# PLAN DE CONTINUIDAD DEL NEGOCIO

**OFICINA DE TECNOLOGÍA**
**DE LA INFORMACIÓN Y LAS COMUNICACIONES**

**Versión 1**

**Enero 28 de 2025**

CONTENIDO

## 1. LISTA DE TABLAS



## 2. LISTA DE ILUSTRACIONES

## 3. INTRODUCCIÓN

La gestión del **Plan de Continuidad del Negocio (PCN)** en las entidades del estado debe responder a una variedad de políticas de restablecimiento de actividades y servicios que apoyen el normal funcionamiento de las infraestructuras de TI y minimicen al máximo las interrupciones o fallas presentadas dentro de la organización. Las entidades deben permanentemente monitorear y reconocer las amenazas más importantes de incidentes que afecten la normal operatividad de los servicios y los sistemas, de tal manera que se debe garantizar la continuidad del negocio a través de mecanismos de recuperación previamente probados y ajustados y que respondan en el menor tiempo posible a las soluciones de los problemas de interrupción.

El fin de la implementación del plan de continuidad de TI, es la protección y recuperación de los servicios críticos que se vean afectados por desastres naturales o interrupciones del servicio ocasionadas ya sea por los sistemas de información y comunicación o ya sean por el hombre en virtud de acciones involuntarias o para beneficio propio. Así mismo, el análisis de impacto de negocios debe convertirse en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias. Las entidades deben contar con un plan de continuidad de Tecnología de Información, que le permita a la organización continuar con sus operaciones, en caso de presentarse fallas o inconvenientes en sus sistemas que le impidan el normal funcionamiento de los servicios de TI, de esta manera, la correcta implementación del plan deberá permitir restaurar en el menor tiempo posible las operaciones de la Entidad.

El análisis de impacto del negocio – BIA por sus siglas en inglés (Bussiness Impact Analysis), está determinado por la construcción de un PCN para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido; el documento generado en este análisis deberá cumplir con lo expuesto en los requerimientos de la ISO/IEC 27001, de este modo el documento BIA debe ser validado e implementado bajo las directrices de cada organización y se requieren planear las acciones necesarias durante el período en que la infraestructura de TI se encuentra inactiva y en proceso de recuperación y reanudación de los servicios para priorizar cuales actividades y servicios deben entrar en operación inmediatamente dentro de la entidad. Finalmente, es necesario tener en cuenta que los responsables del negocio deben conocer la importancia de tener una inversión de TI planeada que permita innovar tecnológicamente y que responda adecuadamente a los problemas generados por la interrupción de los servicios y permita que las organizaciones puedan aplicar exitosamente los criterios de recuperación y reanudación de las operaciones del negocio.

## 4. INFORMACIÓN GENERAL

| | |
|---|---|
| **Nombre del Plan de Acción** | **Plan de Continuidad del Negocio 2025** |
| **Nombre y código:**<br>**Rubro presupuestal** | **Proyecto de Inversión: Código: O230117459920240191**<br>Fortalecimiento de la capacidad institucional para la modernización de la Caja de la Vivienda Popular de la ciudad de Bogotá D.C |
| **Presupuesto asignado ($)** | **Presupuesto Total del Proceso Gestión de TIC's:** $ 3.650.007.000 |
| **Área responsable** | Oficina De Tecnología De La Información Y Las Comunicaciones |
| **Política MIPG y otros** | Política de Gobierno Digital – Política de Seguridad Digital |
| **Proceso** | Gestión De Tecnología De La Información Y Las Comunicaciones |

| | |
|---|---|
| **Fecha inicio del plan** | 02/01/2025 |
| **Fecha fin del plan** | 31/12/2025 |

*Tabla 1 - Información general del Plan*
*Fuente: Elaboración Propia*

## 5. EJE ESTRATÉGICO – OBJETIVO ESTRATÉGICO

El eje estratégico #7: *Transformación Organizacional*, representa el ámbito de acción que debe ser desarrollado para abordar los retos institucionales desde la Oficina de Tecnología de la Información y las Comunicaciones, definiendo la ruta por la cual transitaremos para llegar al destino que la Caja de Vivienda Popular se ha propuesto y constituye una de las aspiraciones que quiere lograr la Entidad entre los años 2024 al 2028.

El objetivo estratégico # 7: *Fortalecer la capacidad y efectividad administrativa y la innovación organizacional, para la modernización de la Caja de Vivienda Popular y el incremento en la confianza ciudadana en la Entidad;* enmarca la gestión de la Oficina de Tecnología de la Información y las Comunicaciones *y* pone en manifiesto lo que se quiere lograr en la vigencia 2024-2028: La Implementación del 100% del Sistema de Información Misional de la CVP y la Garantía de la Disponibilidad de la Infraestructura Tecnológica.

## 6. OBJETIVO GENERAL

Disponer de un documento guía por medio del cual la Caja de la Vivienda Popular (CVP), tenga definidos los lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio.

### 6.1. Objetivos Específicos

- Establecer pautas para poder actuar tras el acontecimiento de hechos que pongan en crisis la operación de la Caja de Vivienda Popular CVP.
- Asignar roles y responsabilidades a cada uno de los funcionarios y contratistas y proveerle guías para la atención de emergencias y recuperación de los procesos, durante interrupciones prolongadas de la operación normal.
- Establecer las actividades, recursos y procedimientos necesarios para llevar a cabo las operaciones y contar con acceso a los sistemas de tecnología de información y comunicaciones de la Caja de la Vivienda Popular, durante la materialización de riesgos de alto impacto en la organización.

## 7. ALCANCE

Este documento contempla los lineamientos de administración de la continuidad, el desarrollo de las fases que componen el plan de continuidad del negocio y las metodologías definidas por la Caja de la vivienda Popular, en caso de presentarse incidentes de interrupción que puedan afectar los procesos críticos.

Este documento también relaciona las estrategias de continuidad implementadas por la Entidad para aumentar su capacidad de recuperación y enfrentar situaciones que amenacen o afecten la integridad física

de sus colaboradores e instalaciones.

## 8. DEFINICIONES

• **Plan de Recuperación de Desastres (DRP):** Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

• **Análisis de Impacto del Negocio (BIA):** Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

• **Continuidad del negocio**: capacidad de una organización para continuar la entrega de productos y servicios dentro de marcos de tiempo aceptables a la capacidad predefinida durante una interrupción.

• **Plan de Continuidad de Negocio (PCN):** Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

• **Emergencia**: Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

• **Interrupción**: Incidente, anticipado o no anticipado, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización.

• **Administración del Plan de Continuidad de Negocios:** Es un sistema administrativo integrado transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estratégicas, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

• **Incidente de Continuidad de Negocio:** Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

• **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.

• **Amenaza:** Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos**.**

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

• **Riesgo:** Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la entidad**.**

• **Frecuencia:** Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

• **Impacto:** Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad,

interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad.

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

## 9. NORMATIVIDAD

La estrategia de TI se encuentra alineada al marco normativo de la Nación, el Distrito y la Entidad, el cual puede consultarse en el documento Anexo 1 – "208-TIC-Nr-01 Normograma-OTIC" que sirve como herramienta para delimitar las normas que regulan la gestión del proceso de la Oficina TIC, y permiten identificar las competencias, responsabilidades y funciones de la dependencia. Las normas están compendiadas y organizadas para que su accesibilidad permita consultarlas, estudiarlas y promoverlas de una manera más fácil para su aplicación.

### 9.1. Actualización Normograma Oficina TIC

Para la actualización del Normograma de la Oficina TIC se recomienda seguir los siguientes pasos:

- Revisar la vigencia de las normas contenidas en el documento publicado.
- Incluir las nuevas normas aplicables al proceso.
- Validar la información con el responsable y el equipo de trabajo del proceso.
- Remitir a la Oficina Asesora de Planeación para consolidación y publicación.

### 9.2. Periodicidad De Actividades Normograma Oficina TIC:

- *Seguimiento:* Trimestral
- *Reporte a Oficina Asesora Planeación:* Semestral
- *Socialización y Publicación:* Semestral.

### 9.3. Normatividad Relevante Para La Construcción PCN

A continuación, se hace referencia a la normatividad más relevante a partir de la cual tienen sustento el desarrollo e implementación de este Plan de Continuidad del Negocio (PCN), y que está incluida en el Normograma de la Oficina TIC, indicado anteriormente.

| Norma | Número | Fecha de Emisión | | | Tipo | Descripción |
|---|---|---|---|---|---|---|
| Decreto | 612 | 4 | 4 | 2018 | EXTERNO | "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" |
| Resolución | 500 | 10 | 3 | 2021 | EXTERNO | "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". |
| Norma ISO/IEC | 22301: 2012 | 30 | 11 | 2012 | EXTERNO | Sistema de Gestión de la Continuidad del Negocio (SGCN). |

| | | | | | | |
|---|---|---|---|---|---|---|
| Norma GTC-ISO-IEC | 27031: 2016 | 7 | 12 | 2016 | EXTERNO | Guía para Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio. |

| Norma | Número | Fecha de Emisión | | | Tipo | Descripción |
|---|---|---|---|---|---|---|
| Ley | 1581 | 17 | 10 | 2012 | EXTERNO | "Por la cual se dictan disposiciones generales para la protección de datos personales". |
| Decreto | 1008 | 14 | 6 | 2018 | EXTERNO | "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". |
| Norma NTC-ISO/IEC | 27001: 2013 | 25 | 09 | 2013 | EXTERNO | Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada. |
| Norma NTC-ISO/IEC | 27001: 2022 | 25 | 10 | 2022 | EXTERNO | Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada. |
| Norma NTC-ISO/IEC | 27005: 2011 | 7 | 12 | 2011 | EXTERNO | Norma internacional emitida por la Organización Internacional de Normalización (ISO) para Tecnología de la información, Técnicas de seguridad, Gestión de riesgo de seguridad de la información. |
| Norma NTC-ISO/IEC | 31000: 2009 | 7 | 12 | 2011 | EXTERNO | Norma internacional para la Gestión de Riesgos. Proporciona principios y guías para que las organizaciones lleven a cabo su análisis y evaluación de riesgos |
| Manual de Gobierno Digital | Decreto 767 | | | 2022 | EXTERNO | "Es un instrumento centralizado, estandarizado y de fácil uso, donde los usuarios pueden consultar interactivamente información de interés sobre la Política de Gobierno Digital, establecida el 16 de mayo con el Decreto 767 de 2022". |
| Modelo de Seguridad y Privacidad de la Información – MINTIC. | Resolución 500 | | | 2021 | EXTERNO | "El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | habilitar la implementación de la Política de Gobierno Digital. |

*Tabla 2 - Normatividad para desarrollo e implementación del PCN*
*Fuente: Elaboración Propia*

## 10. FORMULACIÓN DEL PLAN

### 10.1. Roles Y Responsables

La CVP estableció unos roles y responsables para administrar, promover, apoyar y hacer seguimiento a la Gestión de Continuidad del Negocio, así como para responder efectiva y oportunamente a incidentes de interrupción.

En tal sentido, es necesario que la entidad implemente el modelo de gobierno propuesto en el presente documento, ya que son estos roles quienes se encargarán de la implementación, mantenimiento y mejora de la Continuidad del Negocio de la CVP.

En la siguiente ilustración, se presenta la estructura para para la Gestión de Continuidad del Negocio en la CVP:

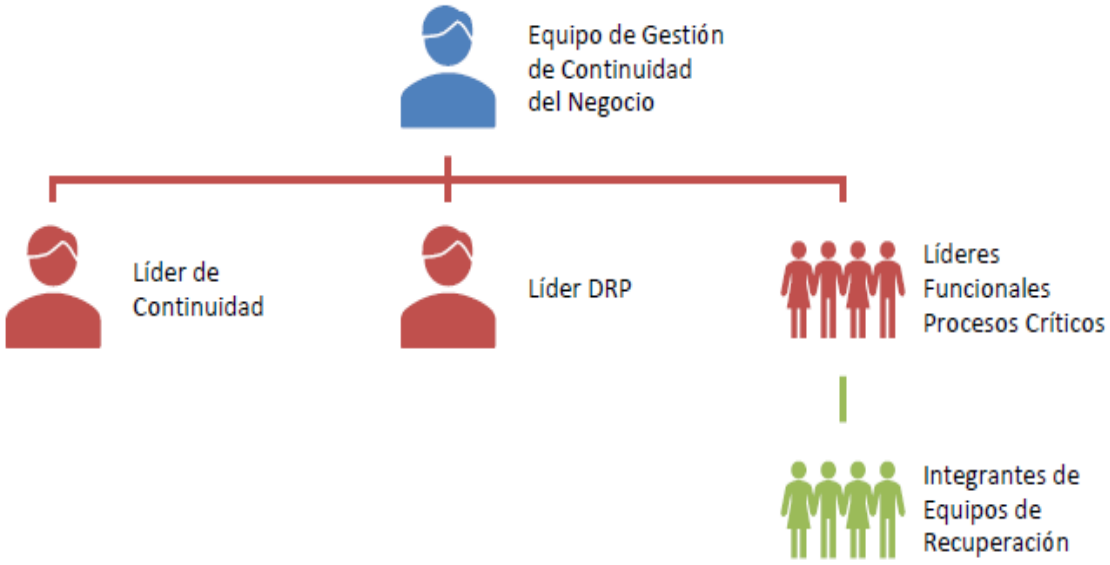


*Ilustración 1 - Estructura Organización Continuidad de Negocio*
*Fuente: Elaboración Propia*

En los siguientes numerales, se describen las responsabilidades para cada uno de los equipos propuestos en la ilustración 1:

#### 10.1.1. Equipo De Gestión De Continuidad Del Negocio

***10.1.1.1. Requisitos del Equipo:***

Se recomienda que este equipo esté conformado por el Líder de Continuidad, el Líder DRP. En caso de requerirse, se podrá convocar a otros participantes.

***10.1.1.2. Perfil del Equipo:***

Los integrantes de este equipo deben contar con conocimientos básicos en Sistemas de Gestión y en Gestión

de Riesgos.

Además, los integrantes del equipo deben contar con los siguientes conocimientos:

- ❖ Norma ISO 22301:2019.
- ❖ Gestión de riesgos orientada en ISO 31001:2018.
- ❖ Manejo de crisis.
- ❖ Lineamientos del sistema de Gestión de Continuidad de Negocio (Directriz, Alcance, Objetivos del sistema).
- ❖ Tener conocimientos relativos a la Continuidad de la Organización, en:
  - ➢ Tiempos objetivos de recuperación.
  - ➢ Procesos críticos.
  - ➢ Proveedores críticos.
  - ➢ Servicios de tecnología críticos.
- ❖ Estrategias de Continuidad del proceso crítico correspondiente.

#### *10.1.1.3. Responsabilidades:*

- Coordinar, verificar y controlar el proceso de implementación, mantenimiento y evaluación de Gestión de Continuidad del Negocio.
- Establecer el alcance de implementación de las Estrategias de Continuidad del Negocio.
- Facilitar la consecución y asignación de recursos que garanticen la implementación de la Estrategia de Continuidad del Negocio.
- Revisar y realizar seguimiento a los requerimientos de entes externos en lo referente a continuidad del negocio.
- Aprobar en primera instancia la Política y Objetivos de Continuidad del Negocio y proponer ajustes cuando se considere pertinente.
- Dar dirección y apoyo a las personas que contribuyen a la eficacia en la Gestión de Continuidad del Negocio promoviendo la mejora continua.
- Realizar seguimiento y evaluación de la Gestión de Continuidad del Negocio, a fin de identificar oportunidades de mejora.
- Llevar a cabo las revisiones periódicas de la Gestión de Continuidad del Negocio.
- Velar por el cumplimiento de los planes de mejoramiento que resulten como evaluación de la Gestión de Continuidad del Negocio.
- Establecer mecanismos que permitan permear la cultura de continuidad de negocio.
- Realizar seguimiento a los compromisos establecidos en las sesiones del equipo.

- Otras funciones que el comité defina, por aprobación unánime.

### 10.1.2. Líder de Continuidad

#### *10.1.2.1. Requisitos del Rol:*

Se recomienda que este rol sea asumido por un integrante del Comité Directivo y que, de igual forma, tenga un conocimiento holístico de la Entidad.

#### *10.1.2.2. Perfil del Rol:*

Además, es necesario que tenga los siguientes conocimientos:

- Conocer todos los elementos de Continuidad del Negocio de la CVP
- Conocer los procesos críticos de la Entidad y prioridad de recuperación.
- Conocer las estrategias de continuidad de la CVP
- Conocer la capacidad de recuperación de la Entidad.
- Conocer los riesgos de interrupción globales, regionales y locales a los que está expuesta la Entidad.

#### *10.1.2.3. Responsabilidades:*

- Validar la planeación de continuidad del negocio, lo cual incluye la definición de los objetivos del sistema, indicadores, metas, recursos y fechas previstas.
- Presentar al comité directivo para su aprobación, la política, objetivos y desempeño del sistema y propender por que se asignen los recursos necesarios para su cumplimiento
- Validar los cambios que surjan y afecten la Gestión de Continuidad del Negocio y presentar al comité directivo el plan para gestionarlos para su aprobación.
- Participar activamente en el Equipo de Gestión de Continuidad del Negocio para validar la pertinencia de actualización del ciclo de continuidad (análisis de impacto al negocio, análisis de riesgos, estrategia, planes y pruebas), de acuerdo con las novedades y cambios organizacionales que puedan afectar el sistema.
- Validar y aprobar el programa de ejercicios buscando siempre la evolución y madurez de la gestión de continuidad del negocio.
- Verificar el cumplimiento de los objetivos de la gestión de continuidad del negocio, la evaluación de indicadores de gestión y definición de planes de acción.
- Propender porque cada vez que se ejecute un ejercicio se generen oportunidades de mejora con base en los resultados.
- Evaluar la respuesta de la Entidad frente a incidentes de continuidad reales y presentar al Comité Institucional de Gestión y Desempeño los resultados y oportunidades de mejora propuestas.
- Presentar al Comité Institucional de Gestión y Desempeño anualmente los resultados de la gestión de continuidad del negocio.
- Verificar el cumplimiento de las acciones de mejora del sistema y de ser necesario gestionar con los

líderes de las acciones el compromiso y cumplimiento de los mismos.

- Proponer acciones para el mejoramiento continuo de la gestión de continuidad del negocio.

### 10.1.3. Líder DRP (Plan de Recuperación Tecnológica)

#### *10.1.3.1. Requisitos del Rol:*

Se recomienda que este rol debe sea asumido por el jefe de la Oficina Tecnología de la Información y las Comunicaciones.

#### *10.1.3.2. Perfil del Rol:*

Además, debe contar con conocimientos en:

- Conocimiento en Gestión / Gobierno de TI (ISACA, COBIT, ITIL V4).
- Conocer la infraestructura tecnológica que habilita los procesos críticos.
- Estrategias y planes DRP con los que cuenta la CVP
- Conocimientos de los procesos críticos y sus tiempos objetivos de recuperación (RTO y RPO).
- Haber participado en el diseño e implementación de estrategias del plan de Recuperación Ante Desastres.
- Haber participado en por lo menos un ejercicio de recuperación de Tecnología (DRP).

#### *10.1.3.3. Responsabilidades:*

- Coordinar las actividades necesarias para el diseño, implementación, gestión y mejora continua de la estrategia DRP.
- Garantizar que la estrategia DRP de la CVP responde y se alinea con los requerimientos de los procesos críticos de negocio.
- Gestionar los cambios tecnológicos que surjan y afecten el sistema de gestión de continuidad del negocio.
- Participar activamente en el Equipo de Gestión de Continuidad de negocio para validar la pertinencia de actualización de las estrategias y planes DRP de acuerdo con las novedades y cambios organizacionales que puedan afectar el sistema.
- Proponer el programa de ejercicios DRP buscando siempre la evolución y madurez de la gestión de continuidad del negocio.
- Evaluar el cumplimiento de los criterios de éxito de los ejercicios DRP y proponer planes de acción de mejora.
- Evaluar la respuesta de la Entidad frente a incidentes de continuidad reales que implican la activación de los planes DRP parcial o totalmente.
- Presentar a la dirección anualmente los resultados de la gestión de la estrategia DRP.
- Garantizar que las acciones de mejora y correctivas de la Estrategia de DRP se cumplan.
- Proponer acciones de mejora y correctivas para el mejoramiento continuo de la Sistema de Gestión de Continuidad del Negocio.

### 10.1.4. Líder Funcional

#### *10.1.4.1. Requisitos del Rol:*

Este rol debe ser asumido por los líderes de cada uno de los procesos críticos de la CVP, identificados en el Análisis de Impacto al Negocio - BIA.

#### *10.1.4.2. Perfil del Rol:*

Debe contar con conocimientos en:

- Conocer los integrantes principales y alternos del equipo de recuperación de sus procesos críticos.
- Conocer los subproceso y actividades críticas de sus procesos, así como sus tiempos objetivos de recuperación.
- Conocer sus proveedores, servicios de tecnología y registros vitales críticos.
- Conocer las estrategias de continuidad de sus procesos críticos.
- Conoces los planes de continuidad de sus procesos críticos.
- Participar activamente en pruebas de continuidad.

#### *10.1.4.3. Responsabilidades:*

- Mantenerse actualizado y garantizar el cumplimiento de lo descrito para su rol en el plan de continuidad.
- Garantizar la correcta gestión del proceso de continuidad del negocio, acorde con los requerimientos de las partes interesadas.
- Actualizar el plan de continuidad a su cargo cuando haya cambios organizacionales y operacionales.
- Mantener actualizado el Call tree o árbol de llamadas (matriz en el cual se encuentran relacionados los datos de contacto de las personas que hacen parte del proceso), de acuerdo con los cambios en los datos de contacto y cambios en los integrantes del equipo de recuperación.
- Verificar la disponibilidad y el funcionamiento del software requerido en ambiente DRP.
- Verificar la disponibilidad de los recursos mínimos necesarios para la continuidad del proceso crítico.
- Verificar que se está realizando backup a los archivos vitales, identificados en el análisis de impacto al negocio.
- Participar activamente en ejercicios, capacitaciones u otras actividades de continuidad del negocio.

### 10.1.5. Equipos de Recuperación

#### *10.1.5.1. Requisitos de los Equipos:*

Este equipo debe ser asumido por los colaboradores principales y alternos que se encargan de dar continuidad a la operación de cada uno de los procesos críticos.

#### *10.1.5.2. Perfil de los Equipos:*

Debe contar con conocimientos en:

- Conocer los subproceso y actividades críticas de sus procesos, así como sus tiempos objetivos de recuperación.
- Conocer sus proveedores, servicios de tecnología y registros vitales críticos.
- Conocer las estrategias de continuidad de sus procesos críticos.
- Conocer los planes de continuidad de sus procesos críticos.
- Participar activamente en pruebas de continuidad.

#### *10.1.5.3. Responsabilidades:*

- Participar activamente en la actualización de su plan de continuidad correspondiente.
- Notificar al líder funcional sobre algún cambio en sus datos de contacto para mantener actualizado el call tree o árbol de llamadas.
- Verificar disponibilidad y funcionamiento del hardware requerido para el plan de continuidad.
- Verificar la disponibilidad de los recursos mínimos necesarios para la recuperación del proceso.
- Realizar ejercicios de software considerando claves de acceso en los equipos que se utilizarán para operar durante el evento de interrupción.
- Verificar que se está realizando backup a los archivos vitales.
- Participar activamente en ejercicios, capacitaciones u otras actividades de continuidad del negocio.
- Reportar las actualizaciones y cambios en su proceso que afecten el plan de continuidad del negocio
- Verificar la disponibilidad de recursos necesarios para garantizar la recuperación y retorno a la normalidad de la Entidad.
- Participar activamente en ejercicios, capacitaciones u otras actividades de continuidad del negocio.
- Reportar las actualizaciones y cambios en el proceso que afecten el plan de continuidad del negocio.

### 10.2. Modelo De Gobierno Para La Continuidad Del Negocio

#### 10.2.1. Política De Continuidad Del Negocio

La Caja de Vivienda Popular se compromete con dar continuidad a los servicios y procesos críticos de la entidad, proporcionando los recursos necesarios para el mantenimiento y mejora continua de sus estrategias de continuidad que permitan responder ante incidentes que puedan interrumpir su operación, minimizando los impactos y afectaciones hacia sus grupos de interés.

#### 10.2.2. Lineamientos Para La Gestión De La Continuidad Del Negocio

- La Matriz de Riesgos forma parte integral del plan de continuidad del negocio. Los riesgos de continuidad identificados en la matriz son identificados para preparar una estrategia de mitigación.

- Se debe realizar por lo menos una vez al año pruebas del plan de continuidad para validar su funcionalidad y que se cumple con los RPO (Recovery Point Objective) y al RTO (Recovery Time Objective), para lo cual la Alta Dirección de la entidad debe proveer los medios y recursos que se requieren.

- El plan de continuidad debe ser actualizado y mejorado de acuerdo con los resultados de los ejercicios, en cuanto a estructura, procesos, recursos, capacitación y demás factores que inciden en la ejecución del plan.

- Todos los sistemas de información que soportan los procesos críticos de La CVP, deben tener un Plan de Recuperación de Desastres (DRP) que le permita a la entidad garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupción mayor.

- La CVP propenderá por seguir los lineamientos metodológicos definidos en la norma ISO 22301:2019 para construir y actualizar su Plan de Continuidad de Negocio.

- La CVP debe establecer estrategias para asegurar que los terceros que soportan sus funciones críticas de negocio presten los servicios contratados, inclusive ante eventos de desastre o interrupción mayor.

- Las nuevas iniciativas tecnológicas, o cambios de proveedores críticos, deben incorporar los requerimientos de Continuidad de Negocio dentro de las fases del proyecto e implementar y probar la estrategia requerida antes de entrar a producción u operación.

- Las estrategias y planes de continuidad definidos para responder a un evento de crisis deben ser revisados y aprobados por la Alta Dirección de la entidad.

- Los dueños de los procesos serán los responsables de mantener documentados los planes de continuidad y de actualizar las actividades a su cargo. Así mismo, son responsables de informar cualquier cambio al Líder de Continuidad de la Entidad.

- La CVP debe implementar un programa de capacitación y sensibilización permanente, con el objeto de dar a conocer esta política y difundir la cultura de Continuidad del Negocio entre los colaboradores, proveedores y asociados del negocio.

### 10.3. Roles Y Responsabilidades Para El Manejo De Eventos De Interrupción Y Crisis

En la siguiente ilustración, se presenta la estructura propuesta para el manejo de eventos de interrupción y crisis.

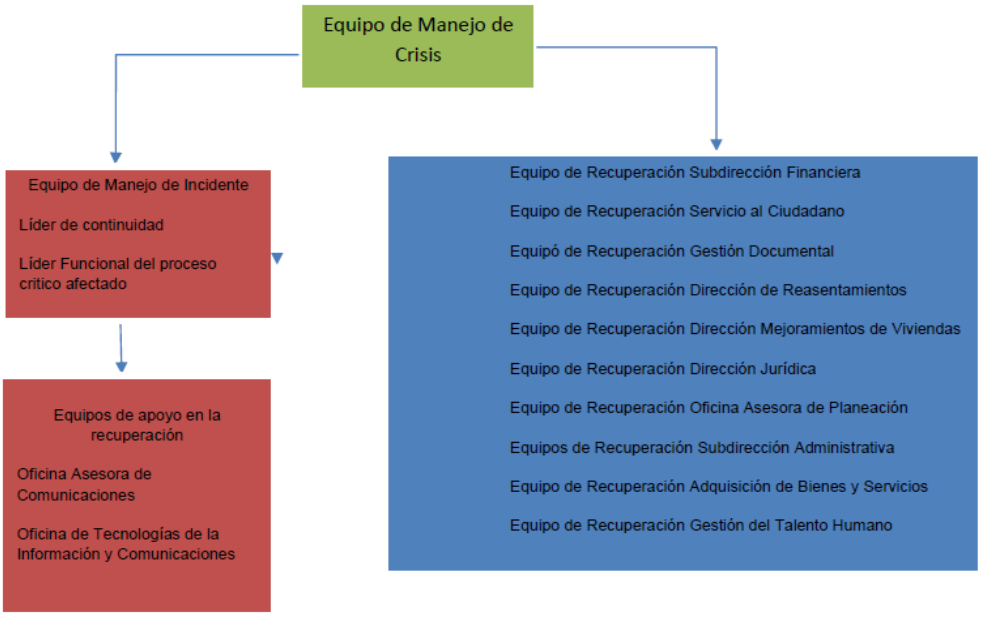


*Ilustración 2 - Estructura para el manejo de eventos de interrupción y crisis*
*Fuente: Elaboración Propia*

En los siguientes numerales, se describen las responsabilidades que tendrán los equipos propuestos en la ilustración 2, cuando ocurran incidentes de interrupción y crisis.

#### 10.3.1. Equipos De Manejo De Crisis:

**Responsabilidades Durante La Crisis**

- El Equipo de Crisis se debe reunir o comunicar periódicamente, con el fin de hacer seguimiento a la recuperación de la operación de la CVP y poder dar una respuesta oportuna a las situaciones que se estén presentando. Dichas reuniones pueden desarrollarse telefónicamente, vía web o presencialmente.

- Durante la primera semana de crisis, el Equipo de Crisis se debe reunir todos los días, a partir de la segunda semana de ocurrido el evento de interrupción, el Equipo en consenso, decidirá cada cuanto deben reunirse.

- Cada integrante del Equipo de Crisis debe presentar la siguiente información:

- Un informe del proceso de notificación de activación de las estrategias y planes de continuidad
- Un informe sobre el avance de recuperación de sus procesos
- Inconvenientes que se estén presentando en la recuperación de los procesos críticos

- El Equipo de Crisis de manera conjunta, deberá dar respuesta a cada uno de los inconvenientes que se estén presentando y generar estrategias.

- El Equipo de Crisis paralelamente para garantizar la continuidad de sus procesos críticos, debe crear sesiones enfocadas a los procesos de retorno a la normalidad.

  - Se deben crear grupos de trabajo específicos al interior enfocados a:
  - Recuperación de las instalaciones afectadas.
  - Recuperación de la información.
  - Estrategias Financieras para garantizar los recursos económicos para la continuidad y retorno a la normalidad.

- Estrategias de recuperación de imagen.

- El Equipo de Crisis debe discutir y analizar la viabilidad y factibilidad de cada uno de estos planes de reconstrucción, recuperación y retorno, priorizarlos y asignar los recursos para la puesta en marcha de estos.

- El Equipo de Crisis debe además crear un cronograma de seguimiento de estos planes y garantizar su cumplimiento.

- Una vez se vaya cumpliendo cada uno de los planes de reconstrucción, recuperación, el Equipo de Crisis se encarga de notificar el retorno a la normalidad.

- El Equipo de Crisis debe evaluar la respuesta al incidente o crisis e identificar oportunidades de mejora.

### 10.3.2. Equipo De Manejo De Incidentes De Interrupción:

**Responsabilidades Durante Un Incidente De Interrupción O Crisis**

- El Equipo de Manejo de Incidentes de Interrupción deberá analizar el incidente y definir si están la capacidad y cuentan con los recursos para solucionar el incidente de interrupción o si se trata de una potencial crisis, en cuyo caso se deberá notificar y activar el Equipo de Manejo de Crisis.

- El Equipo de Manejo de Incidentes de Interrupción revisará los Tiempos Objetivos de Recuperación (definidos en el Análisis de Impacto al Negocio) de

los procesos afectados y la fecha (día y hora) de la interrupción, como herramienta para la toma de decisión en cuanto a la activación o no de los planes de continuidad del negocio.

- El Equipo de Manejo de Incidentes de Interrupción deberá realizar una valoración del incidente para determinar si se puede dar respuesta y controlar por parte del Equipo de Manejo de Incidentes de Interrupción o si es necesario escalar al Equipo de Manejo de Crisis.

- Deberán convocar a los equipos de apoyo de recuperación, dependiendo del evento.

- Realizar seguimiento permanente a la recuperación de los procesos críticos.

- Oficializar el calendario del retorno a la normalidad y coordinar que el traslado a las instalaciones de la CVP se realice de acuerdo con los lineamientos establecidos por el Equipo de Manejo de Incidentes de Interrupción.

- Notificar a los líderes de los procesos críticos, la logística de retorno a operación regular.

- Entregar el informe de cierre del evento de Interrupción al Equipo de Manejo de Crisis.

### 10.3.3. Líder De Continuidad:

**Responsabilidades Durante Un Incidente De Interrupción O Crisis**

- Una vez el Líder de Continuidad reciba el aviso del incidente, debe hacer seguimiento al incidente y evaluarlo, de ser necesario, proceder a convocar al Equipo de Crisis.

- Administrar posibles incidentes de interrupción que enfrente la CVP por parte del Equipo de Manejo de Incidentes de Interrupción, asegurando la continuidad de los procesos críticos, de acuerdo con los objetivos de recuperación definidos en el Análisis de Impacto al Negocio – BIA.

- El Equipo de Manejo de Incidentes se encargará de notificar a los líderes funcionales de los procesos afectados, de acuerdo con el call tree de llamadas, las decisiones y estrategias definidas, en los casos en que el incidente se escale al Equipo de Manejo de Crisis, la notificación estará a cargo de este equipo.

- Una vez convocado al Equipo de Crisis, se encarga de entregar el informe inicial del incidente, que incluya si es necesario, la siguiente información: estado de la infraestructura afectada: descripción del incidente, fecha y hora, diagnóstico o acciones realizadas, si hubo necesidad de evacuación de la edificación, detalle de los daños preliminares, estado de evacuación, colaboradores heridos, fallecidos y desaparecidos por área.

- Si la decisión del equipo de crisis es activar los

planes de continuidad, el líder de continuidad debe notificar a los líderes de los equipos de apoyo para la recuperación que se requieran, para que activen sus planes.

- Monitorear continuamente durante el evento de interrupción, la recuperación de los procesos hasta que el incidente sea estabilizado y la situación vuelva a la normalidad.

- Convocar al Equipo de Crisis con el fin de entregar un reporte periódico del estado de recuperación de la organización y llevar los casos que se deben analizar para tomar dediciones críticas que afecten la recuperación.

- Una vez sea posible el retorno a la normalidad, debe convocar al equipo de crisis para que aprueben la decisión, definirá el cronograma de retorno y liderará el proceso en colaboración con los líderes gerenciales y funcionales.

- Evaluar la respuesta al incidente de continuidad del negocio que se presentó, generar y presentar un informe al comité directivo.

- Identificar y gestionar acciones de mejora a la gestión de continuidad del negocio, teniendo en cuenta los resultados de la evaluación de respuesta al incidente.

### 10.3.4. Líderes Funcionales:

**Responsabilidades Durante Un Incidente De Interrupción O Crisis**

- Seguir los procedimientos descritos en el plan de emergencias de la Entidad, ante un evento de interrupción.

- Solicitar al brigadista de emergencias el reporte de evacuación de su equipo funcional, para identificar el estado de cada uno de los colaboradores del proceso y determinar disponibilidad.

- Reportar al Líder de Continuidad la mayor información disponible del evento de interrupción.

- Notificar a su equipo funcional, la activación del plan de continuidad, una vez sea notificado por parte del Equipo de Crisis.

- Ejecutar todas las alternativas de recuperación definidas para cada proceso crítico, durante el evento de interrupción.

- Realizar control y seguimiento al cumplimiento de las responsabilidades de cada equipo funcional.

- Identificar oportunidades de mejora de la gestión de continuidad del negocio.

- Solucionar y dar soporte a inconvenientes operativos que se puedan presentar durante la recuperación.

### 10.3.5. Equipos De Recuperación De Procesos Críticos:

**Responsabilidades Durante Un Incidente De Interrupción O Crisis**

- Seguir las indicaciones de activación, notificación y movilización que sean entregadas por el líder funcional.
- Reportar al líder funcional la mayor información disponible del evento de interrupción.
- Seguir los lineamientos del plan de continuidad del negocio.
- Identificar oportunidades de mejora según resultados de respuesta a incidentes.
- Reportar al Líder Funcional sus condiciones de salud física y mental, en caso de presentarse incidentes de continuidad que pongan en riesgo su integridad.

### 10.3.6. Equipos De Apoyo En La Recuperación:

**Responsabilidades Durante Un Incidente De Interrupción O Crisis**

- De ser requerido por el Equipo de Crisis deberá activar el plan de recuperación correspondiente.
- Diseñar estrategias y planes de trabajo para la reconstrucción de la Entidad.
- Recuperación de la imagen y reputación de la Entidad.
- Apoyar al Oficial de Continuidad en la construcción del informe inicial del incidente y recolectar toda la información necesaria para presentar un contexto detallado de la situación al Equipo de Crisis.
- Asesorar y acompañar al Equipo de Crisis en la respuesta y atención de incidentes de continuidad, brindando conceptos y conocimientos sobre el SGCN.

## 10.4. Fases De Continuidad Del Negocio

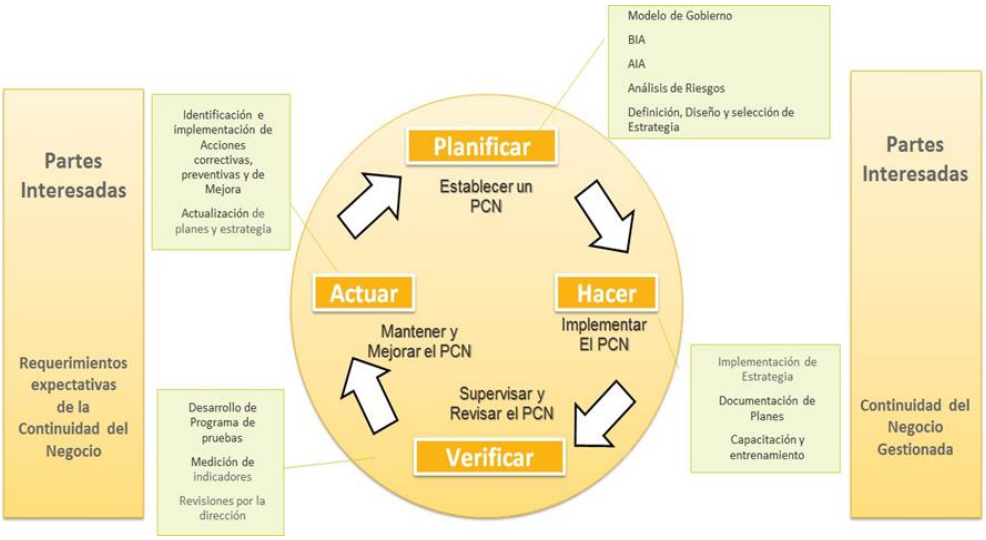


*Ilustración 3 - Fases del SGCN*
*Fuente: Elaboración Propia*

### 10.4.1. BIA (Análisis de Impacto al Negocio)

El Análisis de Impacto del Negocio es una etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción. El principal objetivo de este análisis es identificar los procesos críticos de la entidad, los recursos utilizados para soportar la operación de estos procesos (proveedores, servicios de IT, puestos de trabajo, herramientas y hardware), así como estimar los tiempos objetivos de recuperación para sus procesos críticos. En el siguiente esquema se presentan las actividades realizadas durante el presente estudio:


*Ilustración 4 - Metodología BIA*

Fuente: Elaboración Propia

### 10.4.2. BIA Táctico (Identificación De Los Procesos Críticos)

La calificación de criticidad para los procesos se define con cada uno de los líderes de los procesos de Caja de Vivienda Popular (CVP) tomando como base el mapa de procesos, los eventos de interrupción incluidos en el alcance del análisis y teniendo en cuenta los siguientes criterios y umbral de criticidad:

| Nivel de impacto | Impacto en imagen | Impacto al ciudadano | Impacto legal | Detención o impacto a otros procesos | Impacto operación al Negocio |
|---|---|---|---|---|---|
| 1 | Se afecta la imagen de algún área de la organización | No se generan impactos a los ciudadanos | No existe ningún impacto legal | Si el proceso se detiene, no hay afectación sobre otros procesos | Se podría generar un impacto alto para la Caja de Vivienda Popular al detenerse el proceso por más de 15 días |
| 2 | Se afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores | Retraso en los tiempos de respuesta al ciudadano | Investigaciones internas disciplinarias. | Si el proceso se detiene afecta o detiene a un proceso no misional | Se podría generar un impacto alto para la Caja de Vivienda Popular al detenerse el proceso por un rango de tiempo entre 5 y 10 días |
| 3 | Se afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos | Reclamaciones o quejas de los usuarios por no prestación oportuna del servicio | Silencio Administrativo Positivo | Si el proceso se detiene puede afectar un proceso misional | Se podría Generar un impacto alto para la Caja de Vivienda Popular al detenerse el proceso por un rango de tiempo entre 5 y 3 días |
| 4 | Se afecta la imagen de la Entidad con un efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal | Incumplimiento en la promesa de servicio | Investigaciones penales o fiscales | Si el proceso se detiene, puede detener más de un proceso misional | Se podría generar un impacto alto para la Caja de Vivienda Popular al detenerse el proceso por un rango de tiempo entre 3 y 1 día |

*Tabla 3 - Criterios de Criticidad*
*Elaboración Propia*

| CRITICIDAD | DEFINICIÓN |
|---|---|
| **PROCESOS CRÍTICOS** | Aquellos cuya evaluación es igual o superior a 3.<br>A estos procesos se les definirá e implementará una Estrategia de negocio y Planes de Continuidad. |
| **PROCESOS NO CRÍTICOS** | Aquellos cuya evaluación es inferior a 3.<br>Estos no se tendrán en cuenta dentro de la Estrategia y Planes de Continuidad. |

*Tabla 4 - Umbral de Criticidad*

*Elaboración Propia*

### 10.4.3. BIA Operativo (Recopilación De Información Cualitativa)

Mediante sesiones de trabajo con los líderes de cada proceso crítico se documenta la siguiente información cualitativa:

#### *10.4.3.1. RTO (Recovery Time Objective)*

Es el tiempo máximo que puede estar detenido un proceso crítico antes de afectar considerablemente a la entidad. Este análisis se hace con el fin de establecer las ventanas de tiempo máximas que soportan los procesos críticos en caso de un evento de interrupción de la operación y así garantizar que el proceso de recuperación cubra las necesidades del usuario o ciudadano.

En el Análisis de Impacto al Negocio – BIA se definen los RTO a partir de la identificación del momento en el tiempo en que sería más crítico que sucediera el evento de interrupción de la operación; esta información es vital para que la entidad pueda definir bajo qué tiempo se estaría alineando la estrategia de negocio teniendo en cuenta sus necesidades.

Para el cálculo del RTO se cuenta con la experiencia y conocimientos de cada uno de los líderes de los procesos críticos que participen en las sesiones de trabajo.

#### *10.4.3.2. RPO (Recovery Point Objective)*

Es el punto máximo de tolerancia a la pérdida de información para un proceso crítico. Este resultado es necesario para definir e implementar estrategias que garanticen la disponibilidad de la información con la actualización requerida en caso de un evento de interrupción de la operación.

#### *10.4.3.3. Periodos Críticos*

Al momento de un evento de interrupción de la operación resulta importante conocer cuáles procesos se encuentran en su momento más crítico y cuáles no con el fin de darle mayor prioridad a aquellos que lo requieran. El concepto “momento más crítico” se refiere a los periodos en los que por ejemplo se tiene mayor volumen de operación, se deben entregar informes internos o externos, cierres de mes, entre otros.

#### *10.4.3.4. Proveedores Críticos*

Para el desarrollo de la estrategia también es importante identificar si existen Organizaciones externas que apoyen los procesos críticos, ya sea suministrando productos o servicios, o realizando directamente las actividades propias del proceso bajo un esquema de subcontratación.

#### *10.4.3.5. Servicios de Tecnología*

Esta sección entrega una lista de los Servicios de Tecnología que son requeridos para la ejecución de los procesos críticos, con el objetivo que sean incluidos en la estrategia de recuperación definida por el área de TI y de esta forma se garantice su disponibilidad durante un evento de interrupción.

### *10.4.3.6. Registros Vitales*

La Organización cuenta con una infraestructura de tecnología sobre la cual se tiene la mayor parte de la información de los procesos, sin embargo, pueden existir archivos usados en la operación normal que no están incluidos en esta estructura, es decir, se almacenan localmente en los equipos (PC). Adicionalmente, como registros vitales también se consideran registros físicos que no tienen respaldo virtual y cuya custodia y almacenamiento se realiza en las instalaciones principales.

### *10.4.3.7. Resultados BIA:*

En la siguiente grafica se puede ver la secuencia de recuperación de los procesos críticos de acuerdo con los RTO definidos por los líderes de proceso y la calificación de estos.

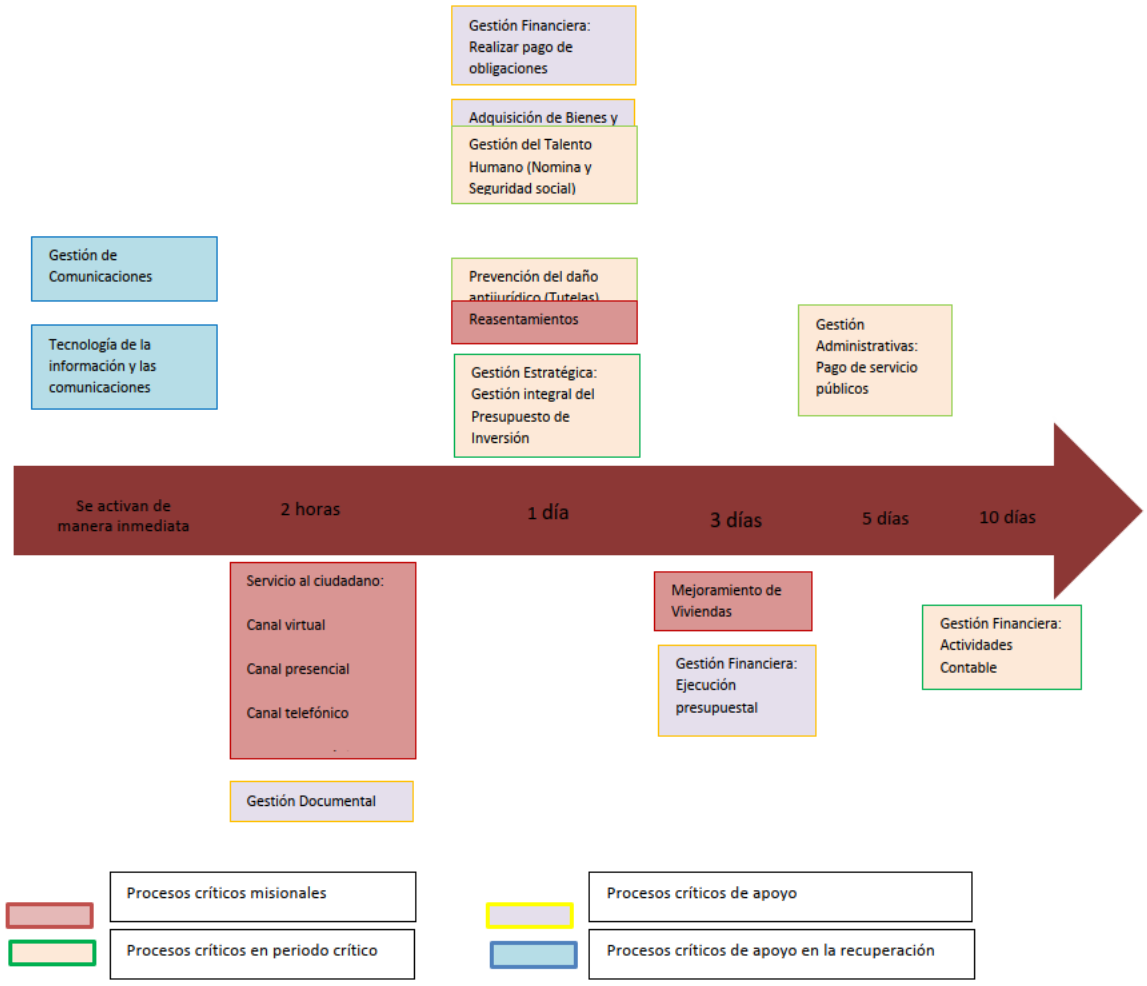


*Ilustración 5 - Secuencia de recuperación de los procesos críticos*
*Fuente: Elaboración Propia*

A continuación, se relacionan los servicios de tecnología que requieren los procesos críticos para operar:

| SERVICIOS DE TECNOLOGIA INTERNOS | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESO | ORFEO | SICAPITAL | GLPI | GIS | SI CAPITAL- ENCAJA | SIMA | SICAPITAL - LIMAY | SISTEMA MISIONAL | SISTEMA DE GESTION INTERNA - AGENDA | PÁGINA WEB | SICAPITAL- SISCO | SICAPITAL- OPGET | SICAPITAL - AYUDAS TEMPORALES |
| Gestión Estratégica | | | | | | | | | | X | | | |
| Prevención del Daño Antijurídico | X | | | | | | | | | | | | |
| Gestión de Comunicaciones | | | | | | | | | | X | | | |
| Gestión de Talento Humano | | X | | | | | | | | | | | |
| Tecnología de la Información y las Comunicaciones | X | X | X | X | X | X | | X | X | X | X | X | |
| Reasentamientos | X | | X | X | X | X | | | | | | | |
| Mejoramiento de Vivienda | X | | | | | | | X | | | X | | |
| Servicio al Ciudadano | X | | | | | X | | | X | | | | |
| Gestión Documental | X | | | | X | | | | | | | | |
| Gestión Administrativa | | | | | | X | | | | | X | | |
| Adquisición de Bienes y Servicios | X | | | | | X | | | | | X | | |
| Gestión Financiera | X | X | | | | | X | | | | X | X | X |

*Tabla 5 - Relación de Aplicativos Críticos Propios*
*Fuente: Elaboración Propia*

| SERVICIOS DE TECNOLOGIA INTERNOS | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PROCESO | GESTIÓN ESTRATÉGICA | PREVENCIÓN DEL DAÑO ANTIJURÍDICO | GESTIÓN DE COMUNICACIONES | TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES | MEJORAMIENTO DE VIVIENDA | SERVICIO AL CIUDADANO | GESTIÓN ADMINISTRATIVA | ADQUISICIÓN DE BIENES Y SERVICIOS | GESTIÓN FINANCIERA |
| PLATAFORMAS BOGDATA – PMR | X | | | | | | X | | X |
| PLATAFORMA SEGPLAN | X | | | | | | | | |
| PLATAFORMA SUIPT | X | | | | | | | | |
| PLATAFORMA SUIT | X | | | | | | | | |
| PLATAFORMA STORM USER | X | | | | | | | | |
| SIPROJWEB | | X | | | | | | | |
| PAGINA RAMA JUDICIAL | | X | | | | | | | |
| Adobe Illustrator | | | X | | | | | | |
| REVIT | | | | | X | | | | |
| MAGIC | | | | | X | | | | |
| FULLCRUM | | | | | X | | | | |
| SIVICOF | | | | | | | | X | |
| PAC | | | | | | | | | X |
| CHIP LOCAL | | | | | | | | | X |
| BOGOTA CONSOLIDA | | | | | | | | | X |
| MUISCA | | | | | | | | | X |
| OFICINA VIRTUAL DE HACIENDA | | | | | | | | | |
| BOGOTA TE ESCCUHA | | | | X | | X | | | |
| SECOP | | | | X | | | X | X | |

*Tabla 6 - Relación de Servicios de Tecnología de Terceros*

*Fuente: Elaboración Propia*

A continuación, se relacionan los principales proveedores críticos identificados:

| PROVEEDOR | SERVICIO CONTRATADO |
|---|---|
| **ETB** | PÁGINA WEB, CONEXIÓN A INTERNET, RED INTERNA, VPN, PROVEEDOR HOSTING |
| **SECRETARÍA DE HACIENDA DISTRITAL** | PLATAFORMAS BOGDATA – PMR |
| **SECRETARÍA DISTRITAL DE PLANEACIÓN** | PLATAFORMA SEGPLAN |
| **DEPARTAMENTO NACIONAL DE PLANEACIÓN** | PLATAFORMA SUIPT |
| **DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA** | PLATAFORMA SUIT |
| **SECRETARÍA DISTRITAL DE AMBIENTE** | PLATAFORMA STORM USER |
| **NOGUERA SERRANO** | FIRMA DE ABOGADOS |
| **PUBLICA** | OPERADOR LOGISTICO |
| **ESRI** | PROVEEDOR PARA SOPORTE PARA CARTOGRAFÍA, PARA REAS Y PARA VIVIENDA |
| **Google** | PROVEEDOR DE CORREO ELECTRÓNICO GMAIL |
| **CARMERFIRMA Y CERTICAMARA** | PROVEEDOR FIRMA Y CERTIFICADOS DIGITALES |
| **KUBERNETS** | SOPORTE AL SERVICIO MISIONAL (OKU), |
| **FORTINET (ADSUME)** | SOPORTE CONEXIONES VPN |
| **472** | PROVEEDOR DE CORRESPONDENCIA |
| **DELIMA MARSH** | INTERMEDIARIO DE SEGUROS |
| **SEGURIDAD CENTRAL** | CONTRATISTAS PARA VIGILANCIA |

*Tabla 7 - Relación de Proveedores Críticos*
*Fuente: Elaboración Propia*

El detalle de la descripción de criticidad y los resultados de la evaluación se encuentra en el informe Anexo 2 – “Informe Análisis De Impacto Al Negocio (BIA)”

En cuanto a la información de periodos críticos, por día, mes y/o semana, registros vitales y requerimientos mínimos de operación para cada uno de los procesos críticos, se encuentra en cada uno de los formularios del BIA Operativo por proceso crítico.

### 10.4.4. Análisis De Riesgos De Interrupción

En esta etapa se identifican y analizan las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura física, información y proveedores externos, que podrían ocasionar riesgos de continuidad para la CVP, con el fin de medir el nivel del riesgo.

La entidad cuenta con el Anexo 3 – "Mapa De Riesgos De Continuidad Del Negocio".

#### *10.4.4.1. Metodología de análisis de riesgo.*

A continuación, se detalla la Metodología de Análisis de Riesgos, la cual cubre los aspectos relacionados a continuación:

- Identificación de riesgos de continuidad
- Cálculo del riesgo inherente
- Evaluación de controles
- Cálculo del riesgo residual
- Plan de Acción

#### *10.4.4.2. Identificación del riesgo.*

A continuación, se relacionan los riesgos identificados y se describen las posibles amenazas que conllevan a una interrupción en la operación.

Las vulnerabilidades están enmarcadas en los siguientes factores de la continuidad:

- No disponibilidad de las Personas
- No disponibilidad de la Infraestructura física
- No disponibilidad de la Infraestructura de tecnología
- No disponibilidad de la Información
- No disponibilidad de los Proveedores

| Causa Inmediata | Causa Raíz | Descripción del Riesgo |
|---|---|---|
| Indisponibilidad de la sede de la Caja de Vivienda Popular | Desastres naturales como terremotos, inundaciones por lluvias, tormentas eléctricas | Posibilidad de que el proceso se interrumpa ante la indisponibilidad de la sede de la CVP, debido un desastre natural en la ciudad de Bogotá |
| Indisponibilidad de la sede de la Caja de Vivienda Popular | Incendio, inundación interna, manifestaciones, desorden público, protestas | Posibilidad de que el proceso se interrumpa ante la indisponibilidad de la sede de la CVP, debido a incendio, inundaciones internas, bloqueos o desorden público que impidan el acceso |
| Indisponibilidad de registros vitales | Pérdida, destrucción y corrupción de los registros vitales | Posibilidad de que el proceso se interrumpa ante una indisponibilidad de los registros vitales, debido a pérdida, destrucción y/o corrupción de los registros vitales |
| Indisponibilidad de los servicios de tecnología de la CVP | Falla de energía, falla de software, falla de hardware, incendio en el centro de cómputo, inundación en el centro de datos, sabotaje | Posibilidad de que el proceso se interrumpa ante una indisponibilidad de los servicios de tecnología, debido a falla de energía, falla de software, falla de hardware, incendio en el centro de cómputo, inundación en el centro de datos, sabotaje |
| Ausentismo igual o mayor al 50% de los colaboradores | Pandemia, endemias, renuncias masivas, demoras o inconvenientes en los procesos de contratación de personal | Posibilidad de que el proceso se interrumpa ante un ausentismo masivo igual o mayor al 50% de los colaboradores, debido a contagios masivos, renuncias masivas, demoras o inconvenientes en los procesos de contratación de personal |
| Falla en la presentación del servicio contratado por parte del proveedor | Ausencia de planes de continuidad del servicio, ausencia de ANS ante incidentes de interrupción del proveedor | Posibilidad de que el proceso se interrumpa ante la falla en la presentación del servicio contratado por parte del proveedor, debido a Ausencia de planes de continuidad del servicio, ausencia de ANS ante incidentes de interrupción. |

*Tabla 8 - Relación de riesgos de interrupción*
*Fuente: Elaboración Propia*

#### *10.4.4.3. Cálculo del riesgo inherente*

El riesgo de continuidad se evalúa con dos (2) variables de medición, una que expresa el impacto del riesgo si ocurriera y otra que expresa la frecuencia de que el riesgo ocurra. En consecuencia, para la evaluación del riesgo de continuidad se utilizar las tablas “Criterios de Probabilidad” y “Criterios de Impacto”, las cuales contienen los criterios que permiten efectuar la evaluación.

**TABLA CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD**

| | Frecuencia de la Actividad | Probabilidad |
|---|---|---|
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año | 20% |
| Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año | 40% |
| Media | La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año | 60% |
| Alta | La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año | 100% |

*Ilustración 6 - Criterios de probabilidad*

*Fuente: Elaboración Propia*

**TABLA CRITERIOS PARA DEFINIR EL NIVEL DE IMPACTO**

| | Afectación Económica (o presupuestal) | Pérdida Reputacional |
|---|---|---|
| Leve 20% | Afectación menor a 10 SMLMV | El riesgo afecta la imagen de alguna área de la organización |
| Menor-40% | Entre 10 y 50 SMLMV | El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores |
| Moderado 60% | Entre 50 y 100 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos |
| Mayor 80% | Entre 100 y 500 SMLMV | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal |
| Catastrófico 100% | Mayor a 500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país |

*Ilustración 7 - Criterios de impacto*
*Fuente: Elaboración Propia*

#### *10.4.4.4. Cálculo del riesgo residual*

Teniendo en cuenta la información seleccionada en el impacto inherente y los controles aplicados para el riesgo, la matriz esta parametrizada para atribuir el (%) correspondiente de acuerdo con la tabla de probabilidad.

#### *10.4.4.5. Definición del plan de acción*

Para mitigar los riesgos se definieron planes de acción que busquen reducir la exposición de la entidad a través de la creación de nuevos controles o la implementación de modificaciones a los controles existentes.

El Líder de Continuidad hace seguimientos de forma trimestral a los planes, y reportar su avance al Comité de Continuidad del Negocio, con el fin de tomar las decisiones respectivas para su tratamiento y mitigación.

Los riesgos clasificados como aceptables y tolerables son evaluados continuamente por el Líder de Continuidad, garantizando la eficacia de los controles. Si se percibe un incremento en el nivel del riesgo se debe de realizar la respectiva reclasificación y acordar acciones.

### 10.4.5. Estrategia De Continuidad Del Negocio

El diseño de la estrategia de continuidad consiste en definir las acciones que se deben tomar con el objetivo de restablecer las operaciones del negocio, en el plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas. Saben qué recursos necesitan. A continuación, se relacionan las estrategias de continuidad para cada uno de los escenarios de interrupción:

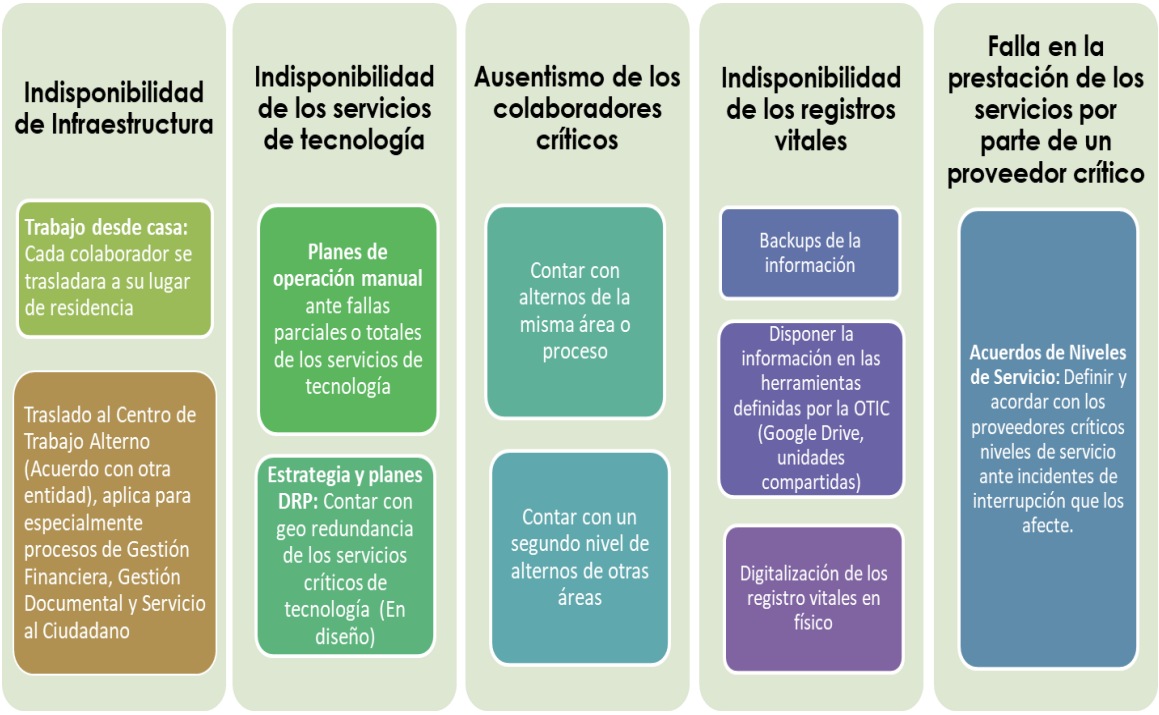


*Ilustración 8 - Estrategias de Continuidad*
*Fuente: Elaboración Propia*

### 10.4.6. Planes de Continuidad y Documentación De Procedimientos De Continuidad

Todos los responsables de las actividades criticas incluidas en la estrategia de continuidad deberán participar en el desarrollo de procedimientos e instrucciones claras e inequívocas para que permitan la gestión del evento que active el plan; con el fin de dar continuidad a las actividades priorizadas procurando el cumplimiento de los objetivos de recuperación que se hayan definido durante el análisis de impacto, la gestión de riesgo y la identificación de escenarios. Los diferentes documentos que conformaran los procedimientos de continuidad incluyen, entre otros:

- Protocolo de comunicaciones durante la continuidad (quien reportará, a quién y por qué medios).
- Pasos detallados y específicos para activar la estrategia seleccionada para operar los servicios en contingencia
- Pasos detallados que aplicaran los responsables de realizar la recuperación de los recursos afectados por el o los eventos que generaron la activación del plan de continuidad
- Pasos detallados que se deben aplicar para reactivar los servicios en la infraestructura una vez se ha superado el evento que genero la pérdida de continuidad
- Responsables de las diferentes actividades aplicar antes durante y después de la contingencia que activo la estrategia de continuidad.

Los planes de continuidad por procesos permiten tener las estrategias y una guía de acción a seguir ante los diferentes escenarios de interrupción que se puedan presentar. A continuación, se relacionan los planes con los que debe contar la Entidad:

• **Planes de continuidad por proceso critico:** Procedimientos documentados que orientan a los integrantes de los equipos funcionales, responsables de la continuidad de un proceso crítico para responder, recuperar, reanudar, y restaurar a un nivel definido de funcionamiento tras interrupciones. Estos documentos describen el paso a paso de qué hacer en las tres fases de un incidente de interrupción: Antes, durante y después.

• **Plan de Manejo de crisis:** Coordinación de los procedimientos para manejar situaciones complejas que representan una amenaza a los objetivos estratégicos, la reputación o la existencia de una organización.

• **Plan de manejo de incidentes:** Describe cómo identificar y analizar un incidente de continuidad, así como el procedimiento para reportar y dar respuesta oportuna, el dueño de este proceso es el Líder de Continuidad.

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


*Ilustración 9 - Escenarios, impactos y Estrategia*
*Fuente: Elaboración Propia*

### 10.4.7. Prueba Y Ejercicios De Continuidad

Consiste en probar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del PCN de la CVP.

Esta etapa le da a la entidad la oportunidad de identificar y prevenir problemas y fallas con sus planes de continuidad de manera que puedan ser atendidas, preparando el negocio para la emergencia real.

#### *10.4.7.1. Practicar los procedimientos ante un incidente o desastre.*

Identificar áreas que necesitan mejora. Permitir al PCN permanecer activo, actualizado, entendible y usable. Demostrar la habilidad de recuperación.

#### *10.4.7.2. Premisas del programa de pruebas.*

Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones a la operación normal sean mínimas y deben comprender los elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral. Las pruebas deben incluir las siguientes tareas:

- Verificar la totalidad y precisión del Plan.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros del grupo de contingencia, proveedores y otros terceros.
- Identificar la capacidad de recuperar registros e información vital.
- Medir el desempeño de los sistemas operativos y computacionales.

Actualmente la Entidad tiene definido desarrollar una prueba funcional al año, mediante escenarios simulados, planeados en el tiempo, teniendo en cuenta los requerimientos de cada prueba y con una revisión exhaustiva de los resultados de estas, para generar mejoras a los planes. Además, la Entidad participa en el simulacro anual en el cual se activa el plan de emergencias. En la siguiente gráfica se muestra el tipo de pruebas a desarrollar:

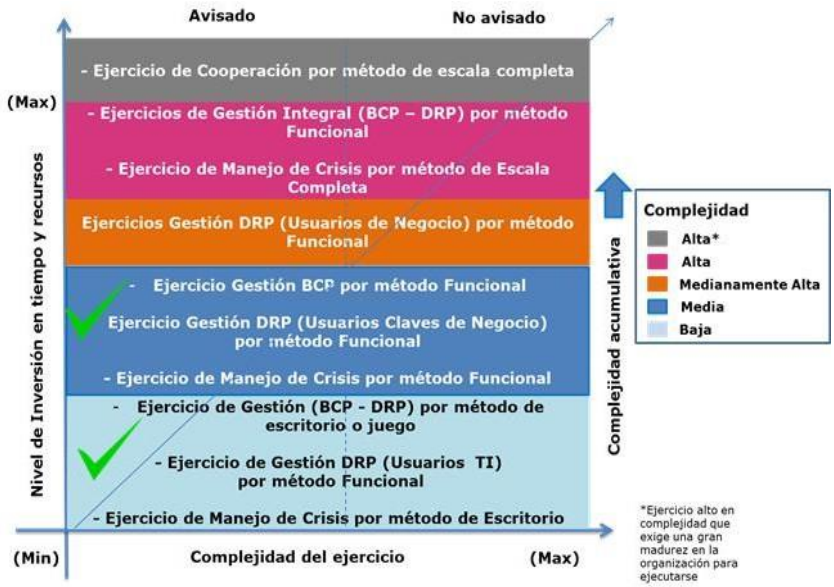


*Ilustración 10 - Tipo de ejercicios*
*Fuente: Elaboración Propia*

### 10.5. Cronograma

| Actividad | Tareas | Fecha Inicio | Fecha Final |
|---|---|---|---|
| **Planeación de las actividades a realizar en la vigencia** | Actualizar las actividades para la implementación del Plan de Continuidad de TI de la CVP. | 02/01/2025 | 30/04/2025 |
| | Verificar y actualizar la metodología para la implementación del Plan de Continuidad de TI de la CVP. | | |
| **Formación y sensibilización.** | Socialización y entrenamiento a los funcionarios y contratistas de la entidad sobre la importancia del Plan de continuidad de la CVP | 02/05/2025 | 30/05/2025 |
| **Recolección de información sobre servicios y sistemas de información, información crítica** | Recolección de resultados de pruebas orientadas a los aplicativos, portales, sistemas de información, servicios y actividades críticas | 1/06/2025 | 31/07/2025 |
| **Actualización y mantenimiento del Plan de Continuidad de TI del Negocio** | Generar documento y definición del Plan de Continuidad del Negocio en caso de que se considere necesario. | 1/08/2025 | 30/09/2025 |

*Tabla 9 – Cronograma de Actividades*
*Fuente: Elaboración Propia*

***NOTA:*** *En caso de ser necesario, las fechas de del seguimiento y planeación son susceptibles a cambios)*

## 11. SEGUIMIENTO Y MEDICIÓN DEL PLAN

La definición de los indicadores está alineada con los objetivos institucionales y de la Oficina TIC, acorde a la programación de metas establecidas en el Proyectos de Inversión de la Caja, para permitir tener una visión de los avances y resultados en el desarrollo de la Estrategia y la gestión integral de la Oficina TIC. Orientados a la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, se formula el indicador que servirá como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora e identificar el nivel de estructuración de los procesos de la Entidad orientados a la continuidad del negocio.

### 11.1. Indicador

El objetivo del proceso de seguimiento y evaluación es determinar la eficacia del Plan de Continuidad del Negocio al interior de la entidad, mediante el siguiente indicador:

| Indicador Plan de Continuidad del Negocio | | | | | |
|---|---|---|---|---|---|
| **Categoría Indicador** | **Tipo Indicador** | **Nombre del Indicador** | **Descripción** | **Variables** | **Fórmulas** |
| Eficacia | Estratégico | Implementación del Plan de Continuidad del Negocio (PCN) | Establecer el porcentaje de cumplimiento cronograma del PCN | ***PCPCN:*** *Porcentaje cumplimiento cronograma PCPCN*<br>***AE:*** *Número de actividades ejecutadas del cronograma, durante el período de tiempo analizado.*<br>***AP:*** *Número de actividades planeadas del cronograma, durante el período de tiempo analizado.* | ***PCPCN = (AE/AP) *100***<br>*CUMPLIMIENTO 100%:*<br>*(Índice de Cumplimiento > 90%)* |

*Tabla 10 - Indicador Plan de Continuidad del Negocio*
*Fuente: Tablero de Indicadores de TI*

### 11.2. Estrategias de Seguimiento y Medición:

• **Resultados De Pruebas y/o Ejercicios De Continuidad:** Permiten revisar procedimientos e identificar errores y omisiones en el contenido de los planes de continuidad de negocio y de las estrategias de recuperación.

• **Medición De Indicadores:** Una vez se encuentren implementados los indicadores que permiten evaluar y visualizar la gestión del Sistema de Gestión de Continuidad de Negocio y el cumplimiento de los objetivos, se deben evaluar de acuerdo con la periodicidad definida y de encontrarse desviaciones respecto a la meta propuesta, se deberá analizar las causas del incumplimiento y definir planes de acción que permitan alcanzar los objetivos del sistema.

• **Resultados De Evaluación De Proveedores:** Se debe evaluar la capacidad de recuperación actual y compararla con los requerimientos de los procesos de negocio con los que se relaciona, de identificarse brechas, se deben definir conjuntamente planes de Acción para cerrarlas.

• **Respuesta A Incidentes Reales:** Una de las principales fuentes para identificar oportunidades de mejora es la evaluación de respuesta a incidentes reales ya que nos ayuda a determinar si las estrategias y planes de continuidad actuales responder de manera efectiva a los incidentes de interrupción o si se identifican brechas entre la respuesta al incidente y los requerimientos del negocio, en cuyo caso se deberán identificar oportunidades de mejorar que permitan aumentar la capacidad de respuesta y recuperación.

• **Auditorías Internas:** Propone recomendaciones para optimizar las prácticas de gestión de la continuidad del negocio, logrando reducir costos e impactos que se puedan presentar por la materialización de riesgos de interrupción.

• **Riesgos Emergentes:** El identificar y evaluar oportunamente los riesgos emergentes permite definir planes de tratamiento para responder a riesgos de origen externo de impacto global, regional o nacional y de los cuales no se tiene control y su dinámica es desconocida.

## 12. PLAN DE COMUNICACIONES

La comunicación de los resultados del desarrollo del Plan de Continuidad del Negocio (PCN) y su puesta en marcha, contempla las actividades tanto para socializar el PCN como los grupos de interés a los que va dirigido.

### 12.1. Canales Presenciales:

- ✓ Presentaciones técnicas y ejecutivas, apoyadas en material visual (presentaciones y/o videos).
- ✓ Talleres de sensibilización y apropiación del PCN.

### 12.2. Canales Virtuales:

- ✓ Publicación y divulgación del PCN a través de la sede virtual y carteleras digitales de la Entidad.
- ✓ Boletines Informativos comunicados mediante correo institucional.

### 12.3. Grupos de Interés PCN:

- ✓ Funcionarios de la Alta Dirección de la Entidad.
- ✓ Directores y dueños de los procesos estratégicos, misionales, de apoyo y de evaluación.
- ✓ Funcionarios públicos y contratistas que se ven impactados con el PCN.
- ✓ Entidades del estado y privadas.
- ✓ Ciudadanía en General.

### 12.4. Responsables:

- ✓ El Comité de Gestión y Desempeño será el encargado de la aprobación del Plan de Continuidad del Negocio (PCN)
- ✓ El Líder del proceso Gestión de Tecnología de la Información y las Comunicaciones, será el responsable de la definición, actualización e implementación Plan de Continuidad del Negocio (PCN).

### 12.5. Frecuencia Actualización:

El Plan de Continuidad del Negocio (PCN) será integrado y divulgado a más tardar el 31 de enero de cada año según el decreto 612 de 2018. También, será actualizado y divulgado según las necesidades de la Entidad y acorde a las solicitudes requeridas.

## 13. ANEXOS E INFORMACIÓN COMPLEMENTARIA

Anexo 1 – “208-TIC-Nr-01 Normograma-OTIC”
Anexo 2 – “Informe Análisis De Impacto Al Negocio (BIA)”
Anexo 3 – “Mapa De Riesgos De Continuidad Del Negocio”