CONTENIDO

1. OBJETIVO

Determinar y coordinar las actividades y acciones a seguir en caso de una falla o evento disruptivo en los sistemas o plataformas tecnológicas que componen el Centro de Comando, Control, Comunicaciones y Cómputo -C4, a través de una descripción detallada de tareas que se deban ejecutar, con el fin de garantizar una respuesta rápida y eficiente para minimizar el impacto en la seguridad y convivencia ciudadana y asegurar la continuidad y monitoreo de los sistemas.

2. ALCANCE

Este Plan de Continuidad del Negocio está organizado para que en el momento en el que se presente un evento disruptivo o falla tecnológica en los sistemas que componen el Centro de Comando, Control, Comunicaciones y Cómputo -C4, se procedan con las actividades de identificación, gestión y restablecimiento normal del servicio.

El plan aborda los siguientes escenarios disruptivos con mayor probabilidad de ocurrencia:

- Falla en el Sistema NUSE 123
- Falla en el Sistema de Videovigilancia
- Falla en el Sistema de Radio
- Falla en la Red Eléctrica

3. ÁMBITO DE APLICACIÓN

El presente documento es aplicable en el proceso de Gestión de Emergencia y Gestión de Tecnológica de Seguridad y Emergencias del Centro de Comando, Control, Comunicaciones y Cómputo – C4 de Bogotá, D.C.

4. NORMATIVIDAD ASOCIADA

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

5. DOCUMENTOS ASOCIADOS

✓ Política de Seguridad y Privacidad de la Información PO-GT-1

- ✓ Manual de Seguridad y Privacidad de la Información MA-GT-1
- ✓ Plan de Contingencia Sistema NUSE 123 PL-GE-08
- ✓ Plan de Contingencia Sistema de Videovigilancia PL-GTS-01
- ✓ Plan de Contingencia Sistema de Radio PL-GTS-02
- ✓ Acta de reunión F-FI-1380

6. GLOSARIO

Análisis de impacto al negocio (BIA): proceso de análisis de las funciones del negocio y del efecto que una interrupción del negocio podría tener en ellas.

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

CAD Policía: Centro Automático de Despacho - (Policía Metropolitana de Bogotá).

CAD: Computer Aided Dispatch (CAD-por sus siglas en inglés): sistema de despacho asistido por computador. 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.

Continuidad del negocio: es un proceso holístico y sistemático, por medio del cual se identifican impactos potenciales que puedan amenazar la continuidad del negocio y provee un marco de referencia para establecer y desarrollar estrategias proactivas, construir respuestas eficaces y eficientes con la flexibilidad y la capacidad necesarias para salvaguardar los intereses de las diferentes partes interesadas, involucradas y afectadas, garantizar la gobernabilidad, la reputación, la imagen y las actividades de creación de valor.

DSS – Decision Support System (Sistema de Apoyo a la Decisión): Sistema tecnológico que analiza información crítica, integra datos operativos y genera reportes, indicadores o escenarios para apoyar la toma de decisiones tácticas y estratégicas durante eventos normales o de crisis.

Eventos Disruptivos: se refiere a eventos, tecnologías o innovaciones que causan una interrupción significativa en una organización

Estrategia de continuidad del negocio: enfoque adoptado para asegurar su recuperación y continuidad ante un desastre u otro incidente mayor o interrupción del negocio.

ESS – Emergency Support System (Sistema de Soporte de Emergencias): Plataforma o conjunto de sistemas que apoyan la atención de emergencias (comunicaciones, registro de

incidentes, coordinación interinstitucional, monitoreo, información operativa), facilitando respuesta oportuna y coordinada.
Grupos de Interés: individuos u organismos específicos que tienen un interés especial en la gestión y los resultados de las organizaciones públicas. Comprende, entre otros, instancias o espacios de participación ciudadana formales o informales. (Adaptado del documento "Guía metodológica para la caracterización de ciudadanos, usuarios o grupos de interés, del DNP, 2014).

Infraestructura crítica cibernética: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

KGS – Knowledge Governance System (Sistema de Gestión del Conocimiento): Conjunto de políticas, herramientas y prácticas para capturar, organizar, almacenar y asegurar el conocimiento institucional, de modo que esté disponible para la operación, toma de decisiones y continuidad del servicio.

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.

Planes de continuidad del negocio (BCP): conjunto documentado de procedimientos e información que se desarrolla, compila y mantiene disponible para usar en un incidente a fin de permitir al C4 continuar ejerciendo sus actividades críticas a un nivel predefinido aceptable.

SDSCJ: Secretaría Distrital de Seguridad, Convivencia y Justicia.

7. DESCRIPCIÓN DEL C4 Y SU CONTEXTO

El Centro de Comando, Control, Comunicaciones y Cómputo - C4 de Bogotá es el corazón de la seguridad y de la atención de emergencias en la ciudad; ofrece los servicios para atender incidentes de convivencia, seguridad ciudadana, ambientales y sanitarios. Para ello, se concibe como un sistema que articula las herramientas tecnológicas, operacionales y humanas dispuestas por el Distrito Capital con el propósito de dar una respuesta coordinada, eficiente y oportuna a los eventos de seguridad y emergencia que ocurren en la ciudad. A la vez genera información centralizada y confiable para la toma de decisiones, como también aporta el conocimiento para la prevención y anticipación en esos eventos.

El C4 tiene la búsqueda del logro de cuatro objetivos principalmente que se pueden resumir de la siguiente manera:

- ✓ Integrar las entidades de seguridad y emergencias, que hacen parte del C4 y aquellas entidades públicas o privadas relacionadas que se puedan incorporar para dar respuesta oportuna y efectiva a los incidentes reportados de seguridad y emergencias. También busca actuar en la prevención de consecuencias mayores y aportar a la mitigación de emergencias, del delito y reducir su impacto sobre la comunidad.

- ✓ Actuar articuladamente para dar respuesta eficiente a los eventos de emergencias y seguridad, implementando procedimientos, protocolos y modelos de operación e interacción, diseñados por la Secretaría Distrital de Seguridad, Convivencia y Justicia, y que sean aprobados por el Comité Operativo de Apoyo y Seguimiento del C4.

- ✓ Recolectar, centralizar, procesar, compartir y analizar la información proveniente de la operación, de los diferentes sensores (GPS, AVL, radios, recursos, dispositivos IoT, etc.) y de los sistemas relacionados con urgencias, emergencias y seguridad para la toma eficiente de decisiones, la asignación asertiva de recursos, la unificación de esfuerzos y la contribución al diseño de estrategias en materia de seguridad y emergencias.

- ✓ Integrar tecnologías; sistemas de comunicación, de información, de analítica y de videovigilancia; equipos de apoyo aéreo tripulado y no tripulado, como los que a futuro hagan más eficiente la operación para disminuir los tiempos de atención, generar alertas y analizar datos.

Así mismo, el Decreto Distrital 510 de 2019 *"Por el cual se reglamenta el Sistema Centro de Comando, Control, Comunicaciones y Computo - C4 y se dictan otras disposiciones",* que en su artículo 1, establece que: “El servicio que presta el Centro de Comando, Control, Comunicaciones y Computo, dirigido a la ciudadanía está enmarcado a garantizar, una respuesta rápida y eficiente para la prevención y atención de los eventos de emergencias y seguridad del Distrito capital, por ende tiene un carácter ***ininterrumpido, continuo y permanente***”.

De la misma forma, el servicio del Centro de Comando, Control, Comunicaciones y Cómputo, dada su funcionalidad se desarrolla dentro del esquema de misión e infraestructura crítica que requieren niveles de disponibilidad, protección física, sísmica y tecnológica.

7.1. Conformación del Sistema C4

El Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 está conformado por los siguientes componentes:

- ✓ Número Único de Seguridad y Emergencias (NUSE 123).

- ✓ Sistema de videovigilancia ciudadana del Distrito Capital.
- ✓ Sistemas de comunicación.
- ✓ Redes de participación cívica.
- ✓ Equipos de apoyo aéreo tripulado y no tripulado.
- ✓ Sistemas de información y análisis de información.
- ✓ El Centro de Operaciones de Emergencias COE.

7.1.1. Número Único de Seguridad y Emergencias (NUSE 123)

Número único liderado por la Secretaría Distrital de Seguridad, Convivencia y Justicia para la atención de requerimientos de la ciudadanía o de entidades nacionales o distritales en cuanto a eventos de seguridad, convivencia ciudadana, urgencias, emergencias y desastres de cualquier tipo, y de despachar las unidades de los organismos de emergencia y seguridad en forma coordinada, para dar una respuesta eficiente y rápida para cada uno de los escenarios de emergencias y seguridad.

El NUSE 123 se encuentra soportado por herramientas tecnológicas, integradas y articuladas con las diferentes entidades que hacen parte del Sistema para realizar los procedimientos de recepción de incidentes de seguridad, convivencia ciudadana, urgencias, emergencias y desastres de cualquier tipo, reportados por los ciudadanos, realizando el trámite correspondiente, documentando y despachando los recursos de las instituciones u organismos de seguridad y emergencia, en forma coordinada para lograr una respuesta oportuna y eficiente a cada uno de los escenarios de seguridad y emergencia.

El NUSE 123 está integrado de la siguiente forma:

- ✓ Secretaría Distrital de Seguridad, Convivencia y Justicia.
- ✓ Policía Metropolitana de Bogotá - Centro Automático de Despacho - CAD.
- ✓ IDIGER - Central de Información y Telecomunicaciones - CITEL.
- ✓ UAECOB - Centro de Coordinación y Comunicaciones de Bomberos Bogotá.
- ✓ Secretaría Distrital de Salud - Centro Regulador de Urgencias y Emergencias - CRUE.
- ✓ Secretaría Distrital de Movilidad - Centro de Gestión de Tránsito - CGT.
- ✓ Secretaría Distrital de la Mujer - Línea Purpura Distrital - LPD.

7.1.2. Sistema de Video vigilancia Ciudadana del Distrito Capital

Es el conjunto de infraestructura física y tecnológica, los protocolos y el personal necesario para capturar, transportar, almacenar, monitorear y analizar la información proveniente de las cámaras instaladas por el Distrito en toda la ciudad y aquellas de otras entidades públicas o privadas que,

por su potencial aporte al sistema, conforme los lineamientos aprobados por el Comité Operativo de Apoyo y Seguimiento del C4.

El Sistema de Videovigilancia está conformado por:

Centros de Monitoreo: Son el conjunto de infraestructura y personal necesario para la visualización de las cámaras en tiempo real. El centro de monitoreo principal se encuentra ubicado en la Oficina Centro de Comando, Control, Comunicaciones y Cómputo - C4 de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Adicionalmente, el Distrito Capital dispone de los siguientes centros de monitoreo: Comandos Operativos de Seguridad Ciudadana COSEC, Estaciones de Policía, Comando Central de la Policía Nacional y Comando Central MEBOG.

Centros de Datos: Es la infraestructura tecnológica para la operación del sistema de videovigilancia y ubicados en los Centros de Monitoreo y en el Data Center (Centro de Datos) de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá, UAECOB.

Puntos de Videovigilancia: Son aquellos ubicados a lo largo y ancho del Distrito Capital de acuerdo con los índices de criminalidad. Cada punto de videovigilancia se compone de: Cámara PTZ, brazo, gabinete, transformador de aislamiento, UPS, tomas eléctricas, equipos de comunicación (router, demarcador y switch), corona anti escalatoria, poste, caja de inspección, sistema puesto a tierra - SPT.

Servicios de Terceros: Son los servicios para ubicar las cámaras de videovigilancia, orientados al uso de la infraestructura del servicio de energía y comunicaciones para la conexión, suministro de energía y telecomunicaciones y demás relacionados para el funcionamiento de las cámaras.

Analítica Video y Analítica Forense: La analítica de video y la analítica forense hacen referencia a las aplicaciones de software y la infraestructura tecnológica que las soporta, permiten generar descripciones (metadatos) de lo que ocurre en el video en tiempo real o sobre la información almacenada respectivamente, la cual se pueden utilizar para identificar situaciones como abandono de paquetes, traspaso de líneas, conteo y generación de aglomeraciones entre otros, generando las alertas correspondientes.

Conformación del Sistema de Videovigilancia: está conformado por el Sistema de la Oficina Centro de Comando, Control, Comunicaciones y Cómputo - C4 de la Secretaría Distrital de Seguridad, Convivencia y Justicia; los sistemas de videovigilancia de Movilidad, Transmilenio, la Corporación Autónoma Regional - CAR, el del apoyo aéreo tripulado y no tripulado y el de los Colegios Distritales.

7.1.3. Sistemas de Comunicaciones

Están constituidos desde el ámbito de las telecomunicaciones por las entidades que conforman y cooperan con el C4, los protocolos, las normas, los recursos tecnológicos y demás relacionados; orientados a garantizar la prestación continua, segura y oportuna de los servicios de comunicación para hacer más eficiente la respuesta y la gestión de seguridad y emergencias en Bogotá, D. C.

Uno de los componentes que hace parte del Sistema de Comunicación, es el de Radio Troncalizado que es un tipo de radio de dos vías (Radio Móvil Terrestre), implementado especialmente para el uso por parte de las entidades de seguridad y emergencia cumpliendo con los parámetros de disponibilidad y funcionalidad especializadas para misión crítica e integración con el NUSE 123, el cual además es interoperable y compatible para todas las entidades que integran el NUSE 123, con el fin de tener unidad en las comunicaciones para la atención de los casos.

7.1.4. Redes de Participación Cívica

El Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 aportará al fortalecimiento y la eficiencia de la operación de las Redes de Participación Cívica a través de su integración con las Estaciones del Sistema de Información de Recepción y Despacho del NUSE - 123 y su inclusión al Sistema de Radio Troncalizado.

7.1.5. Equipos de Apoyo Aéreo Tripulado y no Tripulado

Los equipos de apoyo aéreo tripulados son aquellos equipos aéreos que prestan servicios a la ciudad con personal para atender requerimientos de la ciudadanía o de entidades nacionales o distritales en cuanto a eventos de seguridad, convivencia ciudadana, emergencias o desastres de cualquier tipo con el fin de brindar una respuesta eficiente y rápida para cada uno de los escenarios de emergencias y seguridad.

Los equipos de apoyo aéreo no tripulado, tales como aeronaves y drones, son aeronaves que vuelan sin tripulación, capaces de mantener de manera autónoma un nivel de vuelo controlado y sostenido, propulsado por un motor de explosión, eléctrico o de reacción; los cuales funcionan y son operados de acuerdo con los reglamentos dispuestos por la Unidad Administrativa Especial Aeronáutica Civil para la atención de emergencias o eventos de seguridad en el distrito capital.

Estos equipos se integran al C4 por medio del Sistema de Videovigilancia o de Comunicaciones los cuales se pueden activar en casos de búsqueda, rescate, traslado de equipos, evacuación, acompañamiento, prevención, vigilancia y seguridad ciudadana, entre otros, con el fin de apoyar y brindar una respuesta eficiente en las actividades que tengan un elevado riesgo, tales como pérdida de vidas humanas, ambientes operacionales hostiles, por desastres naturales, catástrofes o lugares de difícil acceso.

7.1.6. Sistemas y Análisis de Información

Es la información centralizada y confiable para la toma de decisiones y la mejora en los tiempos de respuesta en los servicios de seguridad y emergencias en el Distrito Capital para el cumplimiento de los objetivos y la operación eficiente del sistema Centro de Comando, Control, Comunicaciones y Computo - C4, así como el Sistema de Análisis de información que aporta conocimiento para la prevención y anticipación de dichos eventos.

Se podrán integrar otros sistemas de información, plataformas, módulos, aplicaciones de software, fuentes de información o herramientas de captura de información que aporten a potenciar capacidades del sistema Centro de Comando, Control, Comunicaciones y Computo - C4 o del Sistema de Información de Recepción y Despacho para la gestión en seguridad, urgencias y emergencias.

7.1.7. El Centro de Operaciones de Emergencias COE

Está contemplado en el Sistema Nacional para Emergencias y Desastres, responsable de promover, planear, y mantener la coordinación y operación conjunta, entre diferentes niveles, jurisdicciones y funciones de instituciones involucradas en la respuesta y/o atención de eventos.

El Centro de Comando, Control, Computo y Comunicaciones- C4 de la SDSCJ, es el centro de operaciones del Puesto de Mando Unificado- PMU Distrital y el Centro de Operaciones de Emergencia - COE Distrital, los cuales existen en el marco de la Ley 1253 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”, así como el Marco de Actuación del Instituto Distrital para la Gestión del Riesgo y Cambio Climático - IDIGER.

7.2. Infraestructura Crítica Cibernética

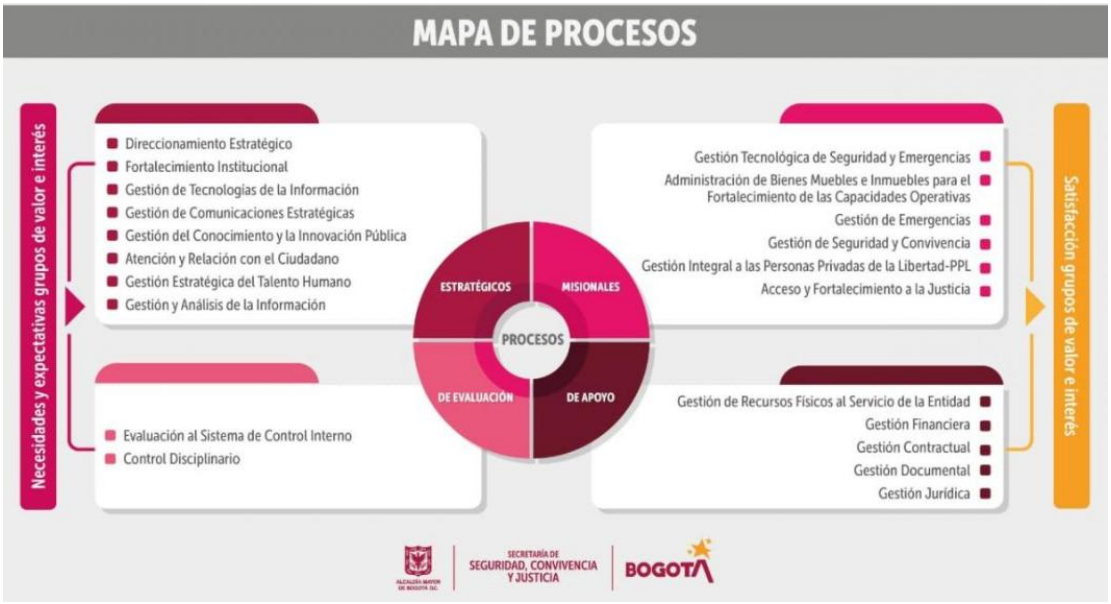
Todos los servicios que ofrece el C4 en su contexto, son catalogados como infraestructura crítica cibernética, teniendo en cuenta el impacto social que tienen sobre la comunidad en general,

cumpliendo uno de los criterios definidos en los Lineamientos de Gestión de Riesgos de Seguridad digital de MinTIC como Entidad pública del orden Distrital que establece lo siguiente: "Una vez se ejecute la identificación de los activos, la entidad pública debe definir si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentado y aprobado por la Línea Estratégica – Alta dirección"

SERVICIO DE TECNOLOGÍA	DESCRIPCIÓN DE USO	IMPACTO SOCIAL	IMPACTO ECONÓMICO	IMPACTO AMBIENTAL
Sistema de Telefonía (Recepción de llamadas)	Servicio para la recepción de llamadas de emergencia y seguridad.	Alto	N.A	N.A
Sistema CAD (Gestión de llamadas)	Servicio para la gestión de llamadas de emergencia y seguridad.	Alto	N.A	N.A
Sistema de Videovigilancia.	Servicio para la vigilancia pasiva de la ciudad de Bogotá.	Alto	N.A	N.A
Sistema de Comunicaciones (Radio)	Servicio para la comunicación a través de radios de todas las entidades del NUSE.	Alto	N.A	N.A
Sistema de Infraestructura eléctrica, redundante y de alta disponibilidad	Servicio para la garantizar la disponibilidad y continuidad de la red eléctrica ante fallos.	Alto	N.A	N.A

7.3. Identificación de procesos misionales C4 – SDSCJ

A continuación, se presenta en la siguiente imagen, el Mapa de Procesos de la Secretaría Distrital de Seguridad, Convivencia y Justicia.



Cómo se refleja en el mapa de procesos, se tienen identificados los siguientes procesos:

✓ Procesos Estratégicos.
✓ Procesos Misionales.
✓ Procesos de Apoyo.
✓ Procesos de Evaluación.

El C4, para el cumplimiento de su función y por ser de vital importancia se encuentra identificada con los procesos misionales, a través de los siguientes procesos.

✓ Gestión de Emergencia
✓ Gestión Tecnológica de Seguridad y Emergencia.

7.4. Partes Interesadas o grupos de interés

A continuación, se relacionan los grupos de interés que componen el C4, además de sus necesidades respecto a continuidad del negocio.

Grupo de Interés	Necesidades respecto a Continuidad del Negocio
Servidores Públicos	● Garantizar la integridad del personal durante un evento disruptivo (desastres y crisis), brindando condiciones óptimas de seguridad y salud en el trabajo. ● Comunicar de manera eficiente y oportuna a las familias de los funcionarios del C4 que se vean involucrados en desastres y crisis. ● Procurar la continuidad laboral a través de una respuesta planificada y probada ante eventos que pongan en riesgo la sostenibilidad de la C4.
Comunidad en General	● Garantizar la continuidad de los subsistemas del C4. ● Garantizar la prestación de los servicios del C4. ● Garantizar las herramientas tecnológicas. ● Gestionar los eventos asociados a interrupciones, desastres y crisis de manera adecuada y oportuna, mitigando los impactos asociados a estos en el servicio. ● Comunicar de manera eficiente y oportuna los incidentes y crisis que puedan afectar o interrumpir la operación C4 y las estrategias de continuidad activadas.
Gobierno Nacional	● Garantizar la continuidad de los subsistemas del C4 ● Garantizar la prestación de los servicios del C4. ● Garantizar las herramientas tecnológicas. ● Gestionar los eventos asociados a interrupciones, desastres y crisis de manera adecuada y oportuna, mitigando los impactos asociados a estos en el servicio. ● Comunicar de manera eficiente y oportuna los incidentes y crisis que puedan afectar o interrumpir la operación C4 y las estrategias de continuidad activadas.

8. LINEAMIENTOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

De acuerdo con los documentos “Política de Seguridad y Privacidad de la Información PO-GT-01 y “Manual de Seguridad y Privacidad de la Información MA-GT-1” el Centro de Comando, Control, Comunicaciones y Cómputo, debe *“Definir e implementar un Plan de Continuidad y Contingencia de Servicios Tecnológicos que propenda por la mitigación de los riesgos sobre la confidencialidad, integridad y disponibilidad de la información.”*

De igual forma, la Seguridad en la Gestión de Continuidad de Negocio, compromete a la Entidad a cubrir las necesidades de continuidad de sus partes interesadas, proporcionando los recursos

necesarios para la implementación y mantenimiento de la estrategia de continuidad, diseñada para responder ante cualquier evento de interrupción que pueda impedir la operación normal del C4, y de esta manera reducir los impactos que puedan poner en riesgo la continuidad en la prestación de los servicios.

Tal como lo establece el documento PL-DE-02 Plan de Continuidad del Negocio de la SDSCJ, este documento complementa las políticas, objetivos, alcance, responsabilidades, análisis de impacto, riesgos y estrategias para asegurar la operación de los servicios críticos ante incidentes como desastres físicos, fallas tecnológicas o ausencia de personal. Define fases antes, durante y después del evento, gobierno de crisis, activación del CAO, DRP y priorización de procesos. Es relevante porque consolida los lineamientos operativos y estratégicos que permiten garantizar la prestación continua de servicios esenciales para la seguridad y atención ciudadana.

9. ANÁLISIS DE IMPACTO DEL NEGOCIO – BIA

Cómo mecanismo de priorización de capacidades para inversión en materia de continuidad técnica u operativa, se aplicó el siguiente enfoque de análisis de impacto al negocio (para entes de gobierno, con énfasis en atención de emergencias, siguiendo lineamientos de ISO 22301):

- ✓ **KGS:** Servicio, actividad o elemento directo que desarrolla el enfoque misional del C4.
- ✓ **ESS:** Servicio, actividad o elemento tecnológico que proporciona soporte o permite que los KGS u otros ESS funcionen o se desempeñen de manera adecuada.
- ✓ **DSS:** Servicio, actividad o elemento que puede ser activado o regenerado luego de atender la situación (incidente disruptivo) sin que afecte la consecución del nivel mínimo operativo.

PILAR	CAPACIDAD	KGS	ESS	DSS	JUSTIFICACIÓN
Pilar 1. Personas y procesos	Personas		X		Se requiere redundancia sobre las personas competentes para la atención de incidentes.
	Procesos			X	La gestión de procesos sucede en condiciones normales, más no de emergencias.
Pilar 2. Comunicaciones	Radio		X		Servicio central que permite mantener los niveles mínimos operativos al suceder incidentes disruptivos.
	Telefonía (y planta telefónica)		X		Servicio que permite mantener los niveles mínimos operativos al suceder incidentes disruptivos.
	Fibra óptica		X		Es un servicio esencial que puede ser reemplazado por mecanismos alternos.
	NUSE 123	X			Es el servicio central del C4.

PILAR	CAPACIDAD	KGS	ESS	DSS	JUSTIFICACIÓN
Pilar 3. Infraestructura IT/OT	Premier 1		X		Servicio central que permite mantener los niveles mínimos operativos al suceder incidentes disruptivos.
	Video vigilancia		X		Es un servicio esencial que no requiere recuperación inmediata.
	Logístico		X		Es un servicio de apoyo que puede ser resuelto por otras agencias o con apoyo de proveedores.
	Data Center		X		Es un servicio esencial que puede ser reemplazado por mecanismos alternos.
	Gestión de la Información			X	La gestión de información es mayor en condiciones normales, no de emergencias, aun cuando debe asegurarse su registro e interoperabilidad.
	Infraestructura interna		X		Es un servicio esencial que puede ser reemplazado por mecanismos alternos.
	Proveedores			X	Se deben evaluar capacidades de proveedores tanto en condiciones normales como de emergencia.

9.1. Resultado del Análisis de Impacto del Negocio - BIA

El Análisis de Impacto en el Negocio (BIA) permitió identificar y evaluar los procesos críticos de la entidad encargada de la recepción y gestión de llamadas de emergencia ciudadana, junto con las amenazas potenciales que podrían afectar su operación. Los resultados de este análisis destacan la importancia de mantener la continuidad de servicios esenciales, tales como la recepción de llamadas, el despacho de emergencias y la coordinación con otras instituciones, dado su impacto directo en la seguridad y bienestar de la comunidad.

Con esta base, la entidad podrá asignar recursos de manera estratégica y priorizar las acciones de mitigación y recuperación para asegurar la resiliencia organizacional y la confianza de la ciudadanía, reflejados en la siguiente gráfica:

PILAR	CAPACIDAD	KGS	ESS	DSS
Pilar 1. Personas y procesos	Personas			X
Pilar 2.	Radio		X	

PILAR	CAPACIDAD	KGS	ESS	DSS
Comunicaciones	Telefonía (y planta telefónica)		X	
	Fibra óptica			X
Pilar 3. Infraestructura IT/OT	NUSE 123	X		
	Premier 1		X	
	Video vigilancia			X
	Data Center			X
	Infraestructura interna (servicios de información)			X

El cuadro anterior, refleja que el Pilar 3. Infraestructura IT/OT, es el que ocasionaría un mayor impacto si llegase a fallar, por lo tanto, es allí en donde se tiene que priorizar las estrategias de continuidad.

10. ESCENARIOS DISRUPTIVOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Los escenarios disruptivos del Plan de Continuidad del Negocio comprenden una variedad de situaciones inesperadas que pueden afectar la continuidad de las operaciones críticas del C4, encargada de la recepción y gestión de llamadas de emergencia. La identificación y anticipación de estos eventos permite a la entidad desarrollar estrategias y respuestas específicas para cada situación, con el objetivo de reducir el impacto en sus servicios esenciales y asegurar una respuesta rápida y eficiente ante cualquier interrupción. A continuación, se enuncia los escenarios:

1. **Imposibilidad de acceso a las Instalaciones**: Hace referencia a la indisponibilidad de las instalaciones principales de C4 por causa de eventos disruptivo como: bloqueos, inundaciones, atentados terroristas entre otros; donde el acceso a la infraestructura puede verse comprometido por un largo periodo de tiempo.

2. **Imposibilidad de uso de la tecnología**: Hace referencia a la indisponibilidad de acceso a la infraestructura tecnológica que soportan los procesos misionales del C4 por causa de evento disruptivo como: falla de un servidor, falla en la conectividad, falla en base de datos y/o fallas con el servicio eléctrico de la entidad.

3. **Imposibilidad de acceso a instalaciones y de uso de tecnología:** Hace referencia a la indisponibilidad de las instalaciones principales de C4 y acceso a la infraestructura tecnológica

que soportan los procesos misionales del C4 por causa de eventos disruptivos que pueden verse comprometidos por un largo periodo de tiempo.

4. **Indisponibilidad de personal crítico:** Considera la ausencia parcial o total del personal clave y funcional de cada proceso crítico (sistema y/o subsistema), evitando la ejecución de este, por causa de un evento que afecta el bienestar e integridad de los colaboradores del C4 y/o operadores tecnológicos.

11. DESARROLLO Y ACTIVACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Para el desarrollo y activación del Plan de Continuidad del Negocio del C4, se tienen documentados planes de contingencia por cada subsistema, que son documentos claves que fortalecen y complementan el Plan de Continuidad del Negocio, proporcionando procedimientos detallados para enfrentar eventos disruptivos y problemáticas de los mismos, que podrían afectar la operación de la entidad, además instrucciones específicas para responder ante incidentes particulares, su implementación asegura que el C4 cuente con lineamientos claros y adaptables a diversos escenarios, permitiendo una respuesta organizada y eficiente que minimice el impacto en los procesos críticos, a saber:

11.1. Plan de Contingencia Sistema NUSE 123 - PL-GE-08

ver en https://portalmipg.scj.gov.co

11.2. Plan de Contingencia Sistema de Videovigilancia PL-GTS-01

ver en https://portalmipg.scj.gov.co

11.3. Plan de Contingencia Sistema de Radio PL-GTS-02

ver en https://portalmipg.scj.gov.co

Así mismo, se describe en el siguiente ítem la contingencia del sistema eléctrico el cual es transversal a las operaciones del C4:

11.4. Contingencia del Sistema Eléctrico C4

La continuidad del sistema eléctrico es fundamental y transversal para el funcionamiento de todo el C4, ya que garantiza el suministro de energía necesario para operar las instalaciones y los sistemas críticos, incluyendo los de comunicación y gestión de llamadas de emergencia.

Dado que una interrupción en el suministro eléctrico podría comprometer la capacidad de respuesta en situaciones de emergencia, este componente es esencial en el Plan de Continuidad del Negocio.

11.4.1. Infraestructura de respaldo eléctrico

El C4 ante la caída o fallas en la energía eléctrica, cuenta con infraestructura robusta que le permite continuar con la prestación de los servicios a los ciudadanos a través de planta eléctrica, UPS, aires acondicionados, transformadores, así como cobertura mediante contratos de soporte y mantenimiento.

✓ **Instalaciones Físicas**

El C4, en su edificio de la sede principal tiene ubicados los sistemas de respaldo eléctrico en el sótano y los cuartos técnicos ubicados en los diferentes pisos, los cuales tienen asignación y distribución específica que permite garantizar la continuidad de las operaciones y servicios a la ciudadanía.

1. **Cuarto de alta tensión**

   El cuarto de Alta tensión cuenta con los siguientes componentes:

   A. Celda de protección
   B. Celda de protección
   C. Celda de medida Edificio C4
   D. Celda de medida Edificio Comando (Bomberos)
   E. Celda de protección
   F. Celda de protección
   G. Entrada de otros proveedores de servicio de internet.
   H. Entrada cometida alta tensión (CODENSA)

Cuarto alta tensión

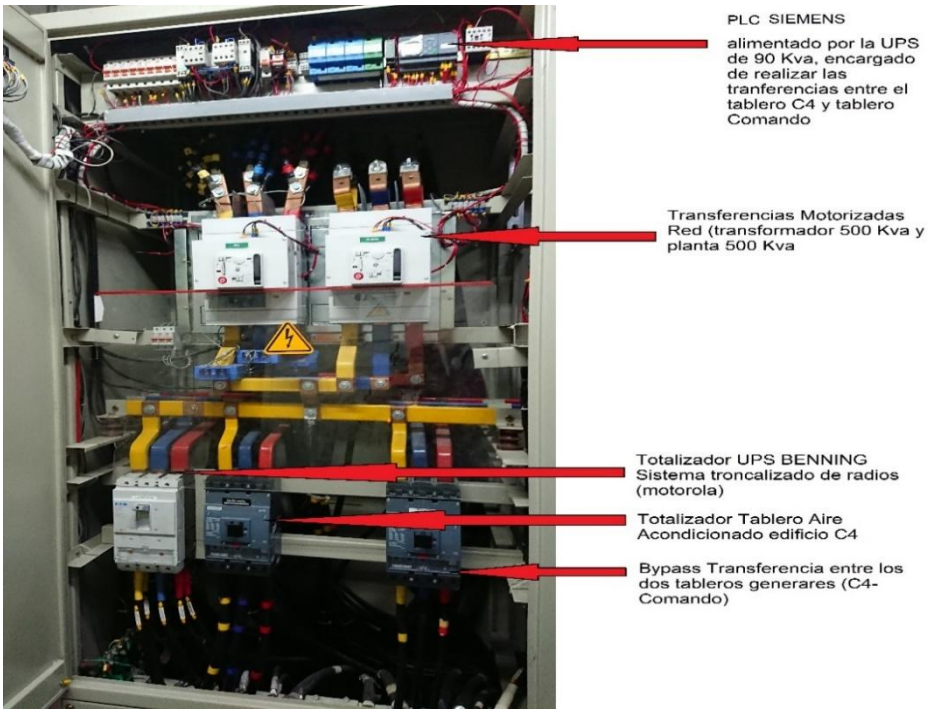
2. **Cuarto de media tensión**

A. Transformador ***500KVA*** que alimenta edificio C4
B. Transformador ***630KVA*** que alimenta edificio Comando (Bomberos)
C. Dámper´s de seguridad

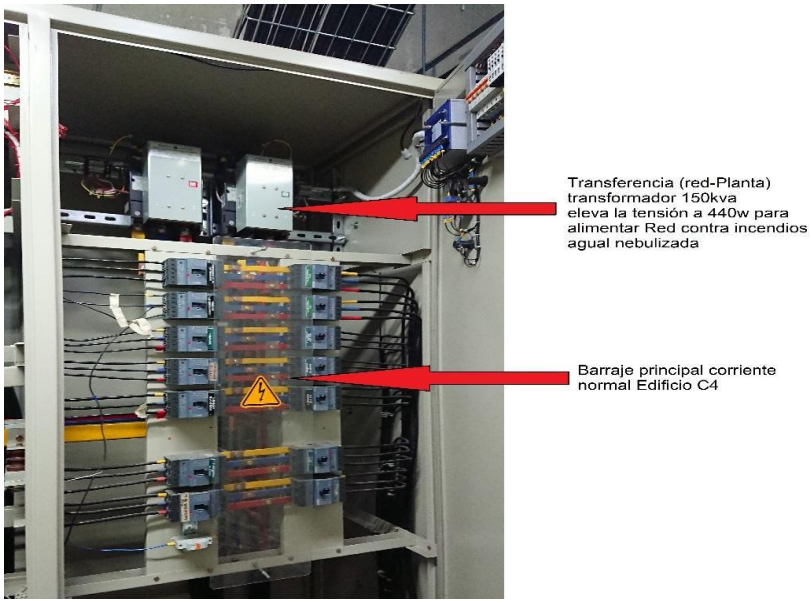
Cuarto de media tensión

3. **Cuarto de baja tensión**

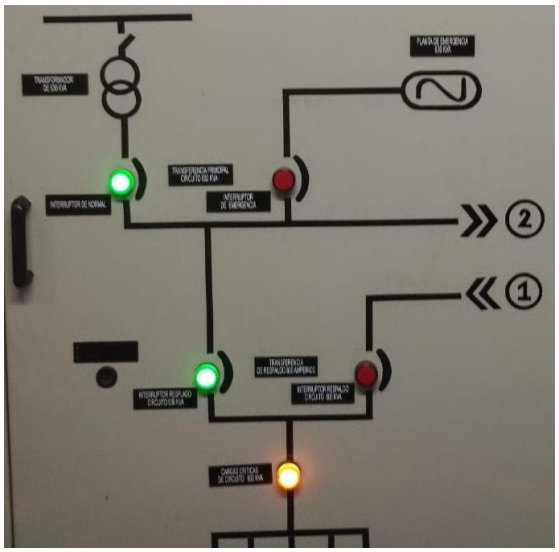
A. Tablero general edificio C4
B. Tablero general edificio comando (Bomberos)
C. Tablero general UPS ***80KVA*** Lievert (corriente regulada edificio C4 Administrativa).
D. Tablero general UPS ***90KVA*** Emerson (edifico Bomberos)
E. Banco de condensadores eléctricos.



I



Tableros Generares (Edificio C4 - UAECOB)



Tablero indicadores

Tablero de control

✓ UPS

El edificio del C4, sede principal, cuenta con un total de seis UPS, con asignación y distribución de la siguiente manera:

- Dos UPS de marca Emerson con capacidad de 90 Kva, cada una funcionando en redundante paralelo (N+1) con dedicación exclusiva y soporte a toda la operación: SUR y CAD, ubicadas en el edificio del C4.
- Una UPS de marca LIEVERT de 80 Kva con dedicación exclusiva a la gestión administrativa del edificio.
- Una UPS de marca Benning de 100 Kva, de soporte al sistema troncalizado de radios comunicaciones, ubicado en el edificio del C4.
- Dos UPS de marca Emerson de 90 Kva, redundante aislado que soporta el datacenter de Bomberos, edificio contiguo al C4.

✓ Planta eléctrica

La planta eléctrica de 500 KVA con que cuenta el edificio del C4, tiene un tanque interior de 284 galones de capacidad de combustible y un tanque externo de 300 galones, los cuales se monitorea periódicamente y de acuerdo con el procedimiento establecido por la coordinación administrativa y Grupo Tecnología C4.

Planta Eléctrica C4

11.4.2. Estrategias Preventivas para el Sistema de Energía

El C4 cuenta con procedimientos preventivos, para cada uno de los elementos del sistema de energía, tal como se describe a continuación:

1. Acciones Preventivas a la Contingencia

✓ **Planta Eléctrica**

Acción	Frecuencia	Responsable
Realizar inspección visual general y al tablero de control	Diaria	Grupo Tecnología C4
Realizar rutina de verificación (Prueba de funcionamiento en vacío) y diligenciar formulario digital	Semanal	Grupo Tecnología C4
Mantenimiento preventivo (Prueba de funcionamiento en vacío) genera registro	Mensual	Contratista externo – Dirección de Bienes
Prueba de funcionamiento con carga, genera registro	Anual	Contratista externo – Dirección de Bienes
Contar con número telefónico para reportar a la supervisión del contrato de mantenimiento	N/A	Líder Grupo Tecnología C4

✓ **UPS**

Acción	Frecuencia	Responsable
Realizar inspección visual general y al tablero de control	Diaria	Grupo Tecnología C4
Mantenimiento preventivo, genera registro	Mensual	Contratista externo – Dirección de Bienes
Realizar cambio de baterías según vida útil y concepto técnico, genera registro	Verificación cada 5 años	Contratista externo – Dirección de Bienes
Contar con número telefónico para reportar a la supervisión del contrato de mantenimiento	N/A	Líder Grupo Tecnología C4

2. Contratos de soporte y mantenimiento

La SDCJ - C4 cuenta con contratos de soportes y mantenimiento para la infraestructura de soporte eléctrico, tendiente a responder oportunamente a cualquier emergencia por ausencia del servicio eléctrico o falla en alguno de sus componentes.

- ✓ Contrato Mantenimiento correctivo y preventivo de aires acondicionados.
- ✓ Contrato Mantenimiento correctivo y preventivo de plantas eléctricas.
- ✓ Contrato Mantenimiento correctivo y preventivo de UPS.

11.4.3. Acciones Durante la Contingencia

Al momento de presentarse la necesidad de activarse el plan de contingencia, el personal encargado y responsable del encendido de los equipos de respaldo eléctrico, deberá permanecer disponible y atento y en constante verificación de pruebas para que una vez se presente la falla, los sistemas de respaldo inicien sin cargas manuales.

Paso	Acción
1	Verificar que la planta eléctrica entre en funcionamiento.
2	Revisar el estado de carga de los bancos de batería de las UPS.
3	Verificar los tableros de control en el cuarto de baja tensión, para identificar el origen de la falla.
3.1	En caso de que el fallo eléctrico sea externo, se procede a reportar a la Dirección de Recursos Físicos para el reporte ante el proveedor eléctrico.
3.2	En caso de que el problema eléctrico sea interno, reportar a la supervisión del contrato de mantenimiento.
4	En el caso que la falla eléctrica se extienda por más de una hora:
4.1	Verificar el nivel de combustible cada hora (tanque auxiliar y principal) de la planta eléctrica.
4.2	Si el nivel de combustible de la planta eléctrica llega al 70%, realizar carga mediante tanque auxiliar, en caso de que no tenga combustible, reportar a la Dirección de Bienes para solicitar abastecimiento.

En caso de que el corte eléctrico se prolongue, la planta eléctrica de 500 kVA del Centro de Comando, Control, Comunicaciones y Cómputo (C4) está preparada para asumir el rol de principal soporte eléctrico de los sistemas críticos de seguridad y atención de emergencias de la ciudad. Esto implica la necesidad de un abastecimiento oportuno de combustible (en menos de 6 horas) desde el momento en que se detecte que el tanque de almacenamiento auxiliar (300 galones) está vacío, con el fin de asegurar la continuidad operativa del edificio sin interrupciones.

Para el proceso de recarga de combustible, es necesario que el vehículo encargado pueda realizar la descarga cumpliendo con las condiciones especificadas en las siguientes imágenes:

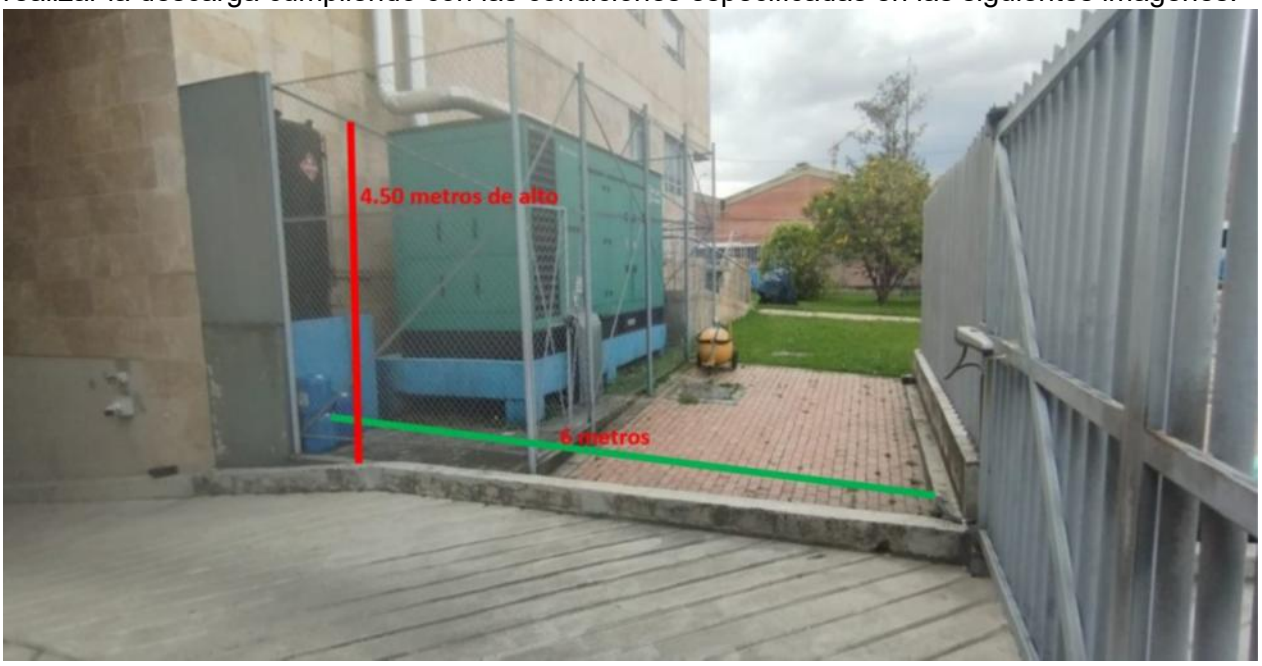


Imagen de referencia para abastecimiento de gasolina

11.4.4. Acciones después la Contingencia

Paso	Acción
1	Verificar nivel de combustible luego del apagado de la planta dejando nuevamente al 100%.
2	Revisar el estado de carga de las UPS.

12. GESTIÓN DE CAMBIOS AL PLAN CONTINUIDAD DEL NEGOCIO

Uno de los principales elementos a gestionar para mantener el Plan de Continuidad y garantizar que esté alineado a la realidad y necesidades del C4 es la Gestión de Cambios que puedan afectar el Plan, las principales fuentes para identificar cambios son:

✓ Creación o eliminación de nuevos servicios

- ✓ Cambios en el organigrama
- ✓ Cambios en los procesos
- ✓ Cambios en la normatividad
- ✓ Reubicación de instalaciones
- ✓ Cambios o novedades en el personal crítico que compone los equipos dentro de la estructura de recuperación
- ✓ Nuevos proveedores para los procesos críticos
- ✓ Nuevas aplicaciones o servicios de TI
- ✓ Nuevos canales de comunicación

En caso de presentarse alguno de estos cambios se deberán seguir los siguientes lineamientos:

- Quien identifica una posible opción de cambio, deberá informarla mediante correo electrónico al responsable de la seguridad de la información del C4 o quien haga sus veces para que de manera conjunta se pueda analizar el impacto del cambio, revisando en detalle si se requiere un diseño o actualización de la estrategia de continuidad y plan de continuidad.

- Aprobación del cambio: El responsable de la seguridad de la información deberá evaluar, junto con el equipo técnico del componente al que afecta el cambio, la procedencia o no de su aplicación, de ser positivo el cambio, proceder a la actualización, en caso negativo descartar el cambio.

13. PRUEBAS

Las pruebas de continuidad son un proceso sistemático y planificado que tiene como objetivo verificar y asegurar que una organización esté preparada para enfrentar y gestionar escenarios de contingencia o interrupciones imprevistas en sus procesos operativos. Estas pruebas buscan evaluar la efectividad de los planes de contingencia diseñados para minimizar el impacto de eventos adversos, garantizando la continuidad del negocio y la rápida recuperación de funciones críticas.

Estas deben ejecutarse durante un tiempo en el que las afectaciones de la operación normal sean mínimas y debe comprender elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral de la Entidad.

Estas como mínimo se realizan con una periodicidad anual, con la coordinación y supervisión de los líderes responsables de los escenarios y las problemáticas planteadas.

Las pruebas tienen la siguiente finalidad:

1. Verificar la totalidad y precisión de las acciones de contingencia
2. Evaluar el desempeño del personal involucrado
3. Evaluar la coordinación entre los responsables de los escenarios, operadores tecnológicos y usuarios funcionales y agencias
4. Medir el desempeño de la plataforma tecnológica del C4
5. Identificar los posibles brechas o falencias que puedan tener el plan de contingencia

13.1. Preparación de las pruebas

Para la preparación de las pruebas se debe contemplar las siguientes actividades:

Actividades	Responsable	Registro
1. Establecer y aprobar la programación de la prueba.	Jefe oficina C4 Apoyo técnico de cada sistema del C4 Responsable de seguridad de la información del C4	Acta de reunión F-FI-1380
2. Informar e involucrar a los participantes en las pruebas.	Apoyo técnico de cada sistema del C4	Correo electrónico
3. Gestionar reuniones con los equipos involucrados en las pruebas (objetivo, alcance, tipo de prueba, resultados esperados y riesgos)	Apoyo técnico de cada sistema del C4	Acta de reunión F-FI-1380 Correo electrónico
4. Definir el cronograma y el tiempo en las que se ejecutarán las pruebas.	Apoyo técnico de cada sistema del C4	Acta de reunión F-FI-1380
5. Garantizar la asistencia de las personas involucradas en la ejecución de la prueba	Apoyo técnico de cada sistema del C4	Acta de reunión F-FI-1380
6. Disponibilidad de las áreas de soporte, operador tecnológico y demás entes involucrados en la ejecución de la prueba.	Apoyo técnico de cada sistema del C4	Acta de reunión F-FI-1380
7. Ejecución de la prueba	Apoyo técnico de cada sistema del C4	Informe de resultados
8. Informe de resultados	Apoyo técnico de cada sistema del C4	Informe de resultados

Nota 1: Para cada uno de los escenarios se desarrollará un protocolo de prueba que permita garantizar la contingencia y verificación de la eficacia de las actividades.

Nota 2: Se aclara que los nombres de los responsables tanto por escenarios como por problemática varían de acuerdo al momento, en este sentido se tiene más en cuenta el rol o la dependencia.

14. SEGUIMIENTO Y MEDICIÓN DEL PLAN

La persona designada de hacer seguimiento al Plan de Continuidad del Negocio debe realizar el monitoreo y seguimiento al plan teniendo en cuenta los siguientes lineamientos:

1. Presentar ante los comités o reuniones estratégicas el Plan de Continuidad del Negocio para su aprobación.

2. Participar en las sesiones del comité interno en donde se revisan los posibles cambios organizacionales y operativos que pueden afectar los Planes para definir acciones al respecto.

3. Mantener y mejorar continuamente las estrategias y soluciones de continuidad y de esta manera lograr reducir los impactos negativos para el C4 y las partes interesadas.

Elaboró: Ana Catherine Mariño Rincón – Contratista C4
Diego Alberto Diaz Mantilla – Profesional Universitario

Revisó: Diego Alberto Diaz Mantilla – Profesional Universitario
Fabio Andrés Albornoz Quintero – Contratista C4
Sandra Milena Martínez Martínez – Contratista C4

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