ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DISTRITAL DE LA MUJER

PLAN DE CONTINGENCIA DE GESTIÓN TECNOLÓGICA

2025

Nota: Si usted imprime este documento se considera “copia no controlada” por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.

Tabla de contenido

INTRODUCCIÓN 3

1. OBJETIVO 3

2. ALCANCE 3

3. DEFINICIONES Y/O GLOSARIO 4

4. LÍNEAS DE ACCIÓN O COMPONENTES 9

5. DESARROLLO DOCUMENTO 11

6. CRONOGRAMA 14

7. DESCRIPCIÓN DE ACTIVIDADES 14

8. RECURSOS 15

Introducción

Este documento contiene el plan de contingencias del proceso Gestión Tecnológica de la Secretaría Distrital de la Mujer (SDMujer). En las primeras páginas encontrará la política de contingencia de los servicios de TI de la Entidad, la cual incluye el objetivo general, los objetivos específicos, el alcance, las responsabilidades y la estrategia a seguir.

El desarrollo del tema incluye entre otros la identificación y clasificación de equipos y servicios clave, análisis del riesgo, análisis del impacto, recursos necesarios, y en general el contexto en el que se debería desarrollar la atención de una contingencia.

En la elaboración de este manual se propendió por la claridad, efectividad y optimización de las soluciones propuestas, para así hacer de este una guía práctica, la cual oriente al administrador o usuario asignado en la búsqueda de una solución ante un problema o incidente determinado que pueda poner en riesgo la continuidad de los servicios de TI que presta la Entidad.

1. Objetivo

El objetivo general de este plan es orientar a los administradores de TI de la Secretaría Distrital de la Mujer (SDMujer) en la búsqueda de soluciones que permitan dar continuidad a la prestación de los procesos misionales de la Entidad ante la ocurrencia de incidentes o eventos en la plataforma tecnológica que pongan en riesgo la disponibilidad o ejecución de los mismos.

2. Alcance

Este plan se enmarca en el proceso de Gestión Tecnológica y en la infraestructura de TI de la Secretaría Distrital de la Mujer (SDMujer), específicamente en sus componentes funcionales de hardware y software; también participan las jefas de oficina, administradores, operadores, personal de apoyo, proveedores y demás integrantes del equipo de TI de la Entidad.

El enfoque de este documento se encuentra en los servicios que el proceso de Gestión Tecnológica presta y soporta para beneficio de los usuarios internos y externos de la SDMujer.

La elaboración, puesta en marcha y posible ejecución de las actividades de este plan dependen de los recursos disponibles para cada etapa. El factor humano, la disponibilidad de los servicios y la existencia en stock de piezas o partes contratadas con terceros, el presupuesto, entre otros, son aspectos determinantes para la correcta, oportuna y eficaz atención de un evento inesperado que pueda afectar la continuidad del negocio.

Aunque la Oficina Asesora de Planeación administra el proceso de Gestión Tecnológica, el cual es considerado como apoyo respecto de otros procesos del sistema de gestión de la Entidad, este plan no incluye análisis, recursos, tiempos ni actividades para el restablecimiento de servicios o productos propios de otras dependencias, más que las necesarias para brindar una plataforma tecnológica que permita desempeñar a cada funcionario de la SDMujer las labores propias de su cargo.

3. Definiciones y/o glosario

Plan de Contingencia: Es una estructura estratégica y operativa, que ayuda a controlar situaciones de emergencia y a minimizar los impactos negativos que esta pueda generar sobre una organización, para esto implementa una serie de procedimientos alternativos que permitan recuperar el funcionamiento normal de la operación en el menor tiempo posible.

RTO (Recovery Time Objective): Es el tiempo y nivel de servicio en el que debe ser restaurado un proceso del negocio después de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

RPO (Recovery Point Objective): Es el período máximo tolerable de pérdida de datos de un Servicio de TI antes de ser restablecido como consecuencia de un desastre o interrupción, con el fin de evitar consecuencias inaceptables para la continuidad del negocio.

Criticidad: Es una medida ponderada de la **“magnitud del problema”** que ocasionaría la falla total o no disponibilidad de un equipo o servicio determinado; la cual considera e*l efecto* y *la complejidad* de la reparación o recuperación del mismo y se clasifica de la siguiente manera:

Baja (1): La falla del sistema afecta a un número mínimo de usuarios internos y se cuenta con los medios para brindar una solución inmediata.

Media (2): La falla del sistema afecta a un número menor de usuarios internos o externos, por ejemplo, un área o un piso, pero se cuenta con los medios para brindar una solución en menos de cuatro (4) horas.

Alta (3): La falla del sistema afecta a un número mayor de usuarios internos o externos, por ejemplo, entre el 50% y 100% de los funcionarios de la Entidad, pero se cuenta con los medios para brindar una solución en un tiempo no superior a ocho (8) horas.

Extrema (4): La falla del sistema afecta a un número mayor de usuarios internos o externos, por ejemplo, más del 50% de las sedes que atienden público por medio del sistema SIMISIONAL, y no se cuenta con los medios para garantizar una solución antes de un tiempo específico.

Impacto[1]: Es la consecuencia que puede ocasionar a la organización la materialización del riesgo. Es una medida ponderada del **"grado de afectación"** que ocasionaría una falla específica en un equipo o servicio determinado; la cual considera e*l efecto* y *la complejidad* de la reparación o recuperación del mismo y se clasifica de la siguiente manera:

Insignificante (1): La falla no compromete la disponibilidad del sistema ya que se cuenta con equipos redundantes y con los medios para brindar una solución inmediata.

Menor (2): La falla compromete la disponibilidad del sistema y puede afectar temporalmente a algunos usuarios internos, pero se cuenta con los medios para brindar una solución inmediata.

Moderada (3): La falla compromete la disponibilidad del sistema temporalmente y afecta a un grupo de usuarios internos o externos, por ejemplo, un área o un piso, pero se cuenta con los medios para brindar una solución en menos de cuatro (4) horas.

[1] *Desarrollado con base en la Guía de Administración del Riesgo. Elaborada por el Departamento Administrativo de la Función Pública DAFP por medio de la Escuela Superior de Administración Pública ESAP. Cuarta Edición 2009.*

Mayor (4): La falla compromete la disponibilidad del sistema permanentemente, puede afectar a un gran número de usuarios internos o externos, por ejemplo, entre el 50% y 100% de los funcionarios de la Entidad, pero se cuenta con los medios para brindar una solución en un tiempo no superior a ocho (8) horas.

Catastrófico (5): La falla compromete la disponibilidad del sistema permanentemente, puede afectar a un gran número de usuarios internos o externos, por ejemplo, entre el 50% y 100% de las sedes que atienden público por medio del sistema SIMISIONAL, y no se cuenta con los medios para garantizar una solución antes de un tiempo específico.

Probabilidad[2]: Grado en el cual es probable que ocurra un evento, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir. La probabilidad la podemos determinar de la siguiente manera:

Raro (1): Puede ocurrir sólo en circunstancias excepcionales.

Improbable (2): Pudo ocurrir en algún momento.

Posible (3): Podría ocurrir en algún momento.

Probable (4): Probablemente ocurrirá en la mayoría de las circunstancias.

Casi certeza (5): Se espera que ocurra en la mayoría de las circunstancias.

Riesgo[3]: Posibilidad de que una vulnerabilidad sea aprovechada por alguna amenaza e impacte negativamente sobre el correcto funcionamiento del sistema o alguno de sus componentes. Posibilidad

[2] *Desarrollado con base en la Guía de Administración del Riesgo. Elaborada por el Departamento Administrativo de la Función Pública DAFP por medio de la Escuela Superior de Administración Pública ESAP. Cuarta Edición 2009.*

[3] [3] *Desarrollado con base en la Guía de Administración del Riesgo. Elaborada por el Departamento Administrativo de la Función Pública DAFP por medio de la Escuela Superior de Administración Pública ESAP. Cuarta Edición 2009.*

de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

El riesgo *R* se evalúa mediante la medición de los dos parámetros que lo determinan, el *impacto* de la pérdida o daño posible *I*, y la probabilidad *P* que dicha pérdida o daño llegue a ocurrir.

Por ejemplo: *R = I x P; R = Grado de Afectación "Catastrófico (5)" x La probabilidad de ocurrencia "Casi certeza (5)"; R = (5) x (5); R = 25.*

Otro ejemplo: *R = I x P; R = Grado de Afectación "Insignificante (1)" x La probabilidad de ocurrencia "Raro (1)"; R = (1) x (1); R = 1.*

El riesgo lo podemos evaluar de la siguiente manera por zonas:

Zona de Riesgo Baja (De 1 a 5): Significa que su probabilidad es rara, improbable o moderada y su Impacto es insignificante o menor, lo cual permite a la entidad asumirlo. Es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Zona de Riesgo Extrema (19 a 25): Significa que su probabilidad es moderada, probable o casi certeza y su Impacto moderado, mayor o catastrófico; por tanto, es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible. De lo contrario, se deben implementar controles de prevención para evitar la Probabilidad del riesgo, de protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

Si el riesgo se sitúa en cualquiera de las otras zonas como: *moderada (De 6 a 11)*, o *alta (De 12 a 18)*, se deben tomar medidas para llevar, en lo posible, los riesgos a la zona moderada o baja. Siempre que el riesgo sea calificado con Impacto catastrófico, la entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.

Complejidad de Recuperación: Es la medida de la percepción sobre qué tan fácil es remplazar, reconfigurar o reanudar los servicios o equipos con los que cuenta la Entidad ante algún imprevisto. El grado de complejidad lo podemos determinar de la siguiente manera:

Fácil (1): Se dispone de los medios y recursos en sitio para brindar una solución inmediata.

Realizable (2): Aunque se dispone de los medios y recursos en sitio no se puede brindar una solución inmediata debido a los tiempos que toman las actividades necesarias para la recuperación del equipo o servicio en cuestión.

Estándar (3): La falla requiere la intervención del fabricante o especialista y se cuenta con la garantía o con el contrato de soporte vigente correspondiente.

Difícil (4): La falla requiere la intervención del fabricante o especialista pero no se cuenta con la garantía del componente ni con un contrato de soporte vigente.

Responsables o líder de proceso

- Liderar la elaboración y actualización del plan de contingencia, así como el manejo de las situaciones consideradas en el mismo.

- Asegurar que los planes que se definan para el manejo de las situaciones de contingencia estén enmarcados en la normatividad interna de la SDMujer.

- Socializar y promover el compromiso del área en la elaboración del plan, así como durante la ocurrencia de una contingencia.

- Tomar decisiones con base en los resultados de las pruebas o incidentes reales para optimizar tiempos, costos y recursos.

4. Líneas de acción o componentes

La Secretaría Distrital de la Mujer cuenta con una infraestructura tecnológica que soporta y apoya la permanente ejecución de los cuatro grupos de procesos que componen su Sistema Integrado de Gestión.

El centro de cómputo de la Secretaría Distrital de la Mujer cuenta con una infraestructura que incluye comunicaciones, seguridad, servidores y planta telefónica. Desde allí se prestan diversos servicios, tales como aplicaciones web, DNS, DHCP, respaldo, políticas de controlador de dominio, telefonía, entre otros.

La plataforma de producción está basada en servidores VMware, mientras que la plataforma de hiperconvergencia Simplivity integra sistema de virtualización, almacenamiento, procesamiento, redes y respaldo. En este sistema operan máquinas virtuales con Windows y Linux, las cuales permiten ofrecer los servicios a funcionarias(os), contratistas y terceros que acceden a la entidad y sus servicios.

Adicionalmente, se dispone de una plataforma de virtualización basada en Windows (Hyper-V) para el desarrollo y pruebas de aplicaciones, páginas web y otros desarrollos utilizados por la entidad.

Se cuenta con un sistema de seguridad perimetral tanto físico como lógico. El primero cubre las necesidades del centro de cómputo principal de la Secretaría, mientras que el segundo protege la nube OCI. Ambos están interconectados mediante una VPN punto a punto, lo que permite la conexión y el trabajo del personal de la entidad.

Para proteger el centro de cómputo principal, se ha instalado un aire acondicionado de precisión de 3 toneladas y dos UPS, uno de 20 KVA y otro de 40 KVA, para regular toda la red central.

Finalmente, la infraestructura de comunicaciones está compuesta por cinco switches de acceso marca Cisco, dos switches Core y dos switches de acceso con PoE, que soportan la telefonía SIP con dispositivos Grandstream.

Plataforma Misional: Son todos los componentes informáticos de hardware y software relacionados directamente con la atención a mujeres: apoyo psicológico, orientación legal, cursos, y en general la programación de actividades. En otras palabras, son los componentes tecnológicos que ayudan a la SDMujer a realizar su misión.

Descripción General de la Plataforma Misional: Se identifican los componentes de la línea base de la arquitectura tecnológica en servicios de infraestructura, entre estos están: nube, servidores, servicio de almacenamiento, servicio de telefonía, redes de comunicaciones LAN, WLAN y WAN, seguridad y periféricos.

La Secretaría Distrital de la Mujer cuenta con dos canales de internet (principal y backup) con el mismo proveedor por diferentes nodos, dos canales de datos (principal y backup) para conectarse con las diferentes sedes, 22 sedes conectadas a nivel central por MPLS, por los cuales realiza consultas a los servicios y salida a internet, 20 canales de internet para los centros de inclusión digital para salida a internet directamente.

En las sedes de la Secretaría se cuentan con los servicios de, red cableada, wifi, servicio de impresión, telefonía IP e internet, además en 18 sedes hay Centros de Inclusión Digital para las usarías.

La Entidad cuenta con un sistema de hiperconvergencia que permite brindar alta disponibilidad de los servicios y aplicaciones que se prestan desde el centro de datos principal, donde está alojado el sistema misional, la administración de la red, infraestructura de servidores Windows y Linux, el sistema de gestión documental, aplicaciones cliente servidor y aplicativos webs entre otros.

Cuenta con una nube de Oracle que se interconecta con el nivel central a través de una VPN entre el firewall virtual y el firewall físico que se tienen desplegados.

Plataforma de Apoyo o Gestión: Son todos los componentes informáticos de hardware y software que soportan la gestión humana, administrativa, recursos financieros, tecnologías de la información y la gestión jurídica.

La plataforma de apoyo igualmente brinda soporte a los procesos de evaluación en actividades de control y a los procesos estratégicos en actividades de planeación y comunicación.

Descripción General de la Plataforma de Apoyo: El esquema de red de la Entidad está conformado por canales de fibra óptica, red lógica cableada y wifi, interconectadas por medio de un firewall perimetral que conecta al nivel central a través de un switch core y a cada una de las sedes por switch de acceso, a través de los cuales se prestan los diferentes servicios; el centro de cómputo principal cuenta con dos sistemas de virtualización el primero en Hyper-v para desarrollo y pruebas, el segundo en VMware para producción.

El esquema de servidores del centro de cómputo del nivel central cuenta con dos sistemas de virtualización, Hyper-v para desarrollo y pruebas, y VMware con Simplivity para producción, donde se tienen servicios de aplicaciones web, servidores de aplicaciones, servidor de archivos, servidores de bases de datos, controladores de dominio y servidores de administración.

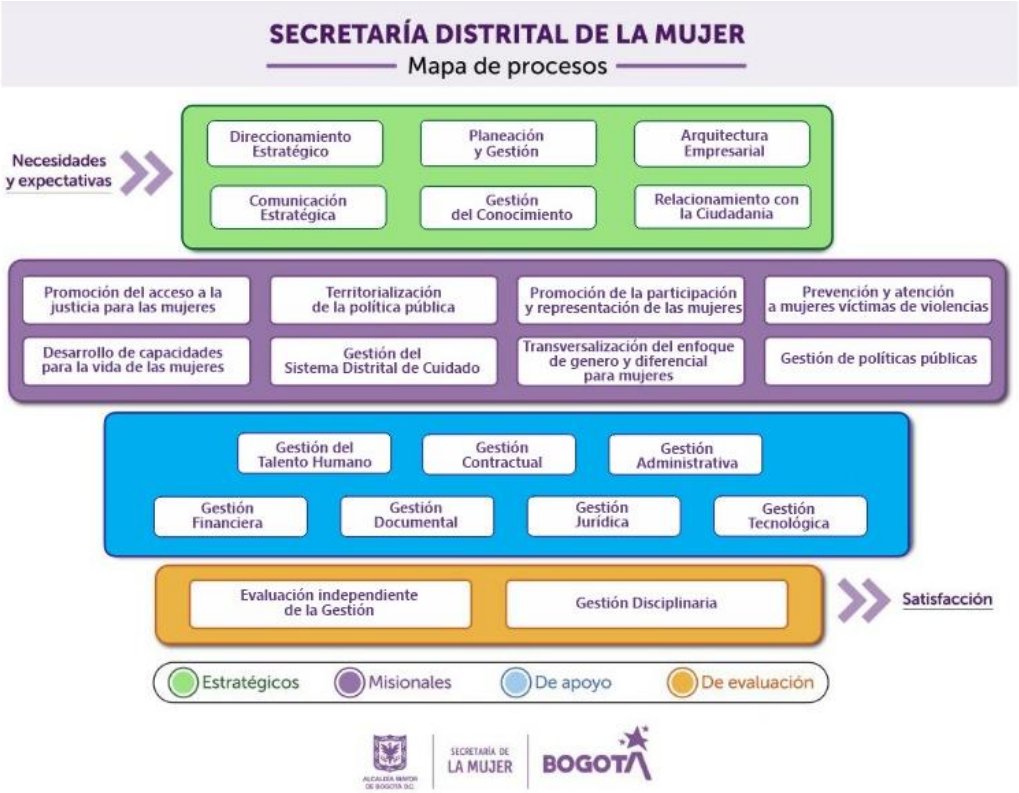
Se tiene un servicio de colocación donde reposa un servidor y un switch, con el cual se están realizando pruebas de DRP para continuidad de los servicios.

Finalmente, la Entidad cuenta con un sistema de mesa de ayuda, dónde soporta la prestación de servicios a las(os) funcionarias(os) y/o contratistas de la secretaría, se tienen definidos los ANS, y se estipulan los tiempos y personal que realizará las incidencias y requerimientos que surjan al interior de la SDMujer y sus sedes.

5. Desarrollo documento

Análisis de los Componentes Tecnológicos

El análisis se ha realizado teniendo en cuenta el mapa de procesos del Sistema Integrado de Gestión y los indicadores de disponibilidad de la plataforma de TI correspondientes al proceso de Gestión Tecnológica.



Para determinar las necesidades y actividades a realizar respecto de la implementación de la contingencia para los diferentes componentes de la plataforma de TI de la Secretaría Distrital de la Mujer, se ha realizado un análisis que incluye factores como la criticidad y el riesgo, con base en los cuales, se realiza una ponderación que indica la prioridad con la que se debe proceder.

Inicialmente se multiplicó el impacto por la probabilidad para hallar el riesgo de cada componente; posteriormente ese riesgo se multiplicó por la criticidad asociada para el componente en cuestión. El resultado de la anterior multiplicación la llamamos “Ponderación”, la cual entre mayor sea su valor, mayor es el nivel de prioridad.

Todos los factores anteriormente mencionados se establecieron conforme la definición y clasificación de este documento. También se tuvieron en cuenta los indicadores de disponibilidad que los administradores de los componentes reportan mensualmente y que se adjuntan a la documentación del sistema integrado de gestión.

Ejemplo:

Componente = SIMISIONAL
Descripción = Sistema para el registro y gestión de atenciones.
Clasificación = Misional
Criticidad = Alta (3)
Riesgo = Impacto x Probabilidad de Ocurrencia (Indicadores de Disponibilidad)
Riesgo = Mayor (4) x Posible (3)
Ponderación = Riesgo (12) x Criticidad (3)
Ponderación = 36
Zona de riesgo: Alta (Rango del 12 al 18)

Entonces se concluye:

La ponderación más alta posible que pudiera alcanzar un componente es de cien (100), al cual habría que asignarle la prioridad uno (1 - la más alta); y la ponderación más baja posible sería uno (1), al Cual habría que asignarle la prioridad más baja posible, distribuyendo proporcionalmente según el número total de componentes.

Estrategia

La Oficina Asesora de Planeación conoce la importancia de contar con un plan de contingencias completo, actualizado, revisado, probado y divulgado al interior del área, por esto ha trabajado en la elaboración de este documento y ha implementado el trabajo en pares para cada servicio y elemento que compone la plataforma de TI de la Secretaría Distrital de la Mujer (SDMujer).

Existe un principal y un suplente sobre la administración y soporte de cada servicio, de esta manera, ante la ausencia del administrador principal, existirá otra persona que estará en capacidades de ejecutar las tareas principales del servicio o dispositivo en cuestión de tal manera que se garantice la disponibilidad de estos.

Con el objetivo de garantizar la disponibilidad de la información de la Entidad se han contratado los servicios de Microsoft para el almacenamiento de información en la nube a través de aplicaciones como: OneDrive, SharePoint y correo electrónico; entre otras aplicaciones complementarias como Planner, Teams y Forms.

Adicionalmente, se cuenta con soporte especializado para las aplicaciones proveídas por terceros, garantía extendida en hardware para los equipos de la plataforma y la adquisición del servicio de DLP el cual permite detectar y prevenir la filtración de datos confidenciales.

6. Cronograma

Las actividades del Plan de Contingencia del proceso Gestión Tecnológica se vienen adelantando desde la vigencia 2024 con la definición de los lineamientos sobre medidas de contingencia y gestión del cambio aplicables en la actualización de sistemas de información. En la vigencia 2025 se ha continuado con el proceso de análisis de componentes con sus respectivas clasificaciones según la evaluación de aspectos como: impacto, probabilidad, riesgo, etc. La cobertura de la plataforma y sus componentes asociados depende de la disponibilidad de las herramientas y de la capacidad de las mismas.

7. Descripción de actividades

ACTIVIDADES REALIZADAS SOBRE LA PLATAFORMA TECNOLÓGICA

DLP (Prevención de Pérdida de Datos)

La Secretaría Distrital de la Mujer se encuentra en proceso de implementación de una solución tipo DLP que sirve para prevenir la fuga voluntaria e involuntaria de información, se trata de un software que ayuda al administrador de redes a controlar los datos que los usuarios pueden transferir. La solución DLP usa reglas de negocio para clasificar y proteger la información confidencial y crítica, para que los usuarios no autorizados no puedan intercambiar datos de manera accidental o malintencionada, cosa que podría poner en riesgo a la organización.

ORFEO

Se realizó la actualización de la versión del sistema de gestión documental Orfeo y adicionalmente se migró la base de datos a la nube de Oracle, la cual garantiza mejores tiempos de acceso; respaldo y restauración de la información mucho más ágil y mayores garantías en los temas relacionados con seguridad de la información.

PANDORA

Se realizó la implementación del sistema Pandora para la automatización y apoyo a la gestión de los procesos de contratación y administrativa de la SDMujer. De igual manera se determinó que la base de datos repose en la solución de nube que ofrece Oracle para contar con mayores garantías en cuanto a acceso, acciones contingentes y seguridad de la información.

SIMISIONAL

Se realizó la implementación del sistema SIMISIONAL 2.0 con alojamiento de la base de datos en la nube de Oracle, así como se realizó la migración de la información de la primera versión al nuevo sistema. Todo lo anterior con el objetivo no solo de prestar un mejor servicio sino aumentar los niveles de velocidad en la transferencia de datos, minimizar las vulnerabilidades y optimizar las acciones en respuesta a las situaciones de contingencia que se puedan presentar.

8. Recursos

Los recursos son los medios, elementos o activos necesarios para llevar a cabo una actividad, proyecto o proceso y alcanzar los objetivos propuestos. Pueden ser tangibles o intangibles y están disponibles en diversas formas, como materiales, humanos, financieros, tecnológicos, entre otros. Sin recursos adecuados, sería difícil ejecutar con éxito cualquier plan o acción.

Tipos de recursos:

- Recursos humanos: Ingenieros administradores de la plataforma tecnológica de Secretaría Distrital de la Mujer.
- Recursos financieros: Presupuesto necesario para financiar adquisición de equipos y servicios de TI.
- Recursos materiales: Infraestructura eléctrica y de redes de datos.
- Recursos tecnológicos: Herramientas digitales, software, plataformas y sistemas de información que facilitan la gestión y ejecución del proyecto.
- Recursos informativos: Datos, informes, investigaciones y conocimientos especializados que proporcionan la base para la toma de decisiones.

Control de cambios

No.	CAMBIOS REALIZADOS
1	Creación del documento

Responsables de elaboración, revisión y aprobación

ELABORADO POR	APROBADO POR	REVISADO POR	AVALADO POR
NOMBRE: José Leonardo Buitrago	NOMBRE: Carlos Alfonso Gaitán Sánchez	NOMBRE: Paula Vanessa Sosa Martin Luz Ángela Andrade Arévalo	NOMBRE: Carlos Alfonso Gaitán Sánchez
CARGO: Profesional Especializado OAP GT	CARGO: Jefe Oficina Asesora de Planeación	CARGO: Contratistas OAP	CARGO: Jefe Oficina Asesora de Planeación