SGCN dentro de la gestión institucional mediante la inclusión obligatoria de una columna de marcado específico en el formato F-FI-1382-V3: "¿Se afecta la Continuidad del Negocio?".

- Criterio de Marcación: Cada líder de proceso debe revisar sus riesgos y marcar "Sí" si este tiene una relación directa con la continuidad, afectando procesos críticos, la dependencia tecnológica o el servicio ciudadano. Si la marcación es "Sí", se requiere la justificación, la cual se documenta en el análisis de riesgos de continuidad por proceso.
- Ejemplo Aplicado (Riesgos Tecnológicos): La falla tecnológica en plataformas misionales, como el sistema NUSE 123 o la sobrecarga en la red de videovigilancia, se marcan como "Sí", ya que comprometen la atención ciudadana en emergencias, siendo riesgos clave para el SGCN.
- Ejemplo Aplicado (Riesgos de Apoyo): Riesgos de la categoría "Daños Físicos" o "Procesos", como la indisponibilidad de vehículos para el traslado de funcionarios al CAO o la pérdida de inventario de suministros, también se marcan como "Sí", dado que su materialización bloquea la posibilidad de ejecutar el plan de continuidad en tiempo y retrasa la recuperación de procesos misionales.

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

Una vez que los riesgos se marcan como relevantes para 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 sigue los lineamientos de la Guía No. 6 del DAFP.

La Fuente de las Actividades Detalladas:

Las actividades detalladas de análisis, valoración, tratamiento y monitoreo de los riesgos provienen del ciclo de gestión de riesgos descrito en el procedimiento o modelo de gestión de riesgos de la SDSCJ, conforme a lo establecido en la Guía No. 6 del DAFP.

Priorización Operativa:

El Plan de Continuidad establece que los riesgos relacionados con la CN deben ser priorizados en la valoración, tratamiento y seguimiento.

- **Impacto Real:** En la SDSCJ, los riesgos tecnológicos asociados a plataformas misionales críticas (NUSE 123) alcanzan frecuentemente niveles de riesgo "Crítico" o "Alto". Esta alta valoración obliga al CIGD y al Líder de Continuidad a definir estrategias inmediatas de respaldo y redundancia (DRP, Centro Alterno).
- **Riesgos de Apoyo**: Incluso los riesgos de apoyo (como la indisponibilidad de transporte o suministros) se valoran en niveles Medios o Altos de riesgo, pues impactan indirectamente la misión al retrasar la capacidad de recuperación.

9.2.4. Uso Operativo de los Riesgos

Los riesgos y su tratamiento consolidado se utilizan en el SGCN de la SDSCJ para:

1. Diseñar Escenarios de Respuesta: Los riesgos de mayor impacto se convierten en los escenarios de desastre que se simulan (ejemplo, un simulacro de falla total del sistema NUSE 123 o un ciberataque).
2. Definir Acciones Preventivas: Las acciones detalladas en el Plan de Tratamiento de Riesgos (como contratos con proveedores alternos, respaldo de inventarios, replicación de datos) se ejecutan en la Fase Preventiva del PCN.
3. Asignar Responsabilidades y Seguimiento: Cada riesgo de CN se vincula al líder de proceso o al Director de Tecnologías y Sistemas de Información correspondiente, asegurando que la acción preventiva o correctiva quede bajo su responsabilidad en el Plan de Continuidad por Proceso (PCP). El seguimiento y la actualización de cada riesgo siguen el ciclo institucional de gestión de riesgos

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 desastre

10.1. Articulación de Escenarios de Crisis

La SDSCJ define sus escenarios de desastre como la manifestación creíble de los riesgos con el potencial de superar los Tiempos Máximos de Inactividad Tolerable (MTPD) de los procesos críticos. Esta articulación se fundamenta en la ISO 22301:2019 y sigue un proceso metodológico que asegura la coherencia entre el riesgo identificado y la estrategia de recuperación:

1. **Selección de Escenarios de Referencia**: Se identifican las amenazas más probables y de mayor impacto para el contexto de Bogotá:

Sismos | Ciberataques | Fallas de servicios | Protestas | Indisponibilidad de sedes

2**. Mapeo de Criticidad:** Se cruzan los escenarios de referencia con los resultados del Análisis de Impacto al Negocio (BIA), enfocándose en los procesos de Muy Alta Criticidad (Ej. RTO 4 horas, como la Gestión de Emergencias / NUSE 123) y aquellos procesos de apoyo que los habilitan (Ej. Gestión de Recursos Físicos).

3**. Vinculación del Riesgo Institucional**: Se validan los escenarios contra los riesgos marcados como de continuidad en la Matriz Institucional de Riesgos (F-FI-1382-V3). Solo aquellos escenarios que materializan riesgos Críticos o Altos son priorizados para el desarrollo de estrategias transversales.

4. **Diseño de Estrategias de Respuesta**: Se definen las estrategias de continuidad (CAO, DRP, Teletrabajo) que se activarán para garantizar los niveles mínimos aceptables de servicio.

Mediante la aplicación del análisis de BIA (Criterios e indicadores aplicados en la SCJ), se han establecido 3 escenarios, que recopilan los eventos con mayor posibilidad, los sitios, procesos o áreas que afectan y la estrategia a aplicar en cada escenario. El detalle podría hacer parte de un plan de continuidad específico para los procesos de mayor afectación, pero en los casos que estos no existieran, se deberá guiar la acción con los presentes escenarios y guías que los complementan:

10.2. Escenario 1: Pérdida Catastrófica del Centro de Comando (C4) o Torre 7 por Daño Físico

Este escenario de Indisponibilidad Física Total modela la materialización de riesgos de la categoría G_Daños_Activos_Físicos que dejan inoperable la sede principal o el C4, impactando directamente la misionalidad.

A. Aplicación al Contexto de la SDSCJ (BIA V2_0):

- Riesgos Materializados: Sismo, Incendio, Bloqueo social y afectación masiva en servicios públicos (energía, agua, gas).

- Afectación Crítica: Indisponibilidad de sedes operativas (C4, Torre 7), lo cual impacta a procesos misionales como la Gestión de Emergencias (MIS-GE) y a procesos de apoyo como la Administración de Muebles e Inmuebles (MIS-AMIFCO) y la Gestión de Recursos Físicos (APO-GRFSE).

B. Estrategia de Continuidad Escenario 1:

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Sismo, incendio, Bloqueo social y afectación masiva en servicios públicos con cierre preventivo de la sede principal (Torre 7) o C4.	Activación del **CAO** y **Plan de Emergencia**.

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Desencadenantes	Evento sísmico que requiere evacuación; Orden de autoridad (IDIGER) que declara el edificio no apto para el ingreso; Daños estructurales visibles.	Declaración de crisis por el CIGD.
Procesos Afectados	Todos los procesos con puestos de trabajo físicos en la sede; Gestión de Recursos Físicos (apoyo clave para movilización).	CAO y Teletrabajo.
Dependencias Críticas	Energía, conectividad de red, acceso al sistema SIGA para inventarios.	Respaldo TIC/DRP para sistemas alojados en el C4 que sigan en línea.
Acciones Inmediatas	**Activación inmediata del Plan de Respuesta a Emergencias**, Notificación a la UAECOBB, movilización de personal vital al CAO.	Priorización del personal vital según el BIA.
Criterio de Retorno	Reapertura segura de la sede verificada técnicamente; Verificación de puestos críticos y actualización de inventarios.	Coordinación con IDIGER (orientaciones de sismo-resistencia/continuidad).

***Tabla 13**. 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 establecer Estrategia Centro Alterno de Operaciones (CAO).*

10.3. Escenario 2: Indisponibilidad Total de Plataformas Misionales (Ciberataque)

Este escenario modela la materialización de riesgos de la categoría D_Fallas_Tecnológicas y se centra en los sistemas misionales cuya RTO es crítica y breve (RTO 6 horas).

A. Aplicación al Contexto de la SDSCJ (BIA V2_0):

- Riesgos Materializados: Ataque Cibernético (DDoS, ransomware), daño en el centro de cómputo.

- Afectación Crítica: Los procesos de Gestión Tecnológica de Seguridad y Emergencias (MIS-GTSE) son directamente impactados, afectando las plataformas misionales (NUSE 123 y Videovigilancia). La recuperación de "Infraestructuras y plataformas tecnológicas operativas y estables" tiene un RTO de 4 horas y MTPD de 8 horas, lo que exige una activación inmediata del Plan de Recuperación de Desastres (DRP).

B. Estrategia de Continuidad Indisponibilidad Total de Plataformas Misionales (Ciberataque):

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Ataque cibernético (DDoS/ransomware) con indisponibilidad de NUSE 123 y videovigilancia.	Activación del **DRP** y **Respaldos TIC**.
Desencadenantes	Alertas confirmadas del SOC; Caída de plataforma crítica $\ge$ 30 minutos; Fallo del sistema NUSE 123.	Declaración de crisis por el CIGD y Dirección de TIC.
Procesos Afectados	Gestión de Emergencias (MIS-GE), Gestión de la Información y Estudios Estratégicos, procesos de apoyo que dependen de la red.	Priorización MIS-GE y MIS-GTSE (RTO corto).
Dependencias Críticas	Acceso a servidores espejo, sincronización de datos (RPO), Canal dedicado de internet.	Uso de tecnología de redundancia (servidor espejo) y copias de seguridad horarias.
Acciones Inmediatas	Notificar a TIC y activar el protocolo DRP. **Restaurar desde servidor espejo y sincronizar datos de los últimos 60 minutos** (si RPO es 1h).	Ejecución del DRP por el Jefe TIC.
Criterio de Retorno	Restauración validada de sistemas; Monitoreo post-incidente; Lecciones aprendidas.	Reporte de conmutación y logs de respaldo.

Tabla 14. *Estrategia de continuidad Escenario 2 - Indisponibilidad Total de Plataformas Misionales (Ciberataque). Fuente: SDSCJ*

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 Vital

Este escenario modela la materialización de riesgos de la categoría E_Relaciones_Laborales o eventos de emergencia sanitaria (pandemia/epidemia) que afectan la disponibilidad del personal mínimo requerido para la operación.

A. Aplicación al Contexto de la SDSCJ (BIA V2_0):

- Riesgos Materializados: Crisis sanitaria, recorte presupuestal que afecta la contratación, huelgas/paros.

- Afectación Crítica: Indisponibilidad del Personal Vital identificado en los anexos del BIA. Esto impacta transversalmente la capacidad de ejecución de cualquier proceso (misional, apoyo o estratégico), especialmente aquellos con alta frecuencia de actividad (Ej. Liquidar nómina o Gestión de pago).

B. Estrategia de Continuidad Indisponibilidad Total de Plataformas Misionales (Ciberataque). Fuente: SDSCJ

Campo	Contenido Operacional SDSCJ	Estrategias Requeridas
Escenario	Ausencia simultánea de personal clave (titular y *back-up*) por crisis sanitaria.	Activación de **Equipos de Recuperación** y **Teletrabajo**.
Desencadenantes	Nivel de ausencia de personal crítico mayor al 30%; Declaración de emergencia sanitaria o laboral que impida el desplazamiento.	Declaración de crisis por el CIGD.
Procesos Afectados	Gestión de Emergencias (operadores C4); Gestión Humana (Liquidación de nómina); Gestión Contractual (para servicios críticos).	Redistribución de talento humano.
Dependencias Críticas	Conocimiento tácito y explícito; Acceso remoto seguro (VPN) a sistemas críticos.	Uso de la matriz de cargos críticos (Anexo 1 del BIA).
Acciones Inmediatas	Activación del **Árbol de Llamadas** y asignación de responsabilidades a suplentes; Implementación de trabajo en casa con herramientas colaborativas.	Definición de las funciones que deben ser desarrolladas por los colaboradores antes, durante y después de un desastre.
Criterio de Retorno	Retorno gradual a la normalidad de acuerdo con las directrices de la autoridad sanitaria; Disolución de los equipos de recuperación.	Verificación de la disponibilidad del personal vital y la actualización del Directorio de emergencia.

Tabla 15. *Estrategia de continuidad: Escenario 3 - Ausencia Masiva de Personal Vital. 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*

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 selección y creación de escenarios de desastre.

11. Gobierno y estructura de continuidad

La gobernanza de la Continuidad de Negocio (CN) de la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) se establece bajo un esquema jerárquico que garantiza el liderazgo de la Alta Dirección, la asignación de recursos, y la supervisión técnica, en concordancia con los requisitos de la ISO 22301:2019 y el Modelo Integrado de Planeación y Gestión (MIPG).

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).

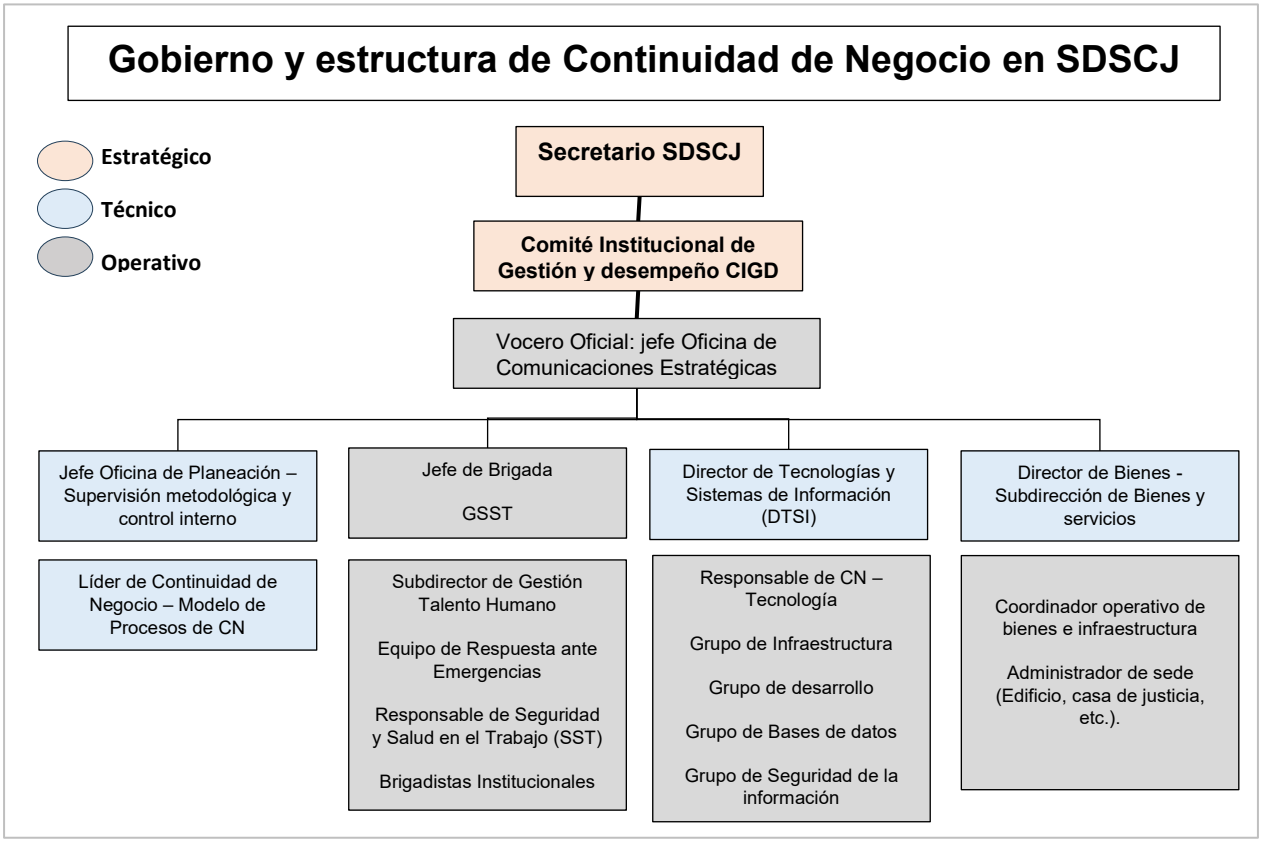


Ilustración 4 - Gobierno y estructura de Continuidad de Negocio. Fuente SDSCJ

11.1. Nivel Estratégico: Liderazgo, Gobierno y Comando de Crisis

Este nivel es responsable de aprobar políticas, asignar recursos, definir el apetito de riesgo y emitir la declaración formal de crisis, asegurando el compromiso de la Alta Dirección con la GCN.

11.1.1. Comité Institucional de Gestión y Desempeño (CIGD)

El CIGD asume las funciones de gobernanza estratégica y de manejo de crisis, siendo el máximo órgano para la toma de decisiones en caso de interrupción.

Justificación y Convocatoria en Emergencia: El CIGD será convocado de manera extraordinaria e inmediata para declarar la crisis y autorizar la activación del Plan de Continuidad (PCN) o el Plan de Recuperación de Desastres (DRP). Esta responsabilidad se fundamenta en la necesidad de consolidar la autoridad de la Alta Dirección para tomar decisiones estratégicas de alto impacto corporativo.

Integrantes 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).

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: Definir los niveles de aceptación de los riesgos de continuidad (apetito de riesgo).
- Activación: Declarar formalmente el estado de crisis y autorizar la activación del PCN o DRP.
- Monitoreo: Evaluar el Informe de Madurez del SGCN y el resultado de las pruebas periódicas, promoviendo la mejora continua.

11.1.2. Director de Emergencia (Secretario Distrital)

El Secretario Distrital, en su rol de más alta autoridad, actúa como Director de Emergencia durante la crisis, tomando decisiones gerenciales y siendo el vocero principal. Funciones principales:

- **Autorización de Crisis**: Tomar decisiones sobre la activación del Plan de Continuidad y la aplicación de las estrategias (CAO, DRP, teletrabajo) ante una contingencia con impacto significativo.
- **Dirección Ejecutiva**: Liderar la estrategia general de manejo de crisis.
- **Vocería Oficial**: Asumir el rol de Vocero Oficial o delegarlo, aprobando los comunicados internos y externos.

11.2. Nivel Táctico: Coordinación y Liderazgo del SGCN

Este nivel se encarga de la gestión operativa, la implementación metodológica y la coordinación de la respuesta entre los equipos técnicos y los procesos misionales.

11.2.1. Líder 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 y/o conocimientos certificados en ISO 22301 como mínimo para que pueda efectuar las actividades de coordinación y supervisión.

Funciones Principales:

- Coordinación Metodológica: Liderar, coordinar y asegurar la implementación, mantenimiento y mejora del SGCN. Definir y actualizar la metodología institucional de continuidad, en coherencia con la norma ISO 22301:2019 y guías nacionales (DAFP, MINTIC).
- Gestión del BIA/Riesgos: Coordinar la elaboración y actualización del Plan de Continuidad Institucional, asegurando que cada proceso cuente con un BIA y análisis de riesgos actualizados, integrándolos a la Matriz Institucional de Riesgos (F-FI-1382-V3).
- Propuesta de Activación: Evaluar la interrupción y proponer al CIGD/Director de Emergencia las recomendaciones técnicas para la activación de las estrategias (CAO, DRP o teletrabajo).
- Monitoreo: Monitorear los indicadores de continuidad (RTO/RPO) y consolidar los informes de avance y madurez del SGCN para el CIGD.
- Pruebas: Coordinar la ejecución del plan anual de pruebas y simulacros, consolidando los resultados e identificando lecciones aprendidas.

11.2.2. Líder Equipo de Tecnología (Director 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 ejecución de las acciones para la recuperación de los servicios críticos de tecnología y la estabilización de las instalaciones principales.

- Soporte: Garantizar el soporte tecnológico necesario para que se pueda cumplir con los objetivos de la misionalidad de la entidad.

11.3. Nivel Operativo: Ejecución y Recuperación

Este nivel es fundamental para la ejecución de las acciones en campo y el restablecimiento directo de los servicios críticos, bajo la dirección del CIGD.

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: El directivo o jefe oficialmente designado en el MIPG como responsable del proceso.

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 y el Plan de Continuidad específico de su proceso.
- 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 de Proceso y a la OAP (2ª línea) el avance, dificultades y cumplimiento de RTO/RPO; cuando involucre DRP/sistemas, incluir a DTSI.
- Pruebas: Participar activamente en pruebas y simulacros, asegurando que su equipo conozca y practique los procedimientos.

11.3.2. Oficina Asesora de Planeación (OAP)

La OAP actúa como la segunda línea de defensa, verificando que las acciones y los planes se desarrollen bajo la metodología institucional.

Rol: Supervisión técnica, orientación metodológica y articulación del SGCN.

Funciones Principales:

- Revisión Técnica: Realizar la revisión técnica de los planes de continuidad por proceso antes de consolidarlos en el plan institucional.
- Aseguramiento: Validar que los planes se ajusten a los lineamientos institucionales y emitir informes periódicos de cumplimiento.
- Facilitación: Actuar como facilitador en simulacros y pruebas, registrando resultados y coordinando lecciones aprendidas para mejorar los planes.
- Repositorio: Administrar el repositorio institucional de Continuidad de Negocio y el control de versiones.

- La Oficina Asesora de Planeación actúa como enlace técnico del CIGD, garantizando la trazabilidad entre las decisiones estratégicas y su implementación en los niveles táctico y operativo.

11.4. Modelo de participación de los roles durante la emergencia

Propósito. Establecer, de manera estandarizada, las funciones por nivel durante la interrupción y el camino de retorno.

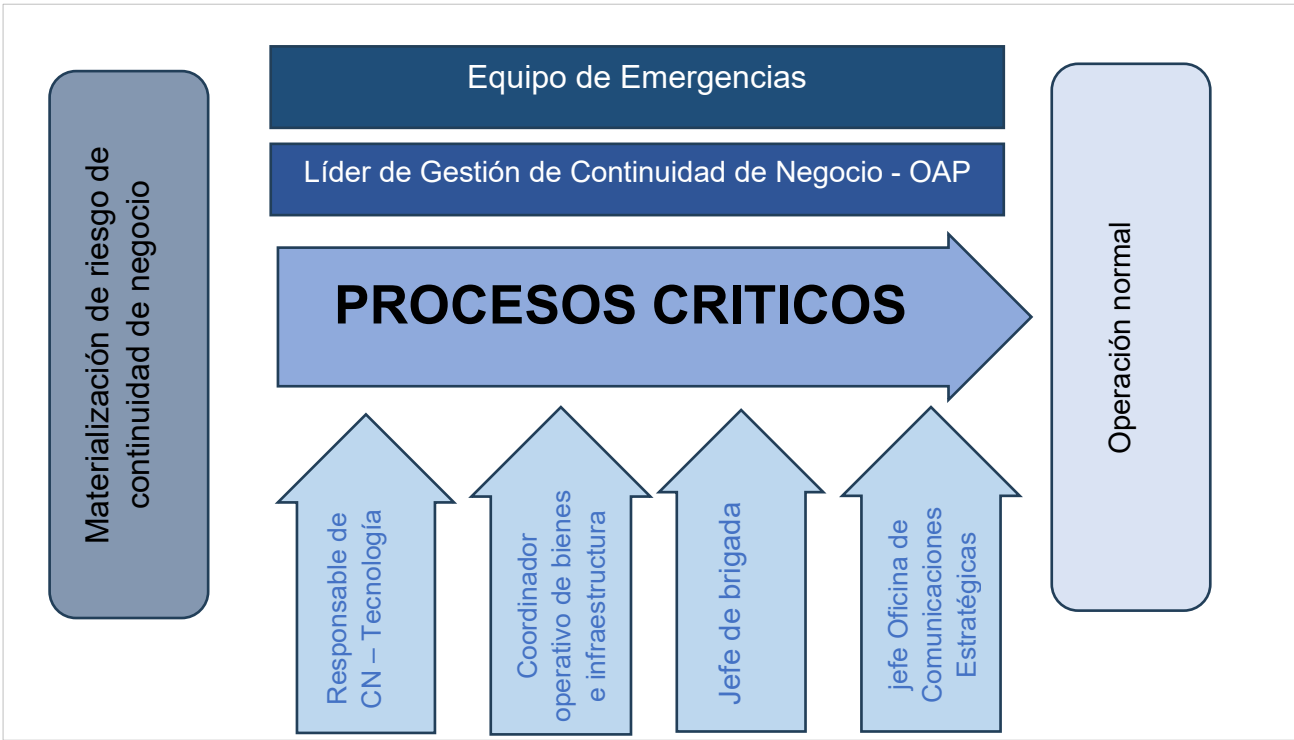


Ilustración 5 - Modelo de participación por roles durante la emergencia. Fuente SDSCJ

12. Fases del Plan de Continuidad del Negocio

La administración del plan de continuidad del negocio se realiza en tres (3) fases de acuerdo con el momento del desastre:

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 continuidad de negocio en la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) no se sostiene únicamente en documentos o planes técnicos. Su efectividad depende de que los servidores públicos comprendan sus roles, conozcan los mecanismos de respuesta y se sientan parte activa de la estrategia institucional. Por ello, la capacitación y la sensibilización se constituyen en un eje transversal del Sistema de Gestión de Continuidad de Negocio (SGCN), asegurando que la cultura organizacional incorpore la prevención, la preparación y la mejora continua.

12.1.1.1. Objetivo del plan institucional de formación y divulgación

El propósito de este componente es garantizar que todos los servidores públicos de la SDSCJ tengan las competencias básicas para actuar durante una contingencia, entendiendo sus responsabilidades y la forma en que su proceso se integra al plan institucional de continuidad. 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

El plan establece una periodicidad anual para la capacitación en continuidad de negocio, dirigida a todos los servidores de planta y contratistas. Estas jornadas deberán articularse con las áreas misionales y de apoyo, adaptando los contenidos a las funciones de cada grupo.

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

Aunque la inducción a nuevos servidores ya contempla aspectos relacionados con misión, visión y procesos de la SDSCJ, se incluirá un módulo específico sobre continuidad de negocio. Este módulo debe explicar, 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.

El responsable principal de la ejecución de este plan será la Oficina Asesora de Planeación, en articulación con la Oficina de Talento Humano y el Líder de Continuidad de Negocio.

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

El Plan de Continuidad de Negocio de la Secretaría Distrital de Seguridad, Convivencia y Justicia establece la estructura general que orienta la elaboración de los Planes de Continuidad por Proceso, los cuales desarrollan, de manera específica, las acciones y mecanismos necesarios para garantizar la operación de cada proceso ante una interrupción.

La formulación, mantenimiento y aplicación de estos planes corresponden al Líder del Proceso y a su equipo de continuidad, quienes deben ajustar su contenido al formato y lineamientos definidos en el Plan General, manteniendo coherencia con su alcance y estructura.

Podrán elaborarse planes de continuidad por área, cuando así lo determine el Líder del Proceso, en atención a la complejidad, tamaño o ubicación de las actividades. En estos casos, dichos planes se considerarán subsidiarios del plan de continuidad del proceso correspondiente.

Todos los planes deberán ser revisados por la Oficina Asesora de Planeación, a fin de verificar el cumplimiento de los requisitos formales y técnicos definidos para este tipo de documentos. La aprobación final será responsabilidad del Líder del Proceso, incluso cuando el plan se origine en una unidad o área bajo su dependencia.

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

Las pruebas de continuidad de negocio son actividades planificadas que permiten validar si los planes documentados funcionan en la práctica y si los equipos responsables saben cómo actuar ante una crisis. Su objetivo es identificar fallas, confirmar tiempos de recuperación (RTO/RPO), validar la comunicación interna y fortalecer la coordinación operativa.

En la SDSCJ, estas actividades se entienden como un proceso progresivo:

2025	**2026**
Fase de diseño documental y calendarización.	Primera ejecución piloto de pruebas, con alcance en procesos críticos, ejercicios institucionales y simulacros en sedes específicas.

La coordinación general corresponde a la Oficina Asesora de Planeación (OAP), que programa las pruebas y consolida los resultados; la ejecución es responsabilidad de los líderes de proceso y sus equipos de recuperación; y cuando los simulacros involucren interacción con la ciudadanía, se integrará la Oficina de Comunicaciones Estratégicas para el manejo de mensajes internos y externos.

Para generar cambios o la creación de nuevos planes subsidiarios o por proceso puede referirse a la guía: *16.7. ANEXO - 7 Metodología para crear plan de Pruebas, ejercicios y simulacros*

12.2. Fase de Respuesta

Esta fase tiene por objetivo contener los daños de un desastre, evaluar los daños ocasionados por el mismo y tomar acción para recuperar los procesos críticos de la SDSCJ mediante la activación de los planes de continuidad del negocio definidos.

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

El plan de gestión de riesgo de desastres para actuar frente a una situación por desastres o amenazas, coadyuvando a la seguridad de los colaboradores, trabajadores en misión, usuarios, contratistas y visitantes.

Define las acciones inmediatas que cada proceso ejecuta al presentarse un incidente disruptivo (sismo, incendio, ciberataque, bloqueo).

Aquí se define “qué hacer en los primeros minutos”. No es el plan completo, sino la reacción inicial para contener el daño. (En muchas ocasiones se relaciona con el plan de emergencias definido por la entidad).

Este plan se encuentra en elaboración durante el 2025 y su propuesta definitiva estará generándose en el mes de diciembre, cuando se publicará y se gestionará en MIPG.

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

Objetivo: Cuantificar los daños a los bienes, los servicios básicos, infraestructura y medio ambiente como resultado de un evento.
Consiste en revisar el impacto del evento sobre instalaciones, equipos, personal o sistemas, para decidir si se activa formalmente el plan de continuidad.

Escenario	Elementos evaluados	Responsable	Tiempo máximo	Evidencia/documento
Caída NUSE 123 (misional)	Estado de servidores, tráfico de red, redundancia activa	Jefe TIC	1 hora	Informe técnico de diagnóstico
Incendio parqueadero (apoyo)	Número de vehículos afectados, estado de pólizas, disponibilidad de suplentes	Jefe Recursos Físicos	2 horas	Acta de evaluación de daños y reporte de aseguradora

Tabla 16. *Ejemplo Fase de Respuesta - Plan de Evaluación de Daños. 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.

Inicia con la decisión de activar el Plan de Continuidad y notificar a los funcionarios y partes interesadas, si es necesario, de la situación

El CIGD es quien toma la decisión de activación del plan de continuidad del Negocio y así mismo de notificarlo a quien corresponda.

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).

Esto muestra cómo volver a operar, aunque sea en forma limitada. “Si aquí no funciona, lo movemos allá” es la lógica principal.

Escenario	Estrategia de recuperación	Responsable	Tiempo meta	Evidencia/documento
Caída NUSE 123 (misional)	Conmutar a servidor espejo en CAO, reubicar 10 operadores en sala alterna	Director C4	4 horas	Acta de activación CAO y reporte de restablecimiento
Incendio parqueadero (apoyo)	Trasladar operación de transporte a proveedor alterno y movilizar 5 vehículos de apoyo	Coord. Logística	8 horas	Contrato alterno activado y reporte de traslado

Tabla 17. Ejemplo Fase de Respuesta - Recuperación en sitio y en CAO. Fuente: SDSCJ

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

Garantizar la disponibilidad de los principales servicios de la Dirección de Tecnologías de la Información (DTSI) para minimizar el daño e impacto de un incidente en los procesos críticos.

Conjunto de acciones específicas para restaurar sistemas TIC críticos dentro de los tiempos de RTO y con pérdida de datos no mayor al RPO.

El detalle de las actividades descritas para cada escenario de interrupción en los servicios de DTI, están definidos en el Plan de Contingencia y Continuidad de Servicios Tecnológicos -DRP.

12.3. Fase de restauración

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

Objetivo: Define las actividades para realizar el retorno a la normalidad, lo que implica desactivar el ambiente Alterno y activar el ambiente Normal.
Implica las actividades de regreso a la normalidad de los procesos críticos de la entidad.

Actividades Para Desarrollar: esta última fase comprende los pasos necesarios para el restablecimiento de las operaciones de negocio en el datacenter principal en el estado que se encontraban, en el momento anterior a la materialización del incidente. Durante esta fase se realizan actividades como evaluación de daños causados y costos de recuperación de recursos afectados.

Actividad	Responsable	Tiempo meta	Evidencia/documento	Observaciones
Migrar operación del NUSE 123 del servidor alterno al servidor principal (misional)	Jefe TIC	24 h después de estabilización	Informe de migración y validación de logs	Hay que asegurar que no haya pérdida de registros
Retomar operación de transporte con flota principal tras incendio (apoyo)	Jefe Recursos Físicos	48 h después de autorización de seguridad	Acta de inspección y disponibilidad de vehículos	Validar pólizas antes del retorno

Tabla 18. Ejemplo Fase de Restauración - Actividades Retorno a la normalidad. Fuente SDSCJ.

12.3.2. DESPUES – Fase de restauración: Interrupción de actividades en contingencia

Objetivo: Define las actividades de interrupción a ser efectuadas por los procesos críticos en la sede alterna de operación, una vez se garantice la vuelta a la normalidad de la sede principal. Acciones para desmontar la operación temporal (en CAO o proveedores alternos) y dejarla lista para un uso futuro.

Actividad	Responsable	Tiempo meta	Evidencia/documento	Observaciones
Deshabilitar servidores espejo y archivar datos de contingencia del NUSE 123 (misional)	Director TIC	1 semana	Acta de cierre DRP y reporte técnico	Mantener copia de respaldo por 6 meses
Finalizar contrato alterno de transporte activado durante la crisis (apoyo)	Coord. Logística	1 semana	Informe de cierre de contrato y facturas	Registrar costos para plan de mejora

Tabla 19. Ejemplo Fase de Restauración - Interrupción de actividades. 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.

Esta es la etapa en la que se formaliza el aprendizaje: todo lo que pasó se convierte en insumos para mejorar la próxima vez.

Actividad	Responsable	Herramienta	Evidencia/documento	Indicadores asociados
Reunión pos-incidente para NUSE 123 (misional)	Líder de Continuidad y Director C4	Taller de lecciones aprendidas	Acta de reunión y plan de mejora	% de RTO cumplidos en simulacro/incidente
Taller de retroalimentación en Recursos Físicos (apoyo)	Líder de Proceso	Encuesta interna y checklist	Informe de evaluación y matriz de acciones	% de disponibilidad de transporte alterno

Tabla 20. Ejemplo Fase de Restauración - Lecciones aprendidas y acciones de mejora. Fuente SDSCJ

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

El plan de cada proceso debe actualizarse después de cada incidente o simulacro, incluyendo indicadores, informes y nuevas acciones.

No basta con hacer el plan una vez; debe revisarse y mejorarse constantemente para que no quede desactualizado. Esto implica revisiones periódicas al menos cada dos años y actualizaciones después de efectuar pruebas o simulacros.

Actividad	Responsable	Frecuencia	Evidencia/documento	Indicadores asociados
Actualizar plan de continuidad del NUSE 123 con hallazgos del simulacro	Líder de Continuidad	Después de cada simulacro o incidente	Nueva versión publicada en micrositio	% de acciones de mejora implementadas
Revisar plan de continuidad de Recursos Físicos y actualizar lista de proveedores	Jefe Recursos Físicos	Cada año o tras incidente	Versión revisada con anexos actualizados	N° de proveedores alternos vigentes

***Tabla 21**. Ejemplo Fase de Restauración - Actualización del Plan de Continuidad. Fuente: SDSCJ.*

13. Mantenimiento y actualización del plan

Este capítulo define cómo se mantiene vigente el Plan de Continuidad de Negocio (PCN) de la SDSCJ y cuándo debe actualizarse. El objetivo es asegurar coherencia entre el plan institucional y los planes por proceso, así como su alineación con el BIA, la matriz de riesgos, el DRP y las capacidades del CAO.

13.1. Periodicidad

Ciclo bienal (Obligatorio)
El PCN institucional y los planes por proceso se actualizan cada 2 años, en sincronía con el ciclo del BIA. Esta actualización incluye: revisión de RTO/RPO/MTPD, estrategias (CAO/DRP/teletrabajo), responsables y evidencias.

Revisiones extraordinarias (cuando aplique).
Además del ciclo bienal, el plan se revisa y ajusta cuando ocurra cualquiera de estas situaciones:

- Cambios estratégicos o normativos (nuevas políticas, lineamientos distritales/nacionales, requerimientos de entes de control).
- Cambios organizacionales (creación/eliminación de procesos, modificaciones del mapa de procesos, reestructuraciones).
- Cambios en riesgos (eventos emergentes o variaciones relevantes en la matriz institucional).
- Cambios en infraestructura (nuevas sedes o cierre de sedes, variaciones en el C4/CAO, redes, energía).
- Cambios TIC (nuevos sistemas críticos, migraciones tecnológicas, contratos de nube/DRP).
- Cambios en terceros críticos (proveedores, convenios de atención, telecomunicaciones).

Pos-incidente / pos-simulacro (obligatorio).
Tras un incidente relevante o un simulacro institucional, se realiza revisión puntual de los planes afectados para incorporar lecciones aprendidas y acciones de mejora.

Ventana sugerida para publicación de cambios.

- Cambio menor (Ejemplo, responsable o dato operativo): publicar en ≤ 15 días hábiles.
- Cambio mayor (Ejemplo, RTO/RPO/estrategia): publicar en ≤ 30 días hábiles luego de la aprobación.

13.2. Responsables

Oficina Asesora de Planeación (OAP) – coordinación metodológica.

- Define y mantiene la metodología institucional de continuidad (formatos, criterios y calendario bienal).
- Programa el ciclo de revisión (bienal y extraordinario), consolida cambios y verifica calidad documental.
- Administra el repositorio/micrositio institucional del PCN y gestiona el control de versiones.
- Integra resultados de simulacros y auditorías y prepara informes de estado para el CIGD.

Líder de Continuidad de Negocio – articulación y control.

- Centraliza las solicitudes de cambio en documentos relacionados con la CN y valida consistencia entre estos (impactos cruzados).
- Verifica que actualizaciones mantengan coherencia con BIA, matriz de riesgos, DRP y CAO.
- Propone aprobación de cambios mayores al CIGD cuando afecten prioridades, RTO/RPO o presupuesto.
- Da seguimiento a acciones de mejora pos-incidente y a indicadores de mantenimiento.

Líderes de Proceso – ejecución y evidencia.

- Monitorean detonantes de cambio; inician las solicitudes de cambio, actualizan su plan de continuidad del proceso y adjuntan evidencias.
- Ajustan procedimientos, listas de verificación, roles y contactos; socializan el cambio con su equipo.
- Actualizan anexos: BIA de proceso (si procede), riesgos específicos, inventarios y dependencias.

CIGD – decisión y priorización (cuando aplique).

- Aprueba cambios estratégicos o de alto impacto (priorización, recursos, políticas) y define su entrada en vigor.

13.3. Condiciones para actualización y procedimiento

13.3.1. Condiciones típicas (detonantes)

- **Estrategia y política**: nuevas directrices distritales/nacionales, observaciones de entes de control, acuerdos sectoriales.
- **Organización y procesos**: creación/eliminación de procesos, cambios de roles críticos, nuevos servicios al ciudadano.
- **Riesgos**: aparición de amenazas (Ejemplo, ciberataques con nueva modalidad), variación sustancial de exposición o impacto.
- **Infraestructura física**: apertura/cierre de sedes (incluidas Casas de Justicia), cambios en C4/CAO, rutas de acceso.
- **Tecnología**: nuevas plataformas misionales, migraciones a nube/DRP, obsolescencia de componentes.

- **Proveedores críticos**: cambios de operador del 123, enlaces de datos, energía, transporte, data center.
- **Lecciones aprendidas**: hallazgos de auditoría, simulacros o incidentes (brechas en RTO, comunicación, logística).

13.3.2. Procedimiento paso a paso

Detección del cambio

- El líder de proceso identifica un requisito o condición que aplica para cambio (Ejemplo: nueva sede o ajuste en RTO) y notifica al Líder de Continuidad.

Solicitud de cambio

- El líder de proceso elabora correo electrónico con la siguiente información:
  - Qué cambia y por qué (incluya evidencia).
  - Impacto en RTO/RPO/MTPD y en dependencias (TIC, logística, CAO).
  - Documentos afectados (plan de proceso, BIA, riesgos, DRP, protocolos, listados).
  - Fecha objetivo de entrada en vigor y responsable del cambio.

Revisión técnica (Líder de Continuidad y OAP)

- Verificación de consistencia con metodología, impactos cruzados y necesidad de aprobación superior.

Aprobación

- Cambios menores: visto bueno del Líder de Continuidad y OAP.
- Cambios mayores (estrategia, RTO/RPO, presupuesto): decisión del CIGD.

Actualización documental

- El líder de proceso implementa el cambio en su Plan de Continuidad del Proceso y anexos; OAP verifica formato/calidad.

Publicación y control de versiones

- OAP publica la nueva versión en micrositio/repositorio y actualiza el registro de versiones (Ejemplo: V3.1 – 2025-10-15: ajuste RTO NUSE 123 a 2 h; actualización DRP y CAO).

Comunicación y socialización

- El líder de proceso comunica cambios a su equipo; si afecta atención al ciudadano, coordina con Comunicaciones Estratégicas los mensajes internos/externos.

Formación puntual y evidencia

- Se realiza inducción breve a los roles impactados (Ejemplo, nuevo procedimiento de conmutación); se archivan listas de asistencia y actas.

Seguimiento e indicadores

- El Líder de Continuidad consolida cumplimiento de publicación en plazo, evidencias y acciones de mejora derivadas.

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
Cumplimiento de RTO	Mide si los procesos críticos se recuperan dentro del tiempo máximo definido.	(N° de procesos recuperados ≤ RTO ÷ N° de procesos afectados) × 100	Semestral (en pruebas) y pos-incidente	Líderes de proceso y OAP
Cumplimiento de RPO	Evalúa si la pérdida de datos está dentro de lo tolerado.	(N° de sistemas que cumplen RPO ÷ N° de sistemas probados) × 100	Semestral (pruebas TIC)	Dirección TIC y OAP.
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
Matriz de riesgos actualizada con continuidad	Proporción de riesgos institucionales con marcación de continuidad revisada.	(N° de riesgos con campo continuidad actualizado ÷ N° total de riesgos institucionales) × 100	Anual	OAP y Líderes de proceso
Riesgos mitigados	Porcentaje de riesgos de continuidad con medidas implementadas.	(N° de riesgos mitigados ÷ N° de riesgos identificados en continuidad) × 100	Anual	Líderes de proceso y OAP
Procesos probados en simulacros	Mide cuántos procesos han participado en al menos una prueba de continuidad.	(N° de procesos probados ÷ N° total de procesos críticos) × 100	Anual	OAP y CIGD
Incidentes gestionados con plan activado	Mide si los incidentes críticos fueron atendidos aplicando el plan de continuidad.	(N° de incidentes con plan activado ÷ N° total de incidentes críticos) × 100	Trimestral	Líder de Continuidad y CIGD

Tabla 22. *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 establecer 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 en ≤ 2 horas desde la decisión del CIGD; retorno seguro y verificado.

Pasos metodológicos (aplicables a cualquier sede)

Paso A **Identificar funciones críticas por sede**

- Levantar procesos y actividades que operan en la sede (misionales, apoyo).
- Marcar dependencias TIC y de servicios (energía, datos, telefonía).
- Señalar recursos físicos clave (puestos, salas, equipos especiales).
- Interpretación sencilla: este paso responde “¿qué mínimo debo mover y a dónde?” antes de que ocurra la contingencia.

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.
- **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 Plan de Recuperación de Desastres

Objetivo

Definir cómo asegurar que los sistemas tecnológicos críticos de la Secretaría se recuperen rápidamente después de un desastre o interrupción, garantizando continuidad en la prestación de servicios misionales como la atención de emergencias y la seguridad ciudadana.

Identificación de sistemas críticos

Paso A …as 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**: ocurre cuando un sistema crítico supera su RTO de falla o cuando el impacto es inmediato (ejemplo: caída total del 123).

- **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 al menos una vez al año, integrando:

- Pruebas técnicas: restauración de datos, conmutación de servidores.
- Pruebas operativas: simulacros en los que operadores usan el sistema alterno.
- Lecciones aprendidas: ajustes en los tiempos de activación y en la configuración técnica.

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.
N° de incidentes críticos sin respaldo operativo	Conteo de incidentes en que el DRP no funcionó	Reportes de incidentes TIC	Identifica brechas en la estrategia de respaldo.

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).

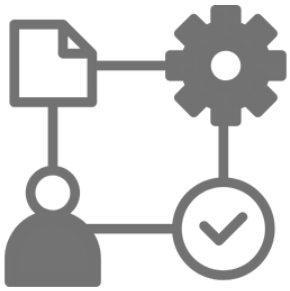
Proceso	Rol	Teletrabajable (Sí/No)	Justificación
Gestión de Emergencias	Operador del 123	No	Requiere consola en sitio o en CAO para atención directa de llamadas.
Gestión Jurídica	Abogado revisor de tutelas	Sí	Accede a expedientes digitales y puede tramitar documentos por medios electrónicos.
Gestión 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.
Tasa de éxito en pruebas de teletrabajo	N° de funcionarios que accedieron y trabajaron correctamente ÷ N° de pruebas realizadas	Evalúa si la estrategia funciona realmente cuando se prueba.

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



La priorización consiste en decidir cuáles procesos y servicios deben recuperarse primero en una emergencia, considerando que no todos pueden atenderse al mismo tiempo. El criterio principal proviene del BIA (Análisis de Impacto al Negocio), que clasifica los procesos según su criticidad y tiempos de recuperación (RTO/MTPD). Para la SDSCJ, esto significa que procesos como Gestión de Emergencias o el NUSE 123 tienen prioridad absoluta sobre otros de carácter administrativo, porque una interrupción en ellos afecta de forma inmediata a la ciudadanía.

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 desastre, 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.

16.5. 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

Indicadores de seguimiento

Indicador	Cómo se mide	Interpretación
Tiempo de respuesta en comunicación interinstitucional	Minutos entre el evento y la confirmación de contacto con la entidad aliada	Evalúa la agilidad de coordinación inicial.

% de simulacros con participación de entidades externas	(N° simulacros con aliados ÷ N° total simulacros) × 100	Mide el nivel de integración real en ejercicios.
Número de acuerdos/documentos de coordinación vigentes	Conteo de convenios, memorandos de entendimiento o protocolos activos	Refleja la solidez de la relación interinstitucional.

La coordinación interinstitucional es un pilar transversal de la estrategia de continuidad: asegura que el esfuerzo interno de la SDSCJ (CAO, DRP, teletrabajo, priorización) tenga respaldo en emergencias reales donde múltiples actores deben actuar al mismo tiempo. Para la SDSCJ, la clave está en mantener protocolos claros, contactos actualizados y pruebas conjuntas periódicas con las entidades estratégicas.

16.6. ANEXO - 6 Metodología para la selección y creación de escenarios de desastre.

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).

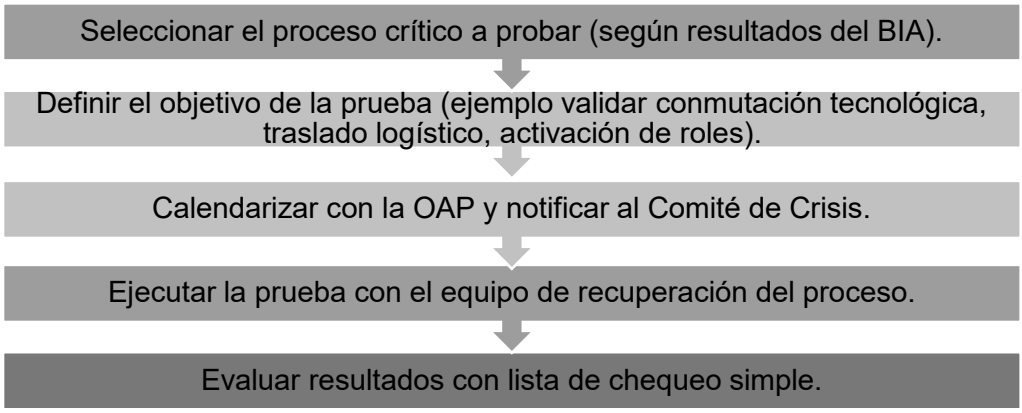
Campo	Contenido (ejemplo aplicado 2024)
Escenario	Ciberataque (DDoS/ransomware) con indisponibilidad de NUSE 123 y videovigilancia
Desencadenantes	Alertas SOC; caída > 30 min; degradación severa de tráfico; confirmación de incidente
Procesos afectados	Gestión de Emergencias (criticidad muy alta; RTO 4h; RPO 1h; MTPD 8h)
Dependencias TIC	NUSE 123, radiocomunicaciones, videovigilancia, conectividad metropolitana
Severidad	**Alta** si afecta atención ciudadana y coordinación interinstitucional
Estrategias	**DRP** (conmutación y restauración desde respaldos), **CAO** para operación manual mínima, campañas de comunicación
Activación	CIGD; líder TIC activa DRP según MINTIC IRBC; coordinación con CSIRT
Retorno	Restauración validada, monitoreo post-incidente, lecciones aprendidas

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

16.7. ANEXO - 7 Metodología para crear plan de Pruebas, ejercicios y simulacros

Pruebas a nivel de procesos

Procedimiento:



Ejemplos aplicados:

- Gestión de Emergencias (NUSE 123, misional): prueba de conmutación al servidor alterno en menos de 30 minutos, con validación de atención mínima del 70% de llamadas.
- Recursos Físicos (apoyo): prueba de activación de contrato alterno de transporte, movilizando un vehículo suplente en menos de 2 horas.

Ejercicios a nivel Secretaría

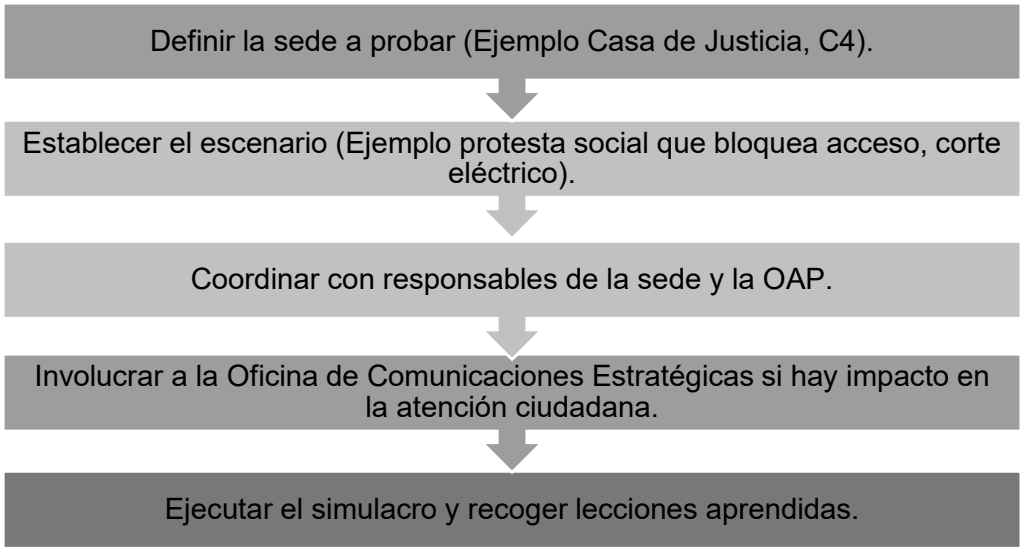
Procedimiento:

Ejemplo aplicado:

- Un ejercicio institucional simula un incendio en la sede central. El CIGD ordena traslado de funciones críticas al CAO en el C4, mientras procesos administrativos se conectan en teletrabajo. La Oficina de Comunicaciones Estratégicas emite un comunicado oficial en web y redes sociales informando que los servicios al ciudadano siguen habilitados de manera remota.

Simulacros a nivel de sedes o ubicaciones físicas

Procedimiento:



Ejemplos aplicados:

- Casa de Justicia: simulacro de cierre por falla eléctrica → atención de usuarios se deriva a otra Casa de Justicia; se comunica a ciudadanos mediante carteleras y redes institucionales.
- C4: simulacro de falla de red metropolitana → se activa redundancia tecnológica y conmutación a plataformas espejo.

Evaluación y mejora de las pruebas

Al finalizar cada prueba, ejercicio o simulacro se debe realizar una evaluación simple con tres preguntas clave:

¿Se cumplieron los tiempos definidos en el BIA (RTO/RPO)?

¿Los roles asignados actuaron según el plan?

¿La comunicación fue clara y oportuna, tanto interna como externa?

Esquema simple de evaluación (lista de chequeo):

- Cumplimiento de RTO/RPO → Sí / No.
- Activación de roles críticos → Sí / No.
- Comunicación efectiva → Sí / No.
- Observaciones y lecciones aprendidas.

Los resultados deben documentarse en un informe breve del proceso, consolidado luego por la OAP en el reporte institucional de continuidad.