



MANUAL PARA LA CONSTRUCCIÓN Y MANTENIMIENTO DE LA CONTINUIDAD DE NEGOCIO

“Es mejor estar preparado para algo que nunca sucederá, a que suceda algo para lo que no estamos preparados”.

Deloitte and Touche.

Código: MN-7

Versión: 2

Vigente a partir de: 25/09/2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	3
2. OBJETIVOS	3
2.1 Objetivo General	3
2.2 Objetivos Específicos.....	3
3. ALCANCE	3
4. PLAN DE CONTINUIDAD DE NEGOCIO	3
4.1 Diagnóstico	4
4.2 Planificación.....	4
4.2.1 Contexto de la organización	4
4.2.2 Alcance.....	4
4.2.3 Política.....	4
4.3 Implementación.....	4
4.3.1 Análisis de Impacto del Negocio - BIA (Business Impact Analysis).....	4
4.3.1.1 Identificar procesos y actividades	5
4.3.1.2 Valorar el impacto.....	5
4.3.1.3 Determinar el RTO (Recovery Time Objective), RPO (Recovery Point Objective) y Período Pico.	7
4.3.1.4 Determinar recursos mínimos de operación.....	7
4.3.2 Análisis de Riesgos de Interrupción (RA):.....	8
4.3.3 Definición de escenarios.....	9
4.3.4 Diseño de estrategias y documentación de planes de continuidad de negocio ..	10
4.3.4.1 Estrategias	10
4.3.4.2 Documentación de Planes	12
4.3.4.3 Definición de roles y responsabilidades	13
4.3.4.4 Definición de actividades del plan.....	13
4.3.5 Pruebas y ejercicios del Plan.....	13
4.3.5.1 Tipos de pruebas:.....	13
4.3.5.2 Premisas para el desarrollo de las pruebas	14
4.3.6 Mantenimiento y actualización del Plan	15
4.4 Seguimiento y medición de la Gestión	16
4.5 Mejora Continua.....	17
5. SOCIALIZACIÓN.....	17
6. GLOSARIO.....	18
7. CONTROL DE CAMBIOS	19

1. INTRODUCCIÓN

La Continuidad de Negocio comprende la planeación, diseño, implementación, prueba y mejoramiento continuo de las actividades que permiten preservar la operación de la entidad ante situaciones de interrupción generadas por eventos naturales o aquellas ocasionadas por el hombre.

En ese sentido, la correcta gestión de Continuidad de Negocio permitirá a la Secretaría Distrital de Hacienda estar preparada para responder adecuada y oportunamente ante la ocurrencia de las interrupciones antes mencionadas, a través de la identificación de potenciales amenazas y la construcción de estrategias de recuperación se obtendrá la capacidad de respuesta necesaria para continuar entregando los servicios a la ciudadanía, entidades del orden nacional y demás partes interesadas.

Este documento se encuentra en el marco de los objetivos del Sistema de Control Interno – SCI que buscan proteger los recursos de la organización, definiendo y aplicando medidas para identificar los riesgos y detectar las desviaciones buscando su adecuada administración.

2. OBJETIVOS

2.1 Objetivo General

Proporcionar los lineamientos para la construcción, implementación y mejora de la Continuidad de Negocio de la SDH, con el propósito de otorgar un grado de seguridad razonable a la sostenibilidad de la entidad a través del restablecimiento de los servicios críticos y de la operación en general.

2.2 Objetivos Específicos

- Suministrar las directrices para la implementación de las etapas de la gestión de riesgo de Continuidad de Negocio.
- Promover en la entidad la cultura de la continuidad de negocio a través de la comunicación y sensibilización de los colaboradores respecto a su rol.
- Gestionar la prestación de servicio o continuidad de operaciones ante la imposibilidad de desarrollar sus procesos en normalidad.

3. ALCANCE

Este manual es de obligatoria aplicación en todas las dependencias de la Entidad, en todos los procesos y por parte de todos los funcionarios, contratistas y particulares que ejerzan funciones públicas en la entidad.

4. PLAN DE CONTINUIDAD DE NEGOCIO

El Plan de Continuidad de Negocio (Business Continuity Plan -BCP-) es un conjunto de protocolos e información documentada que se desarrolla, almacena y mantiene actualizada para su uso en caso de producirse un evento de interrupción que afecte el desempeño de las actividades críticas de la entidad.

A partir del marco metodológico de la ISO 22301 y de los lineamientos del Ministerio de

Tecnologías de la Información y las Comunicaciones de Colombia -MINTIC- para la Continuidad de Negocio¹¹; a continuación, se presenta el esquema de desarrollo para la construcción del Plan de Continuidad de Negocio en la entidad.

4.1 Diagnóstico

La Oficina de Análisis y Control de Riesgo – OACR y la realiza el análisis de brechas respecto a estándares de la NTC ISO 22301 (a pesar de que la entidad no se encuentra certificada) y las mejores prácticas implementadas a nivel internacional.

Con base en los resultados obtenidos se define el plan de trabajo para desarrollar la gestión de Continuidad de Negocio de la Entidad.

4.2 Planificación

Los elementos centrales de la fase de planificación se presentan a continuación:

4.2.1 Contexto de la organización

La base fundamental para la construcción del Plan de Continuidad de Negocio es el entendimiento de la entidad u organización; para lo cual, es necesario considerar aquellas cuestiones internas y externas, centrarse en aquellos aspectos que potencialmente afectan la prestación de los servicios e impactan a las partes interesadas que pueden impedir el cumplimiento de los objetivos estratégicos

4.2.2 Alcance

La OACR debe definir el alcance del Plan de Continuidad de Negocio, delimitando los procesos, servicios, recursos humanos, tecnología e infraestructura identificados como críticos, con el objetivo de mantener el cumplimiento de los objetivos estratégicos y en el marco de la Estrategia Distrital de Respuesta a Emergencia -EDRE-.

4.2.3 Política

La OACR, propone las Políticas de Continuidad de Negocio, a ser presentadas para aprobación de la Alta Dirección de la entidad, a través de la instancia y/o mecanismo establecido para ello.

4.3 Implementación

Pasos previos a la elaboración del Plan de Continuidad de Negocio BCP

4.3.1 Análisis de Impacto del Negocio - BIA (Business Impact Analysis).

El Análisis de Impacto del Negocio BIA (Business Impact Analysis) es la piedra angular para la construcción del Plan de Continuidad de Negocio y consiste en el análisis de las actividades de los procesos, con el propósito de determinar el impacto que puede causar una interrupción sobre el proceso / dependencia / entidad y de esta manera identificar las actividades críticas de cada uno; posteriormente, establecer tiempos objetivo de recuperación, estimar los recursos necesarios y generar las estrategias para reanudar la operación.

¹¹ MINTIC Guía para la preparación de las TIC para la Continuidad del Negocio, documento que fue diseñado con base en el Marco de Seguridad y Privacidad de la Información, el cual define el ciclo de funcionamiento del modelo de operación de Continuidad del Negocio y su funcionamiento dentro del modelo de operación, seguridad y privacidad de la información.

Para el desarrollo del Análisis de Impacto del Negocio es necesario realizar las siguientes actividades:

4.3.1.1 Identificar procesos y actividades

Identificar los procesos y/o actividades que componen las partes de la organización, priorizando las actividades críticas de las dependencias misionales, las cuales deben ser recuperadas a la mayor brevedad.

4.3.1.2 Valorar el impacto

Se realiza la valoración en una escala de uno (1) a cinco (5), siendo uno “Leve” y cinco “Catastrófico” de acuerdo con la herramienta de evaluación que se presenta a continuación:

Escalas de Impacto						
Nivel de impacto	Impacto Económico	Impacto en imagen	Impacto al usuario	Incumplimiento Legal	Detención o impacto a otros procesos	Impacto operacional
5	Impacto económico extremo	Afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en medios de comunicación a nivel local y/o país	Afecta directamente la atención al usuario de manera masiva	Intervención (Plan de saneamiento) de la entidad por parte de un órgano de control u otro regulador	Si el proceso se detiene puede afectar o detener toda la cadena de valor	Se podría generar un impacto alto para la Secretaría de Hacienda Distrital al detenerse el proceso por 8 horas o menos
4	Impacto económico alto	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Entidades distritales), respecto al cumplimiento de sus objetivos	Incumplimiento en la promesa de servicio	Multas o sanciones administrativas para la entidad por parte de entes de inspección, vigilancia y/o control	Si el proceso se detiene, puede detener más de un proceso misional	Se podría generar un impacto alto para la Secretaría de Hacienda Distrital al detenerse el proceso por un rango de tiempo entre 1 y 3 días
3	Impacto económico medio	Afecta la imagen de la entidad frente algunos usuarios de relevancia (Contribuyentes), respecto al cumplimiento de sus objetivos	Reclamaciones o quejas de los usuarios por no prestación oportuna del servicio	Demandas a la entidad por parte de tercero ante jueces de lo contencioso administrativo	Si el proceso se detiene puede afectar un proceso misional	Se podría generar un impacto alto para la Secretaría de Hacienda Distrital al detenerse el proceso por un rango de tiempo entre 3 y 5 días
2	Impacto económico bajo	Afecta la imagen de la entidad internamente (entre sus funcionarios y Directivos), y el tema es abordado en Comités Directivos y otras instancias internas	Retraso en los tiempos de respuesta al usuario	Investigaciones, sanciones, inhabilidades, entre otras, de tipo disciplinario, fiscal y/o penal en contra de alguno(s) de los funcionarios de la entidad	Si el proceso se detiene afecta o detiene a un proceso no misional	Se podría generar un impacto alto para la Secretaría de Hacienda Distrital al detenerse el proceso por un rango de tiempo entre 5 y 10 días
1	No se genera un impacto económico	No hay una afectación relevante a la imagen de la entidad	No se generan impactos a los usuarios	Hallazgos administrativos, observaciones o recomendaciones producto de auditorías	Si el proceso se detiene, no hay afectación sobre otros procesos	Se podría generar un impacto alto para la Secretaría de Hacienda Distrital al detenerse el proceso por más de 15 días

4.3.1.3 Determinar el RTO (Recovery Time Objective), RPO (Recovery Point Objective) y Periodo Pico.

El RTO es el tiempo máximo que puede transcurrir entre la interrupción y la recuperación del proceso sin que se generen impactos para la entidad, este análisis permite establecer las ventanas de tiempo máximas de detención que soportan las actividades.

El RPO es el punto máximo de tolerancia a la pérdida de información para una dependencia o proceso crítico, este resultado es necesario para definir e implementar estrategias que garanticen la disponibilidad de la información en caso de que se presente un evento de interrupción de la operación.

Periodo pico: El concepto se refiere a los periodos en los que se tiene mayor volumen de operación.

4.3.1.4 Determinar recursos mínimos de operación

En el formulario BIA se identifican los recursos necesarios para restablecer las operaciones a un nivel aceptable. Los recursos críticos, son aquellos que son prioritarios e imprescindibles durante la recuperación.

- **Talento humano:** Los funcionarios que son requeridos para la ejecución de las actividades o procesos críticos.
- **Servicios de Tecnología:** Herramientas tecnológicas requeridas para la ejecución de los procesos críticos, por ejemplo: aplicativos como SAP, SIT II, WCC o servicios tecnológicos como internet, intranet, correo electrónico, office 365 etc.
- **Proveedores Críticos:** Son terceros que apoyan las actividades o los procesos críticos, ya sea suministrando productos o servicios o realizando directamente actividades propias de la dependencia.
- **Registros Vitales:** De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio de MinTIC - Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, un registro vital es un registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas.
- **Procesos Manuales:** Son aquellas actividades alternas que pueden desarrollarse de forma manual ante eventos de interrupción de los servicios de tecnología.

La información de los servicios de tecnología con sus tiempos RTO y RPO, se entregan como insumo para que la Dirección de Infraestructura y Tecnología pueda construir las capacidades de recuperación técnica de las soluciones con que cuenta la SDH.

Se identifican los diversos eventos potenciales que pueden afectar la continuidad de sistemas críticos de la información, para lo cual se deben desarrollar las siguientes actividades:

- Identificar mapa de arquitectura tecnológica de la entidad.

- Identificar sitios físicos: validar la lista de instalaciones físicas o entidades en donde operan los servicios de TI de la entidad, el desarrollo de esta actividad está a cargo de la Dirección de Informática y Tecnología con el apoyo del asesor de seguridad de la Información de la entidad.
- Identificar sistemas de información: realizar un listado de los sistemas de información que se poseen en cada instalación y determinar cuáles de ellos están relacionados de forma directa o indirecta con el servicio de TI. Esta actividad está a cargo de la Dirección de Informática y Tecnología.
- Establecer secuencia de recuperación de los sistemas de información de acuerdo con su criticidad basado en la información obtenida a través de BIA (teniendo en cuenta el RTO y RPO de cada sistema) teniendo en cuenta la capacidad y arquitectura tecnológica. Esta actividad está a cargo de la Dirección de Informática y Tecnología con el apoyo del equipo líder de seguridad de la Información de la Subsecretaría General.

4.3.2 Análisis de Riesgos de Interrupción (RA):

En esta fase se identifican los riesgos potenciales a los que está expuesta la Entidad y que podrían causar una alteración, interrupción o pérdida de las operaciones en los procesos de la entidad.

El análisis de los riesgos de interrupción se alinea a la metodología de gestión de riesgo en procesos.

Se identifican como parte del análisis de impacto al negocio que se desarrolla en cada proceso.

Los riesgos de Continuidad de Negocio son riesgos operacionales cuya consecuencia es la interrupción del proceso, por la materialización de una amenaza, originada por la indisponibilidad total o parcial de los recursos mínimos requeridos o recursos habilitadores (tecnología, proveedores críticos, información, funcionarios) de la entidad.

4.3.3 Definición de escenarios

La materialización de los riesgos previamente identificados da lugar a la presencia de diferentes escenarios de falla, los cuales serán enmarcados en los siguientes siete (7) escenarios:

ESCENARIOS	DESCRIPCIÓN DEL ESCENARIO
Escenario de Falla de Servicios Tecnológicos	Fallas en la infraestructura del centro de cómputo principal, Bases de Datos y aplicaciones de la Entidad; fallas en redes y comunicaciones, ataque cibernético.
Escenario de Indisponibilidad de los colaboradores	Eventos de tipo natural, social y/o antrópico (terremoto y/o sismo, orden público, sabotaje, vandalismo, terrorismo, fugas de gas y/o incendio etc.), Intoxicación masiva, epidemia, pandemia.
Escenarios de Impacto Global que afecten la infraestructura	Pandemias, fenómenos meteorológicos, desaceleración económica global, cambios climáticos, conflictos políticos globales.
Escenarios de Impacto Nacional, Regional o Local que afecte la infraestructura	Desastres naturales en el país o en la ciudad de Bogotá como terremotos, inundaciones, huracanes, sismos, orden público, epidemias, endemias, cambios climáticos, sabotaje, vandalismo, terrorismo, manifestaciones, bloqueos).
Escenarios de Impacto Particular que afecte la infraestructura	Situaciones que afecten únicamente a la Secretaría Distrital de Hacienda tales como problemas de orden público, sabotaje, vandalismo, terrorismo, manifestaciones, bloqueos, fugas de gas y/o incendio, inundación, suspensión prolongada de servicios públicos, fallas en los equipos críticos etc.
Escenario de indisponibilidad de proveedores críticos	Contratación a corto plazo de servicios que se requieren en mediano y largo plazo. Ausencia o fallas en el plan de contingencia y continuidad de los proveedores.
Escenario de Indisponibilidad de los Registros Vitales	No acceso, pérdida o destrucción de los registros vitales.

Para el desarrollo posterior de cada uno de los planes y estrategias se desagregarán los escenarios mencionados adaptándolos a las dependencias de la entidad.

4.3.4 Diseño de estrategias y documentación de planes de continuidad de negocio

4.3.4.1 Estrategias

La estrategia corresponde a la guía de acción que se utilizará para responder ante la materialización de los escenarios contemplados, con el fin de minimizar el impacto potencial de las interrupciones.

Se podrán tener dos tipos de estrategias, las operativas y las tecnológicas.

- **Estrategias operativas:** son todas aquellas que se realizan dentro del proceso, pueden implicar operación manual (en caso de fallas tecnológicas), o procedimientos alternos.
- **Estrategias tecnológicas:** son aquellas mediante las cuales se dispone de una tecnología alternativa para soportar el desarrollo de los procesos críticos identificados en el BIA, estas estrategias deben ser proporcionadas por la Dirección de Informática y Tecnología.

Las estrategias de Continuidad de Negocio de la SDH consideran los siguientes aspectos:

- La estabilización, reanudación y recuperación de las actividades priorizadas en los procesos críticos.
- La realización del análisis costo /beneficio de las estrategias de continuidad.
- La selección y el detalle del sitio alternativo y del almacenamiento externo físico o virtual.
- El entendimiento de los términos contractuales de los servicios de continuidad del negocio.
- Recursos como el personal clave, el lugar de trabajo, los componentes de tecnología e información, los suministros, los registros vitales y las acciones focalizadas a las partes interesadas.

Consideraciones para las estrategias de Tecnologías de la información:

- El diseño e implementación de las estrategias de recuperación de los servicios de tecnología está a cargo de la Dirección de Informática y Tecnología.
- Las estrategias de recuperación tecnológica deben dirigirse a acortar el periodo de interrupción y limitar el impacto de las afectaciones sobre los procesos críticos de la entidad.
- La realización del análisis costo /beneficio de las estrategias de continuidad.

Previo a la selección de las estrategias de recuperación tecnológica, la entidad deberá llevar a cabo la evaluación de las diferentes alternativas que se le presenten, teniendo en cuenta las consideraciones mencionadas anteriormente y deberá seleccionar una o podrá realizar la combinación de varias y realizar las gestiones pertinentes que le permitan apropiarse de recursos para su implementación, lo cual está a cargo de la Dirección de Informática y Tecnología (DIT).

Es de aclarar que, la selección de la estrategia de recuperación tecnológica se fundamenta en los resultados del BIA (Business Impact Analysis), el cual considera el valor de los tiempos máximos permitidos de no disponibilidad o downtime (MTD); y asimismo, considera los siguientes aspectos:

- Hot sites: Normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
- Warmsites: En esta opción no se incluyen servidores específicos de altacapacidad.
- Coldsites: En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.
- Sitios móviles.
- Acuerdos recíprocos con otras entidades.
- Mirrorsite: procesamiento de cada transacción en paralelo con el sitio principal.
- Múltiples centros de procesamiento.

Sitio	Costo	Hardware	Telecomunicaciones	Tiempo	Localización
Sitio en frío	Bajo	No	Ninguno	Largo	Fijo
Sitio semi-preparado	Medio	Parcial	Parcial	Medio	Fijo
Sitio preparado (hot site)	Alto	Completo	Parcial	Corto	Fijo
Sitio Móvil	Alto	Variable	Variable	Variable	No fijo
Espejo (Mirror)	Muy Alto	Completo	Completo	Mínimo	Fijo
Sitio Recíproco	Bajo	Parcial	Parcial	Medio	Fijo

- Centro de Datos (Data Center): Dependiendo de los requisitos definidos para el plan de continuidad de negocio, se debe verificar que tipo de datacenter se requiere.
- Centro Alterno de Operaciones: Dependiendo de los escenarios y estrategias definidos para el Plan de Continuidad de Negocio de la Entidad, de establecerán las posibles alternativas para implementar un Centro Alterno de Operaciones.

Consideraciones en caso de requerirse un Centro Alterno de Operaciones. Se deben tener en cuenta los siguientes aspectos:

Ubicación:

- Se requiere conocer si es una zona sísmica o sensible, si está en la misma falla geológica de las instalaciones principales.
- Evitar zonas propensas a incendios o inundaciones
Verificar una distancia segura si las sede en la que se desarrollan las operaciones está cerca de instalaciones militares.
- Garantizar independencia de la misma red eléctrica a las instalaciones primarias.
- A pesar de las consideraciones anteriores, debe existir un balance en el análisis de tales factores, asegurando que, en caso de que los funcionarios que participan en la

recuperación de los procesos críticos de la entidad deban realizar un desplazamiento hasta el sitio alterno, deben arribar allí en el tiempo de recuperación objetivo (RTO) que se haya fijado previamente.

Mecanismo de ingreso:

- El procedimiento para ingresar a esas instalaciones, teniendo en cuenta consideraciones de horario, días y horas tanto hábiles como no hábiles

Listado de elementos:

- Los resultados del Análisis de Impacto de Negocio permitan a la entidad conocer cuáles son los elementos necesarios para que los funcionarios desarrollen las actividades identificadas como críticas, necesidades de espacio físico por funcionario, disponibilidad de los puestos de trabajo, necesidades de comunicación, impresoras, escáner, cantidad de suministros, ciclos de reposición de los mismos, caja fuerte, sellos, entre otros.

Distribución de elementos:

- Se debe especificar la ubicación de cada elemento de hardware, incluyendo direcciones IP, software instalado y funciones que se realizarán.

4.3.4.2 Documentación de Planes

Una vez definidas las estrategias y analizada su viabilidad, se debe proceder con el desarrollo de los planes cuyo objetivo es contar con guías prácticas para saber cómo responder ante un evento de contingencia, crisis y/o emergencia.

- **Plan de Continuidad de Negocio:** Plan construido para cada dependencia de la entidad, en el cual se cubren los diferentes escenarios planteados que pueden afectar la dependencia, incluye la aplicación de estrategias operativas y normales, así como el uso de estrategias tecnológicas previamente definidas.
- **Plan de Recuperación de Desastres:** Es el plan construido para recuperar los servicios de tecnología y telecomunicaciones, haciendo uso de las estrategias definidas para este fin, el cual está a cargo del equipo de la Dirección de Informática y Tecnología de la entidad.
- **Plan de Respuesta a Emergencias:** Es un plan organizacional que define la actuación frente a escenarios de emergencias físicas que puedan afectar a la entidad de forma particular o a la ciudad en general.
- **Plan de manejo de crisis:** Es un protocolo organizacional mediante el cual se articula

la respuesta ante los diferentes escenarios de contingencia que puedan desencadenar una crisis, de acuerdo con niveles de alerta predefinidos asociados a cada uno de ellos. Dentro de este se contempla el desarrollo de un plan específico de comunicación en crisis, que acompañe la respuesta frente a todas las audiencias involucradas.

- Plan de manejo de incidentes: Es un protocolo que contiene los pasos a seguir desde el momento en que se presenta un incidente que afecta el desarrollo de las operaciones de la entidad en condiciones de normalidad, incluyendo la gestión del mismo hasta su resolución y reanudación de las operaciones.

4.3.4.3 Definición de roles y responsabilidades

Dentro de cada uno de los planes que se desarrollen se debe definir el equipo a cargo de su ejecución, incluyendo roles principales y suplentes y sus responsabilidades antes, durante y después de una contingencia.

4.3.4.4 Definición de actividades del plan

Se detallarán las actividades requeridas para poner en marcha cada una de las estrategias asociadas a la dependencia, incorporando anexos en caso de necesitarse y la definición de requerimientos previos en caso de que apliquen.

4.3.5 Pruebas y ejercicios del Plan

Las pruebas y ejercicios son simulaciones de eventos de contingencia que se llevan a cabo con el fin de verificar la suficiencia de las estrategias y planes definidos para atender escenarios de emergencia, contingencia o crisis.

Las pruebas son realizadas en un ambiente que simule las condiciones aplicables en un evento verdadero. Es importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en un evento de crisis.

Beneficios de las pruebas y ejercicios:

- Validar los planes de continuidad del negocio por medio de la educación, socialización y conocimiento de los funcionarios con roles y responsabilidades críticos para la continuidad del negocio.
- Confirmar que se pueden lograr el tiempo objetivo de recuperación (RTO por sus siglas en inglés) y el punto objetivo de recuperación de datos (RPO por sus siglas en inglés) requeridos.
- Identificar los aspectos de preparación o resiliencia que requieren mejoras o actualizaciones debido a cambios en instalaciones, tecnología, información o enlaces de comunicación.
- Confirmar que los planes e instalaciones funcionan según se requiere.
- Demostrar la capacidad de recuperación de la entidad.

4.3.5.1 Tipos de pruebas:

- **Ejercicios de escritorio:** La dinámica de estos ejercicios consiste, básicamente, en simular “sobre papel” la ocurrencia de un incidente y seguir las acciones descritas en el

plan de continuidad, tal y como si dicho incidente se hubiera presentado en la realidad. Para el desarrollo de este ejercicio es necesario reunir en un mismo recinto a todas las personas involucradas en la recuperación y evidenciar así que todos ellos tienen claro qué deben hacer una vez se presente la situación de crisis. Este ejercicio permite identificar de forma sencilla aspectos que no se tuvieron en cuenta en la definición del Plan.

- **Ejercicios de puesto de mando:** El objetivo de estos ejercicios es simular un escenario de crisis lo más real posible en términos de la presión a la que se ve sometida el equipo que debe gestionar la recuperación, información que reciben durante el incidente, entre otras. Durante la realización del ejercicio, se entrega información al equipo en determinados intervalos de tiempo, tal y como se puede presentar ante un incidente real. Para aportar mayor realidad al ejercicio, se podría hacer uso de tecnología que simulará prensa, televisión, radio, redes sociales, etc.
- **Pruebas unitarias:** Tienen como objetivo evaluar la capacidad de recuperación que tiene la entidad sobre un entorno determinado; suelen tener el enfoque de éxito o fracaso y se suelen aplicar a equipamiento o tecnología, nunca sobre personas. Ejemplo: la restauración de un servidor haciendo uso de las cintas de back-up en un tiempo previamente establecido.
- **Simulacros:** El objetivo es practicar y/o probar la eficacia de la respuesta que se ha definido ante la ocurrencia de determinado incidente; para llevarlos a cabo se necesita gran cantidad de recursos económicos, de personal, etc. La diferencia frente al resto de ejercicios está en la realidad; el equipo que lleva a cabo este tipo de ejercicios debe responder al incidente de manera real, utilizando recursos, comunicaciones y tareas reales, etc. Previo a la realización de este tipo de pruebas, se deben haber realizado pruebas unitarias de todos los entornos, y los resultados deben demostrar un nivel de éxito que permita afrontar la prueba con ciertas garantías.

Los simulacros pueden realizarse de forma parcial o total y podrán variar en complejidad dependiendo de la necesidad y del nivel de madurez alcanzado.

La planeación de simulacros se soporta en el análisis de riesgos, lo que permite asegurar que, ante la presentación de alguna falla durante su realización, esto no impactará la ejecución de los procesos críticos de la entidad en condiciones de normalidad, provocando un incidente real.

Para la realización de los ejercicios de prueba al Plan de Continuidad de Negocio, se debe asegurar la participación de las personas adecuadas para planear y ejecutar las actividades correspondientes, aspecto que incrementa su capacidad de respuesta ante la ocurrencia de una situación que interrumpa el normal desarrollo de las actividades, documentando los resultados de las mismas.

4.3.5.2 Premisas para el desarrollo de las pruebas

Como parte de la planeación de las pruebas es necesario realizar las siguientes actividades:

- Definir cronograma de pruebas periódico.

- Para cada prueba según la necesidad de aplicación:
 - Desarrollar los objetivos y el alcance de la prueba.
 - Elaborar el minutograma.
 - Análisis de riesgo de la prueba.
 - Configurar el ambiente de prueba.
 - Preparar los datos de la prueba.
 - Identificar quién dirigirá la prueba.
 - Identificar quién controlará y supervisará la prueba.
 - Preparar cuestionarios de evaluación.
 - Preparar presupuesto para la prueba.
 - Brindar entrenamiento a los grupos de prueba de los procesos involucrados de la entidad.
 - Coordinar la logística de la prueba.
 - Establecer criterios de éxito.

En la fase de ejecución quienes coordinen la prueba y ejecuten la misma realizarán las siguientes actividades:

- Desarrollo de las actividades planeadas.
- Registro de resultados.
- Registro de evidencias.
- Registro de dificultades identificadas.
- Registro de tiempos.

En la fase de evaluación el equipo coordinador de la prueba realizará las siguientes actividades:

- Análisis de los resultados.
- Calificación de la prueba de acuerdo con objetivos planteados.
- Identificación de fortalezas y oportunidades de mejora.
- Definición de planes de mejora.

4.3.6 Mantenimiento y actualización del Plan

Para garantizar la vigencia de todo el programa de continuidad de negocio, es necesario realizar actualizaciones periódicas a los planes disponibles, las cuales se pueden dar por los siguientes elementos:

- Rotación de personal.
- Cambios en los procesos y sus recursos.
- Resultados de pruebas.
- Activaciones por eventos reales.
- Resultados de auditorías internas y/o externas.

4.4 Seguimiento y medición de la Gestión

El seguimiento y medición de la gestión de Continuidad del Negocio se llevarán a cabo de conformidad con lo establecido en la Política de Administración de Riesgo y Cumplimiento de la Secretaría Distrital de Hacienda y los lineamientos del Comité Institucional de Gestión y Desempeño, incluyendo:

- Supervisar el grado en que se cumplen los objetivos y metas de Continuidad de Negocio de la entidad.
- El rendimiento de los procesos, procedimientos y funciones que protegen sus actividades priorizadas.
- El registro de los datos y los resultados del seguimiento y medición para facilitar las acciones de mejoramiento.
- Evaluar los protocolos de Continuidad de Negocio a través de revisiones periódicas en las cuales se tienen en cuenta los resultados de las pruebas, los informes de las mismas y las evaluaciones al desempeño del BCP.
- Evaluar de forma periódica el cumplimiento de los requisitos legales y la normativa aplicable.

Evaluar los cambios significativos en la gestión de Continuidad de Negocio cuando éstos se producen, en especial luego de que se presenta un incidente que interrumpe el desarrollo de las operaciones de la entidad en condiciones de normalidad y que conlleva a la activación de los protocolos de gestión de Continuidad de Negocio.

La Oficina de Control Interno, como tercera línea de defensa, debe llevar a cabo auditorías internas que le permitan proporcionar al Comité Institucional de Coordinación de Control Interno – CICC- y al Comité de Gestión y Desempeño (según agenda temática) información relacionada con el cumplimiento, aplicación y mantenimiento de los requisitos propios y normativos de la Continuidad de Negocio, en cumplimiento del Plan Anual de Auditoría.

La Alta Dirección revisa los resultados de las auditorías a la gestión de Continuidad de Negocio para asegurarse de su conveniencia, adecuación y eficacia, dichos resultados constituyen insumo para tomar decisiones orientadas al mejoramiento continuo del Sistema de Gestión de Continuidad de Negocio; dentro de la revisión se analizan los siguientes aspectos:

- El estado de avance en que se encuentran las acciones ejecutadas en virtud de las revisiones anteriores que haya realizado la Alta Dirección.
- Los cambios en el contexto interno y externo que son relevantes y que potencialmente pueden generar la necesidad de ajustes a las políticas y objetivos para la gestión de Continuidad de Negocio.
- La información sobre el desempeño de la gestión de Continuidad del Negocio, teniendo en cuenta los tratamientos realizados para las no conformidades, el desarrollo de acciones correctivas, los resultados del seguimiento y la medición de la evaluación realizada por la auditoría.
- Los riesgos o problemas que no se hayan abordado de forma adecuada en

- cualquier evaluación de riesgo conocido.
- Los resultados de las pruebas al Plan de Continuidad de Negocio.
- Los protocolos, técnicas o metodologías que pueden ser utilizados en la entidad para mejorar el Sistema de Gestión de Continuidad de Negocio.
- Las lecciones aprendidas.
- Las buenas prácticas en gestión de Continuidad de Negocio.

4.5 Mejora Continua

Uno de los principales insumos para identificar oportunidades de mejora a los planes de continuidad de negocio (BCP), son los resultados de las pruebas y ejercicios de continuidad, debido a que es a través de éstas que se prueba la funcionalidad de los mismos ante los diferentes escenarios de interrupción y se identifican falencias, la cuales permiten fortalecer las estrategias.

Otro insumo importante que contribuye a la identificación de oportunidades de mejora son los incidentes reales de interrupción, ya que le permite a la entidad determinar brechas y falencias entre los planes de continuidad de negocio y la capacidad real de recuperación que tiene la entidad.

5. SOCIALIZACIÓN

Luego de construido y aprobado el Plan de Continuidad de Negocio, éste se socializa con los involucrados en el proceso, con el propósito de que estén preparados para enfrentar situaciones de emergencia o contingencia y se restablezca en el menor tiempo posible la prestación de los servicios.

Los resultados de las pruebas realizadas al Plan de Continuidad de Negocio se socializan por parte de la Oficina de Análisis y Control de Riesgos, en compañía de las dependencias involucradas, según el alcance de las pruebas, con la Alta Dirección con el propósito de que se pueda llevar a cabo un seguimiento riguroso del BCP y se tomen decisiones al respecto, basadas en los resultados de las pruebas.

6. GLOSARIO

- **Análisis de Riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Impacto del Negocio (BIA por sus siglas en inglés Business Impact Analysis):** es el proceso del análisis de actividades, las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.
- **Contexto interno:** describe el entorno en el que se desarrolla la operación de la entidad para dar cumplimiento a los objetivos estratégicos, al respecto se sugiere considerar aspectos tales como el enfoque de la administración, la estructura organizacional, tamaño, objetivos, metas, las relaciones con los contribuyentes y demás partes interesadas, la cultura de la organización, los valores (Código de Integridad), la complejidad de los procesos, las características y complejidad de los servicios, el flujo de procesos e información, entre otras, determinando cómo estos elementos se reflejan en la gestión de la entidad.
- **Continuidad de Negocio (BCM Business Continuity Management):** Capacidad de la organización para mantener los niveles de servicio o entrega de productos a niveles aceptables luego de un evento de interrupción, de tal forma que salvaguarde los intereses de las partes interesadas, su reputación y las actividades que crean valor.
- **Interrupción:** incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal desarrollo de las operaciones en alguna de las ubicaciones de la entidad.
- **Minutograma:** Documento donde se registra minuto a minuto el detalle de las actividades a realizar durante una prueba de continuidad de negocio para cada uno de los procesos que participan.
- **Partes interesadas (Stakeholder):** Público de interés para una organización que permite su completo funcionamiento. Personas u organizaciones que se relacionan con las actividades y decisiones de una empresa como: empleados, proveedores, clientes, gobierno, entre otros.
- **Plan de Continuidad de Negocio:** es el conjunto de protocolos / procedimientos documentados que guían / orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido una vez presentada la interrupción.

- **Registro vital:** de acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio de MinTIC - Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, un registro vital es un registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus clientes y sus partes interesadas.
- **Resiliencia:** capacidad de una organización para adaptarse a los entornos cambiantes
- **Riesgo:** es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
- **SGCN - Sistema de Gestión de la Continuidad del Negocio:** Parte del sistema general de la organización que está encargado de mantener, planificar y mejorar la continuidad del negocio.
- **Sitio alternativo:** es la ubicación alterna de operaciones, seleccionada para ser utilizada por una organización, el sitio alternativo es necesario cuando, como producto de una interrupción, las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales.

7. CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
1	22/Sep/2021	N/A
2	25/09/2024	Revisión y actualización de la totalidad de los numerales, ajustando el contenido a la Política de Administración de Riesgo y Cumplimiento y a la gestión desarrollada en la gestión de continuidad en la entidad