Control de cambios

Versión	Fecha	Descripción de la modificación
01	31 de diciembre de 2015	Primera versión del documento
1	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigencia de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento corresponden íntegramente a los aprobados en la versión 1 de fecha 31 de diciembre de 2015, la cual fue aprobada por Juan Carlos Garzón Barreto, Subsecretario de Planeación y Gestión (E), como líder del proceso Gestión y Adquisición de Recursos, vigente en ese momento.
2	23 de agosto de 2018	Se elabora el documento en el nuevo formato para manual, propuesto y actualizado por OAP, se modifica el Nombre del documento como "Manual Plan de Contingencia Informático", se agregan los numerales Tabla de contenido, alcance, se modifica Introducción, objetivos, definición y descripción del plan de contingencia informático y documentos relacionados. Lo anterior de acuerdo a los lineamientos establecidos.
03	21 de diciembre de 2022	Se cambia el título del documento, de "Plan de Contingencia Informático" a "Plan de Continuidad TI". Se tienen en cuenta los últimos lineamientos de la norma ISO 22301.

Método de Elaboración	Revisa	Aprueba
El documento se elabora de acuerdo con la normatividad que regula la materia, los profesionales de DTI realizan los ajustes correspondientes, a las mesas de trabajo realizadas con las diferentes dependencias y con el apoyo metodológico de la Oficina Asesora de Planeación	**Orlando Benavides Santacruz** Director de Tecnologías e Información **Angela Patricia Cabeza Morales** Profesional OAP – Analista del proceso	**Martha Liliana Soto Iguarán** Subsecretaria de Gestión Institucional Líder de macroproceso Documento revisado y aprobado mediante registro aplicativo Hola No. **283963**

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL

1.1. PROPÓSITO

El presente documento tiene como propósito definir y documentar las estrategias que permitan continuar con la operación de los servicios tecnológicos considerados, ante escenarios indeseables de índole catastrófica o de impacto directo en la confidencialidad, integridad y disponibilidad de la información.

La Secretaría Distrital de Gobierno - SDG, a través de la Dirección de Tecnologías e Información - DTI, como parte de su Modelo de Seguridad y Privacidad de la Información (MSPI) y de su Plan Estratégico de las Tecnologías de la Información (PETI) 2021 – 2024, concretamente el numeral "5.3.3. Gestión de la calidad y seguridad de la información", define como unos de sus puntos "actualizar y ejecutar el plan de continuidad o plan de contingencia informática".

Por lo anterior, el Plan de Continuidad TI (Tecnologías de la Información) busca de una manera armónica potenciar los distintos grupos y habilidades al interior de la DTI, para apoyar el cumplimiento de los objetivos de la SDG y asegurar la continuidad del negocio a través de la definición de lineamientos a seguir antes, durante y después de eventos que puedan producir una interrupción en las operaciones de los Servicios TI. Lo anterior, con el fin de reducir los riesgos, asegurar la restauración inmediata y la gestión de la continuidad buscando el mínimo impacto en las operaciones.

1.2. INTRODUCCIÓN

La información es considerada como uno de los bienes más importantes para las entidades, e integrada con los avances tecnológicos basados en la normatividad vigente han permitido facilitar y beneficiar a la ciudadanía mediante la prestación de sus trámites y servicios en línea, los cuales son publicados y mejorados continuamente en sus sistemas de información. Por lo anterior y para no interrumpir el eficiente desarrollo de sus procesos misionales, es muy importante contar con un Plan de continuidad TI que identifique los posibles riesgos, los mitigue, sea capaz de enfrentar las emergencias presentadas y recupere en el menor tiempo posible los flujos de operación contra caídas o daños que afecten la integridad, confidencialidad y disponibilidad del servicio.

Dentro de los avances tecnológicos de importancia para las entidades, se hacen indispensables la Infraestructura como servicio y la Plataforma como servicio:

- La Infraestructura como servicio - IaaS (del inglés *Infrastructure as a Service*), un tipo de servicio computacional en la nube que ofrece recursos como servidores, almacenamiento y redes por demanda (los cuales son pagados según sea su uso).

- La Plataforma como servicio - PaaS (del inglés *Platform as a Service*) es otro tipo de servicio computacional en la nube que incluye infraestructura (servidores, almacenamiento y redes), pero también middleware, herramientas de desarrollo, sistemas de gestión de bases de datos, etc.

Entonces la Secretaría Distrital de Gobierno, al igual que la mayoría de las entidades del orden nacional y distrital, al contar con IaaS y PaaS, adquiere características de alta disponibilidad y escalabilidad las cuales deben ser tenidas en cuenta en la elaboración del presente documento.

Lo anterior quiere decir, que se deben priorizar los servicios TI que tienen un "parcial" nivel de cobertura con los proveedores de nube. Por ejemplo, los servicios de gestión de bases de datos al ser PaaS, por defecto garantizan una alta disponibilidad (igual o superior al 99,9 %[1]), lo que en la práctica implica que no necesitan ser cubiertos en el presente plan de continuidad TI.

En síntesis, la finalidad del Plan de Continuidad TI es proteger el personal y los recursos tecnológicos que por las razones propias de la entidad estén parcialmente protegidos, para garantizar la continuidad de los procesos que permiten cumplir con la misionalidad de la entidad. Con su implementación se busca complementar un adecuado sistema de seguridad digital para salvaguardar los activos informáticos y recursos tecnológicos de la entidad contra posibles desastres, a través del conjunto de mecanismos y estrategias planteadas.

1.3. OBJETIVOS ESPECÍFICOS

a. Definir las actividades de planeación, elaboración, ejecución y verificación de tareas destinadas a proteger la información contra los daños y perjuicios producidos por caída de servicios, fenómenos naturales o humanos, reduciendo el grado de vulnerabilidad y exposición al riesgo.

b. Garantizar la continuidad de las operaciones de los principales elementos de configuración que componen los sistemas de información y la infraestructura tecnológica, minimizando el tiempo de reacción ante la emergencia y recuperación del servicio.

c. Identificar los principales riesgos que puedan afectar los servicios TI de la entidad facilitando tomar decisiones rápidas ante anormalidades o fallas.

d. Establecer actividades que permitan evaluar los resultados y retroalimentación del plan en general.

e. Cumplir con la normatividad legal vigente.

f. Generar cultura de Seguridad de la información en la Entidad.

1.4. ALCANCE

El Plan de Continuidad TI es implementado en la Secretaría Distrital de Gobierno, a nivel central y localidades, con el fin de salvaguardar los activos de información de la entidad. Se incluyen los elementos de configuración de los sistemas de información, infraestructura y servicios tecnológicos con el fin evitar o minimizar la materialización de riesgos y garantizar el normal funcionamiento de los servicios prestados por la entidad.

1.5. GLOSARIO

[1] https://docs.oracle.com/es-ww/iaas/Content/General/Reference/servicelevelobjectives.htm

- **Activo de información**: Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la Secretaría Distrital de Gobierno. En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en la Secretaría Distrital de Gobierno en el cumplimiento de sus funciones.
- **Acuerdo de confidencialidad:** Es el documento que suscriben los servidores públicos, contratistas, subcontratistas y pasantes-practicantes de la Secretaría Distrital de Gobierno, con el fin de afianzar su compromiso con la entidad respecto del uso pertinente de los recursos informáticos y de la información que la entidad dispone y que les entrega, o a la cual tiene acceso con ocasión al cumplimiento de sus funciones u obligaciones.
- **Alta disponibilidad:** Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible. Este nivel de funcionamiento (o el tiempo máximo de caída) ha de ser acordado entre el proveedor y el cliente en el caso de un servicio, en el marco de un Acuerdo de Nivel de Servicio. Es una funcionalidad necesaria para garantizar los servicios esenciales o imprescindibles de una empresa, cuando esta se enfrenta a incidentes que puedan afectar a su funcionamiento normal o disponibilidad.
- **Ambiente de prueba:** Es un sitio (servidores, URLs, computadores, etc.) donde se alojan las aplicaciones o servicios para que sean probadas (la mayoría de los usuarios aún no tiene acceso), previo a que sean publicados en ambiente de producción (donde todos los usuarios si tienen acceso).
- **Ambiente de desarrollo:** Es un sitio (servidores, URLs, computadores, etc.) que se usa para desarrollar o construir el software de un programa, aplicación o servicio tecnológico (generalmente se usan lenguajes de programación, librerías, frameworks, base de datos, entre otros).
- **ANS:** Acuerdo de Nivel de Servicio o en inglés SLA. Se trata de un acuerdo que define el nivel de servicio que las empresas esperan de un proveedor externo cuando despliega soluciones de los servicios IT a medida de los requerimientos de un entorno corporativo. En este acuerdo, se establecen las métricas por las que se mide el servicio, así como las soluciones o penalizaciones en caso de que no se alcancen los niveles de servicio acordados.
- **Antispyware:** Herramienta de software diseñada para detectar y eliminar programas maliciosos del tipo spyware cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario.
- **Autenticación:** Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico, etc.
- **Backup:** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos tradicionalmente más empleados para llevar a cabo la técnica de backup pueden ser discos duros, discos ópticos, USB o DVD. Recientemente es común la realización de copias de seguridad mediante servicios de almacenamiento basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad, así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.
- **BIA:** Del inglés *Business Impact Analysis*; Se trata de un informe que muestra los escenarios y los planes alternos que se tienen por la interrupción de los procesos críticos de negocio. Este informe permite

asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos. (ISO 22301)

- **Capacidad**: Combinación de todas las fortalezas y recursos disponibles dentro de una organización.
- **Centro de respaldo:** Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia. Las características de un centro de respaldo deben ser las siguientes:
    - Su localización debe ser totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.
    - El equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal.
    - El equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.
- **Compilador:** Es un programa o proceso informático que traduce todo el código fuente o instrucciones de un archivo de software (o conjuntos de archivos de software, lo que se denomina proyecto software) a código máquina antes de ejecutarlo; solo entonces el procesador del computador (o servidor) entiende y ejecuta el software compilado.
- **Confidencialidad**: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información; Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.
- **Control de acceso**: Es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios de los sistemas, recursos o información.
- **Custodio de la información:** Es el funcionario o contratista encargado de administrar el activo de información, aplicar las políticas, procedimientos y protocolos definidos por la Entidad y por el dueño del Activo de Información.
- **Derecho de autor:** "Son los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos". (OMPI, s.f.)
- **Denegación del servicio**: Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. También llamado DoS.
- **Desarrollo seguro:** Es el uso de principios y/o buenas prácticas de seguridad de la información durante el ciclo de vida del software (SDLC), pudiendo ser adquirido o construido al interior de la entidad.
- **Disponibilidad:** Se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.
- **Dispositivos móviles:** También conocidos como computadora de bolsillo o computadora de mano, con capacidades de procesamiento, con conexión a Internet, con memoria y pantalla. Se dividen en: Portátiles, Teléfonos inteligentes y Tabletas.
- **Dueño de la información:** Es el Directivo de una dependencia específica, designado por la SDG, que tiene la responsabilidad de garantizar que el activo de información se clasifique adecuadamente, debe definir, revisar periódicamente las restricciones y niveles de acceso.

- **Escaneo de vulnerabilidades:** Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.
- ***Ethical hacking*:** Es el proceso de identificar y explotar las debilidades existentes en los sistemas de información e infraestructura tecnológica, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los diferentes activos de información ejecutadas por parte de personas autorizadas por la entidad.
- **Firma digital**: es un proceso automatizado para la validación de la firma de un suscriptor basado en algoritmos y criptografía
- **Firma electrónica:** se refiere a todos los métodos para firmar (o validar) un documento electrónico o identificar a una persona.
- **Framework:** es un marco de trabajo, librerías o estructura previa que se puede aprovechar para desarrollar un proyecto, que simplifica la elaboración de una tarea, ya que solo es necesario complementarlo de acuerdo con lo que se quiere realizar.
- **Gestión de cambios:** Es el proceso que reúne un conjunto de prácticas y procesos que ayudan al equipo a enfrentar las transformaciones que puedan ocurrir en la entidad. Esto permite que la oficina o dependencia de TI sustituya tecnologías desactualizadas por soluciones más eficaces o actualizadas.
- **Gestión de proyectos:** Es administrar, planificar, coordinar, seguir y controlar todas las actividades y los recursos asignados para un proyecto de una forma que se pueda cumplir con el alcance en el tiempo establecido y con los costos presupuestados.
- **Gestión de incidentes de seguridad de la información**: Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la entidad. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.
- **Gestión de riesgos de seguridad digital**: Actividades coordinadas para dirigir y controlar dentro de una organización el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **Hardware:** Son aquellos elementos físicos que hacen parte de los sistemas computacionales como los son CPU (procesador), memoria, monitor, teclados, impresoras, parlantes, etc.
- **Impacto:** Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.
- **IDS:** Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es una aplicación usada para detectar accesos no autorizados a un computador, sistema de información o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.
- **Incidente:** Cualquier evento que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la entidad, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información. (ISO 27000)

- **Integridad:** Se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.
- **IPS:** (*Intrusion Prevention System*) - Es un software que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.
- **ISO:** (*International Organization for Standardization*) - Organización Internacional de Estandarización.
- **ISO 27000**: Es la norma para la gestión en la seguridad de la información.
- **ISO 27001:** Es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal.
- **ISO 22301:** Esta norma ha sido diseñada para permitir a las organizaciones alinear e integrar su Sistema de Gestión de la Continuidad del Negocio: Planificar, Hacer, Verificar y Actuar.
- **ISO 31000:** Es la norma internacional para la Gestión de Riesgos, la cual ayuda a las Entidades en sus análisis y evaluaciones de riesgos. Las recomendaciones de mejores prácticas de esta norma internacional se desarrollaron para mejorar las técnicas de gestión y garantizar la seguridad. La gestión del riesgo es parte de la gobernanza y el liderazgo, es fundamental en la manera en que se gestiona la Entidad en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.
- **LAN:** También llamada Red de Área Local, es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos de todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc. Las Redes de Área Local pueden ser cableadas o no cableadas (también conocidas como redes inalámbricas). Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivos.
- **Log:** Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/ salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.
- **Mejores prácticas:** Es una técnica o metodología que, a través de la experiencia y la investigación, ha demostrado llevar de forma fiable a un resultado deseado. Es un compromiso de utilizar todos los conocimientos y la tecnología a disposición de uno para asegurar el éxito.
- **Perfil:** Es la definición de un conjunto de funcionalidades o propiedades que se le pueden asignar a un usuario; la asociación de un usuario a un perfil le permite iniciar una sesión en un sistema, o acceder a ciertas funciones específicas de dicho perfil.
- **Phishing:** Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o por ejemplo información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.
- **Políticas TI:** Son directrices u orientaciones que debe generar la DTI y que reflejan la intención de la alta dirección, con el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas

y terceros que trabajan con la organización y que por sus funciones deben tener acceso a su información y a su infraestructura). Para efecto de este manual, solo serán llamadas políticas.

- **Privacidad:** Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de los actores.
- **Propiedad intelectual:** "La propiedad intelectual (P.I.) se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. La legislación protege la P.I., por ejemplo, mediante las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de P.I. procura fomentar un entorno propicio para que prosperen la creatividad y la innovación". (OMPI, s.f.).
- **Protección de datos personales:** Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.
- **Ransomware:** Malware cuya funcionalidad es secuestrar un dispositivo o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.
- **Recurso tecnológico:** Son todos los bienes tangibles e intangibles que posee la entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias. Los recursos tecnológicos y la Información son de propiedad de la Secretaría Distrital de Gobierno y deben ser utilizados únicamente para propósitos legítimos de la entidad. Se permite que los Usuarios utilicen estos Recursos para facilitarles el desempeño de sus tareas. El uso de estos Recursos es un privilegio que puede ser revocado en cualquier momento.
- **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos.
- **Riesgo de seguridad digital:** Está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- **Seguridad de la información:** Es el conjunto de políticas, medidas técnicas, operativas, organizativas y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Servidor público:** Se refiere a todos los empleados, contratistas, consultores o trabajadores temporales de la Secretaría Distrital de Gobierno.
- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **SGSI:** Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.
- **Software:** Son aquellos elementos informáticos que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión. Están conformados entre otros por:

A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones

- **Spyware:** Es un programa maligno que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos.
- **Teletrabajo:** Es la modalidad de trabajo inteligente que consiste en el desempeño de las actividades remuneradas o prestación de servicios a terceros, utilizando como soporte las tecnologías de la información y comunicación – TIC – para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **Tercero o proveedor:** Es la persona natural o jurídica que provee o suministra profesionalmente de un determinado bien o servicio a la entidad por medio de un acuerdo contractual.
- **Trabajo en casa:** Es la modalidad de trabajo inteligente la cual se aplica por razones apremiantes, urgentes y temporales. En efecto, los recientes hechos de salud pública han evidenciado la necesidad en el sector público de plantear, organizar y desarrollar las actividades laborales a través del trabajo a distancia, cuando se presenten diferentes circunstancias ocasionales, excepcionales, especiales o transitorias, privilegiando el uso de las tecnologías de la información y las comunicaciones.
- **Trabajo inteligente:** Es un proceso de innovación pública basado en un enfoque organizacional del ámbito laboral que busca mejorar la eficiencia y la eficacia en la producción de resultados a través de la combinación de flexibilidad, autonomía y colaboración, en paralelo con el mejoramiento de las herramientas tecnológicas, el equilibrio entre la vida personal y laboral y los ambientes de trabajo de los colaboradores y una gestión basada en resultados.
- **Usuario:** Se refiere a todos los servidores públicos y cualquier otra persona o entidad que utilice los Recursos Tecnológicos de la Secretaría Distrital de Gobierno.
- **Virus:** Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.
- **VPN:** Es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet.
- **Vulnerabilidad**: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre, el fabricante del software o hardware lo solucionará publicando una actualización de seguridad del producto.
- **WAF:** El *Web Application Firewall* (WAF) protege de múltiples ataques al servidor de aplicaciones web y al software que hay detrás (*backend*). La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico. El WAF examina cada petición enviada al servidor, antes de que llegue a la aplicación, para asegurarse de que cumple con las reglas del firewall. Las características WAF pueden ser implementadas:
    - En el software: instalando una aplicación en el sistema operativo
    - En el hardware: integrando las funcionalidades en una solución instalada sobre un dispositivo.

2. ESTRUCTURA DEL PLAN DE CONTINUIDAD TI

El proceso Gerencia de TIC se encuentra dentro de los procesos de apoyo de la Secretaría Distrital de Gobierno, convirtiéndolo en un proceso de vital importancia para la continuidad del negocio por su

transversalidad con todas las áreas. En este orden de ideas, el proceso Gerencia de TIC tiene como objetivo formular e implementar las estrategias de Tecnologías e Información (TI) en materia de seguridad digital, uso y apropiación de los Sistemas de Información y disponibilidad de los servicios de TIC, en el marco de la arquitectura empresarial con procedimientos sistemáticos y eficientes; con el fin de contribuir al logro de los resultados esperados por la Secretaría Distrital de Gobierno, la satisfacción de los diferentes grupos de interés y la toma de decisiones en la Entidad, los cuales se ajustan a las necesidades de los diferentes procesos de la Institución.

El plan de continuidad TI inicia con la definición de los servicios TI que tendrán gestión de la continuidad, sigue con la identificación, análisis y evaluación de los riesgos o amenazas que puedan afectar las operaciones de dichos servicios lo cual permite definir los escenarios de continuidad y finaliza con las estrategias propuestas para proteger los activos y recursos de dichos servicios garantizando la continuidad del negocio en caso de afectación para cada escenario. La metodología propuesta se basa en el ciclo de vida iterativo PDCA (plan-do-check-act, / planificar-hacer-comprobar-actuar).

2.1. SERVICIOS TI QUE TENDRÁN GESTIÓN DE CONTINUIDAD

Al interior de la DTI se hizo un análisis de los servicios TI que deben tener gestión de la continuidad, actualizando en alguna medida la versión anterior del presente documento. El estudio se basó principalmente en las características de soporte y disponibilidad que tienen actualmente dichos servicios TI; en ese orden de ideas, cuando el soporte y la disponibilidad de dicho servicio es cubierto en alta medida por proveedores de la nube (por ejemplo: los sistemas de gestión de bases de datos tienen una disponibilidad en la nube del 99,9% o superior), el mismo es descartado.

Por lo anterior, se escogieron los siguientes cuatros servicios TI que tendrán gestión de la continuidad:

- Portal Web de la Secretaría Distrital de Gobierno: es la aplicación web que sirve de puerta para el acceso a la ciudadanía a sus trámites y para que la entidad publique información de interés general para los ciudadanos; a pesar de tener toda la infraestructura en la nube, su administración y exposición la hacen vulnerable a todos los escenarios descritos en el presente documento.

- Mesa de servicios: es el servicio TI que permite una ruta clara para que los usuarios de la entidad (empleados, contratistas y terceros) informen problemas y hagan solicitudes, o en general creen casos de soporte en relación con las tecnologías de la información y las comunicaciones.

- Todas las fuentes de datos que no estén en bases de datos en la nube: en la entidad existen muchas fuentes de datos (generalmente archivos de Excel en la nube) que son gestionados por los usuarios de las distintas dependencias, y que al no ser gestionadas por bases de datos se tornan en activos de información vulnerables.

- Conectividad de los enlaces de datos: los enlaces de datos son el servicio que soporta la comunicación (a nivel IP o superior) del nivel central con las alcaldías locales y que a la vez permite el acceso a internet; dichas conexiones se hacen vulnerables ante algunos escenarios descritos en el presente documento.

2.2. PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

La metodología para la valoración de riesgos se fundamenta en la norma ISO 31000:2018[2] y se armoniza con el Manual de Gestión del Riesgo (PLE-PIN-M001) de la Entidad. A continuación, se adapta dicha metodología a la gestión de riesgos TI en la Entidad.

2.2.1. Definir el alcance y contexto de la gestión del riesgo

Es necesario conocer el contexto de la Gerencia de TIC en la Entidad, la interrelación de los procedimientos y las actividades ejecutadas con el fin de identificar posibles falencias o vulnerabilidades de los procesos que puedan poner en riesgo la información. Para ello se realiza un entendimiento de la información y las tecnologías que implican los cuatro servicios que tienen gestión de la continuidad; así como entrevistas con los líderes de los servicios TI para profundizar en el contexto interno y externo de la Entidad.

2.2.2. Identificar los riesgos

Se evaluaron la mayoría de las situaciones que pueden poner en riesgo el cumplimiento de los objetivos de los cuatro servicios TI al interior de la DTI; se tuvieron en cuenta los riesgos de origen interno y externo; se consideraron factores como: la probabilidad de los eventos, la naturaleza y la magnitud de las consecuencias, la complejidad y la interconexión, los factores relacionados con el tiempo y la volatilidad, la eficacia de los controles existentes, los niveles de sensibilidad y de confianza.

Con base en todo lo anterior se seleccionaron los siguientes eventos o escenarios más críticos:

- ✓ Indisponibilidad del personal de la DTI
- ✓ Factores de orden público en donde se debe evacuar la entidad
- ✓ Desastre natural
- ✓ Emergencia por ataque informático (interno o externo).
- ✓ Indisponibilidad tecnológica de uno o más componentes del servicio TI.

2.2.3. Análisis de riesgos

El análisis de riesgos se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas, dependiendo de las circunstancias y del uso previsto.

El análisis del riesgo consideró factores tales como:

[2] https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

- ✓ La probabilidad de los eventos y de las consecuencias: teniendo en cuenta la ubicación de la sede central de la entidad (en la Plaza de Bolivar, centro geográfico de las ramas del poder nacional), los factores de orden público tienen una probabilidad considerable.
- ✓ La naturaleza y la magnitud de las consecuencias: las emergencias o desastres naturales causados por terremotos o inundaciones, tienen unas consecuencias de enorme magnitud.
- ✓ La complejidad y la interconexión: los sistemas de información tienen una gran complejidad y generalmente los cambios a dichos sistemas, pueden traer algunos problemas (ej: paso a producción fallido) que pueden llevar a la indisponibilidad tecnológica de algún componente del servicio TI.
- ✓ La eficacia de los controles existentes: los ataques informáticos, se dan porque superan los controles existentes y por lo tanto deben ser considerados.
- ✓ Los niveles de sensibilidad y de confianza: el recurso humano es el más importante y evidentemente los servicios TI son muy sensibles a la falta de dicho recurso.

El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones del riesgo y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones establecidas, cualquier limitación de las técnicas y cómo se ejecutan éstas. Estas influencias se deberían considerar, documentar y comunicar a las personas que toman decisiones.

Los eventos de alta incertidumbre pueden ser difíciles de cuantificar. Esto puede ser una cuestión importante cuando se analizan eventos con consecuencias severas. En tales casos, el uso de una combinación de técnicas generalmente basadas en la experiencia proporciona una visión más amplia.

2.2.4. Valoración del riesgo

La valoración del riesgo consiste, como lo indica el Manual de Gestión de Riesgo (PLE-PIN-M001) de la Entidad, en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial.

Dentro de la Valoración del riesgo cobra especial relevancia el análisis y evaluación de los Controles, que se pueden clasificar en:

- Controles preventivos: va a las causas del riesgo. Ataca la probabilidad de ocurrencia del riesgo.
- Controles Detectivos: detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo.
- Controles Correctivos: atacan el impacto frente a la materialización del riesgo.

2.2.5. Tratamiento del riesgo

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- ✓ Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo.
- ✓ Aceptar o aumentar el riesgo en busca de una oportunidad.
- ✓ Eliminar la fuente de riesgo.

- ✓ Modificar la probabilidad.
- ✓ Modificar las consecuencias
- ✓ Compartir el riesgo (por ejemplo: a través de contratos, compra de seguros).
- ✓ Retener el riesgo con base en una decisión informada.

Como parte del tratamiento del riesgo, se elabora el presente documento que complementa el Manual de Gestión de Seguridad de la Información (GDI-TIC-M004) y se alinea con el Manual de Gestión del Riesgo (PLE-PIN-M001) en su capítulo 11, los cuales basan los controles de seguridad digital en la norma ISO 27001.

2.3. ESCENARIOS DE CONTINUIDAD

Los escenarios de continuidad fueron seleccionados de acuerdo con el análisis de riesgo, tratamiento del riesgo y a las condiciones propias de la Entidad. A continuación, se describen dichos escenarios de continuidad:

- Desastre natural: este escenario es poco probable, sin embargo en caso de presentarse la afectación de las personas y de la infraestructura es bastante grande; normalmente los terremotos son el ejemplo típico ya que dependiendo de su intensidad pueden causar daños relativamente graves y obligar a la evacuación de la Entidad; últimamente debido al cambio climático, las inundaciones toman gran relevancia y se hacen cada vez más probables.
- Factores de orden público en donde se debe evacuar la entidad: debido a las características de ubicación de la entidad, es un escenario típico y muy probable; las situaciones en donde se debe evacuar la entidad se presentan todos los años y por ello es importante estar preparados para ellas.
- Emergencia por ataque informático: estos ciberataques se presentan diariamente, sin embargo los dispositivos de seguridad perimetral (ej: Firewall) normalmente los bloquean; este escenario aplica para aquellas situaciones que superan los dispositivos y controles de seguridad perimetral.
- Indisponibilidad del personal de la Dirección de Tecnologías e Información: es un escenario que debe ser analizado, ya que hay servicios que son en mayor o en menor medida dependientes de los ingenieros de la Dirección de Tecnologías e Información.
- Indisponibilidad tecnológica de uno o más aplicativos: los servicios están compuestos por múltiples aplicativos o tecnologías; a veces alguno de ellos falla (ej: daño en hardware, paso a producción fallido, etc.) y es importante definir la estrategia para estos casos que tienen una probabilidad nada despreciable.

2.4. ANÁLISIS DE IMPACTO AL NEGOCIO

Todo proyecto de continuidad debe contar con un análisis de impacto al negocio (BIA), esto permite identificar cuáles son los elementos funcionales críticos de la organización. Regularmente el BIA se implementa haciendo visitas a las áreas de negocio que están inmersas en los servicios de negocio respectivos; en este caso se tuvieron reuniones con los líderes de los servicios TI que tendrán gestión de continuidad.

Actualmente los ataques cibernéticos y la violación de datos se han vuelto frecuentes en los sistemas de información y las redes de comunicaciones, por tal motivo la prevención es la mejor defensa contra esas

amenazas y ataques. Asimismo, proteger a los usuarios y la infraestructura de tecnologías de la información ante ataques cibernéticos es fundamental y por eso la detección temprana de incidentes y su respuesta es otro factor crítico que debe ser contemplado por la Dirección de Tecnologías e Información; de igual forma se debe tener en cuenta que como una buena medida de seguridad se tiene que los respaldos o backups deben tener una frecuencia adecuada, con la finalidad de que a la hora de un incidente, el punto de recuperación sea el más actualizado posible para la recuperación respectiva.

Igualmente, las amenazas avanzadas que hoy día usan los atacantes son tan sofisticadas, que están evadiendo metódicamente los controles de seguridad empresariales; estos ciberataques provocan continuamente violaciones, robos y pérdidas de datos.

Las Entidad deben considerar la seguridad de la información como un valor agregado de prestigio y confiabilidad para sus usuarios y no como un costo adicional. El costo - beneficio de implementar controles debe ser adecuado de acuerdo con el nivel de importancia del activo de información que maneja la Entidad y el impacto que pudiese causar la vulnerabilidad de este.

La globalización enfrenta a la Entidad a nuevos retos en cuanto a la seguridad digital. Es entonces importante apoyarse en las políticas y mejores prácticas con que cuenta la Entidad, tales como el GDI-TIC-M004 "Manual de gestión de seguridad de la información" que constantemente está siendo actualizado para poder contrarrestar en lo posible las nuevas amenazas que día a día emergen con el único propósito de identificar y aprovechar las vulnerabilidades de los servicios TI.

No menos importante son los eventos poco predecibles, como los desastres naturales o los ataques físicos que puedan sufrir las instalaciones por factores políticos o de orden público.

Los siguientes términos son indicadores usados típicamente en los análisis de impacto al negocio:

- MTPD (del inglés *Maximum Tolerable Period of Disruption*): Periodo máximo de tiempo de inactividad que puede tolerar la Entidad sin entrar en colapso.

- MBCO (del inglés *Minimum Business Continuity Objective*): mínima capacidad o nivel de servicio que es aceptable para la Entidad, para lograr sus objetivos de negocio durante una disrupción.

- RPO (del inglés *Recovery Point Objective*): Punto en el cual los datos deben ser recuperados después de que una interrupción ocurre.

- RTO (del inglés *Recovery Time Objective*): Tiempo que sigue a un incidente, dentro del cual un servicio TI es restaurado.

De los cuatro indicadores descritos anteriormente, se selecciona al RTO como el que mejor ayuda a definir los objetivos de continuidad de la Secretaría Distrital de Gobierno. A continuación se presenta una tabla que resume el análisis de impacto al negocio para cada servicio TI que tiene gestión de continuidad:

Tabla 1. Análisis de impacto al negocio - Secretaría Distrital de Gobierno

Servicio TI	Escenario de continuidad	Descripción de la Alternativa (plan de operación alterno)	RTO (tiempo de recuperación objetivo)
Portal Web	Desastre natural	1. Backups que permitan instalar el servicio en una infraestructura alternativa (dado el caso que se afecte la infraestructura en la nube). 2. Configurar sistemas en alta disponibilidad en producción (por ejemplo en distintas zonas geográficas); esto minimiza el tiempo de inactividad y las interrupciones del servicio. 3. Activar el plan de comunicaciones para informar sobre la no disponibilidad del servicio.	24 horas
Portal Web	Factores de orden público en donde se debe evacuar la entidad	1. Teletrabajo del personal que mantiene el portal. 2. Activar el plan de comunicaciones para informar al personal y que facilite evacuar la Entidad.	12 horas
Portal Web	Emergencia por ataque informático	1. Backups que permitan instalar el servicio en una infraestructura alternativa. 2. Implementar las políticas y controles del GDI-TIC-M004 Manual de Gestión de seguridad de la información. 3. Activar el plan de comunicaciones para informar al personal y a los usuarios del portal.	24 horas
Portal Web	Indisponibilidad del personal de la Dirección de Tecnologías e Información	1. Contar con personal de respaldo en la DTI. 2. Contar con manuales técnicos que permitan delegar las funciones a personal con conocimiento técnico mínimo.	24 horas
Portal Web	Indisponibilidad tecnológica de uno o más aplicativos	1. Backups que permitan instalar el servicio en una infraestructura alternativa. 2. Seguir las políticas del GDI-TIC-M004 Manual de Gestión de seguridad de la información. 3. Activar el plan de comunicaciones para informar al personal y a los usuarios del portal.	24 horas

Servicio TI	Escenario de continuidad	Descripción de la Alternativa (plan de operación alterno)	RTO (tiempo de recuperación objetivo)
Mesa de servicios	Desastre natural	1. Teletrabajo del personal que atiende la Mesa de servicio. 2. Backup que permita instalar el servicio en una infraestructura alternativa. 3. Activar el plan de comunicaciones para informar a todos los usuarios que el servicio tendrá retrasos.	48 horas
Mesa de servicios	Factores de orden público en donde se debe evacuar la entidad	1. Teletrabajo del personal que atiende la Mesa de servicio. 2. Activar el plan de comunicaciones para informar al personal y que facilite evacuar la Entidad. 3. Operación de nivel 1 y 2 con personal directo de la Dirección de Tecnología.	12 horas
Mesa de servicios	Emergencia por ataque informático	1. Backups que permitan instalar el servicio en una infraestructura alternativa. 2. Implementar las políticas y controles del GDI-TIC-M004 Manual de Gestión de seguridad de la información y el procedimiento de Gestión de incidente de seguridad de la información. 3. Atención priorizada a usuarios VIP y responsables de procesos críticos. 4. Operación de la Mesa de servicios en contingencia por el canal o aplicativo que esté disponible (ej: si se dañó el contact center, entonces se reciben casos por correo electrónico).	24 horas
Mesa de servicios	Indisponibilidad del personal de la Dirección de Tecnologías e Información	1. Operación de la Mesa en contingencia, con el personal mínimo y crítico requerido en contingencia 2. Atención priorizada a usuarios VIP y responsables de procesos críticos	24 horas
Mesa de servicios	Indisponibilidad tecnológica de uno o más aplicativos	1. Backups que permitan instalar el servicio en una infraestructura alternativa. 2. Operación de la Mesa de servicios en contingencia por el canal o aplicativo que esté funcionando (ej: si no está disponible el contact center, entonces se reciben casos por correo electrónico)	48 horas
Todas las fuentes de datos que no	Desastre natural	1. Si solo se afectan las instalaciones de la Entidad, según el GDI-TIC-M004 Manual de gestión de seguridad de la información,	12 horas

Servicio TI	Escenario de continuidad	Descripción de la Alternativa (plan de operación alterno)	RTO (tiempo de recuperación objetivo)
estén en bases de datos en la nube		estas fuentes de datos deben estar en Sharepoint en infraestructura en la nube (y por lo tanto no tendrían afectación). 2. Backups que permitan recuperar las fuentes de datos en un estado reciente. Estos backups pueden estar en Sharepoint o en aplicativos institucionales como el correo electrónico.	
Todas las fuentes de datos que no estén en bases de datos en la nube	Factores de orden público en donde se debe evacuar la entidad	1. Activar el plan de comunicaciones para informar al personal y que facilite evacuar la Entidad. 2. Si solo se afectan las instalaciones de la Entidad, según el GDI-TIC-M004 Manual de gestión de seguridad de la información, estas fuentes de datos deben estar en Sharepoint en infraestructura en la nube (y por lo tanto no tendrían afectación).	12 horas
Todas las fuentes de datos que no estén en bases de datos en la nube	Emergencia por ataque informático	1. Si solo se afectan las instalaciones de la Entidad, según el GDI-TIC-M004 Manual de gestión de seguridad de la información, estas fuentes de datos deben estar en Sharepoint en infraestructura en la nube (y por lo tanto no tendrían afectación). 2. Si las fuentes de datos fueron comprometidas en su última versión, se debe ir a versiones de backup que permitan recuperar las fuentes de datos en un estado reciente. 3. Si se afectan los computadores personales corporativos, simplemente el personal usará otro computador no comprometido.	12 horas
Todas las fuentes de datos que no estén en bases de datos en la nube	Indisponibilidad del personal de la Dirección de Tecnologías e Información	Este escenario no aplica, ya que este servicio TI es autoadministrado por el usuario.	N/A
Todas las fuentes de datos que no estén en	Indisponibilidad tecnológica de uno o más aplicativos	1. En caso de que el aplicativo con que se visualizan las fuentes de datos no esté disponible en línea, se debe usar la versión de escritorio.	RTO del proveedor de nube

Servicio TI	Escenario de continuidad	Descripción de la Alternativa (plan de operación alterno)	RTO (tiempo de recuperación objetivo)
bases de datos en la nube		2. En caso de que Sharepoint no esté disponible, se debe hacer efectivo el ANS de la nube.	
Conectividad de los enlaces de datos	Desastre natural	1. Activar el plan de comunicaciones para informar al personal y a los usuarios. 2. Contar con la disponibilidad del proveedor de los equipos tecnológicos para habilitar en contingencia. 3. Disponer del personal de soporte en sitio para el desmonte de los equipos afectados. 4. Disponer del especialista en redes para las configuraciones requeridas.	2 horas
Conectividad de los enlaces de datos	Factores de orden público en donde se debe evacuar la entidad	1. Teletrabajo del personal que atiende los enlaces de datos. 2. Activar el plan de comunicaciones para informar al personal y que facilite evacuar la Entidad.	2 horas
Conectividad de los enlaces de datos	Emergencia por ataque informático	1. Disponer del personal de soporte en sitio para el desmonte de los equipos afectados. 2. Disponer del especialista en redes para las configuraciones requeridas.	2 horas
Conectividad de los enlaces de datos	Indisponibilidad del personal de la Dirección de Tecnologías e Información	1. Contar con personal de respaldo en la DTI. 2. Contar con manuales técnicos que permitan delegar las funciones a personal con conocimiento técnico mínimo.	2 horas
Conectividad de los enlaces de datos	Indisponibilidad tecnológica de uno o más aplicativos	1. Disponer del personal de soporte en sitio para el desmonte de los equipos afectados. 2. Disponer del especialista en redes para las configuraciones requeridas.	2 horas

2.5. ESTRATEGIA DE CONTINUIDAD

La estrategia de continuidad de negocio brinda los procedimientos sustentables de operaciones TI, mientras se lleva a cabo la recuperación de los servicios luego de que estos fueron afectados por una amenaza.

También se puede decir que la continuidad de negocio es el nivel de preparación que tiene la Entidad para mantener las funciones esenciales tras una emergencia o una interrupción. Estos eventos pueden incluir vulneraciones de seguridad, desastres naturales, averías de los equipos o la salida repentina de personal clave (tal como lo mencionan los escenarios de continuidad seleccionados).

La estrategia de continuidad de negocio es clave para cualquier proyecto de continuidad TI. Para este caso el conocimiento de los activos que soportan los servicios críticos cuando ocurre un escenario, determina si la Entidad es capaz de recuperar sus servicios TI en el tiempo adecuado. En los casos donde no se llegue a recuperar en el tiempo establecido, se deberán establecer estrategias de recuperación adicionales.

Algunos de los beneficios más importantes de las estrategias de continuidad son:

- Prevenir y minimizar las pérdidas para el negocio en caso de ocurrencia de un evento.
- Dar visibilidad de los riesgos que podrían impactar en la prestación de los servicios.
- Organizar y priorizar la recuperación de las dependencias.
- Medir posibles pérdidas generadas por la emergencia.

Para mantener respaldada la información, garantizar su integridad, confidencialidad y disponibilidad, poder cumplir con los requerimientos de la continuidad del negocio en la prestación de los servicios TI para la Secretaría Distrital de Gobierno, se usa una metodología la cual permite mitigar y gestionar los riesgos que amenazan la continuidad en la prestación de estos servicios para lo cual se contará, entre otros, con copias de seguridad que permitan restaurar los servicios y aplicativos.

El diseño de la presente propuesta se basa en las mejores prácticas del estándar de la norma ISO 22301:2012, y en guías técnicas de instituciones reconocidas en el campo de la continuidad de negocio. Con el objetivo de entregar a la Entidad la capacidad de resiliencia y dar continuidad a la prestación de sus servicios TI.

El desarrollo de estas estrategias permite establecer un conocimiento para entender la continuidad del negocio, así como la de implementar políticas que permitan la continuidad de los servicios TI para que de una manera fácil y segura se pueda garantizar la integridad, confidencialidad y disponibilidad de la información. El compromiso de la Entidad, en conjunto con prácticas internacionales, protege los intereses propios de la misma, su reputación ante la ciudadanía, de una manera muy importante evita pérdidas de información y de esta forma brinda una mayor estabilidad a los empleados y usuarios. Los fundamentos de la estrategia de continuidad se describe en los siguientes cinco numerales.

2.5.1. Lineamientos de las estrategias de continuidad

- Estas estrategias están orientadas a la protección de las personas, así como al restablecimiento oportuno de la prestación de los servicios TI, frente a eventos de interrupción o desastre.

- Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad de negocio, mediante labores periódicas de formación, divulgación y pruebas del Plan de Continuidad TI.

- Las etapas de las estrategias se deben ejecutar por cada una de las dependencias de la Entidad, con la guía y coordinación de la Dirección de Tecnologías de la Información.

- Se debe realizar por lo menos una prueba anual a las estrategias de continuidad definidas.

- El análisis de impacto del negocio debe actualizarse por lo menos una vez al año o cada vez que un líder de Proceso lo requiera, teniendo en cuenta los cambios de la Entidad y sus necesidades.

- En caso de presentarse la ocurrencia de un evento significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos.

- Equipo de Crisis: El objetivo o función principal de este grupo es planificar, coordinar, unificar percepciones y líneas de acción de todas las personas de la Entidad y la toma de decisiones en caso de que ocurra un evento que cause la interrupción en la prestación de los servicios TI que manejan continuidad en la Entidad. Dentro de sus funciones podemos destacar las siguientes:

    - Analizar la situación para responder oportunamente.
    - Tomar la decisión de activar o no el Plan de Continuidad.
    - Iniciar el proceso de notificación a los funcionarios a través de los diferentes responsables.
    - Definir un presupuesto estimado para gastos que genere la crisis.
    - Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.
    - Tomar decisiones ante situaciones o imprevistos durante la recuperación del servicio.
    - Comunicar a los diferentes comités de la Entidad las decisiones que se tomen.

- Oficina Asesora de Comunicaciones: Es la responsable del manejo de las comunicaciones con todas las partes interesadas. Las comunicaciones tienen como función principal servir de apoyo para que en caso de la ocurrencia de un escenario, se pueda proceder de manera efectiva y eficiente a realizar el contacto de las diferentes personas que conforman el Equipo de crisis. Por lo tanto, los equipos de comunicaciones son los responsables de la elaboración y divulgación de las comunicaciones de la Entidad hacia las partes interesadas tanto externas (usuarios, ciudadanía) como internas (Directivos, funcionarios y contratistas) durante y después de la crisis. En la Entidad, la Oficina Asesora de Comunicaciones, operará en contingencia de la siguiente manera:

    - Comunicaciones con los organismos de control
    - Comunicaciones con las entidades externas y medios
    - La comunicación con los medios o elementos utilizados por estos funcionarios se realizará a través de: el correo electrónico institucional, las cuentas de WhatsApp, las redes sociales, mensajes de texto, la intranet y el portal web de la Entidad.

- Comunicaciones con los funcionarios de la DTI: El Director de la DTI debe tener los contactos telefónicos de sus colaboradores. Los elementos con los que cuenta la Dirección de Tecnologías e Información para comunicarse internamente y para notificar la información correspondiente son: el correo electrónico, el teléfono celular personal, el teléfono de la casa, las redes sociales y las aplicaciones de mensajería de la Entidad.

La Entidad cuenta con el GCO-GTH-P004 "Procedimiento de prevención, preparación y respuesta ante emergencias que se presentan en la SDG" el cual cubre lo propio desde una perspectiva no tecnológica, por lo cual está en cabeza de la Dirección de Gestión del Talento Humano.

2.5.2. Lista de verificación de respuesta inmediata

Es el conjunto de todas las acciones principalmente sistemas de alerta, planes de capacitaciones, equipamiento, de coordinación, centros de reserva, entrenamiento, pruebas y simulacros entre otras, que se necesitan para hacer óptima la ejecución de las respuestas.

De esta forma se establecen las acciones e iniciativas necesarias con base a las estrategias de recuperación, se documentará las mejoras o las lecciones aprendidas y las respectivas actividades llevadas a cabo para recuperar la continuidad.

Se deben considerar todos los incidentes tanto naturales como los ocasionados por el hombre. La efectividad de las respuestas está dada proporcionalmente a las medidas de preparación que se implementen.

Al interior de la Dirección de Tecnologías e Información existe personal al que le deben reportar los incidentes que se presentan; este personal debe trabajar de forma coordinada; la Dirección de Tecnologías e Información debe compartir la información y perspectivas que se tengan, enfatizar la importancia de la seguridad de la información y la mejora continua para todos y cada uno de los actores involucrados en este Plan.

Se requiere que al detectar las señales tempranas de un posible escenario de emergencia estos equipos de respuesta y líderes de respuesta de los diferentes escenarios sean muy proactivos.

Plan de gestión de crisis

Su objetivo es evitar que se tomen decisiones improvisadas que puedan empeorar la crisis o que, simplemente, no se tomen decisiones. Contiene todos los elementos necesarios para la gestión de los momentos iniciales de una crisis.

Un plan de gestión de crisis describe cómo reaccionará la Entidad ante una crisis e identifica quién hará qué y cuáles serán las funciones. El objetivo de este plan es minimizar los efectos negativos y restaurar la prestación de los servicios TI lo antes posible. A continuación las directrices más importantes del plan de crisis de la Secretaría Distrital de Gobierno:

- Para enfrentar una crisis se debe actuar con tranquilidad, transparencia y prudencia.
- Se debe decir la verdad ante cualquier situación de crisis.
- No se deben dar declaraciones a ningún medio de comunicación, sin que pase por la Oficina Asesora de Comunicaciones.
- No se debe exagerar la situación o minimizar el problema.

Coordinación de ayuda con otras entidades

Se debe tener en cuenta que solo se realizan acciones de gestión de la continuidad en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades durante y después del desastre pueden estar dirigidas en buscar ayuda con otras entidades para evitar que las acciones del siniestro causen más daños o destrucciones. Por lo anterior se plantean las siguientes sugerencias:

- Tener en las dependencias los números de teléfono y direcciones de organismos e instituciones de ayuda (ej: Bomberos, Policía, etc.).
- Todo el personal debe conocer la localización de vías de Escape o Salida (deben estar señalizadas las vías de escape o salida).
- Instruir al personal de la entidad respecto a evacuación ante sismos, a través de simulacros; esto se realiza acorde a los programas de seguridad organizadas al interior de la entidad y por otros entes (ej: Defensa Cívil, etc.).
- Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra con ciertos colores fácilmente visibles.
- En caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Hospitales, Centros de Salud, Ambulancias, Seguridad privada, etc.

2.5.3. Activación del plan

El director de la Dirección Tecnologías e Información es el encargado de activar el Plan de Continuidad TI. El director de la DTI delegará a encargados y responsables de centralizar la información de la emergencia, coordinar la solicitud y asignación de recursos, realizar seguimiento a las respuestas de la emergencia.

Es de vital importancia para todos los involucrados en la gestión de incidentes entender el valor que se tiene para reaccionar a tiempo considerando evaluar los riesgos y preparar las medidas de respuesta, manejar lo más pronto posible el incidente, identificar qué información se requiere compartir.

Para cada escenario identificado se definen las estrategias en donde se describen los recursos como equipos, herramientas y los medios necesarios para garantizar la respuesta inmediata a la situación de emergencia.

2.5.4. Plan de operación alterno

Como se describió en el capítulo de análisis de impacto al negocio, para cada escenario de continuidad se tiene un plan de operación alterno. Todos estos planes de operación requieren de una preparación previa y deben estar afinados (a través de múltiples pruebas) para cuando se presente el escenario real.

Una vez se activa el plan, se debe coordinar con:

- El líder del grupo al interior de la Dirección de Tecnologías e Información (ej: para instalar el servicio TI en una infraestructura alterna).

- El director o directora de la Oficina Asesora de Comunicaciones (ej: para iniciar el Plan de Comunicaciones).
- El Responsable de seguridad de la Información (ej: para la gestión de incidentes de seguridad de la información).
- En general con el director de la Dirección de Tecnologías e Información, que coordinará al interior de la DTI y con la demás dependencias en caso de ser necesario.

2.5.5. Resolución del Incidente

El Equipo de Crisis a través de los canales de comunicación oficiales (correo electrónico o celular) recibe confirmación de las autoridades de la finalización de la situación que obligó a la activación del plan.

El Equipo de Crisis también define si se debe autorizar el reinicio de operaciones en las instalaciones de la Entidad. En caso de autorizar el reingreso al nivel central o a las alcaldías locales se comunica la decisión mediante los canales oficiales (correo electrónico, intranet y redes sociales).

La Dirección de Tecnologías e Información junto a la Oficina Asesora de Comunicaciones deben gestionar la transmisión del mensaje de retorno a las instalaciones o en caso de afectaciones importante a las mismas, emitir un mensaje de prolongación del teletrabajo o trabajo remoto debido al mal estado de las instalaciones (a consecuencia del escenario presentado).

Dado el caso de que se haya usado infraestructura alternativa, la Dirección de Tecnologías e Información programará el retorno a la infraestructura principal a través de la respectiva comunicación institucional (por correo electrónico e intranet).

Si es autorizado y comunicado, los empleados y contratistas retornan a sus labores en la sede central y en las alcaldías locales.

De acuerdo con la naturaleza de la emergencia puede llegar a ser necesario reparar alguna de las sedes por daños causados por terremoto, inundación o incendio; también puede ser necesaria la limpieza de áreas con personal especializado en materiales contaminantes o en el peor escenario búsqueda de sedes alternas en caso de que la sede quede inutilizable.

Cuando las autoridades nacionales o distritales de salud así lo indiquen y siguiendo los protocolos de bioseguridad que para tal fin se definan, la Dirección de Gestión del Talento Humano determinará las condiciones de reactivación del trabajo en el nivel central y en las alcaldías locales.

2.6. PRUEBAS, MANTENIMIENTO Y REVISIÓN

De manera general la continuidad TI tiene como objetivo gestionar de manera efectiva en el tiempo las situaciones de crisis TI no deseadas.

El propósito del plan de pruebas es mostrar los distintos tipos de pruebas de contingencia que se deben llevar a cabo, lo cual lleva a la mejora continua del Plan de Continuidad TI.

Por otro lado, el plan de mantenimiento contiene aquellos eventos que deben disparar una revisión o modificación del sistema (por ejemplo, el cambio o migración de Servidores). La ejecución del plan de pruebas y el plan de mantenimiento es vital para garantizar la salud del Plan de Continuidad TI.

El plan de pruebas y el plan de mantenimiento permiten:

- Garantizar que la información del plan de continuidad TI se mantenga actualizada.
- Garantizar que la Entidad pueda recuperarse en los tiempos establecidos, en situación de contingencia, aspecto que puede determinar la continuidad de negocio.
- Incrementar la sinergia del personal implicado en una potencial contingencia.
- Mejorar el conocimiento de los usuarios en relación con las pruebas de continuidad.
- Incrementar la confianza de los usuarios en la Entidad.
- Realizar pruebas continuamente al Plan de continuidad en los cuales se debe dejar constancia de los resultados obtenidos mediante actas, las cuales permitirán definir las diferentes situaciones con el fin de mejorar con base en los resultados obtenidos y de tal manera que se puedan satisfacer necesidades o deficiencias del Plan de Continuidad TI.

Como ya se ha mencionado anteriormente, es necesario llevar a cabo diferentes pruebas al menos una vez al año, sobre los servicios TI que se hayan definido en el alcance. De esta manera cubrir el conjunto de escenarios que se han definido como potencialmente catastróficos, con diferentes grados de complejidad y elaboración. Para la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta los siguientes aspectos:

- Personal técnico implicado en la prueba.
- Usuarios que acceden a los servicios TI.
- Personal externo (ciudadanos, proveedores, etc.).
- Descripción de la prueba a realizar.
- Descripción del resultado esperado luego de la ejecución de la prueba.

- Hora y fecha de realización de la prueba.

Se debe tener en cuenta que siempre que la prueba pueda implicar una pérdida de la prestación del servicio TI, ya sea ejecutada con éxito o no, se debe planificar en un horario extralaboral o de impacto mínimo.

Posteriormente a la prueba, se elaborará un informe que recopile los resultados y describa las posibles incidencias surgidas durante ésta como son: los resultados no esperados, tiempos estimados superados, mala comunicación entre el personal, indisponibilidad de usuarios, proveedores, etc. Cualquier incidencia que se haya producido debe analizarse para la aplicación de las medidas correctivas que sean necesarias.

Se debe plantear un proceso de Concientización, de esta forma se fomenta la mejora continua del Plan de Continuidad TI. Además del análisis e implantación del plan, es necesario que el personal técnico, así como todos los involucrados tengan todo el conocimiento, apliquen las mejoras y las recomendaciones respectivas.

Gracias a lo anterior, se puede mantener actualizado el Plan de Continuidad TI en todo momento y esto permite que su vigencia sea renovada regularmente. Situaciones que disparan la actualización del plan de pruebas y mantenimiento son: cambios de la estructura organizacional, cambios tecnológicos importantes tales como los de Plataforma como servicio (PaaS) o Infraestructura como servicio (IaaS).

Actualización de la documentación

Se debe mantener actualizada toda la documentación cada vez que se produzca un cambio significativo en la Entidad, a nivel de la prestación de los servicios TI, de personal, o de cualquier otro aspecto relacionado.

Esto permitirá que la documentación a utilizar en una situación de crisis refleje plenamente la información de los distintos involucrados en los procesos: infraestructura, personal, proveedores y terceras partes que deben tenerse en cuenta en una situación de contingencia.

2.7. CONCLUSIONES

El presente Plan de continuidad TI de la Secretaría Distrital de Gobierno, tiene como objetivo principal el salvaguardar la infraestructura y los Sistemas de Información asociados a los servicios TI.

Las principales actividades requeridas para la implementación del Plan de Continuidad TI son: identificación de riesgos, minimización de riesgos, análisis de impacto al negocio y la estrategia de continuidad TI.

No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza la Dirección de Tecnología de cada entidad.

Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Continuidad TI.

2.8. RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Continuidad TI, con la finalidad de instruir adecuadamente al personal de la Secretaría Distrital de Gobierno.

Adicionalmente al plan de continuidad se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados. Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento. Cuando los administradores de infraestructura se encuentren ausentes, se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la Entidad no se vea interrumpida.

3. DOCUMENTOS RELACIONADOS

3.1. DOCUMENTOS INTERNOS

Código	Documento
GDI-TIC-P001	Procedimiento para la gestión de requerimientos TI
GDI-TIC-IN015	Instrucciones para la realización de copias de seguridad, pruebas de restauración y restauración de información.
GDI-TIC-M005	Manual de soporte físico y lógico de la infraestructura tecnológica de la secretaría distrital de gobierno.
GDI-TIC-M004	Manual de Gestión de Seguridad de la información
GDI-TIC-P008	Gestión de Incidentes
GDI-TIC-PL001	Plan Estratégico de las Tecnologías de Información (PETI)
GDI-TIC-PL002	Plan de Seguridad y Privacidad de la Información
GDI-TIC-PL003	Plan de Tratamiento de Riesgos de Seguridad
GCO-GTH-P004	Procedimiento de prevención, preparación y respuesta ante emergencias que se presentan en la SDG
PLE-PIN-M001	Manual de Gestión del Riesgo

3.2. NORMATIVIDAD VIGENTE

Norma	Año	Epígrafe	Artículo(s)
NTC 5722	2012	N/A	N/A
ISO 22301	2012	N/A	N/A
ISO 27001	2018	N/A	N/A
ISO 31000	2018	N/A	N/A

3.3. DOCUMENTOS EXTERNOS

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Guía para la preparación de las TIC para la continuidad del negocio.	Versión 1 15/12/2010	MinTIC	Virtual http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf
Ley 1523 de 2012 Sistema Nacional para la Gestión del Riesgo de Desastres.	2012	Congreso de Colombia	Virtual https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=47141