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

PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

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.

Contenido

INTRODUCCIÓN 4

1. OBJETIVO 4

2. ALCANCE 4

3. RESPONSABLES 5

4. DEFINICIONES Y/O GLOSARIO 5

5. OBJETIVOS ESTRATÉGICOS 5

6. LÍNEAS DE ACCIÓN O COMPONENTES 6

6.1 PLANIFICACIÓN 7
6.2 IMPLEMENTACIÓN 8
6.3 EVALUACIÓN Y PRUEBAS 8
6.4 MEJORA CONTINUA 9

7. DESARROLLO DOCUMENTO 10

7.1 ANÁLISIS DE IMPACTO DE NEGOCIO (BIA) 10
7.1.1 IDENTIFICACIÓN DE FUNCIONES Y PROCESOS 10
7.1.2 EVALUACIÓN DE IMPACTOS OPERACIONALES 16
7.1.3 IDENTIFICACIÓN DE PROCESOS CRÍTICOS 17
7.1.4 ESTABLECIMIENTO DE TIEMPOS DE RECUPERACIÓN 18
7.1.5 IDENTIFICACIÓN DE RECURSOS 19
7.1.6 DISPOSICIÓN DEL RTO/RPO 21
7.1.7 IDENTIFICACIÓN DE PROCESOS ALTERNOS 22
7.1.8 GENERACIÓN DE INFORME DE IMPACTO DE NEGOCIO 24
7.1.9 CLASIFICACIÓN DE ESCENARIOS DE RIESGO 27
7.1.10 IDENTIFICACIÓN DE AMENAZAS 28
7.1.11 IDENTIFICACIÓN DE VULNERABILIDADES 29
7.2 ESTABLECIMIENTO DE OBJETIVOS, ALCANCE Y LÍMITES PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO (IRBC) 30
7.2.1 OBJETIVOS ESPECÍFICOS DEL IRBC 30
7.2.2 ALCANCE DEL IRBC 31
7.3 ASIGNACIÓN DE ROLES Y RESPONSABILIDADES A PERSONAL COMPETENTE 33

7.3.1 Estructura de Gobernanza para la Continuidad de TI 33
7.3.2 Roles y Responsabilidades Específicos 34
7.3.3 Equipos de Recuperación 35
7.3.4 Plan de Capacitación y Concienciación 36
7.4 IDENTIFICACIÓN DE BRECHAS ENTRE LOS REQUERIMIENTOS DE CONTINUIDAD Y LAS CAPACIDADES ACTUALES 36
7.4.1 Metodología para el Análisis de Brechas 36
7.4.2 Brechas Identificadas 37
7.4.3 Plan de Acción para Cierre de Brechas 37
7.5 DEFINICIÓN DE LA ESTRATEGIA IRBC ALINEADA CON LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 37
7.5.1 Principios Rectores de la Estrategia 37
7.5.2 Estrategias de Continuidad según Escenarios 38
7.5.3 Estrategias Específicas por Tipo de Recurso 39
7.5.4 Estrategias de Recuperación Tecnológica 40
7.5.5 Integración con la Política de Seguridad y Privacidad de la Información 41
7.6.6 Métricas de Efectividad de la Estrategia 42
7.5.7 Plan de Implementación de la Estrategia 42

8. CRONOGRAMA 43

9. DESCRIPCIÓN DE ACTIVIDADES 43

10. RECURSOS 44

INTRODUCCIÓN

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas permite minimizar el impacto y mejorar la recuperación por pérdida de activos de información de la Secretaría Distrital de la Mujer, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio) deben someterse a un análisis del impacto del negocio (BIA). Por ello, este plan de continuidad permitirá garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la organización estará preparada para responder en forma adecuada y oportuna, reduciendo de manera significativa un daño potencial.

De acuerdo con lo establecido por MinTIC en la "Guía para la preparación de las TIC para la continuidad del negocio" y los avances ya realizados por la Secretaría Distrital de la Mujer, este plan es un componente fundamental para garantizar la operación continua de los servicios tecnológicos que soportan los procesos misionales y estratégicos de la entidad.

1. OBJETIVO

Desarrollar e implementar un plan de continuidad de tecnologías de la información que garantice la restauración oportuna de las operaciones esenciales de la Secretaría Distrital de la Mujer ante eventos disruptivos, mitigando el impacto operacional, reputacional y financiero mediante estrategias efectivas de prevención, respuesta y recuperación.

2. ALCANCE

Este plan abarca todos los servicios tecnológicos críticos que soportan los procesos misionales y estratégicos de la Secretaría Distrital de la Mujer, desde la identificación de activos críticos, pasando por el análisis de impacto de negocio, hasta la implementación y prueba de estrategias de continuidad.

Incluye infraestructura tecnológica, aplicaciones, servicios de conectividad y bases de datos tanto en infraestructura OnPremise como en servicios en nube. Inicia con la planificación de la gestión de continuidad del negocio y finaliza con la evaluación del resultado de las pruebas realizadas al DRP (Plan de recuperación ante desastres), generando acciones correctivas y preventivas para fortalecer la continuidad de la operación.

3. RESPONSABLES

Oficina Asesora de Planeación – Gestión tecnológica.

4. DEFINICIONES Y/O GLOSARIO

- **Activo:** Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO 27000).
- **Análisis de Impacto del Negocio (BIA):** Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301).
- **Continuidad del negocio:** Capacidad de la organización para continuar la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo. (ISO 22301).
- **DRP (Plan de Recuperación ante Desastres):** Documento que contiene procedimientos detallados para recuperar sistemas de TI tras un desastre.
- **MTD (Maximun Tolerable Downtime):** Tiempo máximo que un proceso puede estar inoperante hasta que la entidad comience a tener pérdidas significativas.
- **RTO (Recovery Time Objective):** Tiempo transcurrido entre una interrupción y la recuperación del servicio.
- **RPO (Recovery Point Objective):** Punto en el tiempo hasta el cual se debe recuperar la información después de una interrupción.
- **WRT (Work Recovery Time):** Tiempo invertido en buscar datos perdidos y realizar reparaciones.
- **IRBC (ICT Readiness for Business Continuity):** Preparación de las TIC para la continuidad del negocio.

5. OBJETIVOS ESTRATÉGICOS

El plan de continuidad de TI está alineado con los siguientes objetivos estratégicos institucionales:

- Fortalecer la capacidad institucional mediante el mejoramiento continuo de los procesos, la gestión eficiente del talento humano y los recursos, para la prestación de servicios con oportunidad, calidad y transparencia.
- Diseñar e implementar estrategias para la articulación, coordinación y transversalización de los enfoques de derechos de las mujeres, de género y diferencial en el sector mujeres y los demás sectores de la administración distrital.

- Garantizar la operación continua de los sistemas de información que soportan los servicios a la ciudadanía.
- Implementar buenas prácticas de gestión de TI alineadas con los lineamientos de la Política de Gobierno Digital.

6. LÍNEAS DE ACCIÓN O COMPONENTES

El Plan de Continuidad de Tecnologías de la Información de la Secretaría Distrital de la Mujer se fundamenta en una metodología integral basada en dos documentos clave del MinTIC: la "Guía para la preparación de las TIC para la continuidad del negocio" (Guía No. 10, versión 1.0.0 del 15/12/2010) y la "Guía para realizar el Análisis de Impacto de Negocios BIA" (Guía No. 11, versión 2.0.0 del 12/05/2015).

Imagen 1 – Marco de seguridad y privacidad de la información

La metodología adoptada sigue el ciclo de funcionamiento del modelo de operación de seguridad y privacidad de la información, como se observa en la Ilustración 1, donde se destacan cuatro fases fundamentales: Diagnóstico, Planificación, Implementación, Gestión y Mejora Continua. Para nuestro Plan de Continuidad TI, nos centraremos específicamente en las fases de Planificación, Implementación, Gestión y Mejora Continua, tal como se muestra en la Ilustración 2, que representa el Marco de Continuidad del Negocio para Seguridad y Privacidad de la Información. Este enfoque nos permite establecer un sistema sostenible de continuidad que responda eficazmente a los cambiantes escenarios de riesgo.

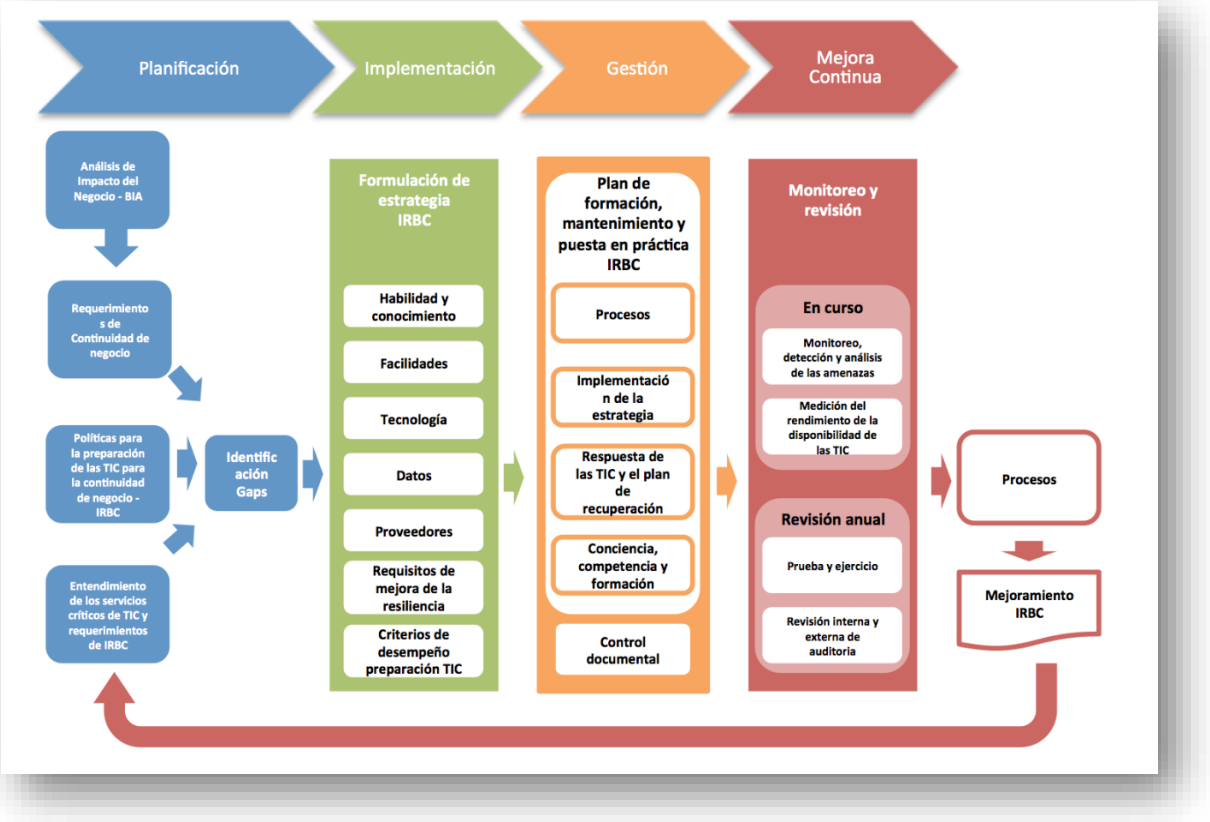

Imagen 2 – Marco de continuidad del negocio para seguridad y privacidad de la información

6.1 Planificación

Esta fase se centra en definir los lineamientos estratégicos para la continuidad de los servicios TIC, basándose en el Análisis de Impacto del Negocio (BIA). Las actividades principales incluyen:

- Establecimiento de objetivos, alcance y límites para la preparación de las TIC para la continuidad del negocio (IRBC).
- Desarrollo y aprobación de la Política para la continuidad del negocio.
- Asignación de roles y responsabilidades a personal competente.

- Desarrollo del Análisis de Impacto del Negocio (BIA) siguiendo los ocho pasos de la metodología de la Guía:
    - Identificación de funciones y procesos críticos
    - Evaluación de impactos operacionales
    - Identificación de procesos críticos
    - Establecimiento de tiempos de recuperación (RTO, RPO, MTD, WRT)
    - Identificación de recursos críticos
    - Disposición del RTO/RPO para cada servicio
    - Identificación de procesos alternos
    - Generación de informe de impacto del negocio
- Identificación de brechas entre los requerimientos de continuidad y las capacidades actuales.
- Definición de la estrategia IRBC alineada con la política de seguridad y privacidad de la información.

6.2 Implementación

Esta fase se enfoca en la ejecución práctica de la estrategia de continuidad TI definida en la fase de planificación. Las actividades principales incluyen:

- Implementación de los elementos de la estrategia IRBC aprobados por la alta dirección.
- Desarrollo de programas de concientización y capacitación sobre continuidad de negocio.
- Implementación de controles de seguridad física y lógica para proteger la infraestructura crítica.
- Establecimiento de estrategias de respaldo y recuperación para datos e infraestructura TI.
- Implementación de arquitecturas tecnológicas resilientes (espera en caliente, tibia o fría).
- Definición e implementación de planes de respuesta a incidentes.
- Documentación detallada de los procedimientos de recuperación para cada servicio crítico.
- Desarrollo de acuerdos con proveedores críticos para garantizar su alineación con la estrategia de continuidad.

6.3 Evaluación y Pruebas

Esta fase permite medir la efectividad del plan de continuidad implementado. Las actividades principales incluyen:

- Desarrollo y ejecución de un plan de seguimiento, evaluación y análisis para la preparación de las TIC.
- Realización de pruebas y simulacros de diferentes escenarios de contingencia.
- Ejecución de auditorías internas para verificar el cumplimiento y efectividad del plan.
- Evaluación del desempeño de los tiempos de recuperación y puntos de restauración.
- Medición de indicadores de cumplimiento y efectividad definidos en la fase de implementación.
- Documentación de resultados y hallazgos para la mejora continua.
- Control documental y mantenimiento de registros relacionados con el IRBC.

6.4 Mejora Continua

Esta fase se enfoca en el perfeccionamiento constante del plan de continuidad. Las actividades principales incluyen:

- Identificación de acciones correctivas para las fallas detectadas durante las pruebas y evaluaciones.
- Revisión periódica del análisis de impacto del negocio para mantenerlo actualizado.
- Actualización de la documentación del plan de continuidad TI según los cambios organizacionales.
- Implementación de mejoras en los controles y procedimientos existentes.
- Comunicación de resultados y plan de mejoramiento a las partes interesadas.
- Aprobación de las mejoras por parte de la alta dirección.
- Incorporación de lecciones aprendidas de incidentes reales o simulados.

7. DESARROLLO DOCUMENTO

7.1 Análisis de impacto de negocio (BIA)

El presente análisis abarca la totalidad de los procesos y sistemas de información críticos de la Secretaría Distrital de la Mujer, con especial énfasis en aquellos que soportan la misión de la entidad. Se han considerado los activos de información identificados en el inventario de aplicaciones, infraestructuras críticas y activos tecnológicos clasificados.

7.1.1 Identificación de Funciones y Procesos

En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad. Este punto tiene como resultado generar un listado de roles y procesos que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

La Secretaría Distrital de la Mujer ha adoptado un modelo de gestión basado en procesos, estructurado en cuatro (4) ejes fundamentales: Estratégicos, Misionales, de Apoyo y de Evaluación. Esta estructura da cumplimiento al Decreto 415 de 2016, el cual modifica el Decreto Único Reglamentario del sector de la Función Pública (Decreto 1083 de 2015) en lo referente a los lineamientos para el fortalecimiento institucional en tecnologías de la información y las comunicaciones (TIC).

Entornos Tecnológicos del Negocio

Categoría	Descripción	Componentes
1. Sistemas de Información	Aplicativos utilizados por los distintos procesos de la Entidad	**Apoyo**: - SIS-03: GLPI - SIS-04: ICOPS - SIS-05-01: ORFEO-WEB - SIS-05: ORFEO - SIS-14: Encuestas - SIS-15: PERNO - SIS-16: LIMAY - SIS-17: Votaciones - SIS-18: FUID - SIS-19: Consejo CTPD - SIS-20: Micrositio FURAG

		- SIS-25: PANDORA **Misional**: - SIS-01: SIMISIONAL - SIS-06: Página Web SDMUJER - SIS-07: intranet - SIS-08: OMEG - SIS-09: Manzanas del Cuidado - SIS-13: Capacitaciones SDMUJER - SIS-23: SIMISIONAL2 **Estratégico**: - SIS-02: LUCHA (kawak)
2. Servicios TI	Servicios tecnológicos que soportan la operación de la entidad	- S01: Correo Electrónico - S02: Mesa de Ayuda - S03: Página Web SDMujer - S04: Intranet - S05: Encuestas - S08: Internet - S09: DNS - S10: Directorio Activo - S11: DHCP - S12: Backups - S14: Servicios en la Nube Oracle - S16: KAWAK
3. Infraestructura Tecnológica Centro de datos principal	Componentes físicos y lógicos que conforman el centro de datos	- IT09: Sistema de hiper convergencia para alta disponibilidad de servicios - IT01, IT07, IT08, IT15: Servidores virtualizados en plataforma VMware para producción - Servidores en Hyper-V para desarrollo y pruebas - IT03: Red de almacenamiento SAN con capacidad de 40TB - IT027: Switch Core principal y redundante para la red LAN - Firewall perimetral Fortinet para seguridad de la red - IT17: Sistema de respaldo Veeam para copias de seguridad - Canales MPLS de 25Mb para la interconexión de 22 sedes

		- Canales de Internet principal y backup con balanceo de cargas - Infraestructura en nube Oracle interconectada mediante VPN - Datacenter de contingencia en modalidad de colocación
4. Recurso Humano	Personal encargado de administrar la infraestructura TI	- Líder de gestión tecnológica - Líder de Infraestructura y seguridad física - Equipo de redes - Equipo de servidores - Equipo de soporte - Líder de seguridad de la información - Líder de grupo desarrollo y BD - Equipo de desarrollo y bases de datos
5. Procesos impactados con gestión TI	Procesos de la entidad que dependen de servicios tecnológicos	- 5 procesos estratégicos - 8 procesos misionales - 8 procesos de apoyo - 2 procesos de evaluación y control

Mapa de procesos de la Secretaría Distrital de la Mujer

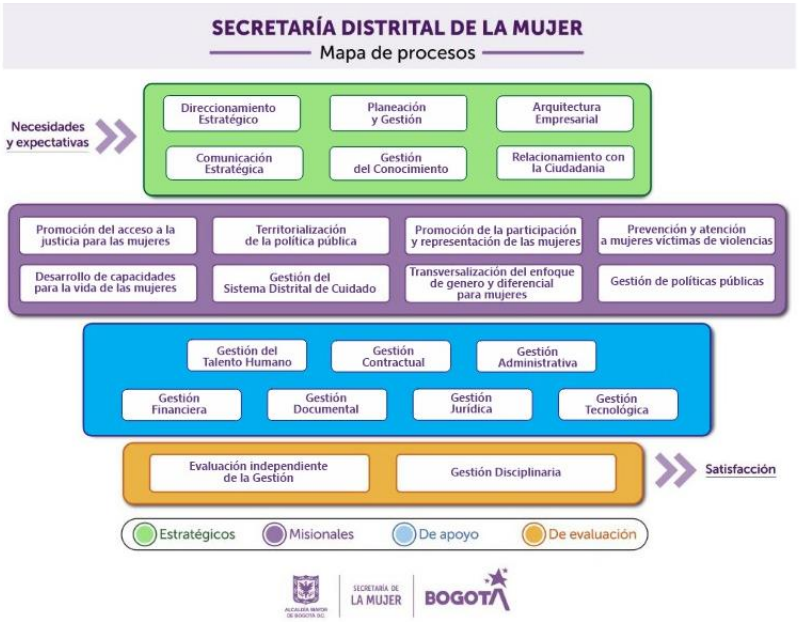

Imagen 3 – Mapa de procesos de la secretaría distrital de la mujer

Procesos Estratégicos	
Proceso	**Objetivo del proceso**
Direccionamiento estratégico	Formular, asesorar y hacer seguimiento a los instrumentos de planeación de corto, mediano y largo plazo, articulados con las prioridades del Gobierno Distrital y las necesidades, expectativas y requisitos de las partes interesadas pertinentes, para la prestación oportuna, eficaz y eficiente de los servicios y cumplimiento de las funciones asignadas a la Secretaría Distrital de la Mujer.
Planeación y gestión	Orientar y asesorar de manera articulada y oportuna a los procesos de la Secretaría Distrital de la Mujer, en la implementación y sostenibilidad del Modelo Integrado de Planeación y Gestión - MIPG, de acuerdo con los lineamientos y normatividad vigente, con el fin de lograr los objetivos y metas propuestas por la Entidad.
Arquitectura empresarial	Desarrollar los mecanismos para la elaboración, formulación y actualización de arquitecturas de referencia y solución mediante el acompañamiento y orientación de ejercicios de arquitectura con el fin de propender por la adecuada articulación, alineación y entrega de valor bajo las perspectivas de la estrategia organizacional, los procesos, procedimientos, información, sistemas de información, infraestructura tecnológica y seguridad de la información a través del desarrollo de proyectos de arquitectura empresarial.
Comunicación estratégica	Divulgar y comunicar los servicios, planes, programas, proyectos, políticas públicas y gestión que desarrolla la Secretaría Distrital de la Mujer mediante la definición e implementación de acciones y estrategias de comunicación, con el propósito de contribuir con el logro de la misionalidad, los objetivos institucionales, la transparencia y el posicionamiento de la entidad.
Gestión del conocimiento	Producir y divulgar información estadística y geográfica rigurosa sobre la situación de derechos de las mujeres con enfoque de género y diferencial; a través de procesos de innovación tecnológica e intercambio de conocimientos, para que se favorezca la toma de decisiones de la gestión pública y el desarrollo de capacidades de las mujeres.
Relacionamiento con la Ciudadanía	Implementar la Política Pública Distrital de Servicio a la Ciudadanía en la Secretaría Distrital de la Mujer, así como gestionar las peticiones, quejas, reclamos y sugerencias (PQRS), denuncias, solicitudes y felicitaciones instauradas por la ciudadanía, mediante el desarrollo de acciones orientadas a garantizar el acceso oportuno, eficaz, eficiente, digno, transparente e igualitario a los servicios que presta la entidad.

Procesos Misionales

Proceso	Objetivo del proceso
Promoción del acceso a la justicia para las mujeres	Promover el acceso a la justicia para las mujeres, mediante la implementación de acciones de coordinación y articulación inter e intrainstitucional y la realización de atenciones de orientación, asesoría y representación socio-jurídica a las mujeres, así como atenciones psicosociales, para avanzar en el reconocimiento, garantía y restablecimiento de los derechos humanos de las mujeres en el Distrito Capital.
Territorialización de la política pública	Desarrollar acciones conducentes a la implementación de la Política Pública de Mujeres y Equidad de Género en el ámbito local, en el marco de la estrategia de Territorialización y de la operación del Modelo de Atención de las Casas de Igualdad de Oportunidades para las Mujeres, mediante la definición de lineamientos y ejecución de acciones que permitan la promoción, reconocimiento y garantía de los derechos humanos de las mujeres y el ejercicio de su ciudadanía.
Promoción de la participación y representación de las Mujeres	Promover y fortalecer la participación y representación de las mujeres en los diferentes ámbitos de la vida social, política y organizativa de la ciudad, así como propiciar ejercicios de diálogo entre las ciudadanas y la Secretaría Distrital de la Mujer.
Prevención y atención a mujeres víctimas de violencias	Coordinar y hacer seguimiento a la implementación de acciones de prevención, atención, protección y sanción en el marco de la garantía del derecho de las mujeres a una vida libre de violencias.
Desarrollo de capacidades para la vida de las mujeres	Diseñar e implementar la estrategia de emprendimiento y empleabilidad a través de alianzas con entidades públicas y el sector privado, que permitan fortalecer las capacidades de las mujeres del Distrito, facilitando su autonomía económica.
Gestión del sistema distrital de cuidado	Gestionar y articular un Sistema Distrital de Cuidado que, bajo un modelo de corresponsabilidad con el sector privado, las comunidades y los hogares, aseguren el acceso al cuidado para personas que requieren un nivel alto de apoyo, con el fin de reducir el tiempo total de trabajo doméstico de las mujeres; redistribuir con los hombres el trabajo de cuidado no remunerado; y contar con mecanismos para su valoración y reconocimiento social.
Transversalización del enfoque de género Y diferencial para mujeres	Brindar asistencia técnica para la transversalización de los enfoques de género y diferencial a los sectores de la administración y las localidades, mediante el diseño e implementación de lineamientos que promuevan el reconocimiento y la garantía de los derechos de las mujeres en sus diferencias y diversidades, así como la igualdad de género en las políticas, programas y proyectos y el Modelo Integrado de Planeación y Gestión de las Entidades.
Gestión de políticas públicas	Orientar técnicamente la formulación, implementación, actualización y seguimiento de políticas públicas lideradas y/o con productos de responsabilidad de la Secretaría Distrital de la Mujer, a partir del enfoque de género en pro de la garantía de los derechos de las mujeres; siguiendo las disposiciones Distritales.

Procesos de Apoyo	
Proceso	**Objetivo del proceso**
Gestión del talento humano	Gestionar el talento humano de la Secretaría Distrital de la Mujer, desarrollando acciones que propendan por su bienestar, fortalecimiento continuo de competencias, mejoramiento del clima organizacional, integridad y promoción de la seguridad y la salud en el trabajo, con el propósito de tener servidoras y servidores públicos íntegros y comprometidos con el cumplimiento y alcance de la misión y objetivos de la Entidad.
Gestión contractual	Desarrollar las actividades de contratación de la secretaría de la mujer de acuerdo con las disposiciones legales vigentes y bajo la observancia de los principios de transparencia, economía, responsabilidad y demás previstos en la Constitución Política, el Estatuto General de Contratación de la Administración Pública - EGCAP y demás normas concordantes y aplicables a la función pública.
Gestión administrativa	Definir políticas y directrices que permitan administrar, custodiar y conservar los bienes a cargo de la entidad, así como gestionar la prestación de servicios generales, con el fin de disponer oportuna y adecuadamente de los recursos físicos, y ser un apoyo transversal para el cumplimiento de la misionalidad de la Entidad.
Gestión financiera	Administrar los recursos financieros de la Entidad, a través de la planeación, registro, seguimiento y control de la gestión presupuestal, de pagos y contable, en cumplimiento de la normativa vigente, con el propósito de suministrar información real y fidedigna, para la toma de decisiones en el cumplimiento de los objetivos institucionales y la rendición de cuentas.
Gestión documental	Establecer políticas y lineamientos técnicos para la planeación, producción, gestión y trámite, organización, transferencia, disposición final de documentos, conservación, preservación a largo plazo y valoración documental de la información producida y gestionada por la Secretaría Distrital de la Mujer, bien sea en medio físico, electrónico y/o digital, a través de herramientas e instrumentos archivísticos implementados en la Entidad.
Gestión jurídica	Determinar los lineamientos jurídicos que se requieran en la Entidad, brindando asesoría, trámite a los requerimientos, defensa judicial, prevención del daño antijurídico de acuerdo con la normativa vigente, funciones asignadas a la Oficina Asesora Jurídica y lineamientos adoptados por la Secretaría Jurídica Distrital en el marco del modelo de Gestión Jurídica Pública (Decreto Distrital 430 de 2018).
Gestión tecnológica	Planificar, gestionar, evaluar y optimizar la infraestructura tecnológica, que responda a los requerimientos solicitados por parte de los usuarios de la Secretaría Distrital de la Mujer, con el fin de garantizar la seguridad y la continuidad de la infraestructura tecnológica y velar por la confidencialidad, integridad, disponibilidad y autenticidad

	de la información; garantizando un servicio eficiente en las tecnologías de la información y las comunicaciones.

Procesos de evaluación	
Proceso	**Objetivo del proceso**
Evaluación independiente de la gestión	Evaluar el Sistema de Control Interno de la Entidad bajo un enfoque por procesos a través de un examen sistemático, objetivo e independiente de las actividades, operaciones y resultados de los procesos, con el propósito de generar valor, contribuir con el mejoramiento de las operaciones y brindar seguridad razonable sobre el cumplimiento de los objetivos institucionales.
Gestión disciplinaria	Ejercer la función disciplinaria al interior de la secretaría de la mujer en la primera instancia - etapa de Instrucción, conforme a lo establecido en la ley, a través de la investigación de conductas que puedan constituir faltas disciplinarias por parte de servidoras (es) y ex servidoras (es) públicas (os), así como por particulares que ejerzan funciones públicas, garantizando la efectividad de la búsqueda de la verdad material, el cumplimiento de los derechos y garantías debidos a las personas que en él intervienen, e implementando estrategias que conlleven a la prevención de la falta disciplinaria.

7.1.2 Evaluación de impactos operacionales

La evaluación de impactos operacionales permite determinar el nivel de criticidad de una interrupción en las operaciones de la Secretaría Distrital de la Mujer. Para realizar esta valoración, se ha utilizado la siguiente escala de medición:

- **Nivel A:** La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse. Impacto alto.
- **Nivel B:** La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica. Impacto medio.
- **Nivel C:** La operación no es una parte integral del negocio. Impacto bajo.

A continuación, se presenta la valoración operacional por niveles de criticidad:

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	SIS-01: SIMISIONAL SIS-23: SIMISIONAL2	A	2	Sistema misional de atención a mujeres
Aplicaciones	SIS-05: ORFEO SIS-05-01: ORFEO-WEB	A	2	Sistema de gestión documental
Aplicaciones	SIS-15: PERNO	B	4	Sistema de nómina y personal
Aplicaciones	SIS-16: LIMAY	B	4	Sistema contable
Aplicaciones	SIS-02: LUCHA (kawak)	B	8	Sistema de gestión institucional
Aplicaciones	SIS-03: GLPI	B	4	Sistema de gestión de incidentes
Aplicaciones	SIS-04: ICOPS	B	4	Sistema de control de pagos a contratistas de prestación de servicios
Aplicaciones	SIS-20: Micrositio FURAG	C	24	Sistema para la consolidación de respuestas del FURAG
Aplicaciones	SIS-25: PANDORA	B	4	Sistema de planeación y gestión institucional
Web	SIS-06: Página Web SDMUJER	A	2	Portal institucional público
Web	SIS-09: Manzanas del Cuidado	A	2	Portal web del programa de manzanas del cuidado
Web	SIS-08: OMEG	A	2	Portal del observatorio de mujeres y equidad de género
Web	SIS-13: Capacitaciones SDMUJER	A	2	LMS de la secretaría de la mujer
Web	SIS-07: intranet	B	8	Intranet de la secretaría de la mujer
Base de Datos	Oracle Cloud	A	1	Bases de datos en nube Oracle
Seguridad de Información	Firewall perimetral	A	1	Protección de perímetro de red
Sistemas de Almacenamiento	IT17: SAN	A	3	Almacenamiento centralizado de datos
Comunicaciones	Red MPLS	A	2	Conectividad entre sedes
Comunicaciones	Internet	B	4	Acceso a servicios externos
Comunicaciones	Red LAN	A	2	Red local de datos
Comunicaciones	IT025: Correo electrónico	A	3	Comunicación institucional
Cuartos de Máquinas	IT033: Centro de Datos	A	1	Infraestructura física tecnológica
Servicios TI	ASTI12: Backups	A	2	Copias de seguridad de la información
Servicios TI	Directorio activo	A	2	Directorio activo

7.1.3 Identificación de procesos críticos

Con base en la clasificación de los impactos operacionales, se han identificado los procesos críticos de la entidad, aplicando los siguientes criterios:

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo

C	La operación no es parte integral del negocio

Los procesos críticos (Nivel A) identificados son:

- SIS-01: SIMISIONAL
- SIS-23: SIMISIONAL2
- SIS-06: Página Web SDMUJER
- SIS-09: Manzanas del Cuidado
- SIS-08: OMEG
- SIS-13: Capacitaciones SDMUJER
- SIS-05: ORFEO
- SIS-05-01: ORFEO-WEB
- Oracle Cloud
- Oracle Blob Storage (respaldos de archivos sistemas críticos)
- Firewall Lógico Oracle
- Firewall perimetral
- Directorio activo
- IT033: Centro de Datos
- ASTI12: Backups
- Oracle Blob Storage
- Firewall Lógico Oracle

7.1.4 Establecimiento de tiempos de recuperación

Para los procesos críticos identificados, se han establecido los siguientes tiempos de recuperación, que son fundamentales para comprender el BIA:

Tiempo de Recuperación	Descripción
RPO (Recovery Point Objective)	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio
RTO (Recovery Time Objective)	Tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración
WRT (Work Recovery Time)	Tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados
MTD (Maximum Tolerable Downtime)	Periodo máximo de tiempo de inactividad que puede tolerar la entidad sin entrar en colapso

A continuación, se presenta la clasificación por prioridades de recuperación, basada en el MTD de cada proceso crítico:

Categoría (Función Crítica del Negocio)	Proceso Crítico (Servicios)	MTD (En días)	Prioridad de Recuperación
Aplicaciones	SIS-01: SIMISIONAL SIS-23: SIMISIONAL2	0.5	1
Base de Datos	Oracle Cloud	0.5	1
Seguridad de Información	Firewall perimetral	0.5	1
Cuartos de Máquinas	IT033: Centro de Datos	0.5	1
Aplicaciones	SIS-05: ORFEO SIS-05-01: ORFEO-WEB	1.0	2
Web	SIS-06: Página Web SDMUJER	1.0	2
Web	SIS-09: Manzanas del Cuidado	1.0	2
Sistemas de Almacenamiento	IT17: SAN	1.0	2
Servicios TI	ASTI12: Backups	1.0	2
Web	SIS-08: OMEG	2.0	3
Web	SIS-13: Capacitaciones SDMUJER	2.0	3
Servicios de TI	Directorio activo	1.0	2
Web	Oracle Blob Storage	1.0	2
Web	Firewall Lógico Oracle	1.0	2

7.1.5 Identificación de Recursos

Para cada función crítica del negocio y sus procesos críticos asociados, se han identificado los recursos tecnológicos esenciales que deben ser priorizados en un evento de recuperación:

Categoría (Función Crítica del Negocio)	Proceso Crítico (Servicios)	Identificación de recursos críticos de Sistemas TI
Aplicaciones	SIS-01: SIMISIONAL SIS-23: SIMISIONAL2	Sistema de entrada de información para los diferentes módulos como hoja de vida de mujer, atenciones, formaciones, transversales, rutas de atención
		Consulta de datos históricos tanto de SIMISIONAL1 como SIMISIONAL 2 con corte de información del día anterior
Base de Datos	Oracle Cloud	Bases de datos ORACLE, PostgreSQL y MySQL recuperadas del inmediatamente anterior
		Servidores de aplicaciones restablecidos del día inmediatamente anterior
Seguridad de Información	Firewall perimetral	Mantener al día la garantía y soporte
		Copia de seguridad de configuración actualizado
Cuartos de Máquinas	IT033: Centro de Datos	Sistema de climatización
		Sistema eléctrico con UPS (para actualizar por obsolescencia)
		Conectividad de red básica (switches de Core)
		Sistemas de almacenamiento
Aplicaciones	SIS-05: ORFEO SIS-05-01: ORFEO-WEB	Sistema de entrada de información de la ciudadanía publicada desde el portal web
		Almacenamiento disponible para la operación del sistema
Web	SIS-06: Página Web SDMUJER	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior
Web	SIS-09: Manzanas del Cuidado	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior
Web	SIS-08: OMEG	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior
Web	SIS-13: Capacitaciones SDMUJER	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior
Servicios TI	Directorio Activo	Servidor y base de datos de LDAP disponible
Web	Oracle Blob Storage	Se debe complementar la identificación de recursos críticos de este apartado
Web	Firewall Lógico Oracle	Se debe complementar la identificación de recursos críticos de este apartado

7.1.6 Disposición del RTO/RPO

Para una adecuada estrategia de continuidad, se han definido los valores de RTO (Recovery Time Objective) y RPO (Recovery Point Objective) para cada proceso crítico. Se incluye también el WRT (Work Recovery Time) que complementa el RTO:

Categoría (Función Crítica del Negocio)	Proceso Crítico (Servicios)	Identificación de recursos críticos de Sistemas TI	RTO (horas)	RPO (horas)	WRT (horas)
Aplicaciones	SIS-01: SIMISIONAL SIS-23: SIMISIONAL2	Sistema de entrada de información para los diferentes módulos como hoja de vida de mujer, atenciones, formaciones, transversales, rutas de atención	4	6	2
		Consulta de datos históricos tanto de SIMISIONAL1 como SIMISIONAL 2 con corte de información del día anterior	6	12	3
		Obtención de información de valor por medio de analítica de datos con corte de información del día anterior	8	24	4
Base de Datos	Oracle Cloud	Bases de datos ORACLE, PostgreSQL y MySQL recuperadas del inmediatamente anterior	3	4	2
		Servidores de aplicaciones restablecidos del día inmediatamente anterior	5	12	3
Seguridad de Información	Firewall perimetral	Archivo de configuración respaldado y actualizado de reglas y políticas	2	24	1
		Configuración de interfaces WAN y LAN	2	24	1
		Reglas básicas de filtrado para permitir acceso a servicios esenciales	1	24	1
		Configuración de NAT/PAT para los servicios críticos	2	24	1
		Reglas de VPN para acceso remoto seguro	3	24	1
Cuartos de Máquinas	IT033: Centro de Datos	Sistema de climatización	2	N/A	1
		Sistema eléctrico con UPS	1	N/A	1
		Conectividad de red básica (switches de core)	3	24	2
		Sistemas de almacenamiento	4	12	2
Aplicaciones	SIS-05: ORFEO SIS-05-01: ORFEO-WEB	Sistema de entrada de información de la ciudadanía publicada desde el portal web	6	24	2
		Almacenamiento disponible para la operación del sistrma	4	6	2
Web	SIS-06: Página Web SDMUJER	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugins y datos con corte de máximo el día anterior	6	24	2

Web	SIS-09: Manzanas del Cuidado	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugins y datos con corte de máximo el día anterior	6	24	2
Web	SIS-08: OMEG	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior	6	24	6
Web	SIS-13: Capacitaciones SDMUJER	Servicio de disponibilidad web con todo el contenido (publicaciones, imágenes o archivos), plugin y datos con corte de máximo el día anterior	6	24	6
Servicios TI	Directorio Activo	Servidor y base de datos de LDAP disponible	X	X	X
Web	Oracle Blob Storage	Se debe complementar la identificación de recursos críticos de este apartado	X	X	X
Web	Firewall Lógico Oracle	Se debe complementar la identificación de recursos críticos de este apartado	X	X	X

7.1.7 Identificación de procesos alternos

Para cada proceso crítico identificado, se han establecido procedimientos alternativos temporales que permitirán mantener la operación en caso de una interrupción:

Proceso Crítico	Procedimiento Alternativo	Recursos Requeridos	Responsable
SIS-01: SIMISIONAL SIS-23: SIMISIONAL2	Registro manual de atenciones a mujeres en formatos offline.	Formatos que permitan registrar información cuando no haya disponibilidad del sistema y una opción de importación de formato offline.	Líderes de Casas de Igualdad y Centros de Atención Equipo de desarrollo SIMISIONAL
	Consolidación manual de estadísticas de atención	Plantillas Excel o Power BI estandarizadas con fuente de datos de equipos locales	Oficina Asesora de Planeación
Oracle Cloud	Uso de réplicas locales de bases de datos para consultas básicas	Servidores de respaldo con réplicas configuradas de forma automática	Equipo de Bases de Datos
	Procedimiento de sincronización manual con archivos CSV	Plantillas de carga predefinidas	Equipo de Desarrollo
Firewall perimetral	Implementación de firewall secundario con reglas básicas	Equipo de respaldo con configuración básica preestablecida	Equipo de Infraestructura
	Acceso mediante VPN alternativa	Servicio VPN alternativo contratado	Seguridad de la Información
Centro de Datos	Activación de servicios esenciales en nube pública	Servicios preconfigurados en nube (OCI)	Líder de Infraestructura
	Activación de data center alterno	Colocation contratada con proveedor externo	Líder de Gestión Tecnológica
Página Web SDMUJER	Activación de sitio web alternativo estático	Hosting externo con copia estática del sitio	Comunicaciones
Manzanas del Cuidado	Activación de landing page informativa	Micrositio alterno alojado en servicio externo	Comunicaciones
Backups	Restauración desde copias offline	Medios de respaldo externos	Equipo de Infraestructura
	Uso de servicio de backup en nube secundario	Servicio con proveedor alterno de backup	Equipo de Infraestructura
OMEG	Publicación de informes vía redes sociales	Documentos en PDF accesibles desde Drive	Observatorio de Mujeres
	Portal web simplificado	Hosting alternativo con estadísticas básicas	Observatorio de Mujeres
Capacitaciones SDMUJER	Sesiones presenciales de formación	Material físico de capacitación	Equipo de Formación
	Compartir contenidos por correo electrónico	Materiales digitales livianos	Equipo de Formación
Directorio Activo	Falta definirlo	Falta definirlo	Falta definirlo
Oracle Blob Storage	Falta definirlo	Falta definirlo	Falta definirlo
Firewall Lógico Oracle	Falta definirlo	Falta definirlo	Falta definirlo

7.1.8 Generación de informe de impacto de negocio

El análisis de impacto del negocio (BIA) realizado ha permitido identificar los siguientes elementos clave para la estrategia de continuidad de TI de la Secretaría Distrital de la Mujer:

Resumen Ejecutivo

El presente análisis de impacto de negocio (BIA) ha identificado 13 procesos/servicios críticos cuya interrupción tendría un impacto significativo en la misión y operaciones de la Secretaría Distrital de la Mujer. La evaluación ha permitido establecer prioridades de recuperación, asignar tiempos máximos tolerables de inactividad (MTD) y definir objetivos de recuperación (RTO/RPO) que servirán como base para el desarrollo e implementación de estrategias de continuidad efectivas.

Hallazgos Principales

1. **Procesos Críticos de Mayor Prioridad**:
   - Los sistemas de información misional (SIMISIONAL/SIMISIONAL2) son los más críticos con un MTD de 0.5 días.
   - Los servicios de infraestructura base (Oracle Cloud, Firewall perimetral, Centro de Datos) también requieren una recuperación en máximo 12 horas.
   - Los servicios web orientados a la ciudadanía tienen un MTD de 1 día, siendo especialmente relevantes para la atención a mujeres.
2. **Dependencias Críticas Identificadas**:
   - Fuerte dependencia de la infraestructura de Oracle Cloud para servicios misionales.
   - Dependencia de la infraestructura de comunicaciones para la operación de las 22 sedes.
   - Dependencia del sistema de correo electrónico para la coordinación interna.
3. **Impactos Potenciales**:
   - **Operacionales**: Interrupción de la atención a mujeres víctimas de violencia, suspensión de servicios en las Casas de Igualdad de Oportunidades.
   - **Financieros**: Posibles sobrecostos por retrasos en procesos contractuales y pérdida de acceso a sistemas financieros.
   - **Reputacionales**: Afectación a la imagen institucional por indisponibilidad de servicios web y canales de atención ciudadana.
   - **Legales/regulatorios**: Incumplimiento de plazos legales para respuesta a PQRS y atención a casos de violencia.

4. **Tiempos de Recuperación**:
    - Los RTOs varían entre 1 y 8 horas dependiendo de la criticidad del servicio.
    - El RPO para la mayoría de los sistemas es de 24 horas, lo que indica que la pérdida de datos de un día es generalmente aceptable.
    - Los WRTs identificados oscilan entre 1 y 6 horas, reflejando el tiempo necesario para verificar y validar la información tras la recuperación técnica.
    - Los sistemas de seguridad y comunicaciones requieren tiempos de recuperación más rápidos que los sistemas web.
5. **Recursos Críticos**:
    - Se identificaron 31 recursos críticos específicos que soportan los 14 procesos/servicios críticos.
    - Sistemas de entrada de información para la atención a mujeres.
    - Infraestructura de bases de datos y aplicaciones en nube Oracle.
    - Equipamiento de seguridad perimetral y su configuración.
    - Sistemas de almacenamiento centralizado de información.
    - Infraestructura de comunicaciones entre sedes.
6. **Procesos Alternos**:
    - Se han definido procedimientos manuales y alternativas tecnológicas para cada proceso crítico.
    - Los procesos alternos permiten mantener las operaciones esenciales durante periodos de interrupción.

Brechas Identificadas

1. **Tecnológicas**:
    - Insuficiente redundancia en sistemas de almacenamiento críticos.
    - Limitada capacidad de procesamiento en el centro de datos alterno.
    - Falta de automatización en procesos de recuperación para algunos sistemas.
2. **Procedimentales**:
    - Procedimientos de contingencia manual no completamente documentados.
    - Ausencia de pruebas periódicas para escenarios complejos de recuperación.
    - Necesidad de fortalecer la coordinación entre áreas técnicas y funcionales.
3. **Organizacionales**:
    - Capacitación limitada del personal en procedimientos de contingencia.
    - Dependencia de proveedores externos para ciertos servicios críticos.
    - Roles y responsabilidades no completamente definidos para escenarios de crisis.

Recomendaciones Estratégicas

1. **Corto Plazo (0-3 meses)**:
   - Documentar detalladamente los procedimientos alternativos para cada proceso crítico.
   - Implementar copias de respaldo adicionales para las bases de datos críticas.
   - Capacitar al personal clave en los procedimientos de contingencia.
2. **Mediano Plazo (3-6 meses)**:
   - Implementar una solución de replicación en tiempo real para los sistemas más críticos.
   - Establecer acuerdos de nivel de servicio (SLAs) con proveedores críticos.
   - Desarrollar y probar planes de contingencia detallados para cada escenario identificado.
3. **Largo Plazo (6-12 meses)**:
   - Implementar una arquitectura de alta disponibilidad para las aplicaciones críticas.
   - Fortalecer el centro de datos alterno para soportar mayor capacidad.
   - Implementar herramientas de monitoreo avanzado para detectar y responder a incidentes.

Conclusiones

El análisis de impacto del negocio ha proporcionado una comprensión detallada de las dependencias tecnológicas críticas de la Secretaría Distrital de la Mujer. Los hallazgos revelan la necesidad de implementar estrategias robustas de continuidad para garantizar la disponibilidad continua de los servicios esenciales para las mujeres del Distrito Capital.

Las brechas identificadas representan oportunidades de mejora que, una vez abordadas, fortalecerán significativamente la resiliencia operacional de la entidad. La implementación de las recomendaciones estratégicas permitirá mitigar los riesgos asociados a posibles interrupciones y garantizar la continuidad de los servicios esenciales para la población objetivo.

Este análisis de impacto del negocio constituye la base fundamental para el desarrollo del Plan de Recuperación ante Desastres (DRP) y las estrategias de continuidad del negocio que se implementarán en las siguientes fases del proyecto.

7.1.9 Clasificación de escenarios de riesgo

A fin de conocer con precisión los riesgos potenciales que afectan a los servicios de tecnologías de la información de la Secretaría Distrital de la Mujer, se ha realizado una clasificación de los posibles escenarios de riesgo, describiendo su nivel de impacto para cada función crítica:

ID	Escenario de Riesgo	Categoría	Procesos/Servicios Afectados	Probabilidad	Impacto	Nivel de Riesgo
ER-01	Falla total del centro de datos principal	Infraestructura	Todos los sistemas y servicios TI	Media	Catastrófico	Alto
ER-02	Interrupción prolongada del suministro eléctrico	Infraestructura	Todos los sistemas alojados en centro de datos principal	Alta	Alto	Alto
ER-03	Falla en sistemas de almacenamiento (SAN)	Infraestructura	Sistemas misionales, bases de datos, correo	Media	Alto	Alto
ER-04	Falla masiva en la red de comunicaciones	Infraestructura	Conectividad entre sedes, acceso a servicios	Media	Alto	Alto
ER-05	Ataque cibernético (ransomware)	Seguridad	Todos los sistemas y datos	Alta	Catastrófico	Extremo
ER-06	Filtración de datos sensibles	Seguridad	Datos de SIMISIONAL, PERNO, información de mujeres	Media	Alto	Alto
ER-07	Falla en servicio de proveedor cloud (Oracle)	Servicios externos	Sistemas misionales, BD, analítica de datos	Baja	Catastrófico	Alto
ER-08	Indisponibilidad de servidores de aplicaciones críticas	Infraestructura	SIMISIONAL, SIMISIONAL2, Orfeo	Media	Alto	Alto
ER-09	Desastre natural (inundación, sismo)	Físico	Infraestructura física y tecnológica	Baja	Catastrófico	Alto
ER-10	Falla en sistemas de respaldo (backups)	Seguridad	Capacidad de recuperación de todos los sistemas	Baja	Catastrófico	Alto
ER-11	Desactualización crítica de seguridad en sistemas	Seguridad	Sistemas operativos, aplicaciones, bases de datos	Alta	Alto	Alto
ER-12	Pérdida de personal técnico clave	Personal	Sistemas críticos según especialidad del personal	Media	Medio	Medio
ER-13	Falla en entorno virtualizado (VMware)	Infraestructura	Todos los servidores virtualizados	Media	Alto	Alto
ER-14	Saturación de canales de internet	Infraestructura	Servicios web, correo electrónico, VPN	Alta	Medio	Alto
ER-15	Corrupción de bases de datos	Aplicaciones	Sistemas que utilizan bases de datos	Media	Alto	Alto

7.1.10 Identificación de amenazas

Las amenazas son todos los factores que pueden generar daños a la infraestructura tecnológica de la Secretaría Distrital de la Mujer. A continuación, se clasifican las amenazas identificadas según el escenario de riesgo:

ID	Amenaza	Origen	Descripción	Escenarios asociados	Probabilidad
AM-01	Fallos de hardware	Interno	Fallos en servidores, almacenamiento, equipos de red por deterioro o fin de vida útil	ER-01, ER-03, ER-08, ER-13	Alta
AM-02	Cortes de energía	Externo	Interrupciones prolongadas en el suministro eléctrico que superan la capacidad de los sistemas UPS	ER-02	Alta
AM-03	Ataques de denegación de servicio (DoS/DDoS)	Externo	Intentos maliciosos de saturar los recursos de sistemas o redes	ER-05, ER-14	Media
AM-04	Malware/Ransomware	Externo	Software malicioso diseñado para dañar sistemas o cifrar datos	ER-05, ER-10, ER-15	Alta
AM-05	Errores humanos	Interno	Acciones no intencionales que comprometen la disponibilidad o integridad	ER-06, ER-08, ER-15	Alta
AM-06	Fallas en aplicaciones	Interno	Errores en software, bugs o problemas de compatibilidad	ER-08, ER-15	Media
AM-07	Desastres naturales	Externo	Eventos como terremotos, inundaciones o incendios	ER-01, ER-09	Baja
AM-08	Fallas en servicios de terceros	Externo	Interrupción en servicios proporcionados por proveedores externos	ER-07, ER-14	Media
AM-09	Acceso no autorizado	Mixto	Intrusiones físicas o lógicas a sistemas o instalaciones	ER-05, ER-06	Media
AM-10	Rotación de personal crítico	Interno	Pérdida de conocimiento técnico por salida de personal clave	ER-12	Media
AM-11	Sobrecarga de sistemas	Mixto	Demanda excesiva de recursos que excede la capacidad disponible	ER-08, ER-14	Media
AM-12	Obsolescencia tecnológica	Interno	Sistemas o equipos desactualizados sin soporte del fabricante	ER-01, ER-03, ER-08, ER-11	Alta
AM-13	Fallos en sistemas de climatización	Interno	Problemas en aire acondicionado del centro de datos causando sobrecalentamiento	ER-01	Media
AM-14	Manipulación de configuraciones	Mixto	Cambios no autorizados o incorrectos en configuraciones críticas	ER-05, ER-08, ER-13	Media
AM-15	Fallos en comunicaciones	Mixto	Interrupciones en redes WAN, MPLS o Internet	ER-04, ER-14	Alta

7.1.11 Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades de seguridad asociadas a los activos de información que pueden ser aprovechadas por las amenazas. Se han identificado las siguientes vulnerabilidades:

ID	Vulnerabilidad	Activos Afectados	Amenazas Relacionadas	Descripción	Nivel de Criticidad
VU-01	Centro de datos sin redundancia completa	Infraestructura de TI	AM-01, AM-02, AM-07, AM-13	El centro de datos principal no cuenta con redundancia N+1 en todos los sistemas críticos	Alto
VU-02	Capacidad limitada de los sistemas UPS	Energía, servidores	AM-02	Las UPS actuales proporcionan autonomía limitada (< 2 horas)	Alto
VU-03	Falta de segregación de redes	Red, seguridad	AM-03, AM-04, AM-09	Segmentación de red insuficiente que podría permitir la propagación de ataques	Alto
VU-04	Políticas de respaldo incompletas	Datos, aplicaciones	AM-04, AM-05, AM-15	Algunos sistemas no tienen configuradas copias de seguridad con la frecuencia adecuada	Crítico
VU-05	Sistemas operativos desactualizados	Servidores	AM-04, AM-09, AM-12	Sistemas sin parches de seguridad recientes	Alto
VU-06	Documentación técnica incompleta	Servicios TI	AM-05, AM-10	Falta de documentación detallada para recuperación de algunos sistemas críticos	Medio
VU-07	Concentración de conocimiento técnico	Personal	AM-10	Dependencia de personal específico para administración de sistemas críticos	Alto
VU-08	Licenciamiento insuficiente de software crítico	Aplicaciones	AM-06, AM-12	Falta de soporte técnico para algunos sistemas por licencias caducadas	Medio
VU-09	Monitoreo limitado de sistemas	Todos los sistemas	AM-03, AM-04, AM-06, AM-11	Ausencia de monitoreo 24/7 y alertas automatizadas para algunos sistemas	Alto
VU-10	Capacidad limitada del enlace MPLS	Comunicaciones	AM-08, AM-11, AM-15	Ancho de banda insuficiente para algunas sedes en horas pico	Medio
VU-11	Falta de entornos de prueba	Aplicaciones	AM-05, AM-06, AM-14	Cambios implementados directamente en producción sin validación previa	Alto
VU-12	Ausencia de firewall de aplicaciones web (WAF)	Aplicaciones web	AM-03, AM-04, AM-09	Sistemas web expuestos sin protección específica contra ataques de aplicación	Alto

VU-13	Control de acceso inadecuado	Sistemas críticos	AM-05, AM-09, AM-14	Deficiencias en la gestión de usuarios privilegiados	Alto
VU-14	Almacenamiento insuficiente para crecimiento	Datos	AM-11	Capacidad limitada para absorber el crecimiento de datos	Medio
VU-15	Falta de redundancia en equipos de comunicaciones	Red	AM-01, AM-15	Puntos únicos de falla en switches core y routers	Alto
VU-16	Contrato de soporte limitado con proveedores críticos	Servicios externos	AM-08	SLAs con tiempos de respuesta insuficientes para infraestructura crítica	Alto
VU-17	Pruebas de recuperación insuficientes	Procedimientos de DR	AM-05, AM-10	Falta de validación periódica de procedimientos de recuperación	Crítico
VU-18	Ausencia de sincronización automática de datos con sitio alterno	Datos	AM-01, AM-07	Replicación manual o con intervalo extenso para algunos sistemas	Alto
VU-19	Protección física inadecuada	Centro de datos	AM-07, AM-09	Controles de acceso físico con deficiencias	Medio
VU-20	Ausencia de cifrado en datos sensibles	Información crítica	AM-04, AM-09	Datos de mujeres víctimas sin cifrado adecuado	Crítico

7.2 Establecimiento de objetivos, alcance y límites para la preparación de las TIC para la continuidad del negocio (IRBC)

7.2.1 Objetivos específicos del IRBC

El Plan de Continuidad de Tecnologías de la Información de la Secretaría Distrital de la Mujer tiene los siguientes objetivos específicos:

1. Garantizar la recuperación oportuna y controlada de los servicios tecnológicos críticos identificados en el análisis de impacto de negocio.
2. Establecer tiempos de recuperación (RTO y RPO) realistas y alcanzables para cada servicio crítico, priorizando aquellos que soportan directamente la atención a mujeres.
3. Implementar procedimientos de contingencia que permitan la operación continua de los procesos misionales durante eventos disruptivos.
4. Reducir el impacto operacional, reputacional y financiero de las interrupciones tecnológicas mediante estrategias preventivas y reactivas.

5. Asegurar la protección y disponibilidad de la información crítica, con especial énfasis en datos sensibles de mujeres víctimas de violencia.
6. Establecer un modelo de gobernanza para la gestión de la continuidad que defina roles, responsabilidades y mecanismos de coordinación.
7. Desarrollar capacidades institucionales para responder efectivamente ante incidentes que afecten la continuidad de servicios TI.
8. Garantizar el cumplimiento de requisitos normativos relacionados con la continuidad de servicios públicos digitales.

7.2.2 Alcance del IRBC

El alcance del Plan de Preparación de las TIC para la Continuidad del Negocio (IRBC) de la Secretaría Distrital de la Mujer comprende:

1. **Servicios Tecnológicos**: Todos los servicios tecnológicos identificados como críticos en el análisis de impacto de negocio, incluyendo:
    - Sistemas de información misionales (SIMISIONAL, SIMISIONAL2)
    - Portales web institucionales y de servicios (Página web SDMUJER, Manzanas del Cuidado, OMEG)
    - Servicios de infraestructura (bases de datos, correo electrónico, almacenamiento, comunicaciones)
2. **Infraestructura Tecnológica**:
    - Centro de datos principal
    - Sistemas de almacenamiento
    - Infraestructura de comunicaciones
    - Servicios en nube (Oracle Cloud)
    - Equipos de seguridad perimetral
    - Centro de datos alterno en modalidad de colocación
3. **Procesos de Gestión TI**:
    - Gestión de incidentes de seguridad
    - Procedimientos de respaldo y recuperación
    - Administración de infraestructura tecnológica
    - Soporte técnico y mesa de ayuda
4. **Ubicaciones**:

- Sede administrativa central
- 22 Casas de Igualdad de Oportunidades para las Mujeres
- Centro de datos alterno en modalidad de colocación

5. **Temporalidad**: El plan establece estrategias para:
   - Recuperación a corto plazo (0-24 horas)
   - Recuperación a mediano plazo (1-5 días)
   - Recuperación a largo plazo (más de 5 días)

7.2.3 Límites del IRBC

El Plan de Continuidad de TI establece los siguientes límites:

1. **Exclusiones**:
   - Procesos y sistemas no críticos identificados en el BIA
   - No contempla la continuidad de servicios no tecnológicos
   - No incluye planes de evacuación o gestión de emergencias de personal
   - No abarca sistemas en fase de pruebas o desarrollo
   - No incluye dispositivos de usuario final (equipos de escritorio, portátiles, impresoras)
   - No contempla sistemas, aplicaciones o infraestructura que no están bajo la administración directa de la Oficina Asesora de Planeación - Gestión Tecnológica
2. **Restricciones**:
   - Depende de la disponibilidad presupuestal asignada a la continuidad de negocio
   - La capacidad de recuperación está limitada por las tecnologías y soluciones disponibles
   - La capacidad de respuesta está condicionada por la disponibilidad de personal técnico especializado
   - El tiempo de recuperación total está condicionado a la magnitud del evento disruptivo
3. **Dependencias externas**:
   - Servicios de proveedores de telecomunicaciones
   - Disponibilidad de servicios en nube (Oracle)
   - Soporte de fabricantes de hardware y software
   - Disponibilidad de servicios públicos (energía, agua)

7.3 ASIGNACIÓN DE ROLES Y RESPONSABILIDADES A PERSONAL COMPETENTE

7.3.1 Estructura de Gobernanza para la Continuidad de TI

La Secretaría Distrital de la Mujer establece la siguiente estructura de gobernanza para la gestión de la continuidad de tecnologías de la información:

1. **Comité Institucional de Gestión y Desempeño**
    - Aprobar la política y plan de continuidad de TI
    - Asignar los recursos necesarios para la implementación del plan
    - Supervisar el cumplimiento de los objetivos de continuidad
    - Evaluar periódicamente la efectividad de las estrategias implementadas
2. **Equipo de Gestión de Crisis**
    - Declarar la activación del plan de continuidad
    - Coordinar la respuesta institucional ante eventos disruptivos
    - Tomar decisiones estratégicas durante situaciones de contingencia
    - Gestionar la comunicación con partes interesadas externas
3. **Coordinador de Continuidad de TI**
    - Liderar la implementación del plan de continuidad de TI
    - Coordinar las pruebas y ejercicios de continuidad
    - Mantener actualizada la documentación del plan
    - Reportar al Comité Institucional sobre el estado de la continuidad
4. **Equipos Técnicos de Recuperación**
    - Ejecutar los procedimientos técnicos de recuperación
    - Realizar las pruebas de los componentes tecnológicos
    - Documentar los resultados de las pruebas y eventos reales
    - Proponer mejoras a los procedimientos de recuperación

7.3.2 Roles y Responsabilidades Específicos

Rol	Cargo/Área	Responsabilidades
Patrocinador Ejecutivo	Secretaria Distrital de la Mujer	- Aprobar recursos y presupuesto - Liderar la gestión ante entes externos - Comunicación oficial en crisis
Líder del Plan de Continuidad	Jefe Oficina Asesora de Planeación	- Supervisar la implementación del plan - Reportar avances a la alta dirección - Coordinar actualizaciones periódicas
Coordinador de Continuidad TI	Líder de Gestión Tecnológica	- Coordinar actividades técnicas - Liderar pruebas de recuperación - Mantener documentación actualizada
Líder de Infraestructura	Profesional Especializado de Infraestructura	- Recuperar sistemas de infraestructura - Mantener configuraciones actualizadas - Coordinar con proveedores técnicos
Líder de Bases de Datos	Profesional Especializado DBA	- Recuperar bases de datos - Verificar integridad de información - Gestionar respaldos y restauraciones
Líder de Aplicaciones	Profesional Especializado Desarrollo	- Recuperar aplicaciones críticas - Verificar funcionalidad de sistemas - Coordinar con usuarios funcionales
Líder de Seguridad de la Información	Profesional Especializado Seguridad	- Verificar controles de seguridad - Evaluar vulnerabilidades post-incidente - Asegurar acceso seguro durante recuperación
Líder de Soporte Técnico	Coordinador Mesa de Ayuda	- Coordinar soporte a usuarios - Gestionar incidentes durante contingencia - Documentar soluciones aplicadas
Líderes Funcionales	Directores y Subdirectores de áreas misionales	- Validar funcionalidad de sistemas recuperados - Coordinar procedimientos alternos - Priorizar recuperación según necesidades
Oficial de Comunicaciones	Jefe Oficina Asesora de Comunicaciones	- Gestionar comunicaciones internas y externas - Coordinar mensajes oficiales - Mantener informadas a las partes interesadas

7.3.3 Equipos de Recuperación

Equipo	Integrantes	Funciones	Activación
Equipo de Evaluación Inicial	- Coordinador de Continuidad TI - Líder de Infraestructura - Líder de Seguridad	- Evaluar impacto del incidente - Recomendar la activación del plan - Identificar sistemas afectados	Inmediatamente después de la detección del incidente
Equipo de Recuperación de Infraestructura	- Líder de Infraestructura - Administradores de servidores - Administradores de red - Especialista en virtualización	- Recuperar servidores físicos y virtuales - Restaurar conectividad de red - Activar infraestructura alterna	Tras la declaración de contingencia
Equipo de Recuperación de Datos	- Líder de Bases de Datos - Administradores de BD - Especialista en almacenamiento - Especialista en respaldos	- Restaurar bases de datos - Verificar integridad de datos - Recuperar información desde copias de seguridad	Tras la recuperación básica de infraestructura
Equipo de Recuperación de Aplicaciones	- Líder de Aplicaciones - Desarrolladores de sistemas críticos - Analistas de QA - Administradores de aplicaciones	- Restaurar aplicaciones críticas - Verificar funcionalidad - Realizar pruebas de integración	Tras la recuperación de bases de datos
Equipo de Soporte a Usuarios	- Líder de Soporte Técnico - Analistas de mesa de ayuda - Técnicos de soporte en sitio	- Atender incidentes de usuarios - Apoyar en procedimientos alternos - Capacitar en el uso de sistemas recuperados	Durante todo el proceso de recuperación
Equipo de Logística	- Coordinador Administrativo - Profesional de contratación - Profesional de recursos físicos	- Gestionar espacios físicos alternos - Coordinar transporte de equipos - Adquirir recursos de emergencia	Según necesidades durante la contingencia

7.3.4 Plan de Capacitación y Concienciación

Para asegurar que todo el personal involucrado en el plan de continuidad cuente con las competencias necesarias, se establece el siguiente plan de capacitación:

1. **Capacitación básica en continuidad**: Para todos los funcionarios y contratistas.
   - Frecuencia: Anual
   - Duración: 2 horas
   - Contenido: Conceptos básicos, roles, procedimientos de notificación
2. **Capacitación técnica para equipos de recuperación**: Para integrantes de equipos técnicos.
   - Frecuencia: Semestral
   - Duración: 4 horas
   - Contenido: Procedimientos detallados, herramientas, simulaciones prácticas
3. **Capacitación para líderes de continuidad**: Para coordinadores y líderes de equipos.
   - Frecuencia: Semestral
   - Duración: 4 horas
   - Contenido: Gestión de crisis, toma de decisiones, coordinación de equipos
4. **Campaña de concienciación institucional**:
   - Frecuencia: Trimestral
   - Canales: Intranet, correo electrónico, carteleras digitales
   - Contenido: Importancia de la continuidad, responsabilidades individuales, lecciones aprendidas

7.4 IDENTIFICACIÓN DE BRECHAS ENTRE LOS REQUERIMIENTOS DE CONTINUIDAD Y LAS CAPACIDADES ACTUALES

7.4.1 Metodología para el Análisis de Brechas

Para identificar las brechas entre los requerimientos de continuidad y las capacidades actuales, se ha utilizado la siguiente metodología:

1. **Evaluación de capacidades actuales**:
   - Inventario de recursos tecnológicos disponibles
   - Revisión PETI 2024 – 2027.
   - Evaluación de procedimientos existentes
   - Análisis de competencias del personal
   - Revisión de acuerdos con proveedores

2. **Comparación con requerimientos**:
   - Contraste entre RTOs/RPOs requeridos vs. capacidades actuales
   - Análisis de disponibilidad de recursos vs. necesidades identificadas
   - Evaluación de procesos documentados vs. procesos necesarios
3. **Categorización de brechas**:
   - Críticas: Impactan directamente la capacidad de recuperación de servicios vitales
   - Significativas: Afectan tiempos de recuperación, pero no impiden la restauración
   - Menores: Representan oportunidades de optimización

DEFINIR LAS BRECHAS CON LOS EQUIPOS CORRESPONDIENTES

7.4.2 Brechas Identificadas

ID	Categoría	Brecha Identificada	Requerimiento	Capacidad Actual	Impacto	Prioridad
BR-01	Infraestructura	Capacidad insuficiente del centro de datos alterno	Soportar 100% de sistemas críticos	Capacidad actual para XX% de sistemas críticos	No cumplimiento de RTOs para sistemas misionales	Alta
BR-02	Datos	Frecuencia de respaldos inadecuada para algunos sistemas críticos	RPO de 4 horas para BD Oracle	Respaldos cada XX horas	Pérdida potencial de hasta XX horas de datos	Alta

7.4.3 Plan de Acción para Cierre de Brechas

ID Brecha	Acción de Mejora	Responsable	Plazo	Recursos Requeridos	Indicador de Éxito
BR-01	Ampliar capacidad del centro de datos alterno	Líder de Infraestructura	6 meses	Presupuesto para equipamiento, espacio físico	Capacidad instalada para 100% de sistemas críticos
BR-02	Implementar replicación en tiempo real para BD críticas	Líder de Bases de Datos	3 meses	Licenciamiento, almacenamiento adicional	RPO reducido a 1 hora o menos

7.5 DEFINICIÓN DE LA ESTRATEGIA IRBC ALINEADA CON LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.5.1 Principios Rectores de la Estrategia

La estrategia de Preparación de las TIC para la Continuidad del Negocio (IRBC) de la Secretaría Distrital de la Mujer se fundamenta en los siguientes principios:

1. **Priorización basada en criticidad**: Los recursos y esfuerzos se asignarán según la criticidad de los sistemas para la misión institucional.
2. **Defensa en profundidad**: Implementación de múltiples capas de protección y recuperación para reducir puntos únicos de falla.
3. **Mejora continua**: Revisión y actualización periódica de estrategias basadas en resultados de pruebas y cambios en el entorno.
4. **Enfoque integral**: Consideración de aspectos tecnológicos, humanos y procedimentales en las estrategias de continuidad.
5. **Cumplimiento normativo**: Alineación con requisitos de la Política de Gobierno Digital y estándares como ISO 22301 e ISO 27031.
6. **Seguridad por diseño**: Integración de controles de seguridad en todas las fases de la continuidad del negocio.
7. **Resiliencia adaptativa**: Capacidad para ajustar estrategias según la naturaleza y duración de los incidentes.

7.5.2 Estrategias de Continuidad según Escenarios

Escenario	Descripción	Estrategia Principal	Controles Clave	Alineación con Política de Seguridad
Falla total del centro de datos principal	Indisponibilidad completa del datacenter por falla eléctrica, incendio, inundación, etc.	Activación de centro de datos alterno en modalidad de colocación y servicios en nube	- Centro de datos alterno preconfigurado - Procedimientos de conmutación documentados - Pruebas periódicas de failover	- Protección de la disponibilidad - Gestión de la continuidad del negocio - Control de acceso
Ciberataque/Ransomware	Compromiso de sistemas por malware, ransomware o intrusiones	Aislamiento, recuperación desde respaldos aislados (air-gapped)	- Backups aislados y verificados - Procedimientos de restauración seguros - Imágenes "doradas" preconfiguradas - Plan de respuesta a incidentes	- Gestión de incidentes - Protección contra malware - Respaldo de información - Control de acceso
Pérdida de conectividad	Fallas en enlaces MPLS o Internet	Activación de enlaces redundantes, acceso alternativo a servicios críticos	- Enlaces de comunicación redundantes - VPN alternativa - Balanceadores de carga - Procedimientos operativos alternativos	- Transferencia de información - Gestión de redes - Teletrabajo
Falla de sistemas específicos	Falla en aplicaciones o bases de datos críticas	Recuperación específica del sistema afectado	- Procedimientos de recuperación por sistema - Automatización de restauración	- Gestión de vulnerabilidades - Desarrollo seguro - Control de cambios

			- Pruebas específicas por componente	

7.5.3 Estrategias Específicas por Tipo de Recurso

Tipo de Recurso	Estrategia de Continuidad	Objetivo de Implementación	Alineación con Política de Seguridad
Infraestructura de Servidores	- Virtualización con capacidad de migración en vivo - Replicación de servidores críticos en sitio alterno - Aprovisionamiento automatizado basado en templates	- Reducción de RTOs a menos de 4 horas para servidores críticos - Eliminación de puntos únicos de falla - Flexibilidad de recursos	- Seguridad física y del entorno - Gestión de activos - Seguridad en la operación
Bases de Datos	- Replicación síncrona/asíncrona según criticidad - Respaldos incrementales frecuentes - Estrategia de recuperación punto-en-el-tiempo	- RPOs de 1 hora o menos para datos críticos - Integridad de datos asegurada - Capacidad de recuperación granular	- Protección de la información - Copias de seguridad - Controles criptográficos
Aplicaciones	- Arquitectura de alta disponibilidad para sistemas críticos - Despliegue en múltiples zonas/regiones para sistemas en nube - Estrategia de desarrollo que facilite recuperación	- Disponibilidad del 99.9% para sistemas misionales - Minimización de dependencias - Despliegues automatizados	- Desarrollo seguro - Gestión de cambios - Protección contra código malicioso
Almacenamiento	- Replicación de datos críticos a sitio secundario - Respaldos en múltiples medios y ubicaciones - Snapshots programados para recuperación rápida	- Redundancia de datos críticos - Recuperación rápida desde snapshots - Protección contra corrupción de datos	- Gestión de medios - Controles criptográficos - Registro y supervisión
Comunicaciones	- Redundancia de enlaces para sedes críticas - Soluciones de conectividad alternativas (4G/5G) - Balanceo de carga y conmutación automática	- Conectividad ininterrumpida para sedes críticas - Capacidad de acceso remoto seguro - Aislamiento controlado de segmentos de red	- Seguridad de las comunicaciones - Transferencia de información - Control de acceso a redes
Acceso de Usuarios	- Soluciones de VPN redundantes - Equipos de respaldo para personal crítico - Procedimientos de trabajo remoto	- Acceso seguro a sistemas desde ubicaciones alternativas - Continuidad de operaciones para personal clave - Flexibilidad de métodos de acceso	- Control de acceso - Seguridad en recursos humanos - Teletrabajo

7.5.4 Estrategias de Recuperación Tecnológica

7.5.4.1 Estrategias para Centro de Datos y Servidores

La Secretaría Distrital de la Mujer implementará una estrategia híbrida para la recuperación de su centro de datos, combinando:

1. **Centro de Datos Alterno en modalidad de Colocación**:
   - Ubicación geográficamente separada del centro principal
   - Capacidad para hospedar equipos críticos de la entidad
   - Conexión de red redundante con el centro principal
   - Controles físicos y ambientales acordes a estándares
2. **Infraestructura Virtualizada**:
   - Servidores virtualizados para facilitar portabilidad
   - Capacidad de migración de máquinas virtuales entre sitios
   - Snapshots periódicos para recuperación rápida
   - Templates preconfigurados para aprovisionamiento rápido
3. **Servicios en Nube**:
   - Replicación de servicios críticos en nube pública (Oracle Cloud)
   - Arquitectura híbrida que permita conmutación controlada
   - Servicios SaaS para funciones no críticas
   - Estrategia de recuperación cross-cloud para servicios críticos

7.5.4.2 Estrategias para Datos y Aplicaciones

Para garantizar la recuperación efectiva de datos y aplicaciones, se implementará:

1. **Gestión de Respaldos**:
   - Política de respaldos alineada con RPOs identificados
   - Múltiples niveles de respaldo (full, incremental, diferencial)
   - Almacenamiento de respaldos en sitios geográficamente separados
   - Respaldos aislados (air-gapped) para protección contra ransomware
   - Pruebas periódicas de restauración
2. **Replicación de Datos**:
   - Replicación síncrona para bases de datos críticas
   - Replicación asíncrona para datos de importancia media
   - Monitoreo continuo de la sincronización
   - Procedimientos para conmutación controlada
3. **Arquitectura de Aplicaciones**:
   - Diseño de aplicaciones con principios de resiliencia
   - Redundancia de componentes críticos
   - Desacoplamiento de servicios para minimizar dependencias
   - APIs documentadas para facilitar integración alternativa

7.5.4.3 Estrategias para Comunicaciones

Para mantener la conectividad durante eventos disruptivos:

1. **Redundancia de Enlaces**:
   - Enlaces MPLS principales y secundarios con proveedores diferentes
   - Conexiones a Internet redundantes con balanceo de carga
   - Enlaces dedicados entre centro de datos principal y alterno
2. **Soluciones Alternativas de Conectividad**:
   - Conectividad 4G/5G para sedes críticas
   - VPN sobre Internet como respaldo a MPLS
   - Soluciones de SD-WAN para optimización y redundancia
3. **Segmentación y Priorización**:
   - Segmentación de redes críticas para aislamiento controlado
   - Priorización de tráfico para servicios esenciales
   - Configuraciones preestablecidas para escenarios de contingencia

7.5.5 Integración con la Política de Seguridad y Privacidad de la Información

La estrategia IRBC se integra con la Política de Seguridad y Privacidad de la Información de la Secretaría Distrital de la Mujer a través de los siguientes mecanismos:

1. **Confidencialidad**:
   - Mantenimiento de controles de acceso durante contingencias
   - Cifrado de datos en tránsito y reposo, incluso en situaciones de recuperación
   - Procedimientos seguros para restauración que protejan información sensible
2. **Integridad**:
   - Verificación de integridad en procesos de restauración
   - Controles para evitar corrupción de datos durante recuperación
   - Validación de sistemas recuperados antes de su puesta en producción
3. **Disponibilidad**:
   - Estrategias multinivel para garantizar disponibilidad
   - Arquitecturas redundantes para servicios críticos
   - Procedimientos alternativos documentados para funciones esenciales
4. **Autenticidad**:
   - Mantenimiento de mecanismos de autenticación durante contingencias
   - Validación de identidad para acceso a sistemas recuperados
   - Trazabilidad de acciones durante procesos de recuperación
5. **Gestión de Riesgos**:
   - Alineación de controles con riesgos identificados
   - Evaluación periódica de efectividad de las estrategias
   - Adaptación de controles según evolución de amenazas

7.6.6 Métricas de Efectividad de la Estrategia

Para evaluar la efectividad de la estrategia IRBC, se implementarán las siguientes métricas:

Métrica	Descripción	Objetivo	Método de Medición	Frecuencia
Tiempo real de recuperación	Tiempo efectivo para restaurar servicios críticos en pruebas o incidentes reales	≤ RTO establecido para cada servicio	Cronometraje durante pruebas o incidentes	Trimestral
Punto real de recuperación	Cantidad de datos efectivamente perdidos en una recuperación	≤ RPO establecido para cada servicio	Análisis de datos recuperados en pruebas	Trimestral
Tasa de éxito en pruebas	Porcentaje de pruebas de recuperación completadas exitosamente	≥ 95%	Registro de resultados de pruebas	Según plan de pruebas
Tiempo de detección de incidentes	Tiempo transcurrido entre ocurrencia y detección	≤ 15 minutos para incidentes críticos	Registro de incidentes y monitoreo	Mensual
Disponibilidad de sistemas críticos	Porcentaje de tiempo de funcionamiento de sistemas misionales	≥ 99.9%	Herramientas de monitoreo	Mensual
Cumplimiento del plan de pruebas	Porcentaje de pruebas realizadas vs. planificadas	100%	Registro del plan de pruebas	Trimestral
Efectividad de la capacitación	Conocimiento demostrado por personal clave	≥ 90% de aprobación en evaluaciones	Evaluaciones post-capacitación	Semestral
Tiempo de actualización del plan	Días para actualizar el plan tras cambios significativos	≤ 30 días	Registro de control de cambios	Por evento

7.5.7 Plan de Implementación de la Estrategia

La implementación de la estrategia IRBC se realizará de manera escalonada, priorizando las acciones de mayor impacto y menor complejidad:

Fase 1: Fundamentos (0-3 meses)

- Formalización de la política y estructura de gobierno
- Documentación de procedimientos básicos de recuperación
- Implementación de mejoras en respaldos para sistemas críticos
- Capacitación inicial del personal clave

Fase 2: Fortalecimiento (4-6 meses)

- Implementación de replicación para datos críticos
- Mejora de enlaces redundantes para sedes principales
- Desarrollo de automatizaciones básicas para recuperación
- Primera prueba integral del plan

Fase 3: Optimización (7-12 meses)

- Implementación de centro de datos alterno con capacidad completa
- Automatización avanzada de procesos de recuperación
- Integración de servicios en nube para continuidad
- Pruebas regulares de escenarios complejos

Fase 4: Madurez (12+ meses)

- Implementación de recuperación casi-continua para sistemas más críticos
- Automatización completa de conmutación para servicios prioritarios
- Integración de continuidad en ciclo de vida de desarrollo
- Mejora continúa basada en métricas y lecciones aprendidas

El plan de implementación será revisado trimestralmente para ajustar prioridades, recursos y cronograma según los resultados obtenidos y cambios en el entorno tecnológico u organizacional de la Secretaría Distrital de la Mujer.

8. CRONOGRAMA

Las actividades del Plan de Continuidad 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 aplicable 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.

9. DESCRIPCIÓN DE ACTIVIDADES

Las actividades del Plan de Continuidad del proceso Gestión Tecnológica se vienen adelantando de la siguiente manera:

- Definición de objetivos
- Definición del alcance
- Definiciones de variables a aplicar en el ejercicio de análisis de componentes
- Definición de responsabilidades
- Definición de componentes
- Análisis de componentes tecnológicos
- Definición de la estrategia
- Aplicación de las variables a los componentes para definir criticidad
- Determinación de prioridades según criticidad estimada

.

10. 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: Cristian Camilo Calderón Tapia	NOMBRE: Carlos Alfonso Gaitán Sánchez	NOMBRE: José Leonardo Buitrago Paula Vanessa Sosa Martin Luz Ángela Andrade Arévalo	NOMBRE: Carlos Alfonso Gaitán Sánchez
CARGO: Contratista OAP TIC	CARGO: Jefe Oficina Asesora de Planeación	CARGO: Profesional Especializado OAP-TIC Contratistas OAP	CARGO: Jefe Oficina Asesora de Planeación