



Departamento Nacional de Planeación



MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)

Departamento Nacional de Planeación
Bogotá, 2024

TABLA DE CONTENIDO

1 OBJETIVO	4
2 ALCANCE.....	4
3 TÉRMINOS Y DEFINICIONES.....	4
4 MARCO DE REFERENCIA.....	6
4.1 LOCALIZACIÓN	7
4.2 PARTES INTERESADAS PARA EL DNP	7
4.3 MAPA DE PROCESOS E IDENTIFICACIÓN DE PRODUCTOS Y/O SERVICIOS	8
4.4 FACTORES QUE AFECTAN LA CONTINUIDAD DEL NEGOCIO	9
4.4.1 Análisis contexto del DNP	10
4.4.2 Acciones para prevenir eventos externos.....	10
4.4.3 Acciones para atender eventos externos:.....	11
5 REFERENCIAS NORMATIVAS.....	11
6 GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN).....	12
6.1 OBJETIVO GENERAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	13
6.2 POLÍTICA DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	13
6.3 ALCANCE DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.....	13
6.4 LIDERAZGO Y COMPROMISO.....	13
6.5 ACTIVIDADES DEL PLAN DE CONTINUIDAD DEL NEGOCIO.....	13
6.5.1 Planear	14
6.5.2 Hacer	15
6.5.3 Verificar	17
6.5.4 Actuar	17
6.6 ACTIVIDADES DEL PLAN DE CONTINUIDAD DEL NEGOCIO.....	17
6.6.1 Estructura de la Gestión de Continuidad del Negocio	17
7 GESTIÓN DEL RIESGO Y ANÁLISIS DE IMPACTO AL NEGOCIO	28
7.1 GESTIÓN DE RIESGOS	28
7.1 Análisis de Impacto del Negocio -BIA	28
8 PLAN DE RECUPERACIÓN DE NEGOCIO.....	28
8.1. DEFINICIÓN DE LAS ESTRATEGIAS DE RECUPERACIÓN	29

8.2 CICLOS DE OPERACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO	29
8.3 ACCIONES POR ESCENARIOS DE FALLAS	29
8.3.1 Falla en el Centro de Datos Principal (CDP).....	30
8.3.2 Falla en el edificio de operación principal o edificios opera el DNP	30
8.3.4 Ausencia de personal clave.....	31
8.3.5 Otros eventos críticos - Ataque Cibernético.....	32
8.3.6 Fallas de Proveedores Críticos	34
9 ACCIONES DE MANEJO DE CRISIS	34
9.1 Evaluación de impacto de incidentes	34
9.2 Comunicaciones en Crisis.....	36
9.2.1 Comunicaciones Internas	36
9.2.2 Comunicaciones Externas.....	36
10 PLANES DE EMERGENCIAS	38
PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS (DRP).....	38
11 PLAN DE PRUEBAS DE GCN	39
11.1 Tipos de Pruebas.....	39
11.2 Estructura metodológica de pruebas	39
11.2.1 Organización y Preparación	40
11.2.2 Ejecución de Pruebas.....	41
11.2.3 Cierre de la Prueba.....	42
12 CAPACITACIÓN , SENSIBILIZACIÓN Y DIVULGACIÓN	42
13 CAMBIOS RELACIONADOS A LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	44
14 MEJORA CONTINUA	45

1 OBJETIVO

Definir la gobernanza de Continuidad del Negocio mediante el establecimiento de los roles y responsabilidades para llevar a cabo la planeación, ejecución, control, monitoreo y mejora del componente de Gestión de Continuidad del Negocio (GCN), con el fin de estructurar estrategias acordes con las necesidades del Departamento Nacional de Planeación (DNP).

2 ALCANCE

El DNP define y brinda aplicabilidad a la Gestión de Continuidad de Negocio (GCN) a los productos, procesos y servicios que ofrece a las partes interesadas desde la ejecución del plan preventivo, pruebas, medición, y mantenimiento a todos los planes que lo conforman.

3 TÉRMINOS Y DEFINICIONES

Análisis de impacto al negocio (BIA - Business Impact Analysis): proceso de evaluación de los productos y/o servicios y del efecto que una interrupción tendría en ellos. Incluye la identificación de los activos, funciones, procesos y recursos críticos, junto a la evaluación de los posibles daños o pérdidas que afectarían al DNP como resultado de una interrupción o un cambio en el negocio.

Aplicación crítica: sistema computacional que soporta una función crítica de negocio.

Árbol de llamadas: mecanismo que implementa la cadena de llamadas y las responsabilidades de cada funcionario, incluye contactos de colaboradores, proveedores, firmas de outsourcing (sí aplica), organismos de control y demás partes interesados de la o GCN

Administradora de Riesgos Laborales (ARL): es el conjunto de entidades públicas y privadas, normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos de las enfermedades y los accidentes que puedan ocurrirles con ocasión o como consecuencia del trabajo que desarrollan.¹

Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia También se puede entender como la institución que ésta al servicio de la gestión administrativa, la información, la investigación y la cultura.

Atención de la contingencia: actividades encaminadas a afrontar un evento no planeado presentado sobre la plataforma de tecnología informática, sobre las vidas de las personas o la infraestructura física de la entidad, desde que ocurre hasta que se soluciona el problema y se retorna a la operación normal.

Brigada de emergencias: conjunto organizado de personas, entrenado para responder a situaciones de crisis, que ejecutan los procedimientos del Plan de Prevención y Atención de Emergencias.

Canal dedicado: canal de comunicaciones que se establece entre un sitio y otro, con utilización de ancho de banda exclusivo para los usuarios de este, es la comunicación en doble vía que se da entre los dos sitios involucrados.

Centro de datos alterno (CDA): es el lugar de procesamiento alterno y almacenamiento de información que soporta la operación de la entidad en caso de presentarse una contingencia.

Centro de datos principal (CDP): es el lugar de procesamiento y almacenamiento de información que soporta la operación normal de la entidad.

Centro alterno de operación: Centro de continuidad con espacios de trabajo acondicionados como oficina alterna, permitiendo mantener la operación principal del cliente ante eventos fortuitos.

Continuidad del negocio: capacidad de la Entidad para continuar desarrollando y entregando los productos y/o servicios en un nivel aceptable predefinido, luego de un incidente.

¹ Fuente: Ministerio de Salud y Protección Social de Colombia

Copias de seguridad: Una copia de seguridad de datos es un respaldo de los datos del sistema, la configuración o la aplicación que se almacena por separado del original.

Contingencia: suceso que puede suceder o no, especialmente un problema que se plantea de forma imprevista. En tecnología, es un conjunto de procedimientos para atender en forma oportuna, eficiente y eficaz, para dar respuesta activando los mecanismos tecnológicos ante una interrupción en la prestación de los servicios ofrecidos por medio de los diferentes recursos tecnológicos de la entidad

Crisis: suceso o percepción de amenaza a las operaciones, el recurso humano, los accionistas, las partes interesadas, la marca, la reputación, la confianza, a los objetivos estratégicos o de negocio.

Emergencia: 1. Situación inesperada que puede derivar en lesiones o muerte, daño a la propiedad o interrupción de la operación normal del DNP. 2. Suceso imprevisto y repentino que requiere de una acción inmediata.

Equipo de Emergencias: es el equipo conformado por los directivos, que en el momento de una emergencia se reúne para mantener el control de la situación por medio de la toma de decisiones que minimicen el impacto a las personas, los procesos y el capital de la entidad. Es la estructura responsable de coordinar la ejecución de las actividades antes, durante y después de una emergencia o desastre.

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

Evacuación: acciones organizadas y coordinadas por las brigadas de emergencias para apoyar en el traslado de colaboradores de la entidad desde sus oficinas a un lugar de menor riesgo, por una ruta lo más segura posible.

Evento contingente: es un incidente que afecta la continuidad de los procesos críticos del negocio de la entidad, que puede ocurrir durante el normal desarrollo de las actividades del DNP, en horarios laborales o no laborales.

Desastre: es el daño o alteración grave de las condiciones normales de la vida, causado por fenómenos naturales o acción del hombre en forma accidental.

Función crítica de negocio: es una actividad que debe ser restablecida dentro de un tiempo de interrupción mínima, para que los productos y procesos continúen dando servicio a terceros o servicios internos.

Gestión de la continuidad del negocio: la gestión de continuidad de negocio se enmarca en los lineamientos de un proceso holístico y organizado en un esquema de mejora continua alineado con el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) que identifica las amenazas potenciales de una organización, así como los impactos a las operaciones del negocio que puedan causar estas amenazas y que permita generar la capacidad de respuesta efectiva para salvaguardar los intereses.

Infraestructura física: inmuebles, muebles y enseres y demás activos fijos de los que hace uso la entidad ya sea en operación normal, o en operación en contingencia.

Infraestructura tecnológica: equipos de cómputo, servidores, dispositivos de almacenamiento e impresión, equipos activos de red, licencias de programas, y todo componente de hardware y software que permita soportar la función tecnológica y de redes de la entidad, ya sea en operación normal o en operación en contingencia.

Mitigación: acciones desarrolladas antes, durante y después de un evento contingente, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del plan de continuidad del negocio, hasta tanto se efectúe su recuperación.

Personal de administración del edificio: persona o personas encargadas del cuidado de los bienes de uso común, de la administración del edificio y de la preservación de estos bienes, los cuales son: Administrador, Consejo de Administración y Asamblea de Copropietarios.

Personal vital: recurso humano mínimo requerido para continuar operando los procesos críticos del DNP al porcentaje definido durante una contingencia.

Plan de emergencias: son los planes enfocados a atender situaciones que presenten emergencias (atentados, incendios, desastres naturales, entre otros) para la organización, en los cuales se busca la protección de las vidas y de los activos. Usualmente involucra personal de varias dependencias y elementos de seguridad industrial y salud ocupacional, por ejemplo, la brigada de emergencias.

Plan de pruebas: permite especificar lo que se desea probar y cómo ejecutar dichas pruebas. Un plan de pruebas se puede aplicar a una iteración concreta de un proyecto.

Plan de recuperación ante desastres (DRP - Disaster Recovery Plan): documento que contiene un conjunto de procedimientos y acciones definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.

Puntos objetivos de recuperación (RPO - Recovery Point Objective): punto de referencia anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Las dependencias del Departamento Nacional de Planeación DNP deben definir su "*pérdida máxima de información*" permitida para cada proceso de negocio.

Recuperación: actividad final en el proceso de respuesta a una emergencia. Consiste en restablecer la operatividad de un sistema interferido.

Resiliencia: capacidad de una organización para anticipar y adaptarse a riesgos emergentes con estrategias que permitan proteger los intereses de las partes interesadas.

Tiempos de objetivos de recuperación (RTO Recovery Time Objective): periodo inmediatamente posterior a la ocurrencia de un incidente, dentro del cual deben reanudarse o recuperarse: la entrega de productos o servicios, las actividades críticas y los recursos. El RTO debe ser inferior al tiempo en que los impactos financieros y operacionales identificados en el BIA sean considerados inaceptables.

Vulnerabilidad: condiciones en las que se encuentran las personas y los bienes expuestos ante una amenaza. Se relaciona con la insuficiencia para afrontar y controlar con sus propios recursos en una situación de emergencia.


4 MARCO DE REFERENCIA

El DNP como entidad técnica, cabeza del sector planeación y perteneciente a la Rama Ejecutiva del poder público en el orden nacional, identifica y actualiza periódicamente su contexto organizacional como base fundamental para la estructuración y fortalecimiento del Sistema Integrado de Gestión (SIG).

El DNP consciente de la existencia de amenazas que pueden interrumpir el normal desarrollo de su operación, ha decidido tomar como marco referente el adecuar la Gestión de Continuidad del Negocio (GCN) orientada a incorporar los lineamientos de la Norma Internacional de Gestión de Continuidad de Negocio ISO 22301 de 2019 y referencias externas. Asimismo, identificar los riesgos y escenarios que pueden afectar la conducta operacional y los principios, criterios generales y parámetros mínimos que la entidad recomienda proporcionar para que sus colaboradores conozcan, entiendan y asuman roles y responsabilidades dentro del desarrollo de los planes de contingencia y de continuidad del negocio. Los procedimientos y actividades descritos dentro de la GCN son una guía para la respuesta a escenarios de falla o situación de contingencia; el adecuado seguimiento de la Gestión de Continuidad del Negocio y del Análisis de Impacto del Negocio (BIA) soportará la recuperación oportuna de los procesos definidos como críticos para el DNP.

Este documento contiene una secuencia de las actividades a seguir por cada escenario de falla identificado en el BIA, para así reducir el tiempo de la toma de decisiones y restablecer los procesos críticos en contingencia. El desarrollo del plan depende de la disponibilidad, experiencia y conocimiento del personal (funcionarios, contratistas y actores claves) del DNP para apoyar los esfuerzos de recuperación, independientemente de las causas que den origen a la interrupción. La intención de este plan no es recrear de forma idéntica los procesos y operaciones existentes, no está concebido como único y definitivo curso de acción en una contingencia; los miembros de los grupos que en este documento se mencionan, pueden requerir ajustar o cambiar el documento e identificar otras actividades o soluciones, para responder y recuperar las operaciones en situaciones específicas que no estén detalladas en el presente manual.

El DNP, en cabeza de la Secretaría General, es consciente de la necesidad de cumplir la normativa vigente en materia de archivo que se encuentra en el Programa Específico de Documentos Vitales o Esenciales orientado a recuperar de manera oportuna la información institucional ante una emergencia de origen natural, biológico o humano ajeno a su gestión, para ello articulará a la Subdirección Administrativa y Relacionamento con el Ciudadano, el Grupo de Biblioteca y Archivo, la Oficina de Tecnología de la Información, Subdirección de Gestión del Talento Humano, entre otras dependencias de la entidad que llegaran a ser necesarias.

 Departamento Nacional de Planeación	MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)	CÓDIGO: M-PG-14
		Página 7 de 47 VERSIÓN: 1

4.1 LOCALIZACIÓN

Las oficinas principales del DNP se encuentran ubicadas en Bogotá en las instalaciones físicas el Edificio FONADE (pisos 2, 3, 4, 5, 6, 7, 8, 9, 12, 14, 15, 16, 17, 18, 23, 24, 27, 31, 32, 33, 34, 35, 36 y local primer piso), Edificio Gómez (pisos 5, 6 y 7), Edificio Colombiana de Capitalización Seguros Patria (piso 7) y Edificio World Service (pisos 4, 5, 8, 9, 10, 14, 15, 16, 18, 19 y 20). El detalle de las localizaciones se refleja en los planes de emergencias del DNP:

Tabla 1 Localización DNP².

SOPORTE DOCUMENTAL	DESCRIPCIÓN
Plan de Emergencias y Contingencias Edificio FONADE	Los planes detallan en los numerales los aspectos relevantes de: 1) Actividades que desarrolla el DNP, 2) Descripción de la ocupación, 3) Características de las instalaciones y 4) Geo-referenciación Externa.
Plan de Emergencias Edificio World Services	
Plan de Emergencias Edificio Gómez	
Plan de Emergencias Edificio Seguros Patria	

Fuente: Planes de emergencia DNP.


4.2 PARTES INTERESADAS PARA EL DNP

El DNP adopta su mapa de procesos, esquema que integra los productos y procesos desde la orientación del Sistema Integral de Gestión (SIG):

Tabla 2 Partes interesadas para la continuidad del negocio – DNP

PARTES INTERESADAS PARA LA CONTINUIDAD DEL NEGOCIO – DNP	
PARTES INTERESADAS	NECESIDADES ESPECÍFICAS
Presidente de la República	<ol style="list-style-type: none"> 1. Contar con disponibilidad de sistemas de información y aplicaciones en las que exista interoperabilidad, manteniendo el flujo de la información y disponibilidad entre el DNP para consulta y toma de decisiones. 2. Protección de la infraestructura crítica cibernética. 3. Respuesta oportuna en caso de emergencias. 4. Cumplimiento legal y normativo asociado que se derive de la prestación de servicio del DNP. 5. Mantener procesos y procedimientos actualizados 6. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico.
<ul style="list-style-type: none"> • Beneficiarios directos de productos • Entidades del Orden Nacional Nivel Central • Entidades del Orden Nacional Nivel Descentralizado • Entidades del orden territorial 	<ol style="list-style-type: none"> 1. Contar con disponibilidad de sistemas de información y aplicaciones en las que exista interoperabilidad, manteniendo el flujo de la información y disponibilidad entre la DNP para consulta y toma de decisiones. 2. Protección de la infraestructura crítica cibernética. 3. Respuesta oportuna en caso de emergencias. 4. Cumplimiento legal y normativo asociado que se derive de la prestación de servicio del DNP. 5. Mantener procesos y procedimientos actualizados 6. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico.

² <https://www.dnp.gov.co/DNP/gestion/sistema-integrado-gestion/Paginas/Planes-de-Emergencia.aspx>

 Departamento Nacional de Planeación	MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)	CÓDIGO: M-PG-14
		Página 8 de 47 VERSIÓN: 1

PARTES INTERESADAS PARA LA CONTINUIDAD DEL NEGOCIO – DNP	
PARTES INTERESADAS	NECESIDADES ESPECÍFICAS
<ul style="list-style-type: none"> • Órganos de control, Fiscalía y otros • Congreso de la República 	<ol style="list-style-type: none"> 1. Disponibilidad de la información en caso de suceder un evento de interrupción que afecte la continuidad operativa y/o tecnológica del DNP. 2. Cumplimiento legal y normativo asociado que se derive de la prestación de servicio del DNP. 3. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico.
Ciudadanía	<ol style="list-style-type: none"> 1. Disponibilidad de la información en caso de suceder un evento de interrupción que afecte la continuidad operativa y/o tecnológica del DNP. 2. Disponibilidad de los sistemas de información y portales del DNP. 3. Mantener las estrategias de continuidad del negocio activas y actualizadas. 4. Atención oportuna. 5. Apertura de canales alternos como medida contingente para atender las operaciones del DNP sobre los servicios ofrecidos. 6. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico.
Servidores Públicos (funcionarios y contratistas)	<ol style="list-style-type: none"> 1. Disponibilidad de la información en caso de suceder un evento de interrupción que afecte la continuidad operativa y/o tecnológica del DNP. 2. Continuidad de los sistemas de información y portales. 3. Disminución de los efectos colaterales de un posible incidente que ocasione una interrupción en operación y/o plataforma tecnológica del DNP. 4. Cumplimiento de la legislación y normativa aplicable. 5. Protección de la infraestructura crítica cibernética. 6. Mantener procesos y procedimientos actualizados 7. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico.
<ul style="list-style-type: none"> • Aliados- Entidades en convenio • Proveedores de información • Entidades con interacción en emergencias 	<ol style="list-style-type: none"> 1. Disponibilidad de la información en caso de suceder un evento de interrupción que afecte la continuidad operativa y/o tecnológica del DNP. 2. Cumplimiento de Acuerdo de Nivel del Servicio (ANS) y requisitos contractuales establecidos. 3. Recuperación de procesos mediante la ejecución de estrategias de recuperación, bajo el escenario de falla de personal crítico

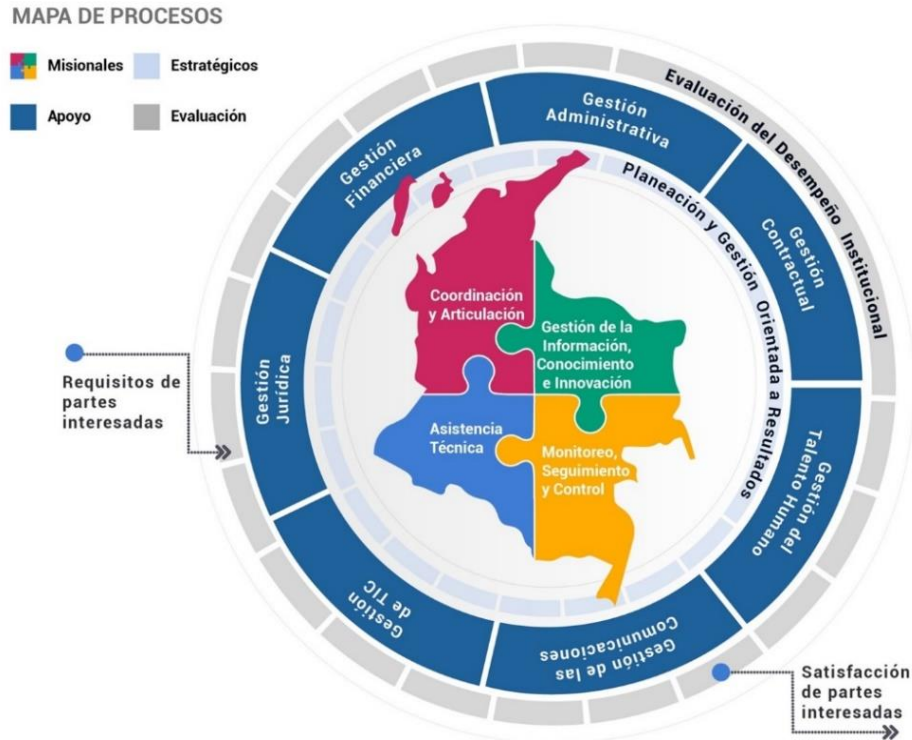
Fuente: Oficina Asesora de Planeación.

Las necesidades específicas de las partes interesadas para la continuidad del negocio del DNP abordadas en el Manual del SIG numeral “*Partes interesadas - grupos de valor*”, en la cual se relacionan las estrategias de atención por parte del DNP a través de expectativas razonables garantizando la disponibilidad de los servicios principales.

4.3 MAPA DE PROCESOS E IDENTIFICACIÓN DE PRODUCTOS Y/O SERVICIOS

El DNP ha identificado sus procesos y procedimientos a partir de la definición de los productos que genera y provee la entidad. Este esquema se refleja en el Manual SIG en el numeral “*Modelo de Operación por Procesos*”. La representación gráfica de los procesos se muestra a continuación:

Ilustración 1 Mapa de Procesos DNP



Fuente: Manual del SIG.

4.4 FACTORES QUE AFECTAN LA CONTINUIDAD DEL NEGOCIO

Con el objeto de identificar los factores que puedan afectar la continuidad de la operación, la GCN del DNP tiene en cuenta el análisis y conocimiento del contexto interno y externo. Para ello se contempla el análisis sobre los factores del entorno del DNP y los riesgos que afectan las operaciones de la entidad. Estos se detallan en el Plan de emergencias y contingencias FONADE numeral “Análisis de vulnerabilidad de elementos”, y Plan de emergencias Gomez numeral “Identificación de amenazas”.


A continuación, se relacionan los principales vulnerabilidades y amenazas riesgos que materializarían un riesgo asociado a la GCN:

Tabla 3 Escenarios que afectan la continuidad del negocio.

ESCENARIOS QUE AFECTAN LA CONTINUIDAD DEL NEGOCIO		
Daño a personas	Efectos en el medio ambiente	Consecuencia económica
Natural	Social	Tecnológicas
Recurso Humano	Antrópica no intencional ³	

Fuente: Propia Oficina Asesora de Planeación.

³ Antrópica no intencional: Es un tipo de amenaza provocada por el ser humano como (Eventos biológicos, incendios, derrames, fugas e inundación por falla en redes hidráulicas)

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 10 de 47 VERSIÓN: 1</p>

4.4.1 Análisis contexto del DNP

La oficina principal del DNP se encuentra ubicada en Bogotá en las instalaciones físicas el Edificio FONADE, la cual alberga una gran cantidad de colaboradores. Esta zona es muy concurrida por peatones, debido a la gran variedad de accesos viales, entidades financieras, estaciones de transporte, entre otros; como característica especial en las horas de la noche la afluencia de personas es mínima. Esto se especifica en el documento del *“Plan de Emergencias y Contingencia FONADE”*. El punto de correspondencia también puede considerarse como punto crítico, dado que están expuestos al riesgo de colocación de artefactos explosivos, generando la posibilidad de toma de instalaciones, restricción de ingreso a las mismas y/o daños a la infraestructura.

Para las demás instalaciones u oficinas del DNP se analizan los posibles escenarios contingentes los cuales se evidencian en los documentos: 1) Plan de Emergencias Gomez en el numeral *“Análisis de amenazas”*, 2) Plan de Emergencias Seguro Patria en el numeral *“Análisis de amenazas”* y 3) Plan de Emergencias Word Service en el numeral *“Determinación de la Vulnerabilidad”*.

Desde la Oficina de Tecnologías y Sistemas de Información se cuenta con un Plan de Recuperación de Desastres (DRP Disaster Recovery Plan) en el cual se contemplan estrategias y acciones para el restablecimiento de los servicios asociados al factor tecnológico estos se detallan el numeral de *“Aplicabilidad Escenarios de Fallas”*, y se requiere robustecer los controles de backup en Azure, AWS y Oracle, para evaluar los costos de activar los componentes del DRP antes de su implementación.

4.4.2 Acciones para prevenir eventos externos

Para determinar en nivel de riesgos a las cuales está expuesta la Entidad, se recomienda considerar en su naturaleza: la posibilidad de exposición, características del sector y/o población expuesta, posibilidad de que ocurra, magnitud y sus consecuencias. Para esta identificación es importante conocer la diferencia entre amenaza, vulnerabilidad y riesgo. Para el análisis de riesgos se contemplan tanto las amenazas naturales y sociales, como aquellas relacionadas con la generación de impactos ambientales en la entidad, detalladas en los planes de emergencias. Las acciones generales para mantener la continuidad del negocio se orientan a:


Gestión de seguridad de la información:

- Identificación avanzada de amenazas a través de detección de patrones y tendencias a través de la correlación de eventos.
- Plan de análisis de vulnerabilidades anual para los sistemas de información, aplicativos y portales.
- Mesas de trabajo para la mitigación de vulnerabilidades.
- Protección de la información física bajo los lineamientos y directrices de la Gestión Documental

Seguridad física de las instalaciones:

Como parte de la seguridad de la información, este incluye medidas para garantizar la protección de las instalaciones del DNP:

- Vigilancia privada.
- Planes de reacción con apoyo de la fuerza pública.
- Evaluación continua de la infraestructura física para identificar posibles riesgos (como incendios, intrusiones o daños en las instalaciones).
- Implementación de tecnologías de monitoreo y alarmas en tiempo real para la detección de intrusiones.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 11 de 47 VERSIÓN: 1</p>

4.3.3 Acciones para atender eventos externos:


- Actividades definidas para el escenario de sitio normal no disponible evidenciadas en el DRP.
- Orientado a los planes de emergencias que contienen un conjunto de acciones destinadas a prevenir y hacer frente a situaciones de crisis o contingencia, respecto a aspectos de carácter legal y/o normativo, de servicio, de operación e imagen.

5 REFERENCIAS NORMATIVAS

A continuación, se visualizan los requisitos legales y normativos que tienen que ver con la continuidad de negocios, los cuales podrán ser tomados como lineamientos o directrices del DNP.

Tabla 4 Documentos de referencia de continuidad del negocio.

DOCUMENTOS REFERENTES DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO		
LINEAMIENTO INFORMATIVO	DESCRIPCIÓN DEL DOCUMENTO	REFERENCIA
Guía para la preparación de las TIC para la continuidad del negocio. Guía No. 10 MINTIC de 2010	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.	Se aplican las disposiciones definidas en la guía No.10 como referente para la continuidad del negocio, por medio de las fases del desarrollo del modelo aplicables al DNP, logrando la implementación de la estrategia de continuidad del negocio.
Norma Técnica Colombiana NTC 5722 de 2012	Norma Técnica Colombiana que especifica los requisitos para la creación y gestión de la Gestión de Continuidad de Negocios efectivo.	Este requisito define los componentes claves aplicables para desarrollar el Plan de Continuidad de Negocio para el DNP.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.	Anexo. Ítem 4: Programa de Gestión Documental (PGD) describe los datos generales de la entidad, incorporando los requisitos del Sistema de Gestión de Calidad de la entidad, para el control de los documentos.
Guía para la realizar el análisis de impacto de negocios. BIA Guía No. 11 MINTIC de 2015	Guía del Ministerio de Tecnologías de la Información y las Comunicaciones establece lineamientos de seguridad ante situaciones de emergencia para mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan las operaciones del negocio.	Se aplican las directrices y procedimientos establecidos en la guía No. 11 BIA, para la definición del Plan de Continuidad de Tecnología de la Información y análisis de impacto del DNP logrando la implementación de la estrategia del negocio.
Ley 594 de 2000, Ley General de Archivos Decreto 106 de 2015.	Por el cual se reglamenta el Título VIII de la Ley 594 de 2000 en materia de inspección, vigilancia y control a los archivos de las entidades del Estado y a los documentos de carácter privado declarados de interés cultural; y se dictan otras disposiciones.	La presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
Norma Internacional de Gestión de Continuidad Negocio ISO 22301 de 2019	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 de Negocio.	Está norma establece los parámetros generales con los cuales se desarrolla el Plan de Continuidad del negocio para el DNP.

 <p>Departamento Nacional de Planeación</p>	MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)	CÓDIGO: M-PG-14 Página 12 de 47 VERSIÓN: 1
--	--	--

DOCUMENTOS REFERENTES DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO		
LINEAMIENTO INFORMATIVO	DESCRIPCIÓN DEL DOCUMENTO	REFERENCIA
Documento Técnico del Plan de Continuidad del Negocio - Función Pública de 2020	Este documento cuenta con herramientas que nos permiten prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo al personal que presta sus servicios para la entidad, los visitantes de la oficina principal, afectar el debido desarrollo de las actividades propias de Función Pública, impedir la prestación y continuidad del servicio a los Grupos de Valor o el cumplimiento de los compromisos establecidos en la planeación estratégica institucional. La Entidad ha consolidado el conjunto de acciones que se emprenden para dar respuesta a estos eventos en el Plan de Continuidad del Negocio.	Este documento define lineamientos de continuidad del negocio tiene en cuenta las obligaciones legales aplicables a la Función Pública.
Circular externa 018 de 2021 Superintendencia Financiera de Colombia	Numeral 4.3.1.3.2. Administración de la continuidad del negocio. De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, la entidad debe definir, implementar, probar y mantener la gestión para la continuidad del negocio, el cual incluya elementos como: prevención y atención de emergencias, administración en escenarios de crisis, planes de contingencia y capacidad de retorno a la operación normal de la entidad.	La circular externa cubre los aspectos de identificación de los riesgos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.
Resolución 500 de 2021 Ministerio de tecnologías de la información y las Comunicaciones	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	Artículo 17 literal 1.1.1: Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información.
Circular externa 022 de 2022 Superintendencia Financiera de Colombia	Por medio de la cual se adoptan en forma permanente algunas instrucciones transitorias emitidas durante la emergencia sanitaria con ocasión de la pandemia del COVID-19	La circular externa cubre aspectos de i) preservar la continuidad del negocio en situaciones de contingencia y ii) garantizar la atención a los consumidores financieros y otros grupos de interés de las entidades vigiladas en tales situaciones.
Norma Internacional de Gestión de Seguridad de la Información ISO 27001 de 2022	Este documento especifica los requisitos para establecer, implementar, mantener y continuamente mejorar una adecuada gestión de seguridad de la información dentro del contexto de la organización. El documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptado a las necesidades de la organización. Contiene controles de aspectos de seguridad de la información en la gestión de continuidad del negocio.	Está norma establece los parámetros generales en gestión de seguridad de la información en la cuales se aplican controles de gestión de continuidad del negocio para el DNP.

Fuente: Propia Oficina Asesora de Continuidad del Negocio.

6 GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)

La administración de la continuidad del negocio es un proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos potenciales a las operaciones del negocio permitiendo construir la capacidad para tener una respuesta efectiva para salvaguardar los intereses de los principales interesados, la reputación y las principales fuentes de generación de valor. Este es un proceso cíclico enmarcado en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), el cual se mantiene activo a través del tiempo y responde a los cambios en la tecnología, los procesos (productos) y las necesidades del DNP.

El DNP desde la Oficina Asesora de Planeación articula la GCN con apoyo de la Oficina de Tecnologías y Sistemas de Información, Subdirección Administrativa y Relacionamento con la Ciudadanía, Oficina Asesora de Comunicaciones, Subdirección de Gestión del Talento Humano y apoya con una gestión transversal la Subdirección Financiera y Subdirección de Contratación, identificaron el equipo que coordinará las estrategias y buscará posicionar una imagen positiva de la entidad hacia sus grupos de valor y fomentar en su cultura organizacional orientado a la Gestión de Continuidad del Negocio (GCN).

6.1 OBJETIVO GENERAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

El objetivo de la GCN es sostener en niveles previamente definidos y aceptados, las operaciones y servicios de Tecnologías de Información apoyados por portales de terceros y reguladores necesarios a los grupos de interés del DNP. Lo anterior, a través de la estructuración de planes y procedimientos, los cuales serán desarrollados, probados, monitoreados y mantenidos en permanente validación para su uso durante y después de una interrupción o desastre.

6.2 POLÍTICA DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

El DNP cuenta con una política integral, la cual acoge lineamientos y propósitos del SIG orientados a la continuidad de las operaciones, para dar cumplimiento y logro de los objetivos institucionales y compromisos de la entidad. Esta se ve reflejada en el numeral “*Política del SIG*” del Manual del SIG.

6.3 ALCANCE DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

El alcance de la GCN para el DNP está orientado a los procesos críticos, tanto misionales, estratégicos, de evaluación o de apoyo, que le permitan a la entidad, cumplir con la misión, objetivos y actividades relacionadas con sus productos y servicios, de acuerdo con los resultados generados por el BIA.

6.4 LIDERAZGO Y COMPROMISO

La entidad identifica la GCN como una de las responsabilidades claves en su gestión, avalada por la Dirección, alineándose con los objetivos del negocio, asignando los recursos necesarios para la implementación de las estrategias y la implementación de mecanismos de control y seguimiento a los resultados esperados, así como, estableciendo y comunicando el gobierno para la GCN.

6.5 ACTIVIDADES DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Durante el año se sugiere ejecutar actividades correspondientes al ciclo PHVA de la GCN, iniciando por la planeación de las actividades a realizar en la vigencia, la recolección de resultados de pruebas orientadas a los aplicativos, portales, sistemas de información, procesos, servicios y actividades críticas; permitiendo analizar los riesgos asociados a la continuidad, actividades de continuidad, pruebas y sensibilización, mantenimiento del Plan de Continuidad del Negocio y termina con la implementación de los planes de acción generados.


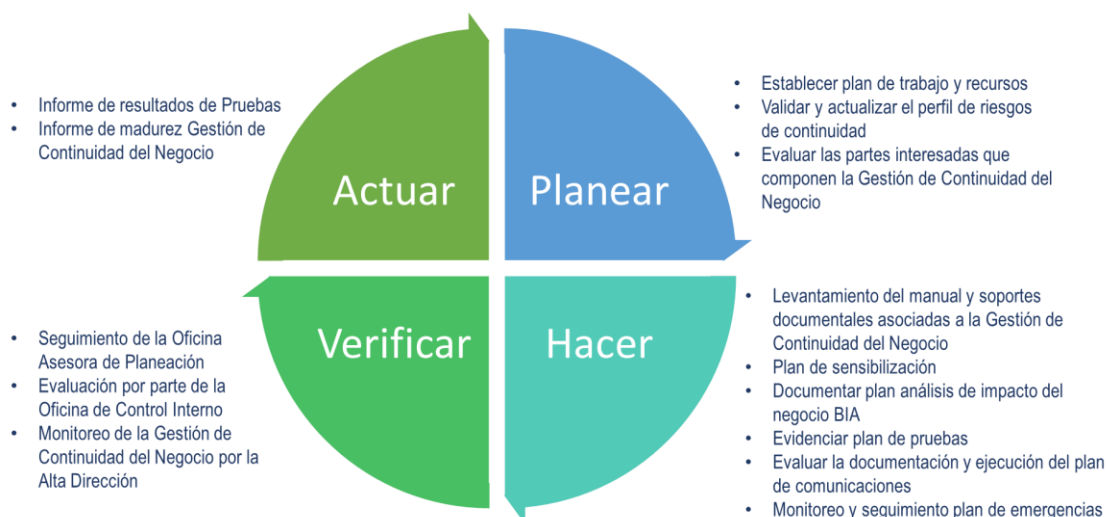
 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 14 de 47 VERSIÓN: 1</p>

Ilustración 2 PHVA – Gestión de Continuidad del Negocio



Fuente: Propia Oficina Asesora de Planeación

A continuación, se presentarán de forma detallada los componentes del ciclo PHVA para la GCN del DNP.

6.5.1 Planear

- **Establecer plan de trabajo y recursos**

Durante el primer trimestre de cada vigencia, se recomienda realizar la planeación de las actividades a realizar como parte de la estrategia de continuidad y generar un plan de trabajo relacionando las actividades principales asociadas a las metodologías y directrices que orientan al robustecimiento de la GCN. Este se sugiere ser aprobado por el Comité Institucional de Gestión y Desempeño (CIGD) o quien haga sus veces.

El plan de trabajo contempla como mínimo los siguientes campos:

- Descripción de la actividad: resumen de la actividad a realizar, incluyendo procedimientos y formatos si aplica.
- Periodicidad: instancia en la cual se sugiere realizar la actividad, según los procedimientos, buenas prácticas o normativa aplicable.
- Responsable: persona encargada de liderar la actividad.
- Personal de apoyo: personas requeridas para la ejecución de la actividad.
- Fecha de inicio: fecha en la que se comenzará a desarrollar la actividad.
- Fecha final: fecha máxima en la que se recomienda tener realizada la actividad.

Dentro del plan de trabajo se propone contemplar como mínimo las siguientes actividades:

- ✓ Ejecución de las actividades relacionadas en los procedimientos que hacen parte de la GCN y planes de emergencias.
- ✓ Verificación de los requerimientos y Acuerdo de Nivel del Servicio (ANS) de los componentes de la estrategia de continuidad.
- ✓ Verificación de los equipos de respaldo y apoyo a emergencias (planta eléctrica, detectores de humo, luces de emergencia, gabinetes de incendio, equipos de respuesta a emergencia, entre otros).

- ✓ Actividades relacionadas con el mantenimiento y fortalecimiento de la estrategia de continuidad.
- ✓ Plan de sensibilización y capacitación: propone incluir como mínimo la capacitación a cada uno de los equipos del plan de continuidad, así como la capacitación general a todos los colaboradores del DNP incluyendo los protocolos de seguridad y prevención de riesgos externos.
- ✓ Plan de pruebas donde se recomienda probar como mínimo una vez al año cada uno de los componentes de la estrategia de continuidad, así como los procedimientos de operación en contingencia y retorno a la operación normal.

Se propone definir los recursos necesarios para la ejecución de las actividades de la GCN para la vigencia actual, incluyendo el mantenimiento, monitoreo y operación de los componentes de la estrategia y los recursos a nivel tecnológico, logístico y de personal; con el fin de mantener operativa la GCN, siempre en búsqueda de la mejora continua y madurez de la continuidad del negocio.

- **Validar y actualizar el perfil de riesgos de la GCN**

Se recomienda realizar una vez al año la actualización del perfil de riesgos de la GCN como parte de proceso de la planeación, debido a que de los resultados se definen las actividades necesarias para ejercer controles efectivos que ayuden a disminuir el riesgo residual de cada uno de los riesgos evidenciados en relación con la metodología del componente de Gestión de Riesgos. Este perfil actualizado se sugiere sea publicado en el SIG.

- **Evaluar las partes interesadas que componen la GCN**

Como parte de la implementación de estrategias contingentes establecidas por el DNP se recomienda garantizar el normal funcionamiento de la operación, en particular para las partes interesadas, lo cual se refleja en el numeral “PARTES INTERESADAS PARA EL DNP” de este documento.

6.5.2 Hacer

- **Levantamiento del manual y soportes documentales asociados a la GCN**

La GCN garantiza el propósito, alcance y objetivos de la misionalidad de la entidad. Estos se sugieren a través de la evaluación de los vínculos con otros procedimientos o documentos pertinentes o requeridos. La GCN recomienda garantizar e incluir los siguientes lineamientos:

- Criterios y procedimientos de activación para un evento crítico.
- Procedimientos de implementación que apoyen la gestión.
- Requisitos y procedimientos de comunicación para actuar en escenarios contingentes.
- Identificación de las partes interesadas y actualización del contexto de la entidad (Sí aplica)
- Necesidades de recursos tecnológicos y humanos.
- Establecer la periodicidad de la presentación de información de gobierno para la evaluación de la GCN.
- El flujo de información y los procesos de documentación.

Los procedimientos documentados permiten una evaluación detallada de la situación y sus impactos, la determinación de las tareas y los planes de recuperación. Durante la recuperación, es posible que la organización necesite hacer lo siguiente:

- **Plan de sensibilización y capacitación**

El plan de sensibilización y capacitación busca generar los conocimientos necesarios en todos los colaboradores de la entidad, con la finalidad de generar valor y concientizarlos ante la ocurrencia de un evento contingente. El plan de sensibilización y capacitación se detalla en el numeral “13 CAPACITACIÓN Y SENSIBILIZACIÓN” de este manual.

- **Documentar y actualizar el Análisis de Impacto al Negocio – (BIA)**

El Análisis de Impacto al Negocio – (BIA Business Impact Analysis) es el insumo más importante para la GCN. Con los resultados de este análisis se determina la mejor estrategia que orienta a implementar la entidad para la administración de la crisis en caso de ocurrencia de un evento contingente que detenga la operación. Durante la ejecución del BIA, se realiza el levantamiento de la información necesaria para determinar cuáles son los procesos críticos del negocio y, como resultado de esto, los recursos a nivel de personal, tecnológicos y logísticos para operar en contingencia.

El BIA permite no solo priorizar los procesos más relevantes para la entidad, sino también establecer los tiempos de recuperación necesarios (RTO) y las pérdidas tolerables de datos (RPO) que la organización está dispuesta a aceptar, lo cual facilita la toma de decisiones estratégicas. Además, con esta información se pueden desarrollar planes de contingencia más eficaces, alineados con las necesidades reales del negocio y con un enfoque en la optimización de recursos durante la crisis.

El BIA, acorde con la normatividad existente y buenas prácticas, es importante realizarse por lo menos una vez al año, sin embargo, se aclara que este es un documento activo en el escenario de requerir una actualización que impacte los resultados del negocio, tales como cambios en la estructura organizacional, cambios en los aplicativos, cambios en el personal, entre otros. Para la realización de este análisis se recomienda utilizar el documento guía “*Guía metodológica para el análisis de impacto al negocio (BIA)*”.

- **Plan de pruebas**


Las pruebas hacen parte de los componentes, procedimientos, guías y formatos que componen el GCN. Durante la vigencia se recomienda probar cada uno de los componentes de la estrategia de continuidad, tales como el Centro de Datos Principal (CDP) y el Centro de Datos Alterno (CDA). Es importante probar los procedimientos de activación de la GCN al igual que el retorno a la operación normal. La planeación de las pruebas se sugiere estar ceñida al procedimiento “*Pruebas al Plan de Continuidad del Negocio*”, y es parte integral del plan de trabajo. El plan de pruebas se detalla en el numeral “12 PLAN DE PRUEBAS DE GCN” en este manual.

- **Evaluar la documentación y ejecución del plan de comunicaciones**

El efecto de una contingencia, especialmente aquellas de mayores consecuencias y proporciones, genera un impacto negativo que puede reducirse al mínimo si se estructuran medidas rápidas y eficaces a tal efecto y se mantiene bien informados a los diversos sectores del público interesado. Por lo tanto, es fundamental que los detalles de la crisis se manejen de manera responsable con los medios periodísticos, el público, empleados y clientes. De acuerdo con el Manual de Comunicaciones del DNP.

- **Evaluación del plan de emergencia**

Los planes de emergencias definidos para el DNP consisten en la principal guía protocolaria y procedimental para la atención de eventos de calamidad, desastre o emergencia en las distintas fases, con el fin de controlar, mitigar y reducir

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 17 de 47 VERSIÓN: 1</p>

al máximo los efectos negativos durante los mismos que se presenten dentro o en los alrededores de la entidad. Este aspecto se detalla en el numeral “10 PLANES DE EMERGENCIAS” de este manual.

6.5.3 Verificar

- **Seguimiento de la Oficina Asesora de Planeación**

Se define en el plan de acción anual el tratar, tolerar, terminar o transferir los riesgos mediante planes de acción o acciones mitigantes, y monitorear los riesgos en todas las etapas del proceso, con el fin de validar la eficacia de las acciones tomadas para un mejoramiento continuo el cual es supervisado por la Oficina Asesora de Planeación el cual se refleja en el procedimiento PT-PG-01 “*Gestión Integral de Riesgos*”.

- **Monitoreo del GCN**

La GCN generará un plan de implementación de los resultados al mantenimiento sobre la continuidad, el cual se recomienda sea planificado por todos los responsables de la gestión y presentado para aprobación al Comité Institucional de Gestión y Desempeño (CIGD) o quien haga sus veces, para aprobación.

En esta etapa se recolectan las evidencias de la ejecución de las actividades relacionadas con los procedimientos de contingencia, los resultados de la ejecución de las pruebas al GCN y la realización de las actividades programadas en el plan de trabajo. El monitoreo busca medir el nivel de cumplimiento, efectividad y calidad de las actividades relacionadas con la GCN y presentarlas a la Alta Dirección para su evaluación y, de ser necesario, generar planes de acción a los resultados del monitoreo.

6.5.4 Actuar

- **Informe de resultado plan de pruebas**

Se propone asegurar la efectividad de las pruebas comprometidas en el plan de trabajo y la aplicación de lecciones aprendidas u oportunidades de mejora por parte de la Alta Dirección, evaluando los recursos logísticos, tecnológicos, activos críticos y personal que participó en la prueba.

- **Informe de madurez del GCN**

La Alta Dirección del DNP evalúa el compromiso y liderazgo del desarrollo de la GCN asegurando que las políticas y objetivos establecidos en el sistema sean compatibles con la planeación estratégica de la entidad, integrando la continuidad del negocio a los diferentes procesos y productos generados, a través de recursos necesarios para el desarrollo, mantenimiento y mejora del plan de continuidad del negocio.

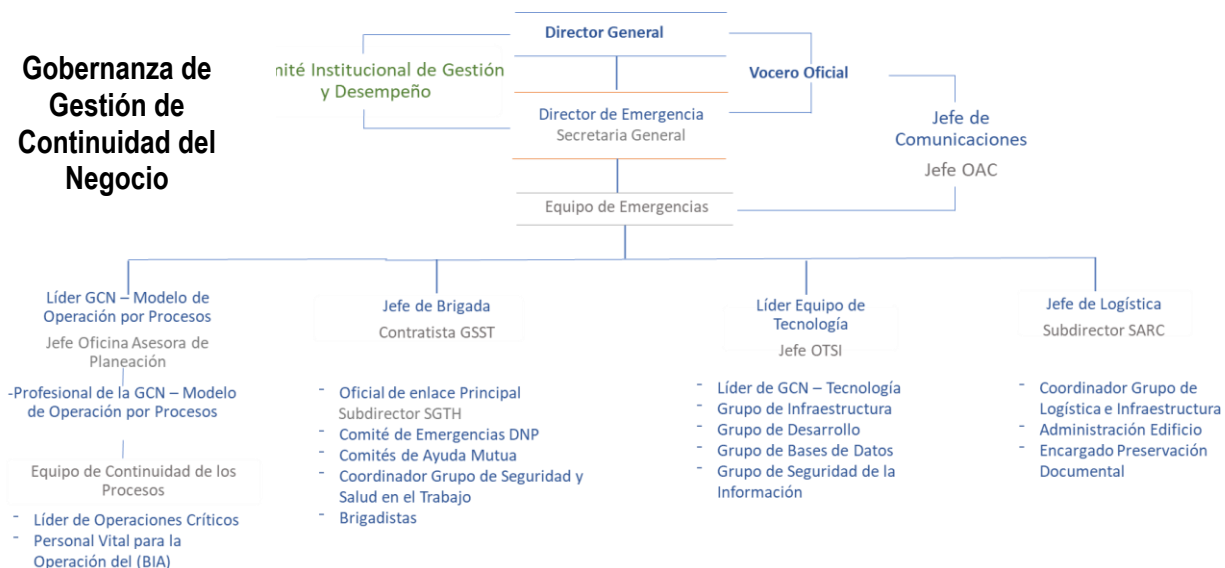
6.6 ACTIVIDADES DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El DNP ha establecido una estructura estratégica, táctica y operativa que tiene el propósito de lograr el aseguramiento de la recuperación de los procesos y productos definidos como críticos y la adecuada atención de situaciones de crisis; asimismo, busca soportar el mantenimiento y la actualización de los diferentes componentes asociados a la GCN.

6.6.1 Estructura de la Gestión de Continuidad del Negocio

Los equipos definidos están orientados a la ejecución de los procedimientos que se establecen dentro de cada uno de los planes relacionados en la estrategia de continuidad.

Ilustración 3 Estructura de la Gestión de Continuidad del Negocio



Fuente: Propia Secretaría General

Por otro lado, en la “Tabla 5 Actuar de la gestión de continuidad del negocio” se especifican los planes en los cuales cada equipo tiene una o varias funciones, siempre bajo la directriz de trabajar antes, durante y después de una situación adversa.

Las funciones se clasifican en:

- **Ejecuta:** tiene procedimientos que recomiendan ejecutar dentro del plan correspondiente (plan preventivo, plan de prevención y atención de emergencias, plan de reanudación y recuperación, plan de retorno a situación normal).
- **Apoya:** responde a los requerimientos del equipo en el desarrollo de los procedimientos del plan respectivo, pero no se relaciona directamente con la ejecución.
- **Controla:** tiene responsabilidades de mantenimiento en el plan respectivo.
- **Seguimiento:** es responsable de analizar y evaluar la eficacia y efectividad las actividades de GCN.

Tabla 5 Actuar de la gestión de continuidad del negocio

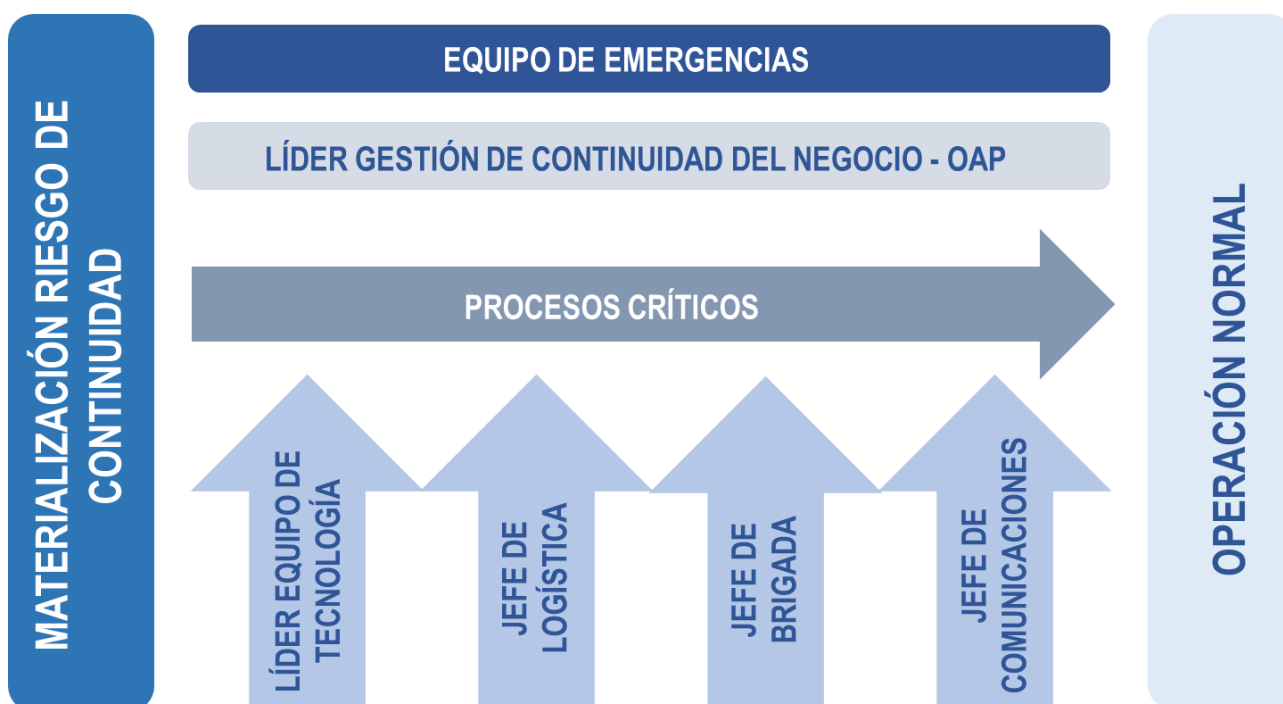
ACTUAR DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO				
Responsables de la GCN	Plan Preventivo	Plan de Prevención y Atención de Emergencias	Plan de Reanudación y Recuperación	Plan de Retorno a Situación Normal
Dirección General	Seguimiento	Seguimiento	Seguimiento	Seguimiento y Ejecuta
Comité Institucional de Gestión y Desempeño	Seguimiento	Seguimiento	Seguimiento	Seguimiento y Ejecuta
Director de Emergencia	Seguimiento	Seguimiento	Seguimiento	Seguimiento y Ejecuta
Vocero Oficial	Seguimiento	Seguimiento	Seguimiento	Seguimiento y Ejecuta
Equipo de Emergencias	Ejecuta y Controla	Ejecuta y Controla	Seguimiento	Seguimiento y Ejecuta
Jefe de Comunicaciones	Ejecuta y Apoya	Apoya	Apoya	Apoya
Jefe de Logística	Ejecuta, Apoya y Controla	Ejecuta y Controla	Apoya	Apoya
Jefe de Brigada	Ejecuta, Apoya y Controla	Ejecuta y Controla	Ejecuta y Controla	Ejecuta y Controla

ACTUAR DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO				
Responsables de la GCN	Plan Preventivo	Plan de Prevención y Atención de Emergencias	Plan de Reanudación y Recuperación	Plan de Retorno a Situación Normal
Líder Equipo de Tecnología	Ejecuta, Apoya y Controla	Ejecuta y Controla	Ejecuta y Controla	Ejecuta y Controla
Líder de Gestión de Continuidad del Negocio - MOP	Apoya y Controla	Apoya y Controla	Apoya y Controla	Apoya y Controla
Equipo de Continuidad de los Procesos	Ejecuta	Apoya	Ejecuta y Controla	Ejecuta y Controla
Organismo de Apoyo Externo	Apoya	Apoya	-	-
	ANTES	DURANTE		DESPUÉS

Fuente: Propia Oficina Asesora de Planeación.

Ante una activación de la GCN, estos grupos son responsables de restablecer la operación de los procesos identificados como críticos, dentro de los plazos establecidos por el BIA.

Ilustración 4 Estructura de la Gestión de Continuidad del Negocio




Fuente: Oficina Asesora de Planeación

Dirección General y Director de Emergencia (Vocero Oficial)

Estos actores en el DNP demuestran su compromiso y liderazgo en el desarrollo de la GCN por medio de las siguientes acciones:

- Asegurando que las políticas y objetivos establecidos en la GCN son compatibles con la planeación estratégica del DNP.
- Integrando y monitoreando la continuidad del negocio a los diferentes procesos y productos del DNP.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 20 de 47 VERSIÓN: 1</p>

- Suministrando los recursos necesarios para el logro de tiempos identificados en el BIA y el desarrollo, mantenimiento y mejora de la GCN.
- Propendiendo por el logro de los resultados esperados en el GCN.
- Tomando decisiones sobre el análisis e informe emitido por el Equipo de Emergencias.
- Apoyando al personal y líderes que contribuyen a la eficacia de la GCN y promoviendo la mejora continua de este.

Comité Institucional de Gestión y Desempeño (CIGD)

Avala la documentación asociada al GCN, las estrategias de prestación de servicio a las partes interesadas, las estrategias de tecnología e infraestructura tecnológica, el presupuesto para el mantenimiento del plan y los protocolos de comunicación interna y externa. Además, da la visión ejecutiva de las estrategias del programa de GCN y define los niveles de aceptación de los riesgos.

Equipo de Emergencias

El Equipo de Emergencias tiene como objetivo establecer jerarquías para la autorización y presentación de información a entes externos, dentro de un marco de trabajo donde se definan los diferentes mecanismos de decisión y comunicación durante un evento de crisis. Uno de estos mecanismos es la conformación del Equipo de Emergencias.

Dicho equipo será convocado y liderado por el Jefe (a) de la Oficina Asesora de Planeación o Director de Emergencias (Secretaría General) cuando los eventos de contingencia ocurridos tengan un alto impacto corporativo y afecten la continuidad de la operación de la entidad. Los eventos que no sean clasificados como eventos de contingencia serán tratados por los equipos que conforman la estructura de continuidad definida, según corresponda.

Algunos factores que determinan si un evento de crisis requiere la activación del Equipo de Emergencias, son:

- La magnitud del incidente y el impacto (reputacional, económico, legal y operativo) en la entidad a nivel local, regional o global.
- La disponibilidad de los recursos para tratar la interrupción.
- La necesidad de escalar al nivel de la Secretaría General o Dirección General para la resolución del evento.
- Los previstos en la definición de evento contingente.

Tabla 6 Funciones Equipo de Emergencias

DEFINICIÓN	CONFORMACIÓN DEL EQUIPO
<p>El Equipo de Emergencias es convocado cuando los eventos de crisis ocurridos tienen un alto impacto corporativo y afectan la operación de la entidad. Integra el personal del nivel jerárquico de la entidad, con el fin de propender por el cumplimiento del programa de preparación para emergencias, asegurando los medios administrativos y técnicos necesarios para su implantación, mantenimiento y puesta en práctica. Los eventos no clasificados como contingentes que puedan ser solucionados por equipos individuales, no requieren que se convoque.</p> <p>Los miembros del Equipo de Emergencias no están limitados a las personas que se mencionan en este manual. Puede convocarse a otros funcionarios o colaboradores de la entidad, según se requiera de</p>	<p>Líder: Secretaría General – Director de Emergencia.</p> <p>Integrantes principales:</p> <ul style="list-style-type: none"> • Líder GCN - MOP • Jefe de Brigada • Líder Equipo de Tecnología • Jefe de Logística • Jefe de Comunicaciones • Director(a) y subdirectores(as) técnicos y/o administrativos, según el tema correspondiente, de acuerdo con las circunstancias

acuerdo con el tipo de evento contingente que se presente.
En casos no contemplados que no permitan cumplir con las suplencias aquí definidas, se sugiere consultar el Árbol de Llamadas para cubrir este requerimiento en cada Grupo.

RESPONSABILIDADES

- Requerir a los equipos de apoyo administrativo, al equipo de respuesta a emergencias y al equipo de tecnología, los informes de evaluación de daños producidos en las personas, así como en la infraestructura física y tecnológica, provocados por el evento contingente para analizar esta información.
- Tomar decisiones estratégicas entre las que se encuentra activar el Plan de Continuidad del Negocio (PCN) ante una contingencia que tenga un impacto significativo, representado en la pérdida de las habilidades y recursos del DNP para continuar con sus operaciones básicas de negocio por un periodo no aceptable.
- Notificar a los colaboradores del DNP, mediante los mecanismos establecidos.
- Comunicar la activación del plan de continuidad a la ciudadanía y medios, si aplica, a través de su rol de Vocero Oficial ante los medios de comunicación y utilizando los canales apropiados para la comunicación con las partes externas interesadas.
- Monitorear el desempeño de la ejecución del plan de continuidad, desde su activación, pasando por la operación realizada en contingencia, hasta el adecuado retorno a la situación normal y restauración de la operación en las instalaciones principales, a través de los informes realizados por los diferentes equipos de la estructura de continuidad del negocio.
- Informar la declaración de la emergencia a los colaboradores y Director General de la entidad.

Fuente: Propia Oficina Asesora de Planeación.

Director de Emergencia – Secretaría General


Encargado de la dirección de emergencias, dirige todas las acciones necesarias para la atención y control de emergencias. Tiene la responsabilidad de realizar las siguientes actividades:

- Recibe la información de posibles eventos contingentes por parte de los grupos afectados y los equipos de la GCN y realiza una primera evaluación sobre si se requiere activar las estrategias contingentes y convocar al Equipo de Emergencias.
- Reunir al Equipo de Emergencia, en caso de presentarse un evento contingente.
- Tomar decisiones gerenciales sobre el manejo de la crisis, la operación en contingencia y el retorno a la operación normal.
- Generar y controlar, junto con el Equipo de Emergencias las comunicaciones tanto internas como externas que se publicarán sobre la situación de crisis, con el apoyo del Jefe de Comunicaciones.
- Coordinar con las Directivas los recursos y acciones a tomar para superar la crisis.

Líder de la GCN desde la articulación del Modelo de Operación por Proceso (MOP) – Jefe(a) de la Oficina Asesora de Planeación

El Líder de la GCN es el encargado de dirigir y liderar todas las actividades de la GCN para articular la incorporación de prácticas de continuidad del negocio en la cultura organizacional del DNP, apoyar la asignación del presupuesto y los recursos requeridos para su implementación, pruebas, mejora continua con las dependencias que hacen parte del Gobierno de Continuidad del Negocio, así como reportar el desempeño de la GCN a la Secretaría General y la Dirección General. Es el encargado de reunir y comunicar al Comité de Emergencia la situación de indisponibilidad en los procesos presentada. Tiene la responsabilidad de realizar las siguientes actividades:

- Recibe la información de posibles eventos contingentes por parte de los grupos afectados y los equipos de la GCN a nivel de procesos y realiza una primera evaluación sobre si se requiere activar las estrategias contingentes a nivel de procesos y convoca al Equipo de Emergencias.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 22 de 47 VERSIÓN: 1</p>

- Coordinar con las Directivas los recursos y acciones a tomar para superar la crisis.

Profesional de la GCN desde la articulación del Modelo de Operación por Proceso (MOP)

El Profesional de GCN realiza la parte de control y ejecución del plan de trabajo del GCN. Tiene la responsabilidad de realizar las siguientes actividades:

- Liderar la realización del BIA, en concordancia con las metodologías institucionales establecidas, consolidar y presentar sus resultados al Comité Institucional de Gestión y Desempeño (CIGD).
- Apoyar y asesorar al equipo directivo en la selección de las estrategias de continuidad más eficientes en términos costo - beneficio.
- Elaborar la propuesta del plan anual de actividades en materia de continuidad del negocio con la participación de las dependencias que intervienen y presentarlo a las instancias correspondientes, realizar seguimiento al mismo e informar sus resultados.
- Consolidar la propuesta de plan de pruebas de la GCN con la participación de los líderes de los equipos de continuidad, presentarlo al Comité Institucional de Gestión y Desempeño (CIGD) para su aprobación, coordinar la ejecución de las pruebas definidas y hacer seguimiento a las mismas.
- Requerir a los líderes de los equipos de continuidad la documentación de los resultados de las pruebas asociadas a la continuidad del negocio, consolidar los mismos y generar los informes que correspondan y estén definidos en el plan de pruebas.
- Coordinar la planeación y ejecución de las actividades de sensibilización y capacitación con la participación de los líderes de los equipos de continuidad.
- Realizar las gestiones para la creación y actualización permanente de la documentación que soporta la GCN, acorde con la forma de operación del DNP, y siguiendo los lineamientos del SIG.
- Preparar informes que se requieran sobre el avance y estado de la implementación de la GCN, incluyendo el informe de revisión por la Dirección; así como los requeridos por los entes de control.
- Apoyar la identificación, evaluación, control y tratamiento de los riesgos relacionados con la continuidad del negocio.
- Gestionar el análisis, atención y documentación de incidentes que se puedan ocasionar relacionados con la GCN.
- Gestionar la formulación y ejecución de acciones preventivas y correctivas relacionadas con la GCN.

Equipo de Continuidad de los Procesos

Tabla 7 Funciones Equipo de Continuidad de los Procesos

DEFINICIÓN	CONFORMACIÓN DEL EQUIPO
<p>Estos equipos tienen por objetivo identificar, implementar y probar las acciones que les permitan continuar con la operación de los procesos críticos del negocio, en un momento dado, determinado por la ocurrencia de un evento contingente.</p>	<p>Líder: Jefe (a) Oficina Asesora de Planeación y/o responsable del proceso.</p> <p>Suplente: Líder de GCN desde la articulación del Modelo de Operación por Proceso (MOP) y conocedor del proceso.</p> <p>Integrantes: Todos los colaboradores identificados como personal vital para continuar con el proceso según lo especificado en el Árbol de llamadas.</p>
RESPONSABILIDADES	

RESPONSABILIDADES DE LOS LÍDERES DE EQUIPOS DE CONTINUIDAD DE LOS PROCESOS CRÍTICOS DEL NEGOCIO

- Divulgar y capacitar a todos los colaboradores de su dependencia sobre las responsabilidades y acciones establecidas con respecto a la GCN, especialmente con los que conforman el Personal Vital (integrantes del equipo), los cuales estarán recuperando los procesos del negocio frente a una emergencia.
- Adelantar y supervisar las pruebas de los planes que componen la estrategia de Continuidad del Negocio.
- Conocer la estrategia definida para la recuperación de su proceso.
- Informar a la Oficina de Tecnologías y Sistemas de Información sobre las necesidades identificadas para la completa y correcta implementación de los procedimientos de continuidad del negocio.
- Informar a la Oficina de Tecnologías y Sistemas de Información los cambios técnicos (F-TI-18) y a la Oficina Asesora de Planeación los cambios de impacto misional en los procesos y procedimientos ([Gestión de cambios](#) F-PG-24) s presenten en el proceso y afecten la estrategia de continuidad definida.
- Mantener informado al Equipo de Emergencias sobre el avance de la situación, en caso de que éste lo requiera.
- Verificar que el Personal Vital el cual se identifica en el BIA definido para operar en contingencia registra y remite a custodia las claves de acceso a aplicativos, conexiones y demás, requeridos para el procesamiento de transacciones.
- Verificar que los colaboradores del grupo coordinan con el Equipo de Tecnología de la Información, los procesos de respaldo de la información crítica, en las periodicidades definidas y que se cuenta con esta para la ejecución de la recuperación del proceso.
- Verificar que se de buen uso a los perfiles de excepción de los aplicativos y conexiones en situación de contingencia.
- Gestionar la actualización periódica del Árbol de llamadas, respecto al listado de colaboradores del Equipo de Continuidad de los Procesos Críticos del Negocio, así como del personal vital.

RESPONSABILIDADES DEL SUPLENTE DEL EQUIPO

- Retomar y adelantar las acciones y responsabilidades del Líder del Equipo, en el momento en que éste falte por alguna condición programada (vacaciones, permisos, entre otros.) o no programada.
- Apoyar al Líder en sus actividades de control y seguimiento para la recuperación del proceso del negocio.

RESPONSABILIDADES DE LOS INTEGRANTES

- Operar los procedimientos definidos para ejecutarse al momento de una contingencia.
- Mantener una constante comunicación con el Líder del equipo, ya sea para solicitar apoyo o informar del avance en la recuperación de los procesos.
- Ejecutar las tareas relacionadas con la verificación o apoyo en la estabilización de los recursos necesarios en las oficinas principales con el fin de restablecer la operación normal.
- Participar en las pruebas de la GCN que se programen.

Fuente: Propia Oficina Asesora de Planeación.

Equipo de Tecnología - Líder Equipo de Tecnología

Tabla 8 Funciones Equipo de Tecnología

DEFINICIÓN	CONFORMACIÓN DEL EQUIPO
Este equipo tiene por objetivo implementar y probar las acciones que les permitan, ante eventos de contingencia, mantener y recuperar los servicios de tecnología utilizados por los procesos críticos de la entidad y que serán restablecidos dentro de la estrategia de continuidad de negocio.	Líder: Líder Equipo de Tecnología - Jefe (a) Oficina de Tecnologías y Sistemas de Información.
El equipo se divide en tres grupos que son:	Suplente de líder: Colaborador designado por la Oficina de Tecnologías y Sistemas de Información.
<ul style="list-style-type: none"> • Infraestructura. 	Líderes de grupos: <ul style="list-style-type: none"> • Grupo de Infraestructura: - Arquitecto de Plataforma - Grupo de Gestión de Plataforma.

- Bases de datos.
- Aplicaciones, sistemas de información y portales.

Este equipo está conformado por un líder, un suplente y los integrantes que participan en las tareas de prevención, recuperación y estabilización de los servicios de tecnología en el evento de presentarse una emergencia.

- **Grupo de Desarrollo:** Ingeniero Líder de Desarrollo.
- **Grupo de Bases de Datos:** Ingeniero, responsable de la Administración de las Bases de Datos – DBA.
- **Grupo de Seguridad de la Información:** Oficial de Seguridad de la Información.
- **Líder DRP- GCN:** Arquitectos de Plataforma.

Suplentes de Líderes: cada uno de los líderes tendrá un suplente que se relacionará junto con los demás integrantes del equipo en el Árbol de Llamadas. Se contará con Ingenieros desarrolladores y personal de soporte tecnológico de la Entidad o contratistas que apoyen el proceso.

RESPONSABILIDADES

RESPONSABILIDADES DEL LÍDER DEL EQUIPO DE TECNOLOGÍA

- Formular las propuestas de actualización de la infraestructura tecnológica que hace parte de la gestión de continuidad del negocio y ponerlas en consideración del Comité Institucional de Gestión y Desempeño (CIGD) y la Dirección General.
- Gestionar y supervisar la adecuación, implementación, documentación y pruebas del Plan de Recuperación de Desastres (DRP) de TI y coordinar las actividades periódicas de mantenimiento de este.
- Presentar las propuestas de modificación de la estrategia de continuidad a nivel tecnológico para el concepto del Comité Institucional de Gestión y Desempeño (CIGD).
- Liderar la ejecución de las acciones preventivas que a nivel tecnológico se recomiendan ser implementadas, con el ánimo de prepararse para afrontar un evento de mayor impacto que afecte los servicios de tecnología.
- Liderar la ejecución de las acciones a llevar a cabo al momento de realizar la recuperación de los servicios críticos de tecnología, así como las concernientes a la estabilización de las instalaciones principales de procesamiento de información de la entidad y el retorno a la operación normal.
- Capacitar y divulgar las responsabilidades del equipo para todos sus integrantes.
- Gestionar el mantenimiento de la infraestructura tecnológica asociada a las estrategias contingentes en su componente tecnológico, así como el mantenimiento de la documentación de este.
- Participar y motivar la participación de los integrantes del equipo en las pruebas a los diferentes planes que componen la estrategia de continuidad del negocio.
- Liderar la formulación, ejecución y documentación del plan de pruebas de continuidad del negocio en cuanto al componente tecnológico.
- Requerir a los Líderes de los equipos de continuidad los informes de los resultados de la activación de las estrategias contingentes, junto con todos los soportes resultantes de la ejecución de los diferentes planes que lo componen, consolidar y remitir a la Oficina Asesora de Planeación y los formatos e informes que correspondan o que esta Dependencia solicite, a fin de que efectúe el monitoreo correspondiente.
- Mantener informado al Líder del Equipo de Emergencias sobre las actividades a nivel tecnológico desarrolladas en respuesta a la situación contingente.
- Gestionar la actualización periódica de la matriz de grupos de interés, respecto a los proveedores de servicios tecnológicos.

RESPONSABILIDADES DE LOS SUPLENTES

- Retomar y adelantar las acciones y responsabilidades del líder de Dependencia, en el momento en que éste falte por alguna condición programada (vacaciones, permisos, entre otros.) o no programada.
- Apoyar al Líder en sus actividades de control y seguimiento para la recuperación de los servicios de tecnología.

RESPONSABILIDADES DEL GRUPO DE INFRAESTRUCTURA - LÍDER DRP - GCN

- Coordinar y participar en la ejecución de los procedimientos del plan de continuidad que estén bajo su responsabilidad.
- Mantener la disponibilidad de equipos y recursos de comunicación en el CDA.
- Coordinar la activación del CDA en caso de declararse la activación de una contingencia.

- Vigilar el cumplimiento de las políticas y procedimientos de respaldo de información a fin de garantizar la integridad y disponibilidad de esta.
- Mantener informado al Líder del Equipo de Tecnología sobre las actividades desarrolladas.
- Mantener actualizada la documentación de la infraestructura para la recuperación de esta en el CDA.
- Capacitar y divulgar las responsabilidades del grupo para todos sus integrantes.
- Informar a la Oficina Asesora de Planeación sobre los cambios en la plataforma tecnológica de la Entidad y sobre las repercusiones en la estrategia de continuidad definida, así como integrar el CDA al plan de capacidad de Tecnologías de la Información.
- Mantener actualizado el listado de proveedores externos relacionados con servicios de tecnología y coordinar con ellos la prestación de los servicios en el momento de una contingencia.
- Ejecutar las pruebas a la infraestructura tecnológica que soporta la GCN y documentar los resultados de estas.
- Informar al Líder de la Oficina de Tecnologías y Sistemas de Información sobre los resultados de la activación de la GCN.
- Verificar constantemente que la plataforma tecnológica del CDA (servidores, comunicaciones, software, entre otros.) tenga la capacidad necesaria para ejecutar los aplicativos y servicios de TI definidos como críticos y que hacen parte del DRP.

RESPONSABILIDADES DEL GRUPO DE DESARROLLO

- Coordinar y participar en la ejecución de los procedimientos del plan de trabajo de continuidad que estén bajo su responsabilidad.
- Vigilar el cumplimiento del mantenimiento preventivo de software.
- Ejecutar las pruebas a las aplicaciones críticas que soporta el plan de trabajo de continuidad del negocio y documentar los resultados de estas.
- Informar al Líder de la Oficina de Tecnologías y Sistemas de Información la activación de las estrategias contingentes.
- Mantener actualizada la documentación de las aplicaciones para la recuperación de estas en el CDA.
- Capacitar y divulgar las responsabilidades del grupo para todos sus integrantes.
- Verificar constantemente que los aplicativos del CDA se encuentren en las mismas versiones, parches y actualizaciones que los presentes en el CDP.


RESPONSABILIDADES DEL GRUPO DE BASES DE DATOS

- Coordinar y participar en la ejecución de los procedimientos del plan de trabajo de continuidad que estén bajo su responsabilidad.
- Vigilar la conservación de la integridad de los datos a ser recuperados en el CDA.
- Ejecutar las pruebas a las bases de datos de los aplicativos críticos que soporta el Plan de trabajo de continuidad del negocio y documentar los resultados de estas.
- Informar al líder de la Oficina de Tecnologías y Sistemas de Información sobre los resultados de la activación de la GCN.
- Mantener actualizada la documentación de las bases de datos de los aplicativos críticos para la recuperación de estas en el CDA.
- Capacitar y divulgar las responsabilidades del grupo para todos sus integrantes.
- Verificar constantemente que el motor de bases de datos y las bases de datos del CDA se encuentren en las mismas versiones, parches y actualizaciones que los presentes en el CDP.

COLABORADORES DE TECNOLOGÍAS DE LA INFORMACIÓN - GRUPO DE SEGURIDAD DE LA INFORMACIÓN

- Ejecutar los procedimientos definidos para efectuar la recuperación de los servicios críticos de tecnología del DNP y también las acciones para encontrarse preparados ante la ocurrencia de eventos contingentes.
- Mantener una constante comunicación con el líder del grupo correspondiente, ya sea para solicitar apoyo o informar del avance en la recuperación o gestionar las soluciones a los problemas que se puedan presentar.
- Ejecutar las tareas relacionadas con la verificación o apoyo en la estabilización de los recursos necesarios en las oficinas principales con el fin de restablecer la operación normal, una vez terminada la contingencia.

Fuente: Propia Oficina Asesora de Planeación.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 26 de 47 VERSIÓN: 1</p>

Equipo de Apoyo Administrativo - Jefe de Logística

Tabla 9 Funciones Equipo de Apoyo Administrativo

DEFINICIÓN	CONFORMACIÓN DEL EQUIPO
<p>Es el equipo definido para apoyar y mantener la infraestructura física, servicios generales, vigilancia y demás apoyo que sea identificado como necesario para mantener los procesos del negocio en operación.</p>	<p>Líder: Subdirector Administrativo y Relacionamento con el Ciudadanía Suplente de líder: Profesional SARC. Líderes de grupos: Coordinador Grupo de Logística e Infraestructura y Coordinador Grupo de Gestión Documental y Biblioteca. Suplentes de Líderes: Cada uno de los líderes tendrá un suplente que se relacionará junto con los demás integrantes del equipo en el Árbol de llamadas.</p>
RESPONSABILIDADES	
<p>RESPONSABILIDADES DEL LÍDER DE EQUIPO DE APOYO ADMINISTRATIVO:</p> <ul style="list-style-type: none"> • Liderar la implementación y mantenimiento de los recursos que permitan la recuperación de los procesos claves de negocio en coordinación con el Líder de la Oficina de Tecnologías y Sistemas de Información. • Mantener los contactos con el corredor de seguros para activar las reclamaciones respectivas en caso de daños a las instalaciones o infraestructura, producto de una situación contingente. • Liderar el procedimiento de evaluación de daños físicos una vez presentada la contingencia e informar de los resultados al Director de Emergencia. • Realizar la adquisición de los elementos de oficina necesarios para la operación en contingencia. • Apoyar a la Dependencia de Tecnología y a los equipos de continuidad de los procesos del negocio, para la operación durante la contingencia. • Coordinar con los proveedores externos la prestación de servicios de apoyo a los procesos claves del negocio. • Gestionar la actualización periódica del Árbol de llamadas en cuanto a los proveedores externos que prestan servicios de apoyo a la entidad y a los procesos claves del negocio, así como de los organismos de apoyo externo. <p>RESPONSABILIDADES DEL SUPLENTE DEL LÍDER DEL EQUIPO</p> <ul style="list-style-type: none"> • Retomar y adelantar las acciones y responsabilidades del Líder del equipo, en el momento en que éste falte por alguna condición programada (vacaciones, permisos, entre otros.) o no programada. • Apoyar al Líder en sus actividades de control y seguimiento para la recuperación de los procesos de negocio. <p>RESPONSABILIDADES DE LOS INTEGRANTES</p> <ul style="list-style-type: none"> • Ejecutar los procedimientos del plan de trabajo de continuidad del negocio que estén bajo su responsabilidad. • Mantener una constante comunicación con el Líder del equipo, ya sea para solicitar apoyo, informar del avance en la recuperación o gestionar las soluciones a los problemas que se puedan presentar. • Ejecutar las tareas relacionadas con la verificación o apoyo en la estabilización de los recursos necesarios en las oficinas principales con el fin de restablecer la operación normal. 	

Fuente: Propia Oficina Asesora de Planeación

Equipo de Comunicaciones - Jefe de Comunicaciones

Tabla 10 Funciones Equipo de Comunicaciones - Jefe de Comunicaciones

DEFINICIÓN	CONFORMACIÓN DEL EQUIPO
<p>Es el equipo responsable de diseñar, implementar y monitorear la estrategia de comunicación interna y externa en situación de continuidad del negocio y crisis, garantizando que la información</p>	<p>Líder: Jefe(a) de la Oficina Asesora de Comunicaciones. Suplente: Profesional especializado en comunicación estratégica o relaciones públicas.</p>

relevante se transmita de manera clara, precisa y oportuna a todas las partes interesadas, y manteniendo la imagen y reputación de la entidad.

Integrantes: Todos los miembros del equipo de comunicaciones, así como cualquier otro colaborador designado para roles específicos en la estrategia de comunicación en situaciones de continuidad del negocio.

RESPONSABILIDADES

- Establecer el canal de comunicación y mecanismos para suministrar información de acuerdo con las indicaciones dadas por el Director de Emergencia.
- Abrir líneas de comunicación controladas para audiencias internas y externas.
- Ser la fuente primaria de información sobre la crisis.
- Asegurar la coherencia y continuidad de los mensajes.
- Ser el único punto de contacto de la entidad para informar el estado de la crisis con funcionarios y audiencias externas como medios de comunicación, redes sociales y ciudadanía.
- Procurar que el cubrimiento de la crisis sea equilibrado y las versiones oficiales sean tenidas en cuenta.
- Capacitar a los voceros.
- Validar demás actividades asociadas.

RESPONSABILIDADES DEL LÍDER DE LA OFICINA ASESORA DE COMUNICACIONES:

- Coordinar la estrategia global de comunicación en casos de contingencia, incluyendo la comunicación interna y externa.
- Mantener informadas a todas las partes interesadas, incluidos servidores públicos y colaboradores, medios de comunicación y ciudadanía, sobre la situación actual y las medidas adoptadas por la entidad.
- Diseñar y aprobar los mensajes clave y oficiales que se transmitirán en caso de una crisis.
- Coordinar con otros líderes de equipos y la Estructura de la Gestión de Continuidad del Negocio para garantizar una comunicación coherente y unificada.
- Gestionar la relación con los medios de comunicación, actuando como portavoz principal o designando a un vocero en situaciones específicas.
- Garantizar la preparación y capacitación del Equipo de comunicaciones y voceros en gestión de crisis.
- Evaluar la efectividad de las comunicaciones y realizar ajustes según sea necesario.

RESPONSABILIDADES DEL SUPLENTE DE LA OFICINA ASESORA DE COMUNICACIONES:

- Asumir las responsabilidades del Líder en su ausencia, garantizando la continuidad de la estrategia de comunicación.
- Apoyar en la elaboración y difusión de mensajes clave.
- Coordinar y supervisar las actividades del Equipo de comunicaciones.


RESPONSABILIDADES DE LOS INTEGRANTES:

- Implementar la estrategia de comunicación definida por el Líder y el Suplente, adaptándola según el medio o canal específico de comunicación (por ejemplo, redes sociales, comunicados de prensa, correos electrónicos internos, entre otros.).
- Monitorear y reportar las reacciones y feedback de las partes interesadas, incluyendo la percepción del público y medios de comunicación.
- Mantenerse en constante comunicación con el Líder y el Suplente, informando sobre cualquier cambio, desafío o necesidad relacionada con las comunicaciones.
- Participar en sesiones de capacitación y actualización sobre gestión de comunicaciones en crisis.

Fuente: Propia Oficina Asesora de Planeación.

Jefe de Brigada - Coordinación Grupo de Seguridad y Salud en el Trabajo

Coordinar y dirigir las operaciones de la brigada para el control inicial de la emergencia, difundir entre los brigadistas las órdenes que imparta el Director de la emergencia.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 28 de 47 VERSIÓN: 1</p>

Nota: Las funciones, responsabilidades y los miembros del Equipo de Respuesta de Emergencias del DNP se establecen en la Resolución Interna 964 de 2020 anexa a este documento y se relacionan en el Plan de Emergencias y Contingencias FONADE relacionado en el numeral “*Esquema Organizacional para la Atención de Emergencias*”.

Vocero Oficial - Director de Emergencia (Secretaria General)

De acuerdo con lo establecido en el Manual de Comunicaciones del DNP, el Director General del DNP es el vocero principal de la entidad, hace los anuncios institucionales, tiene el direccionamiento de los mensajes del Gobierno Nacional y asume o delega vocerías sobre temas misionales, en situaciones de crisis o coyunturas especiales. Se sugiere capacitarlos para responder a las solicitudes de los medios en caso de ausencia del vocero principal.

7 GESTIÓN DEL RIESGO Y ANÁLISIS DE IMPACTO AL NEGOCIO

7.1 GESTIÓN DE RIESGOS

El análisis de los riesgos de continuidad de negocio para el DNP se toma como referencia sobre los lineamientos establecidos en el estándar internacional ISO 22301:2019, este contempla los lineamientos establecidos en el numeral “6.5.1 *Planear*” orientados por el componente de Gestión de Riesgos del SIG.

7.1 Análisis de Impacto del Negocio -BIA

El BIA, tiene como finalidad establecer donde se especifican los factores o variables de impacto para tener en cuenta y de igual manera la metodología utilizada para tal fin. El BIA es un proceso diseñado para identificar, categorizar y priorizar los procesos y productos de la entidad, que se puedan afectar por la no ejecución o actuación inoportuna por parte de las dependencias en sus procesos. Los objetivos principales del BIA son:

- Identificar procesos y productos críticos.
- Valorar impacto operativo y financiero en procesos críticos.
- Determinar los tiempos objetivos de recuperación (RTO).
- Priorizar los procesos para su recuperación.
- Determinar los recursos mínimos de recuperación.
- Identificar previamente las estrategias de recuperación de los procesos y productos del DNP.

A través de cuestionarios básicos realizados por medio de entrevistas a los responsables de cada uno de los procesos, se determina la criticidad, los Tiempos de Objetivos de Recuperación (RTO) y los Puntos Objetivos de Recuperación (RPO). Este se estructura y documenta con la guía metodológica del BIA y en conjunto con Líder de continuidad de negocio del componente tecnológico. El BIA es actualizado una vez al año.

8 PLAN DE RECUPERACIÓN DE NEGOCIO

El plan de recuperación del negocio de cada dependencia es el conjunto de procedimientos a seguir, en caso de ocurrir un incidente de tal magnitud que afecte las operaciones y procesos en forma parcial o total del DNP. Define los recursos humanos, procesos, productos, tecnología y de infraestructura, las actividades, tareas y datos requeridos para administrar el proceso de recuperación del negocio en el evento de una interrupción. El plan está diseñado para orientar la restauración de los procesos dentro de las metas de recuperación establecidas.

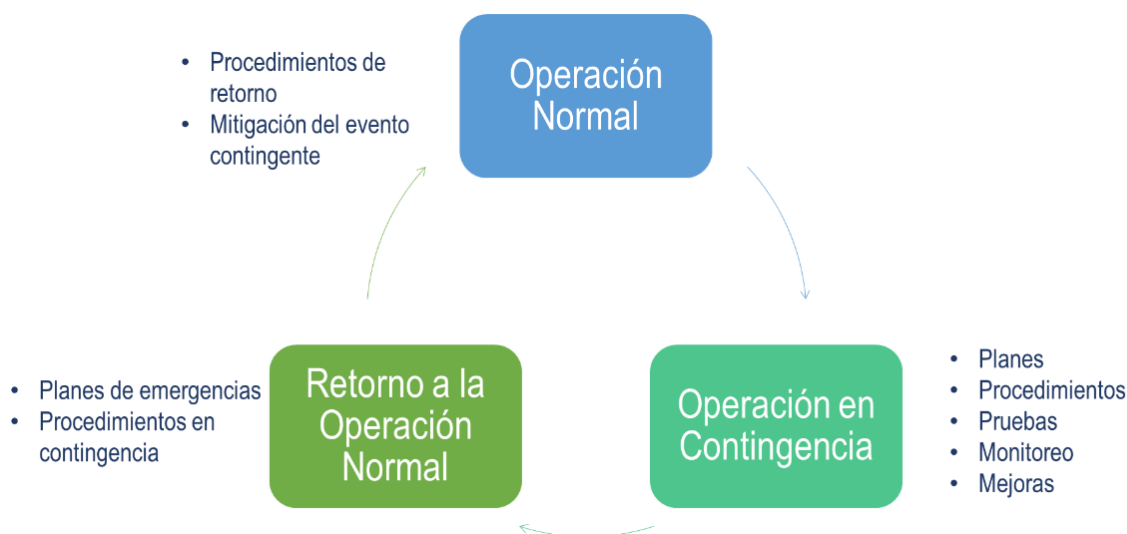
8.1. DEFINICIÓN DE LAS ESTRATEGIAS DE RECUPERACIÓN

El Plan de Recuperación de Desastres en ingles Disaster Recovery Plan (DRP) el cual cubre escenarios de falla, los cuales describen las actividades de recuperación de los subprocesos y actividades.

El DNP está expuesto a otros escenarios críticos como lo son: pandemias, atentados terroristas, desastres naturales, ataque cibernético entre otros. Para lo cual se tendrán en cuenta los lineamientos impartidos por la Alta Dirección, el Gobierno Nacional, y la normatividad aplicable, además de las estrategias descritas anteriormente mencionadas.

8.2 CICLOS DE OPERACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Ilustración 5 Ciclos de operación del plan de continuidad del negocio




Fuente: Oficina Asesora de Planeación.

El GCN sugiere:

1. Ejecución de pruebas exitosas.
2. Socialización a los grupos de interés. Ser conocido por todos los interesados
3. Cubrimiento de los siguientes aspectos:
 - Identificación de los riesgos que pueden afectar la operación
 - Actividades para realizar cuando se presentan fallas
 - Alternativas de operación y regreso a la actividad normal

8.3 ACCIONES POR ESCENARIOS DE FALLAS

Ante cualquier circunstancia que pueda afectar la normal prestación de servicios del DNP, lo primero y más importante es cuidar y proteger la salud e integridad de las personas que trabajan en la entidad; bajo cualquier esquema de contratación directa o indirecta, visitantes y población flotante. La vida y bienestar de todos son la base principal de la Gestión de Continuidad de Negocio (GCN) del DNP; por lo tanto, antes de intentar recuperar cualquier proceso,

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 30 de 47 VERSIÓN: 1</p>

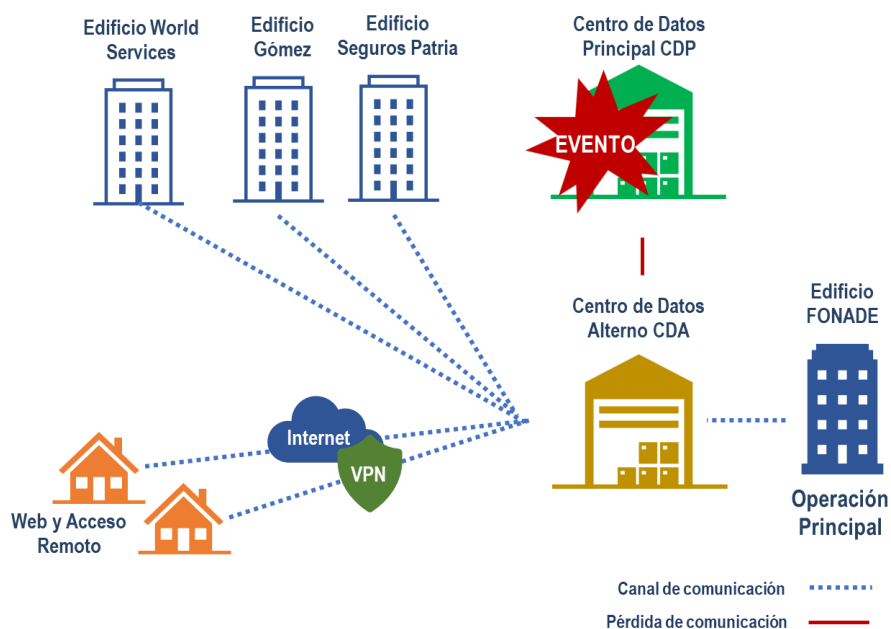
servicio, dependencia funcional, servidor, aplicativo, entre otros; se propone establecer que todo el personal al servicio del DNP se encuentra fuera de peligro.

8.3.1 Falla en el Centro de Datos Principal (CDP)

Comprende los edificios al servicio del DNP disponibles y el Centro de Datos Principal (CDP) no disponible. Diseñado para simular que las instalaciones u oficinas se pueden usar, pero la infraestructura tecnológica del CDP no se encuentra disponible.

Estrategia de recuperación: Centro de Datos Alterno (CDA).

Ilustración 6 Escenario de Falla en el Centro de Datos Principal – CDP



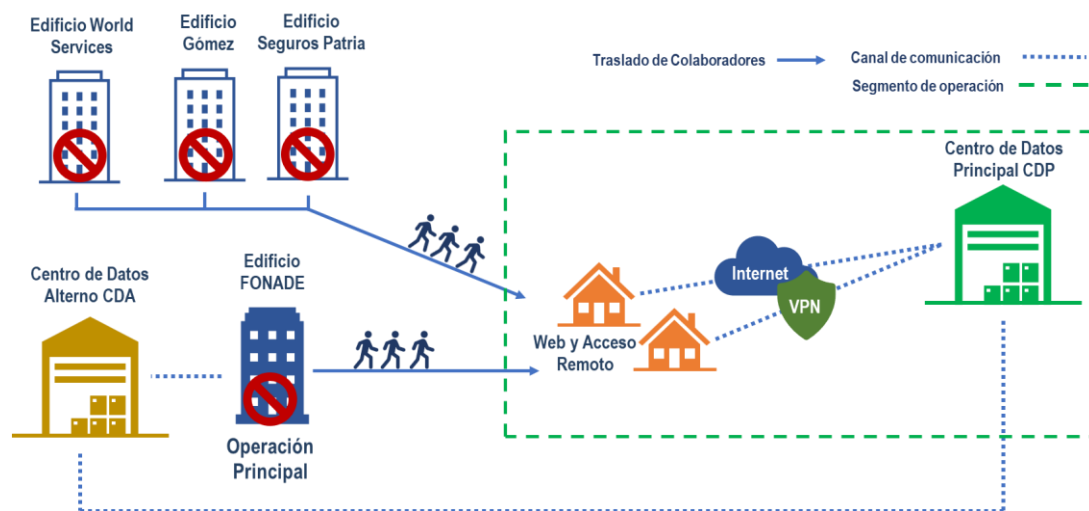
Fuente: Propia OTSI y OAP.

8.3.2 Falla en el edificio de operación principal o edificios opera el DNP

Para el escenario de indisponibilidad de los edificios donde opera el DNP y el Centro de Cómputo Datos Principal esté disponible frente a la infraestructura tecnológica.

Estrategia de recuperación: Accesos remotos seguros.

Ilustración 7 Escenario de falla en el edificio de operación principal o edificios opera el DNP



! Fuente: Propia OTSI y OAP.


8.3.4 Ausencia de personal clave

1. En el caso de presentarse una contingencia la cual afecte los procesos y productos del DNP, la prioridad es la recuperación de los procesos considerados como críticos y, para ello, se recomiendan tener en cuenta el personal encargado de estos y los posibles escenarios contingentes en su ausencia: Los cargos críticos cuentan con un Colaborador *back up*. Adicional de contar con respaldo de la información crítica de su cargo. En el escenario que falle se activa la siguiente estrategia.
2. Se sugiere realizar contratos de emergencia.

Tabla 11 Ausencia de personal Clave

Ítem	Qué se propone hacer	Responsable
1	Las dependencias afectadas, reportan el número de vacantes que se encuentran por cubrir.	Líder del Proceso
2	Ejecutar las estrategias de recuperación correspondiente al proceso o procesos afectados, bajo el escenario de falla de personal.	Líder del Proceso Líder GCN – MOP
3	Se recomienda consultar en la base de datos de contratistas que ha laborado en el DNP en forma temporal, cubriendo incapacidades, vacaciones, licencias o prácticas estudiantiles. El Jefe que solicita al personal puede solicitar una(s) persona(s) específica(s) con las cuales haya trabajado en el pasado y que cumplan con el perfil definido para el cargo.	Líder Subdirección de Contratación Líder del Proceso
4	Selección hojas de vida, según el perfil definido para el cargo, buscar perfiles adecuados.	Líder Subdirección de Contratación Líder del Proceso
5	Contactar a las personas para verificar su disponibilidad.	Líder Subdirección de Contratación Líder del Proceso
6	Validación de personas pre-seleccionadas, Una vez se definan las personas pre-seleccionadas, se recomienda validar con el Jefe del Proceso.	Líder Subdirección de Contratación Líder del Proceso
7	Ejecución de funciones asignadas.	Nuevo Contratista

Fuente: Propia Oficina Asesora de Planeación

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 32 de 47 VERSIÓN: 1</p>

8.3.5 Otros eventos críticos - Ataque Cibernético

El DNP siguiendo los lineamientos orientados del componente de la Seguridad de la Información, valida el cumplimiento de los controles asociados a la infraestructura tecnológica. A continuación, se relaciona los principales literales de la norma orientados a la continuidad del negocio:

- Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un Centro de Operación de Seguridad (SOC), que puede ser manejado desde el exterior. El análisis permite identificar las características del proveedor y herramientas y servicios que se contratarán.
- Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar al DNP y establecer controles para su mitigación.
- Considerar dentro de la GCN la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.
- Realizar pruebas de la GCN que simulen la materialización de ataques cibernéticos.

De acuerdo con lo anterior, el DNP cuenta con Centro de Operación de Seguridad (SOC) en el cual permite identificar, notificar y gestionar los incidentes de seguridad de la información de forma estructurada que permita responder de manera oportuna frente a cualquier evento, incidente y debilidad de seguridad que afecte la ejecución normal de los servicios de Tecnología de la Información en el DNP. A continuación, se detallan algunas de las actividades que se realizarán dependiendo el tipo de amenaza tecnológica en el escenario de materialización y previa notificación por parte del Centro de Operación de Seguridad (SOC):

a. Malware, Ransomware:

Impacta los equipos que se vean afectados por código malicioso, al punto de impedir al usuario trabajar y en algunos casos perder información por no contar con *backup*.

Actividades Técnicas:

- Se procede a aislar los componentes afectados de la red para el DNP, sí el análisis de las acciones realizadas así lo determinan.
- Identificar los archivos infectados y escanear las máquinas para validar si se realizó la limpieza de los archivos infectados.
- Formatear el equipo y realizar la instalación del sistema operativo con la semilla DNP.
- Restauración *backup* si es necesario.

Actividades Continuidad:

- El Líder de Continuidad de Negocio del componente Tecnológico y Arquitecto de Plataforma - Grupo de Gestión de Plataforma, avisarán al Líder de GCN – MOP y Líder de Seguridad de Información del incidente presentado.
- El responsable de continuidad en conjunto con el Líder de Incidentes evalúa el impacto del incidente.
- El responsable de continuidad escala al Líder de la Aplicación y/o infraestructura con el fin de validar tiempos de recuperación y deciden si activa o no la contingencia.
- El responsable de continuidad escala a las dependencias afectadas, con el fin de activar la GCN de las dependencias.
- Dependiendo el impacto y/o la afectación se convocará a los líderes de la Estructura de la Gestión de Continuidad del Negocio.

b. DDoS Attack: Ataque de negación del servicio distribuido.

El alcance de este tipo de ataque está enfocado a los servicios expuestos en internet. Se pueden presentar dos escenarios: uno relacionado con la falla a nivel de comunicaciones y otro a nivel de web server.

Actividades Técnicas:

- Validar con la Oficina de Tecnologías y Sistemas de Información desde la óptica de telecomunicaciones todas las peticiones que se hagan a la IP del dominio afectado.
- Reportar los componentes que se ven afectados para realizar las acciones correspondientes, como bloquear las IP no identificadas.
- Dependiendo de la plataforma, se propone contactar al Proveedor, para iniciar soporte de primer nivel.

Actividades Continuidad:

- El Líder de Continuidad de negocio del componente Tecnológico y Arquitecto de Plataforma - Grupo de Gestión de Plataforma, avisarán al Líder de GCN – MOP y Líder de Seguridad de Información del incidente presentado.
- El responsable de continuidad y el Líder de Seguridad de la Información en conjunto con el Líder de Infraestructura evalúan el impacto del incidente.
- El responsable de continuidad y Líder de Seguridad de Información escalan al Líder de la Aplicación y/o infraestructura con el fin de validar tiempos de recuperación y decidir si se activa o no la contingencia.
- El responsable de continuidad escala a las dependencias afectadas, con el fin de activar la GCN con cada una.
- Dependiendo el impacto y/o la afectación se convocará al Comité Estratégico de Manejo de Eventos de Crisis.

c. Insider and Privilege Misuse: Mal uso de privilegios:

Puede ser cualquier sistema interno, aplicaría a los activos de información que soportan procesos de tecnología, de mayor criticidad según clasificación de activos de la entidad.

Actividades Técnicas:

- El Líder de Infraestructura procede a identificar el sistema afectado.
- Validar las funcionalidades activas
- Solicitar el informe de privilegios, validar privilegios.
- Realizar el bloqueo de las funcionalidades que no corresponden.
- Realizar la investigación.

Actividades Continuidad:

- El Líder de Gestión de incidentes avisará al Líder de Continuidad del incidente presentado.
- El responsable de continuidad y Líder de Seguridad de la Información en conjunto con el Líder de Infraestructura evalúan el impacto del incidente.
- El responsable de continuidad y el Líder de Seguridad de la Información escalan al Líder de la aplicación y/o infraestructura con el fin de validar tiempos de recuperación y decidirán si activa o no la contingencia.
- El responsable de continuidad escala a las dependencias afectadas, con el fin de activar la Gestión de GCN con cada una.
- Dependiendo el impacto y/o la afectación se convocará al Comité Estratégico de Manejo de Eventos de Crisis.

8.3.6 Fallas de Proveedores Críticos

La OTSI solicita a los proveedores críticos la certificación de que cuentan con la GCN documentado, aprobado y probado anualmente, con el fin de asegurar su efectividad y garantizar la prestación del servicio contratado por el DNP.

Para los proveedores contratados que cuentan con la infraestructura tecnológica en la nube, y/o soportan los servicios con aplicaciones en la nube, se recomienda incluir dentro del plan de continuidad la disponibilidad de los servicios, estrategia de recuperación utilizada y copia de respaldo de la información del DNP para así garantizar la continuidad y disponibilidad del servicio contratado.

9 ACCIONES DE MANEJO DE CRISIS

Las acciones tienen como propósito ofrecer a la Alta Dirección del DNP una ruta de gestión para enfrentar situaciones críticas, como incendios, atentados, sismos, fallas de equipos, huelgas, incumplimiento de proveedores, entre otros.

El plan de manejo de crisis especifica:

- Equipo ejecutivo de manejo de crisis.
- Equipo funcional de respuesta a incidentes.
- Plan de comunicaciones para la crisis.
- Equipos de soporte.
- Apoyo externo.
- Tipos de eventos que se pueden presentar.
- Reporte de eventos.
- Documentación de eventos de crisis.

9.1 Evaluación de impacto de incidentes

Al ocurrir un evento de crisis o una interrupción, se propone realizar un análisis para determinar la causa. Este diagnóstico permite establecer además el impacto de la situación, considerando lo siguiente:

- Establecer cuáles son los servicios y proveedores externos que pueden ser necesarios para enfrentar la crisis.
- Cuantificar el impacto de la crisis, identificando los daños y el estado de la infraestructura.
- Evaluación de la infraestructura tecnológica que soporta la operación de los procesos críticos.
- Dependiendo del evento presentado se definen los públicos afectados, para establecer las acciones y mensaje respectivo. De su correcta definición se derivan las características del mensaje dado al momento de una crisis a los públicos afectados que hacen parte de las partes interesadas.

Si al realizar el análisis de incidentes o evento materializado de riesgo es calificado referente al apetito de riesgo del DNP (aceptable, tolerable, importante e inaceptable), este riesgo se lleva a la base de datos de la gestión de riesgos para ser tratado bajo esta metodología. Si el evento presentado materializa un riesgo importante o inaceptable, además de ser reportado como un evento de riesgo, el análisis de la causa determinará la estrategia de mitigación a ejecutar.

El Procedimiento de gestión y monitoreo de incidentes es el siguiente:

- Se presenta el evento.
- Se efectúa análisis de la causa del evento presentado.

- Si se define la causa analizada como asociada a un riesgo de continuidad de negocio, se recomienda activar el plan con base en las estrategias definidas. En el caso contrario, se sugiere efectuar un análisis adicional y aplicar acciones preventivas, efectuando seguimiento sobre las mismas hasta quedar mitigadas.

Para atender adecuadamente un incidente se propone evaluar su nivel, conforme a las siguientes consideraciones:

Tabla 12 Ausencia de personal Clave

Nivel de Crisis	Descripción
Nivel 1	<ul style="list-style-type: none"> • Fallas parciales a nivel operativo. • Supera el RTO del proceso y/o servicio. • Identificadas por el colaborador y pueden ser atendidas inicialmente por el Líder del proceso.
Nivel 2	<ul style="list-style-type: none"> • Fallas parciales a nivel operativo y tecnológico. • El tiempo estimado de solución supera el RTO del proceso y/o servicio. • Atendidas por el Líder del proceso, registradas en base de la gestión de riesgos y notificado al profesional de GCN - MOP.
Nivel 3	<ul style="list-style-type: none"> • Fallas generales a nivel tecnológico, operativo y de personal. • El tiempo estimado de solución supera los tiempos de recuperación RTO del negocio. • Llevados a la Alta Dirección por el Líder GCN – MOP o vicepresidente afectado. • Involucra a más de un plan del Sistema de Gestión de la Continuidad.

Fuente: Propia Oficina Asesora de Planeación.

A continuación, se presentan las actividades claves del proceso de gestión de crisis:

Impacto Nivel 1:


1. Aplicar la estrategia de recuperación correspondiente.
2. Efectuar seguimiento.
3. Si se soluciona el evento, se recomienda registrar las lecciones aprendidas y actualizar los planes de continuidad correspondientes, en caso contrario se escala al nivel 2.

Impacto Nivel 2:

1. Se informa al profesional o Líder de GCN -MOP.
2. Se convoca al grupo de gestión de continuidad y a la dependencia afectada.
3. Se aplica la estrategia operativa y/o tecnológica según corresponda.
4. Efectuar seguimiento.
5. Si se soluciona el evento, se propone registrar las lecciones aprendidas y actualizar los planes de continuidad correspondientes, en caso contrario se escala al nivel 3.

Impacto Nivel 3:

1. La Secretaria General (Director de Emergencia) – MOP convoca al Equipo de Emergencias.
2. Se convocan a los grupos de apoyo (Equipo de Respuesta a Emergencias, Equipo de Continuidad de los Procesos, Equipo de Tecnología y Equipo de Apoyo Administrativo) según corresponda.
3. Definir la aplicación de estrategias de continuidad y de comunicación.
4. Efectuar seguimiento.

 Departamento Nacional de Planeación	MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)	CÓDIGO: M-PG-14
		Página 36 de 47 VERSIÓN: 1

5. Si se soluciona el evento, se sugiere registrar las lecciones aprendidas y actualizar los planes de continuidad correspondientes.

9.2 Comunicaciones en Crisis

En el contexto de una entidad pública como el DNP, es crucial entender que una contingencia puede influir no solo en las operaciones internas sino también en la percepción pública. Enfrentarla con transparencia, rapidez y eficacia minimiza su impacto. Recuerde que una crisis bien manejada operativamente, pero mal comunicada siempre será recordada como una crisis mal manejada.

Es esencial manejar la crisis con responsabilidad y sensatez, orientando la comunicación hacia los públicos afectados, la ciudadanía, y los colaboradores de la entidad, tal y como está estipulado en el Manual de Comunicaciones del DNP. Los medios de comunicación y las redes sociales son algunos de los canales idóneos para comunicar de manera pública los mensajes que la entidad requiera difundir.

El objetivo principal de la Oficina Asesora de Comunicaciones o del vocero oficial durante una crisis es garantizar que la información y los mensajes transmitidos reflejen de manera auténtica los valores del DNP, protejan su imagen y reputación institucional, y mitiguen el impacto de la situación. Para ello, se prioriza una respuesta ágil y transparente, que refuerce la autoridad de la entidad, manteniendo un control efectivo de los canales de comunicación y promoviendo una interacción clara y confiable con los públicos clave.

9.2.1 Comunicaciones Internas

Es imperativo tener un Árbol de Llamadas que detalle cómo contactar a los colaboradores de la entidad en caso de una contingencia y este será estructurado y definido por los líderes de este Manual con apoyo de la Oficina Asesora de Comunicaciones en el momento en el que se requiera.

9.2.2 Comunicaciones Externas

La comunicación con la ciudadanía, medios de comunicación, y otros actores relevantes será gestionada directamente por el Director General, el Jefe de la Oficina Asesora de Comunicaciones o su designado. Esta comunicación se recomienda ser basada en la siguiente información proporcionada por el equipo de Administración de Crisis:

- Información actualizada sobre recursos humanos involucrados.
- Descripción precisa de la causa y naturaleza del problema.
- Evaluación del impacto o daño.
- Estimación del tiempo para la normalización de operaciones.
- Actualizaciones constantes del desarrollo y resolución de la crisis.

Tabla 13 Fase de Contingencia

Fase de Contingencia	Dependencia Responsable	Responsabilidad de Comunicarse Con
Gestión del evento de interrupción	Subdirección de Gestión del Talento Humano	Atención al personal, a familiares del personal, a hospitales y soporte Psicológico, Cooperación con la Policía, Defensa Civil, Bomberos, Servicios de emergencias.
	Director General, Oficina Asesora de Comunicaciones o Vocero Oficial	Atención a prensa, medios de comunicación, redes sociales, y ciudadanía.
	Líder GCN - MOP	Comunicación con los miembros del Comité Estratégico de Manejo de Eventos de Crisis.
Operación en contingencia	Oficina de Tecnologías y Sistemas de Información	Comunicación con proveedores de tecnología.
	Subdirección de Gestión del Talento Humano	Comunicados al personal, contrataciones de emergencia, gestión de remuneraciones.
	Subdirección de Contratación	Comunicados al personal, contrataciones de emergencia, gestión de remuneraciones.
	Líderes de Procesos	Administración de turnos de personal y reemplazos.
Retorno a la operación normal	Presidente – Comunicaciones	Atención a medios de comunicación y ciudadanos para informar finalización de la crisis.
	Líder del GCN - MOP	Comunicación con los miembros del Grupos que conforman el Comité Estratégico de Manejo de Eventos de Crisis.
	Director General	Comunicaciones con el Gobierno Nacional – Presidencia de la República.

Fuente: Propia Oficina Asesora de Planeación.

A partir de estos datos, se estructurarán los mensajes clave para el público. Se diseñarán comunicados oficiales, publicaciones en redes sociales, y otros materiales de comunicación conforme sea necesario. Es esencial comunicar de manera transparente y puntual a diferentes públicos:

Tabla 14 Público Objetivo

Público Objetivo	Medio de Comunicación	Colaborador Responsable del Contacto
Proveedores	<ul style="list-style-type: none"> Llamada telefónica Correo electrónico 	Subdirección de Contratación
Público en general	<ul style="list-style-type: none"> Comunicados de prensa Intervención en medios de comunicación Publicaciones en redes sociales propias y/o del Gobierno Nacional. Rueda de Prensa Avisos pagos en medios de comunicación e internet 	Director General o Vocero delegado

Fuente: Oficina Asesora de Planeación.

La frecuencia de estas comunicaciones se propone ser determinada y analizada por la gravedad y evolución de la situación, no solo por demandas externas. Es imperativo comunicar en todas las etapas de la crisis: al momento del evento, durante la recuperación y una vez la situación haya sido resuelta.

Tras la resolución de la contingencia, se recomienda trabajar conjuntamente con el equipo de comunicaciones para evaluar y aprender de las reacciones tanto internas como externas, garantizando que se tomen medidas para mejorar en futuros eventos.

10 PLANES DE EMERGENCIAS

El objetivo del plan del DNP es el de salvaguardar la vida de las personas expuestas a una situación de emergencia, asegurando su retiro o salida del lugar generador del peligro hasta uno de menor riesgo. Se está comprometido en adelantar el plan de preparación, prevención y atención, el cual se refleja en: 1) Plan de Emergencias Gomez, 2) Plan de Emergencias Seguro Patria, 3) Plan de Emergencias Word Service y 4) Plan de Emergencias y Contingencias FONADE, con el fin de evitar que las actividades desarrolladas ocasionen amenazas a la salud de los colaboradores y contratistas, proveedores, visitantes o de la comunidad.

Estos planes contemplan actividades protocolarias y procedimentales para la atención de eventos de calamidad, desastre o emergencia en las distintas fases, con el fin de controlar, mitigar y reducir los efectos negativos durante los mismos que se presenten dentro o en los alrededores de la entidad.

Es administrado por la Subdirección de Gestión del Talento Humano con apoyo de la Subdirección Administrativa y Relaciónamiento con la Ciudadanía, logrando establecer los procedimientos básicos para evacuar los edificios de la entidad, para evaluar y atender la salud de los colaboradores, ante la materialización de algún evento de riesgo que pueda originar lesiones en los colaboradores del DNP. Para más información sobre el Plan de Emergencias y sus procedimientos, remitirse a los documentos de Planes de Emergencia⁴.

PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS (DRP)

El Plan de Recuperación de Desastres Informáticos (DRP) por sus siglas en inglés, hace parte integral de la GCN y tiene como principal objetivo la recuperación de los recursos tecnológicos requeridos para operar en contingencia los procesos determinados como críticos en el BIA.

En el DRP se recomienda describir las estrategias generadas por Tecnologías de la Información para la replicación de los sistemas de información, aplicativos, herramientas y servicios de TI que son requeridos por el BIA, así como incluir guías de recuperación paso a paso para la activación del Centro de Datos Alterno (CDA). Como regla general, para toda estrategia de replicación se recomienda cumplir con tres cualidades:

- Reducir la posible pérdida de datos (RPO): en el marco de la estrategia de replicación, se sugiere siempre propender por reducir la diferencia de los datos entre el CDP y el CDA lo más cercano a tiempo real, queriendo decir con esto, que una vez ingresa un dato al CDP, este sugiere ser replicado al CDA en el menor tiempo posible.
- Minimizar los tiempos de Activación (RTO): en el marco de la estrategia de replicación, se busca siempre la tecnología más eficiente, de forma tal que una vez se requiera activar el CDA, el tiempo que toma desde esta notificación hasta que los usuarios funcionales tengan disponibles los aplicativos críticos sea lo más corto posible.
- Mejora constante: se busca constantemente las mejores tecnologías de replicación, buscando la mejora continua del proceso, garantizando que la activación del CDA sea un proceso fácil, automático, claro y eficiente.

El DRP tiene como función principal guiar las actividades a realizar, desde el componente tecnológico. Una vez se activa el plan de continuidad hasta que el personal vital pueda ingresar a los aplicativos críticos, así como las guías a seguir para el retorno de los datos desde el Centro de Datos Alterno (CDA) al Centro de Datos Principal (CDP).

⁴ <https://www.dnp.gov.co/DNP/gestion/sistema-integrado-gestion/Paginas/Planes-de-Emergencia.aspx>

Adicionalmente al DRP, se tiene establecido el procedimiento mediante el cual se hace una revisión sobre la replicación de los datos en el CDA, así como la verificación de versiones, parches, actualizaciones en comparación con lo que se tiene en el CDP. Esta revisión busca garantizar que el CDA se mantenga acorde con lo que se encuentra en el CDP, de tal forma que en caso de ocurrencia de un evento contingente que requiera la activación del CDA, o durante pruebas y simulacros, se tenga certeza de la capacidad para recibir la operación de los procesos críticos de la Entidad.

Finalmente, se recomienda tener un monitoreo constante de la replicación de los datos entre los centros de cómputo, garantizando que se pueda verificar el estado actual de los datos, los servidores, los sistemas de información, los canales de comunicación y los servicios de TI críticos.

Del resultado de pruebas y simulacros, se propone actualizar las guías paso a paso de activación del CDA. Estas actividades se ven reflejadas en el Plan de Recuperación de Desastres custodiado por la Oficina de Tecnologías y Sistemas de Información (documento en resguardo de esta oficina).

11 PLAN DE PRUEBAS DE GCN

Las pruebas de la GCN son una herramienta fundamental para validar la efectividad de este y complementan las actividades de actualización consideradas en el esquema de administración y mantenimiento.

Durante la ejecución de las pruebas se pueden identificar ajustes en la GCN definido y aportar al nivel de madurez de esta gestión. Es preferible que las fallas se detecten durante esta actividad y no que sucedan al ejecutar el plan ante una interrupción real. Algunas de las razones más importantes para el cumplimiento de estas pruebas son:

- Permiten validar los planes y procedimientos diseñados para garantizar la continuidad del negocio y los sistemas de información.
- Proveen tiempos de recuperación medidos para prepararse ante eventos reales.
- Transmiten experiencias de recuperación a colaboradores de la entidad.
- Ayudan a determinar todas las responsabilidades de los miembros del equipo de tecnología en casos de recuperación de la Oficina de Tecnologías y Sistemas de Información.

11.1 Tipos de Pruebas

Los sistemas de información, aplicativos y/o portales deben cumplir, documentar y actualizar pruebas funcionales y no funcionales de acuerdo con el ciclo de vida de pruebas establecido en el M-TI-01-Manual Operativo para la implementación y Mantenimiento de Sistemas de Información del DNP, incluyendo los nuevos desarrollos y extensibilidad de funcionales de los sistemas de información, aplicativos y/o portales en operación.

11.2 Estructura metodológica de pruebas

Para el diseño y desarrollo del plan de pruebas de la GCN, se sugiere tener en cuenta los tipos de actividades que se realizarán antes, durante y después de la ejecución de éstas, así:


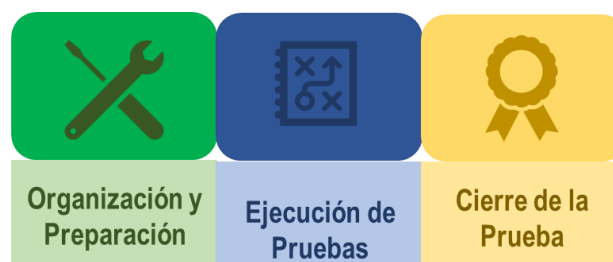
 Departamento Nacional de Planeación	MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)	CÓDIGO: M-PG-14 Página 40 de 47 VERSIÓN: 1
---	--	--

Ilustración 9 Estructura metodológica de pruebas



Fuente: Propia Oficina Asesora de Planeación.

Estas fases buscan direccionar la ejecución de las siguientes actividades:

- Definir el plan de pruebas considerando objetivos, alcance de las pruebas, recursos tecnológicos requeridos, personas involucradas y cronograma de pruebas, entre otros aspectos.
- Definir las actividades claves para tener en cuenta durante la ejecución de las pruebas, tales como la adecuada documentación de estas.
- Realizar el análisis de las pruebas, una vez ejecutado el plan de pruebas, generando compromisos que lleven a la actualización de la GCN.
- Publicar y notificar los resultados de las pruebas a los diferentes participantes en las mismas.

Nota: Los sistemas de información, aplicativos y/o portales deben cumplir, documentar y actualizar pruebas funcionales y no funcionales de acuerdo con el ciclo de vida de pruebas establecido en el M-TI-01-Manual Operativo para la implementación y Mantenimiento de Sistemas de Información del DNP, incluyendo los nuevos desarrollos y extensibilidad de funcionales de los sistemas de información, aplicativos y/o portales en operación.

A continuación, se describen cada una de las fases:

11.2.1 Organización y Preparación

La fase tiene como objetivo definir la estrategia anual de pruebas que aplica el DNP, relacionada con los procesos, productos y sistemas de información críticos priorizados.

Dentro de esta fase se propone desarrollar las siguientes actividades:

- Definir la estrategia global para diseñar las pruebas y el tipo de prueba. La estrategia proporciona un marco para la ejecución de las pruebas durante el año. El diseño considera:
 - ✓ Objetivos generales de las pruebas a programar.
 - ✓ Premisas sobre las cuales se ejecutarán las pruebas.
 - ✓ Consideraciones especiales para el éxito de la ejecución de cada una de las pruebas.
 - ✓ Frecuencia de las pruebas definidas.
 - ✓ Periodos de ejecución de pruebas durante el año.
 - ✓ Escenarios generales considerados para las pruebas.
 - ✓ Procesos y áreas de la compañía a ser incluidas en el plan.

Nota: Se recomienda realizar y/o ajustar este proceso al menos una vez al año.


- Ejecutar actividades iniciales de preparación de la prueba.

- ✓ Asignar los coordinadores de las pruebas.
 - ✓ Establecer los objetivos de la prueba.
 - ✓ Establecer el alcance de la prueba. Para apoyar esta definición, considere los siguientes cuestionamientos:
 - ¿El proceso/función/área tiene implementados los recursos de la estrategia de continuidad?
 - ¿En qué fecha espera tenerlos disponibles?
 - ¿Existen recursos o ambientes temporales que se puedan utilizar para las pruebas?
 - ¿Se usará información/transacciones reales o de prueba?
 - ¿Se utilizará el ambiente de TI productivo o el alterno?
 - ¿Qué transacciones o servicios probará? ¿Son los más representativos del proceso? ¿Qué volumen de transacciones manejará durante la prueba?
 - ¿Cuánto tiempo operará en el ambiente alterno? ¿Cuánto tiempo espera operar así?
 - ¿Cuántas personas del proceso participarán?
 - ✓ Definir los recursos logísticos, tecnológicos, registros vitales y personal que participará en la prueba. Cada recurso contempla tener una persona responsable de su consecución, considerando las fechas establecidas en el cronograma de pruebas.
 - ✓ Definir el escenario de plan de pruebas y ejecución de las actividades, con las fechas y personal responsables de realizar la tarea. Este cronograma incluye las actividades para alistamiento de recursos, ejecución y finalización de las pruebas.
 - ✓ Definir la posibilidad de invitar a evaluadores independientes al proceso de pruebas.
 - ✓ Definir las capacitaciones necesarias, para que los participantes puedan ejecutar apropiadamente las pruebas.
- Evaluar la planeación de la prueba realizada, hay que asegurar que todo el diseño esté finalizado antes de iniciar la ejecución de las pruebas.
 - Definir los criterios con los cuales se evaluará la prueba una vez ésta se haya ejecutado. Para apoyar esta actividad se encuentra disponible el documento.
 - De manera general para definir el tipo de pruebas a ejecutar, se considera las siguientes recomendaciones:
 - A. Para procedimientos considerados como críticos (RTO 1 hora y 4 horas) así como los de administración de crisis, o en los que se requiera validar principalmente la habilidad y el conocimiento de cada rol de continuidad para desarrollar sus responsabilidades, se recomienda ejecutar pruebas de escritorio/recorrido.
 - B. Para procedimientos críticos donde las personas del DNP ya tienen un alto nivel de conocimiento de las acciones a ejecutar en una continuidad y han participado en varios procesos de pruebas exitosas, realizar simulacros totales y simulaciones no anunciadas.
 - C. Rotar el personal que ejecuta las pruebas, para asegurar la transferencia y respaldo de las habilidades de conocimiento sobre continuidad. Por ejemplo, pruebas con titulares y otras con suplentes y/o sin el involucramiento de los expertos.

La preparación de la prueba se realiza en el formato de pruebas *“Preparación, ejecución y cierre de pruebas al plan de continuidad”*.

11.2.2 Ejecución de Pruebas

Para ejecutar las pruebas, se sugiere ejecutar las siguientes actividades:

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 42 de 47 VERSIÓN: 1</p>

Desarrollar todas las actividades de preparación de pruebas definidas en el formato Plan de Pruebas de la GCN. Durante la ejecución de la prueba el Líder de GCN orientado al MOP y los líderes de los procedimientos críticos gestionan las siguientes actividades:

- Comunicar a los colaboradores requeridos para el desarrollo de la prueba.
- Gestionar las firmas requeridas en los formatos.
- Medir los tiempos de respuesta durante la ejecución de la prueba.
- Después de realizar las pruebas realizar las siguientes acciones:
 - A. Validar el resguardo de los registros utilizados.
 - B. Asegurar la entrega y resguardo de los elementos logísticos usados durante la prueba.
 - C. Asegurar la realización de las copias de respaldo de información al centro externo de almacenamiento de información.

11.2.3 Cierre de la Prueba

El principal objetivo de ejecutar las pruebas es identificar los ajustes que se sugieren realizar sobre las políticas en continuidad de los procedimientos críticos para que éstos se mantengan efectivos. Por tanto, se recomienda realizar las siguientes actividades, una vez las pruebas han sido ejecutadas:

- Consolidar la información generada durante las pruebas por parte de los participantes.
- Gestionar la finalización y formalización de los formatos de pruebas.
- Ejecutar una reunión con los participantes en las pruebas. En esta reunión consolidar y validar los cambios identificados a los procedimientos críticos.
- Generar un informe ejecutivo del plan de pruebas con los resultados obtenidos.
- Evaluar el proceso de pruebas, según los criterios de éxito pactados en la etapa de planeación.
- Comunicar los resultados, conclusiones y oportunidades de mejora a los involucrados en el proceso de pruebas.
- El resultado de la evaluación se propone consignarlo para su seguimiento y mejora (sí aplican), en el formato Informe de Pruebas a la GCN.

12 CAPACITACIÓN , SENSIBILIZACIÓN Y DIVULGACIÓN

Con el fin de mantener las competencias de los colaboradores del DNP y su participación en la GCN, se programan capacitaciones o asistencia a eventos informativos, cuando sea posible. Así mismo, se hace seguimiento a la ejecución de capacitaciones sobre la GCN.

Los involucrados en estas actividades con la entidad se sugiere contemplarlos en el plan de sensibilización de la GCN:

Ilustración 10 Plan de sensibilización



Fuente: Propia Oficina Asesora de Planeación.

El Plan de Divulgación incluye información que permite:

- Facilitar el acceso a la información relacionada con los aspectos generales de la GCN: conceptos generales, estructura, escenarios de falla, tiempos de recuperación, procesos críticos, riesgos, entre otros.
- Difundir las acciones que se realizan para mantener y actualizar la gestión referente a los resultados de pruebas y simulacros, oportunidades de mejora y buenas prácticas.
- Publicación de documentos relacionados con el tema de Continuidad de Negocios y que se consideren de importancia para la Entidad.
- La información de la GCN estará a disposición de los funcionarios y colaboradores del DNP, a excepción de la información que se considera confidencial, en el catálogo documental la Rebeca.

La formación es esencial para asegurar que todo el personal conozca qué hacer cuando hay una contingencia que genere la interrupción de las operaciones en el DNP.

- Las iniciativas incluyen capacitaciones a los nuevos colaboradores, reinducciones a todos los colaboradores de la Entidad y a los equipos que componen la estructura del GCN.
- La apropiación del conocimiento se valida a través de las evaluaciones generadas durante las capacitaciones, los resultados de las pruebas y simulacros planeados.

Los colaboradores en general reciben formación relacionada con la GCN así:

Tabla 15 Temas plan de capacitación

FUNCIONARIOS / COLABORADORES	INTEGRANTES ESTRUCTURA DEL GCN	LIDERES EQUIPOS DEL GCN
* ¿Qué es un GCN?	* ¿Qué es GCN?	* ¿Qué es GCN?
* ¿Por qué se tiene un GCN?	* ¿Por qué se tiene una GCN?	* ¿Por qué se tiene una GCN?
* Normatividad	* Normatividad	* Normatividad
* Estructura de la GCN y responsabilidades	* RPO y RTO	* Escenarios de Falla
* RPO y RTO	* Estructura del GCN y responsabilidades	* RPO y RTO
* Estrategias en caso de una contingencia	* Responsabilidades del equipo dentro de la estructura de la GCN.	* Responsabilidades de los equipos dentro de la estructura de la GCN
* Equipos de atención a emergencias	* Estrategias en caso de una contingencia.	* Simulacros con actividades antes, durante y después de la contingencia
* Evacuación	No aplica	No aplica

Fuente: Propia Oficina Asesora de Planeación.

- El Plan de sensibilización se complementa con las acciones de capacitación y socialización que mediante las comunicaciones realice permanentemente la entidad.
- El Plan de sensibilización aumentará la conciencia y el conocimiento entre los funcionarios y colaboradores en general, en temas de continuidad del negocio.
- La metodología en la sensibilización se adapta a los diferentes niveles organizacionales que existen en la Entidad.
- El programa es útil, interactivo, conciso y práctico y puede apalancarse con piezas comunicacionales creativas.
- Una vez desarrollado el Plan de sensibilización es necesario medir su nivel de apropiación por lo menos dos veces al año.
- Todas las iniciativas de sensibilización lograrán apalancarse en los medios de comunicación con los que cuenta la GCN.

13 CAMBIOS RELACIONADOS A LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Es importante identificar los cambios correspondientes a definiciones y prácticas de continuidad dentro del DNP que pueden surgir por diferentes actividades, tales como:

- **Posibles contingencias reales:** que requieren el uso de las estrategias, procedimientos y activos críticos de la GCN. En este sentido, las lecciones aprendidas de situaciones pasadas pueden generar ajustes en los procedimientos y en la identificación de nuevos riesgos o amenazas que no se habían considerado previamente.
- **Cambios en la operación de los procesos:** cuando se presentan modificaciones en los procesos operativos dentro del DNP, ya sea por evolución de los negocios, la adopción de nuevas tecnologías, o la reestructuración de la entidad, es necesario revisar y actualizar los planes de continuidad para garantizar que los procesos críticos continúen funcionando sin interrupciones.
- **Novedades sobre el personal de continuidad:** cambios en los roles o responsabilidades del personal encargado de la GCN, como la rotación de personal clave, la capacitación del personal nuevo o la reasignación de tareas dentro de los equipos, que requieren una revisión de la capacidad de respuesta ante crisis y la actualización de los procedimientos operativos.
- **Cambio de proveedores críticos:** los cambios en la relación con proveedores clave o la sustitución de proveedores que proporcionan servicios esenciales para la continuidad del negocio pueden implicar la necesidad de reevaluar los acuerdos de nivel de servicio (SLAs), los procedimientos de recuperación y las medidas de mitigación de riesgos asociados.

- **Auditorías o revisiones internas o externas** que se reciban por entes de control. Las auditorías, tanto internas como externas, proporcionan una oportunidad para identificar posibles debilidades o áreas de mejora en los planes de continuidad, lo que puede derivar en la actualización o implementación de nuevas prácticas para reforzar la capacidad de respuesta ante crisis.
- **Procesos de pruebas ejecutadas sobre los procedimientos críticos** y funciones o servicios críticos de la GCN. Las pruebas periódicas (simulacros, ejercicios de contingencia) ayudan a evaluar la efectividad de los planes de continuidad y permiten identificar ajustes o mejoras en la respuesta ante emergencias.

Estos cambios y acciones deben ser evaluados de manera integral para asegurar que la entidad mantenga una **respuesta ágil y efectiva** ante cualquier evento disruptivo. Además, es fundamental que dichos cambios sean **presentados y aprobados por los líderes de Gobernanza de la Gestión de Continuidad del Negocio** antes la **Secretaría General**, quienes deben coordinar con todos los departamentos relevantes para garantizar que los ajustes sean implementados de manera oportuna.

Es necesario que los cambios sean gestionados de forma **transparente y comunicada adecuadamente** a todos los niveles dentro de la organización, asegurando que los **equipos de trabajo estén alineados** con los nuevos procedimientos o estrategias. Además, los **planes de continuidad deben ser revisados de manera periódica**, tomando en cuenta los cambios del entorno y las posibles nuevas amenazas, para adaptarlos de manera proactiva y mantener la efectividad en la protección y recuperación de las operaciones.

Este enriquecimiento incluye aspectos sobre la **gestión proactiva de los cambios**, la **importancia de las pruebas y auditorías periódicas**, la **coordinación entre departamentos** y la **evaluación continua** de la capacidad de respuesta ante situaciones de crisis. También subraya la necesidad de mantener una **comunicación efectiva** dentro de la organización para asegurar que todos los actores estén informados y preparados.


Es importante identificar los cambios correspondientes a definiciones y prácticas de continuidad dentro del DNP que pueden surgir por diferentes actividades, tales como:

- Posibles contingencias reales que requieren el uso de las estrategias, procedimientos y activos críticos de la GCN.
- Cambios que se presentan eventualmente en el DNP como: cambios en la operación de los procesos, novedades sobre el personal de continuidad, cambio de proveedores críticos, entre otros.
- Auditorías o revisiones internas o externas que se reciban por entes de control.
- Procesos de pruebas ejecutadas sobre los procedimientos críticos y funciones o servicios críticos de la GCN.

Estos cambios y acciones deben ser evaluadas y presentadas por parte de los líderes de Gobernanza de la Gestión de Continuidad del Negocio antes la Secretaría General.

14 MEJORA CONTINUA

La Gestión de Continuidad de Negocio (GCN) del DNP se encuentra alineado con la política del SIG en la cual orienta su gestión a satisfacer a sus clientes, con talento humano competente, comunicación efectiva y herramientas tecnológicas, que garantizan un excelente servicio, basado en el mejoramiento continuo de sus procesos y productos. Por ello, y con base a los lineamientos de desempeño, se ejecuta un plan de pruebas para asegurar una mejora permanente al GCN.

 <p>Departamento Nacional de Planeación</p>	<p>MANUAL DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO (GCN)</p>	<p>CÓDIGO: M-PG-14</p>
		<p>Página 46 de 47 VERSIÓN: 1</p>

Fecha aprobación: 10/12/2024

Elaboró:

ORIGINAL FIRMADO

Ruby Lizeth Galeano Villada
Contratista Profesional Oficina Asesora de Planeación

ORIGINAL FIRMADO

Cristian Eduardo Oviedo Rodriguez
Contratista Profesional Oficina Asesora de Planeación

Revisó OAP:

ORIGINAL FIRMADO

Isabel Cristina Ramirez Botero
Contratista Profesional Oficina Asesora de Planeación

Aprobó:

ORIGINAL FIRMADO

Ernesto Sandoval Diaz
Jefe Oficina Asesora de Planeación

ORIGINAL FIRMADO

Adriana Elena Cuellar Ramirez
Jefe Oficina Asesora de Comunicaciones

ORIGINAL FIRMADO

Bellaniris Avila Bermudez
Subdirectora Administrativa y Relacionamiento con la Ciudadanía

ORIGINAL FIRMADO

Mayer Durley Velasco Parra
Subdirectora de Gestión del Talento Humano (E)

ORIGINAL FIRMADO

Orlando Benavides Santacruz
Jefe de la Oficina de Tecnologías y Sistemas de Información