



Plan de Contingencia y Continuidad del Negocio

Código SG/MIPG 127-PPPDE-16
Vigencia desde 27/12/2022
Versión 1

Proceso Direccionamiento Estratégico

Tabla de Contenido

1. Introducción	4
2. Marco Legal.....	4
3. Objetivos.....	6
3.1 Objetivo General.....	6
3.2 Objetivos específicos	6
4. Alcance	6
5. Definiciones y Siglas.....	6
6. Roles y responsabilidades	7
7. Generalidades metodológicas.....	8
7.1 Identificación del Escenario de Pérdida de Continuidad del Negocio	8
7.2 Detección.....	8
7.3 Activación.....	9
7.4 Plan de operación alternativo.....	9
7.5 Recuperación y restablecimiento - Resolución del incidente	9
8. Proceso Metodológico de Construcción del Plan de Contingencia y Continuidad del Negocio.....	9
8.1 Análisis del entorno institucional.....	9
8.1.1 Factores del Contexto Externo que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.....	9
8.1.2 Factores del Contexto Interno que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.....	10
8.1.3 Factores del Contexto del Proceso que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.....	10
8.2 Análisis de impacto al negocio.....	11
8.3 Riesgos asociados a la continuidad del negocio	12
8.4 Definición de escenarios de pérdida de continuidad	12
8.5 Definición de estrategia de continuidad.....	13
8.6 Identificación y selección de recursos	13
8.7 Documentación de procedimientos de continuidad.....	14



8.8	Pruebas y revisión periódica del plan.....	14
8.9	Gestionar el plan de continuidad.....	15
8.9.1	Escenarios de continuidad de negocio	15
8.9.2	Estrategia institucional de gestión de contingencia y continuidad.....	16

1. Introducción

Este documento “Plan de Contingencia y Continuidad del Negocio del DADEP” es una herramienta para prevenir o reaccionar ante los posibles incidentes que puedan poner en riesgo el cumplimiento de la misionalidad de la entidad, la prestación o continuidad de los servicios del DADEP, o poner en riesgo la integridad de su personal y los visitantes de la institución; esto a través de un conjunto de acciones para dar respuesta a estos eventos en un Plan de Contingencia y Continuidad del negocio. Por lo tanto, se espera que con estas acciones diseñadas y ejecutadas de forma planificada respondan de eficiente ante una emergencia, restablezcan en el menor tiempo posible la prestación de los servicios y mitiguen el impacto negativo de la pérdida de recursos.

El plan presentado a continuación es una guía de trabajo que está dividida en dos partes; la primera parte, define los elementos críticos a controlar a partir del análisis de los riesgos asociados, los responsables, etapas, definiciones y generalidades; la segunda parte presenta las actividades y secuenciales, fechas de ejecución, recursos requeridos y el desarrollo del análisis de brechas de cada una de ellas, teniendo en cuenta las restricciones de la entidad.

2. Marco Legal

El desarrollo del Plan de Contingencia y Continuidad de Negocio para el Departamento Administrativo de la Defensoría del Espacio Público – DADEP, se fundamenta en la necesidad de preservar la disponibilidad y continuidad de los servicios que presta la entidad, dentro del marco de la implementación de la política de gobierno digital y los lineamientos generales en el uso de servicios digitales ciudadanos. Igualmente, se articula con el Modelo Integrado de Planeación y Gestión – MIPG, a través de la 3ª Dimensión: Gestión con valores para resultados. No obstante, se orienta con los siguientes marcos legales:

- **NTC/ISO 22301:2012**, Norma internacional para la gestión de la continuidad de negocio.
- **Ley 1523 de 2012**, “Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones”, en su Artículo 2º. De la responsabilidad. La gestión del riesgo es responsabilidad de todas las autoridades y de los habitantes del territorio colombiano. En cumplimiento de esta responsabilidad, las entidades públicas, privadas y comunitarias

desarrollarán y ejecutarán los procesos de gestión del riesgo, entiéndase: conocimiento del riesgo, reducción del riesgo y manejo de desastres, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres. (negrilla fuera de texto).

- **Decreto 1072 de 2015**, "Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo", donde se establece la política nacional de gestión del riesgo de desastres y las obligaciones en materia de Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), Artículo 2.2.4.6.4. El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG - SST) consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua y que incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo. (negrilla fuera de texto).
- **Decreto 1078 de 2015**, "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **Ley 1955 de 2018**, "por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad"", en su Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros.
- **Manual Operativo del Modelo Integrado de Planeación y Gestión. Versión 4 (2020), MIPG, 3ª.** Dimensión: Gestión con valores para resultados, en sus numerales:
 - 3.2.1.3 Política Gobierno Digital, Gobierno Digital es la política de MIPG que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. La política de Gobierno Digital

contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes.

- 3.2.1.4 Política de Seguridad Digital. En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

3. Objetivos

3.1 Objetivo General

Establecer lineamientos para seguir un evento de interrupción, definiendo las actividades detectivas, preventivas, reactivas y correctivas para gestionar adecuadamente las situaciones que sean calificadas como emergencia y puedan comprometer la seguridad de las personas, la prestación de servicio o la continuidad de las funciones misionales del DADEP.

3.2 Objetivos específicos

- Disminuir el impacto de la materialización de una situación de emergencia, buscando el cumplimiento de las actividades misionales de la entidad.
- Disminuir los tiempos de interrupción y mantener en niveles aceptables las actividades misionales, en caso ocurrencia de una emergencia, esto a través de la identificación de las actividades críticas, los recursos y los procedimientos necesarios.
- Generar una pronta recuperación de los servicios en caso de una emergencia.
- Dar la protección de las personas dentro de las instalaciones de la Entidad en caso de que se materialice una emergencia.

4. Alcance

El Plan de Contingencia y Continuidad del negocio, inicia con la identificación de los escenarios de emergencia, la definición de las actividades, responsables y recursos en caso de materialización de la situación o escenario y finaliza con la estrategia de recuperación.

5. Definiciones y Siglas

- **Análisis de Impacto del Negocio:** proceso de análisis del impacto a lo largo del tiempo de una interrupción en la organización
- **Continuidad del negocio:** capacidad de una organización para continuar la entrega de productos y servicios dentro de marcos de tiempo aceptables a la capacidad predefinida durante una interrupción
- **Emergencia:** Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata
- **Interrupción:** Incidente, anticipado o no anticipado, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización
- **Plan de continuidad de negocio:** información documentada que guía a una organización para responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.

Siglas:

- **BCP:** Plan de continuidad de negocio (siglas en Ingles).
- **BIA:** Análisis impacto del negocio (siglas en Ingles).
- **DADEP:** Departamento Administrativo de la Defensoría del Espacio Público.
- **SG SST:** Sistema de Gestión de Seguridad y Salud en el Trabajo.
- **EIR:** Estrategias Institucionales de Respuesta.

6. Roles y responsabilidades

Rol	Responsabilidad	Representantes	Mecanismos
Equipo de gestión de emergencias.	Activación del Plan de continuidad ode emergencia y Plan de restablecimiento.	• Director(a). • Subdirectores. • Jefe de la Oficina de tecnologías de la información y las comunicaciones. • Jefe de la Oficina Asesora de Planeación. • Jefe de la Oficina Asesora de Comunicaciones.	• Declaración formal de inicio de actividad de contingencia o continuidad.
Líderes de proceso Estratégicos, Misionales y de Apoyo.	Evaluar los riesgos e impactos de la pérdida de continuidad.	• Líderes de procesos de acuerdo con sus responsabilidades definidas en el plan de continuidad.	• Evaluar los riesgos que puedan generar pérdida de continuidad. • Análisis impacto del negocio.
Jefe de la Oficina Asesora de Planeación, Jefe de la Oficina de tecnologías de la información y las comunicaciones y Subdirectora de Gestión Corporativa	Asesorar, coordinar y documentar el plan de continuidad de negocio.	• Jefe de la Oficina Asesora de Planeación y equipo de trabajo. • Jefe de la Oficina de tecnologías de la información y las comunicaciones y equipo de trabajo. • Subdirectora de Gestión Corporativa	• Aplicar las guías y metodologías institucionales. • Metodología de riesgos. • Análisis de la información.

Rol	Responsabilidad	Representantes	Mecanismos
		Asesor y enlaces de los procesos.	- Identificación de escenarios de pérdida de continuidad. - Análisis y selección de la estrategia de continuidad. - Inclusión de los planes de respuesta en el plan de acción anual.
Equipo de gestión de emergencias.	Activación del Plan de continuidad o de emergencia y plan de restablecimiento.	- Director(a). - Subdirectores. - Subdirectora de Gestión Corporativa. - Jefe de la Oficina de tecnologías de la información y las comunicaciones. - Jefe de la Oficina Asesora Planeación.	Declaración formal de inicio de actividad de contingencia o continuidad.

7. Generalidades metodológicas

El Plan de Contingencia y Continuidad del Negocio, está integrado de actividades que busca mantener aceptable el funcionamiento de la misionalidad del DADEP, con la prestación de sus servicios en eventos o contingencias que impidan de significativamente el desarrollo normal de los procesos.

El plan de Continuidad se establece en cinco momentos:

7.1 Identificación del Escenario de Pérdida de Continuidad del Negocio

Esta parte inicial, identifica los aspectos generales del plan, tales como: la identificación del riesgo de la no continuidad del negocio por proceso, el escenario en que puede incurrir y su descripción, las posibles causas de la pérdida de continuidad, sus consecuencias, el responsable de generar la respuesta dentro del plan y la definición del equipo de trabajo para la ejecución del plan (quienes deben estar preparados en caso de presentarse un evento inesperado).

7.2 Detección

En esta fase se involucra la identificación de las alertas y la forma de su confirmación, generando acciones de preparación de las áreas para iniciar una contingencia y la articulación de la gestión institucional en los diferentes procesos del DADEP; como resultado de lo anterior, estas acciones de monitoreo o indicadores de la ocurrencia potencial de una emergencia, serán las acciones de prevención que se deben fortalecer en las políticas internas, los canales de comunicación y las estrategias de activación de la respuesta a contingencias.

En este aspecto, está orientado a generar las acciones necesarias para confirmar la materialización de un incidente que pondrá en riesgos la continuidad de la prestación de los servicios misionales, comunicar la emergencia identificada y la toma de decisión por parte del equipo de gestión de emergencias.

7.3 Activación

Aquí se realizarán las acciones para activar el Plan de contingencia y Continuidad del negocio, según el escenario, para después realizar la operativización las contingencias y resolver emergencia.

7.4 Plan de operación alterno

En esta fase, se desarrollará el cubriendo de todas las tareas que se ejecutarán para mantener la operación de los servicios institucionales en niveles aceptables (buscando disminuir los tiempos de interrupción) mientras exista la emergencia activa, esta fase activan los planes de operación alterna y las acciones al alcance de la entidad para resolver las afectaciones sobre la Entidad que generó la situación de emergencia.

7.5 Recuperación y restablecimiento - Resolución del incidente

En este momento, se define todas las actividades necesarias para retomar las actividades en su estado normal de funcionamiento una vez se han superado las situaciones que generaron la emergencia, se han restablecido los sistemas afectados o se han reparado las estructuras afectadas.

8. Proceso Metodológico de Construcción del Plan de Contingencia y Continuidad del Negocio.

8.1 Análisis del entorno institucional

A partir de las funciones y obligaciones normativas delegadas al DADEP, los compromisos con los diferentes grupos de valor y partes interesadas, y los datos históricos de la operación institucional, se consolidan los factores que pueden afectar el desarrollo adecuado de las actividades, representadas así:

8.1.1 Factores del Contexto Externo que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Políticos: Cambios de gobierno, legislación, políticas públicas y regulación (Cambios en la administración central y territorial que genera cambios en los planes de desarrollo).

Económicos y financieros: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. Restricciones de orden económico que pueden afectar el

funcionamiento de la entidad o la ejecución de los proyectos, cambios en la asignación presupuestal de la entidad o para el proyecto por cambio de prioridades de la administración.

Sociales y culturales: Demografía, responsabilidad social y orden público. Mayor demanda de espacio público por Incremento de migración de población hacia Bogotá y desplazamiento de esta a la periferia de la ciudad y sus municipios circunvecinos, Requerimientos de las partes interesadas externas (Vecinos, comerciantes, alcalde, concejales).

Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

Ambientales: Emisiones y residuos, energía, catástrofes naturales y desarrollo sostenible. Cambio de las políticas que propendan por disminuir la afectación ambiental a través de procesos de mitigación de impacto ambiental, Manejo de residuos y Contribución al desarrollo sostenible

Legales y Reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos). Nuevas disposiciones legales que afecten a la Entidad (laborales, contratación, manejo de espacio público, sectoriales).

8.1.2 Factores del Contexto Interno que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Personal: Competencia del personal, disponibilidad, seguridad y salud ocupacional.

Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo

Comunicación Interna: Canales utilizados y su efectividad, flujo de la información adecuado.

8.1.3 Factores del Contexto del Proceso que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Diseño del proceso: claridad en la descripción del alcance y objetivo del proceso.

Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.

Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.

Activos de Seguridad de la Información del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 8 y 9.

8.2 Análisis de impacto al negocio

El Departamento Administrativo de la Defensoría del Espacio Público evalúa los impactos y las prioridades de recuperación de las actividades que apoyan a sus diferentes productos y servicios. El análisis de impacto al negocio incluye la identificación de todas las actividades que apoyan la provisión de productos y servicios, la evaluación en el tiempo de la imposibilidad de realizar dichas actividades, el establecimiento de tiempos y priorización del orden de restablecimiento de las actividades a niveles mínimos aceptables.

Para el desarrollo del análisis del impacto se siguen los siguientes pasos:

1. Listar todas las funciones del negocio.
2. Determinar los criterios bajo los cuales se medirá la criticidad de cada función de negocio (Financiero, Reputacional, Legal / Regulatorio, Contractual, Misional).
3. Valorar la pérdida de continuidad total o parcial de cada función de negocio de acuerdo con los criterios seleccionados.
4. Priorizar las funciones de negocio de acuerdo con la valoración del impacto por pérdida de continuidad.
5. Determinar funciones y recursos que son esenciales para las funciones que fueron priorizadas como críticas.
6. Presentar los resultados del análisis de impacto de negocio en el Comité Institucional de Gestión y Desempeño.

Los resultados del análisis de impacto se utilizan para determinar los tiempos de respuesta de las diferentes etapas del BCP (Plan de continuidad de negocio por sus siglas en Ingles), en particular:

- Tiempo máximo tolerable que pueden una actividad permanecer suspendida antes de que los daños para la entidad sean totalmente irremediables.
- Tiempo de necesario para el restablecimiento de los servicios y recursos indispensables para el funcionamiento normal de las actividades priorizadas.
- Identificación del nivel máximo tolerable de pérdida de datos que obligue a su recuperación mediante procedimientos manual.

8.3 Riesgos asociados a la continuidad del negocio

Los riesgos asociados a la continuidad del negocio se analizan al mismo tiempo que se realiza la identificación de riesgos institucionales con cada proceso y se registra en el mapa de riesgos como “perdida de continuidad”, los riesgos de continuidad del negocio estarán implícitos en los riesgos institucionales asociados a cada proceso, se identifican siguiendo la misma metodología Institucional de Gestión de Riesgos.

Los riesgos de pérdida de continuidad se agrupan en escenarios de pérdida de continuidad cuando sus causas son comunes o que conducen a la interrupción del servicio total o parcial, de una o varias funciones calificadas como críticas. El DADEP, contempla implícitamente en la gestión de sus procesos la identificación y administración de los riesgos como práctica para impedir que eventualidades internas o externas impidan cumplir sus objetivos institucionales.

Al desarrollar el plan de continuidad del negocio se integra la metodología de riesgos y los controles preventivos, detectivos y correctivos de los planes de tratamiento de riesgos, los cuales quedan asociados al mapa de riesgos institucional.

8.4 Definición de escenarios de pérdida de continuidad

Los riesgos identificados con mayor probabilidad de ocurrencia e impacto a nivel de continuidad se analizan y se determina si tienen entre sí, causas comunes o correlaciones que permitan su análisis como un escenario factible de pérdida de continuidad. Este análisis se realiza para concentrar los esfuerzos en aquellos eventos que combinados tendrán una probabilidad razonable de impedir la continuidad de los servicios institucionales.

Como resultado del análisis de los riesgos se describen escenarios de pérdida de continuidad sobre los cuales se diseñará una estrategia de continuidad, paralelamente la documentación de los escenarios permite documentar los criterios que debe aplicar el Comité de Crisis para realizar la declaración de emergencia y autorizar la activación del plan de continuidad.

Aquellos riesgos que no se puedan correlacionar o consolidar en algún escenario, se deben reevaluar para determinar si constituyen un escenario independiente que por su naturaleza obligan a la activación de la continuidad o simplemente se pueden tratar por los procedimientos ya definidos para manejo de eventos de riesgo con planes de tratamiento ya definidos.

Para cada actividad priorizada dentro de los escenarios de emergencia se establecen los mínimos operativos que el Departamento Administrativo de la Defensoría del Espacio Público se compromete a mantener durante la fase de operación en contingencia y el tiempo máximo que se puede mantener la operación en contingencia antes de que las afectaciones sean irremediables.

8.5 Definición de estrategia de continuidad

El DADEP a partir de los escenarios de emergencia seleccionados se determina la estrategia específica que se debe aplicar en caso de que el escenario se materialice. Para cada caso específico se debe establecer:

- Cual o cuales son las formas apropiadas para proteger las actividades priorizadas.
- Determinar si las actividades afectadas se estabilizarán con los recursos disponibles, si se reanudarán las actividades con otros recursos propios o de terceros.
- Determinando las dependencias de las actividades priorizadas frente a las actividades de apoyo.
- Información vital que permita la continuidad de las actividades priorizada.

Aunque la estrategia específica que se aplicará a cada escenario particular depende de la naturaleza de este, se deben considerar alternativas como:

- Recuperación de la actividad dentro de las mismas instalaciones de la entidad con recursos propios de la entidad.
- Recuperación de la actividad en instalaciones de otra entidad usando recursos propios del DADEP.
- Recuperación de la actividad en las instalaciones o con los recursos de un proveedor independiente, como por ejemplo centros de cómputo alternos o infraestructura de nube.
- Combinación de diferentes modelos de opciones de recuperación, utilizando recursos internos como externos.

8.6 Identificación y selección de recursos

Usando los resultados del análisis de impacto y la selección de estrategia se determinan los recursos necesarios para implementar la estrategia de continuidad definida, estos recursos deben incluir, pero no limitarse a:

- Personas
- Información y datos
- Instalaciones físicas
- Equipos y elementos consumibles

- Tecnología de información
- Transporte
- Recursos financieros
- Proveedores y contratistas

8.7 Documentación de procedimientos de continuidad

Todos los responsables de las actividades críticas incluidas en la estrategia de continuidad participan en el desarrollo de procedimientos e instrucciones claras e inequívocas para que permitan la gestión del evento, que activó el plan de continuidad y dar continuidad a las actividades priorizadas, dando cumplimiento los objetivos de recuperación que se hayan definido en durante el análisis de impacto, la gestión de riesgo y la identificación de escenarios. Los diferentes documentos que conformaran los procedimientos de continuidad incluyen, entre otros los siguiente:

- Manual de Crisis, siendo este el protocolo de comunicaciones durante la continuidad (quien reportara a quién y por qué medios).
- Documento anexo Plan de Contingencia y Continuidad del Negocio "Estrategia institucional de gestión de contingencia y continuidad", donde se presentarán los pasos detallados y específicos, referenciando:
 - Pasos detallados y específicos para activar la estrategia seleccionada para operar los servicios en contingencia.
 - Pasos detallados que aplicaran los responsables de realizar la recuperación de los recursos afectados por el o los eventos que generaron la activación del plan de continuidad.
 - Pasos detallados que se deben aplicar para reactivar los servicios en la infraestructura una vez se ha superado el evento que genero la pérdida de continuidad.
 - Responsables de las diferentes actividades aplicar antes durante y después de la contingencia que activo la estrategia de continuidad.

8.8 Pruebas y revisión periódica del plan

En las sesiones de Comité Institucional de Gestión y Desempeño del DADEP se aprueba y monitoriza el Plan de Contingencia y Continuidad del Negocio; las acciones preventivas se llevarán a cabo en toda la Entidad según la planificación de por los procesos de Gestión del Talento Humano (relacionadas con las personas), de Gestión de Recursos (relacionadas con la infraestructura y con la gestión de escenarios de crisis financiera) y de Gestión Documental (relacionadas con la información), las cuales estarán coordinadas por la Subdirección de Gestión Corporativa y con el proceso de Gestión de la Tecnología y la Información liderado por la Oficina de tecnologías de la información y las comunicaciones (lo relacionado con la infraestructura tecnológica y la seguridad de la información); durante la definición de la planificación institucional se definen y autorizan las prueba y los simulacros, del plan de

contingencia y continuidad, según los recursos económicos con los que se cuente en cada vigencia, los cuales se harán de manera planificada y concertada con el Comité de Crisis; de igual manera los resultados y el seguimiento se realizará en el Comité Institucional de Gestión y Desempeño.

8.9 Gestionar el plan de continuidad

Una vez construido y aprobado el plan de contingencia y continuidad del negocio, la Entidad emprenderá las acciones necesarias para socializarlo a los grupos de valor; de esta manera se buscará someterlo a una evaluación externa, su mejoramiento y apropiación; preparando a la entidad para enfrentar situaciones de emergencia y restablecer en el menor tiempo posible el servicio.

8.9.1 Escenarios de continuidad de negocio

Con el fin de adoptar un enfoque ordenado y metodológico para el manejo de los incidentes que puede afectar la continuidad de negocio, la entidad ha definido 6 escenarios que permiten agrupar los riesgos institucionales que por su naturaleza pueden conducir la pérdida de continuidad de las funciones esenciales.

8.9.1.1 Emergencia social

Imposibilidad de uso de las instalaciones debido a revueltas civiles o sociales, asonadas, pérdida del orden público o retención arbitraria de personal (secuestro) que hace imposible la prestación del servicio o generación del producto.

8.9.1.2 Desastre natural y colapso de infraestructura física

Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor.

8.9.1.3 Desastre tecnológico

Pérdida total o parcial de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos a causa de factores tecnológicos y de otro tipo.

8.9.1.4 Crisis financiera

Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos

8.9.1.5 Crisis Sanitarias

Presencia de una crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye brote epidémico, epidemia, pandemias o endemia declaradas por los organismos de salud del Estado.

8.9.1.6. Indisponibilidad del talento humano

Ausencia del perfil requerido o con los conocimientos adecuados para el desarrollo o funcionamiento de los procesos institucionales.

8.9.2 Estrategia institucional de gestión de contingencia y continuidad

Con el fin de afrontar los escenarios definidos por el DADEP dentro de su Plan de Contingencia y Continuidad del Negocio, se adoptan las siguientes estrategias para cada escenario, **ver Plan de Contingencia y Continuidad del Negocio "Estrategia institucional de gestión de contingencia y continuidad"**.

Proyectó: Luis Fernando Arango – Profesional Oficina Asesora de Planeación y Alexander Oliveros Paredes – Contratista de la Oficina Asesora de Planeación.

Aprobó: Lina María Hernández Acosta– Jefe Oficina Asesora de Planeación.

Código de archivo: 120

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
1	27/12/2022	Creación del documento.

INSTRUCCIONES
PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO
"Estrategia institucional de gestión de contingencia y continuidad"

ITEMS	INSTRUCCIONES
Identificación del Escenario de Pérdida de Continuidad del Negocio	
Proceso	Escribir el proceso al que se pertenece.
Riesgo de pérdida de continuidad del negocio	Escribir el riesgo de pérdida de continuidad del negocio identificado, este sea por análisis de contexto, por mapa de riesgos u otra metodología. Ejemplo: Daño o pérdida de la información, Daños ocasionados a los equipos de cómputo, etc.
Escenario	Escribir el escenario concluido al que pertenece el riesgo de pérdida de continuidad del negocio identificado. Ejemplo: Desastre Tecnológico, Colapso de Infraestructura Física, Emergencia Social, Crisis Financiera y Endemia o Pandemia.
Descripción del escenario	Describir el escenario concluido para la pérdida de continuidad del negocio identificado. Ejemplo: Pérdida total o parcial de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos a causa de factores tecnológicos y de otro tipo.
Causa de la pérdida de continuidad	Escribir la causa(s) de la pérdida de continuidad del negocio identificado. Ejemplo: * Afectación de tipo lógico o físico de las bases de datos. * Ataques cibernéticos.
Consecuencia de la pérdida de continuidad	Escribir la consecuencia(s) de la pérdida de continuidad del negocio identificado. Ejemplo: * Inoperatividad de los sistemas de información por daño o pérdida total o parcial de a información.
Líder de respuesta	Escribir el cargo y dependencia del líder responsable de efectuar respuesta al escenario de la pérdida de continuidad del negocio identificado. Ejemplo: * Jefe de la Oficina de tecnologías de la información y las comunicaciones o Líder de Seguridad de la Información - Contratista / Oficina de tecnologías de la información y las comunicaciones.
Equipo de respuesta	Escribir el equipo de responsable de dar respuesta al escenario de la pérdida de continuidad del negocio identificado. Ejemplo: * Líder de Seguridad de la Información - Contratista Oficina de tecnologías de la información y las comunicaciones
Fase 1: Detección	
Identificación de alertas	Escribir las alertas o controles que pueden identificar o detectar la ocurrencia del escenario de pérdida de continuidad del negocio. Ejemplo: Para un escenario Emergencia Social: El área de Comunicaciones a través de la revisión de mensajes en redes sociales identifica mensajes de alerta asociados a convocatorias de manifestaciones y reuniones con el propósito de realizar protestas en la zona de trabajo de la Entidad.
Confirmación	Escribir la(s) actividad(es) de confirmación de la ocurrencia del escenario de pérdida de continuidad del negocio. Ejemplo: La Dirección o Subdirección a través de los canales oficiales de comunicación con Secretaría de Gobierno Distrital o la Alcaldías locales (contacto telefónico, correo o electrónico, sitio web) confirman la situación de alerta por desórdenes y mediante mensaje instantáneo vía WhatsApp en el Equipo de Gestión de Emergencias (Director (a) Subdirector (a), Jefe de OTIC o Jefe de la OAP), (notifican al jefe del grupo de gestión de talento humano que se debe activar el manejo de emergencias por crisis social.
Fase 2: Activación	
Activación	Escribir la(s) actividad(es) a realizar para activar el plan de continuidad según el escenario. Ejemplo: Cuando el Líder del Grupo de Gestión de Talento Humano recibe la confirmación sobre ocurrencia de crisis por emergencia social, recopila la información de confirmación de la crisis y en llamada grupal con los miembros del Equipo de Gestión de Emergencia (Director, Subdirectora, Jefe de OTIC y Jefe de OAP) expone la situación y somete a consideración la necesidad de iniciar la activación del plan de continuidad por la ocurrencia del escenario 1 (emergencia social).
Fase 3: Plan de operación alternativo	
Plan de operación alternativo	Escribir el plan operativo alternativo (actividades a desarrollar) para garantizar la continuidad del negocio para el escenario activado. Ejemplo (El Líder de Talento Humano comunica al Jefe de SGC vía telefónica o mediante mensaje instantáneo, que se deben cerrar las instalaciones y publicar mensaje en portera sobre suspensión de actividades por el día.
Fase 4: Resolución del incidente	
Resolución del incidente	Escribir la resolución del incidente que aplica a escenario presentado, buscando reactivar las actividades del servicio. Ejemplo: El Equipo de Gestión de Emergencias (Director (a) Subdirector (a), Jefe de la OTIC , o Jefe de la OAP) a través de canales oficiales de comunicación (Secretaría de Gobierno, Alcaldía) reciben confirmación de las autoridades de la finalización de la situación que obliga a la evacuación de las instalaciones y la posibilidad de retorno.

