

INFORME PLAN DE CONTINGENCIA INSTITUCIONAL DE LA SDHT CBN-1107

Objetivo General:

Presentar las acciones realizadas durante la vigencia 2024, que aseguraron que la Entidad contará con los mecanismos necesarios para mitigar los impactos, proteger su funcionamiento y minimizar riesgos ante cualquier eventualidad

Objetivos Específicos:

- Identificar y evaluar los posibles riesgos y amenazas que puedan afectar el normal funcionamiento de la institución, considerando factores como desastres naturales, emergencias sanitarias, riesgos tecnológicos y sociales, entre otros.
- Identificar áreas de mejora y definir acciones específicas para garantizar la actualización y efectividad del plan de continuidad, así como para asegurar que los requerimientos de los servicios institucionales sean atendidos de manera adecuada tanto a los actores internos como externos.

Alcance:

El Plan de Contingencia Institucional cubre todas las áreas de la entidad, incluyendo el personal, la infraestructura, la tecnología y los procesos críticos para la prestación de servicios a la comunidad. Las estrategias de continuidad deben integrar estos elementos y desarrollar planes y acciones que respondan a las necesidades específicas de cada uno. Si bien los esfuerzos tecnológicos son clave para garantizar la continuidad, la evaluación de los servicios institucionales y de los procesos ofrece una visión más amplia y complementaria del contexto general.

Marco Conceptual:

- **Definiciones:**

Contingencia: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

elementos en riesgo: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

Vulnerabilidad: Es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.

Riesgo: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co



Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

Incidente: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización.

Activo: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

MINTIC: Ministerio de Tecnologías de la Información y Comunicaciones

Plan de contingencia: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios y procesos críticos de la SDHT que lo afecte de forma parcial o total.

- **Normatividad Relacionada:**

En Colombia, la normatividad relacionada con los planes de contingencia tecnológica y la continuidad de servicios se fundamenta en las siguientes disposiciones:

Ley 1523 de 2012: Establece la Política Nacional de Gestión del Riesgo de Desastres y crea el Sistema Nacional de Gestión del Riesgo de Desastres (SNGRD). Esta ley obliga a las entidades públicas y privadas a desarrollar planes de gestión del riesgo, incluyendo aspectos tecnológicos, para garantizar la continuidad de sus operaciones.

Decreto 2157 de 2017: Adopta directrices generales para la elaboración del Plan de Gestión del Riesgo de Desastres en entidades públicas y privadas, en el marco del artículo 42 de la Ley 1523 de 2012. Este decreto enfatiza la necesidad de incluir estrategias para la continuidad de los servicios tecnológicos en dichos planes¹.

Decreto 2672 de 2013: Modifica parcialmente la estructura de la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD) y establece lineamientos para la incorporación de la gestión del riesgo en los planes de ordenamiento territorial, lo que incluye la infraestructura tecnológica².

Estrategia de la SDHT para implementar el Plan de Contingencia de la Entidad

¹ Tomado de funcionpublica.gov.co

² Tomado de portal.gestiondelriesgo.gov.co

La estrategia del Plan de Contingencia de la Secretaría Distrital del Hábitat - SDHT, está diseñada para garantizar la continuidad de sus procesos informáticos, en el momento de afrontar fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos tecnológicos e información con las menores pérdidas posibles, de forma rápida, eficiente y oportuna. Esta estrategia es integral, adaptable y alineada con los principios de la gestión pública, priorizando la eficiencia operativa y el cumplimiento de la normativa legal.

La Subsecretaría de Gestión Corporativa de la SDHT, en su objetivo de fortalecer el Sistema de Gestión de Seguridad de la Información alineado con el Modelo de Seguridad y Privacidad de la información (MSPI) definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC; optó, como medida estratégica, seguir los lineamientos que nos ayuden a preservar la integridad, la disponibilidad y la confidencialidad de la información de valor de la entidad.

Para establecer un plan de contingencia institucional efectivo, se consideraron las siguientes etapas o elementos claves para su implementación.



ILUSTRACIÓN 1 PLAN DE CONTINGENCIA INSTITUCIONAL

Evaluación de Riesgos:

Se identifican los riesgos y sus potenciales impactos en el caso que se materialicen en la continuidad operativa de la entidad. Dentro de los riesgos más comunes que afectan la continuidad se pueden identificar los siguientes:

- Desastres naturales (inundaciones, terremotos, incendios).
- Fallas tecnológicas (ciberataques, interrupción de servicios de TI).
- Factores humanos (huelgas, ausentismo masivo del personal).
- Crisis sanitarias (pandemias, brotes epidemiológicos).

Riesgos de Tecnología

Secretaría Distrital del Hábitat
Servicio al ciudadano: Carrera 13 No. 52-13
Sede Principal: Calle 52 No. 13-64
Teléfono: 601-3581600
Código Postal: 110231
www.habitatbogota.gov.co



Respecto a los riesgos relacionados con el proceso de tecnología, en la vigencia 2024 se realizó una revisión de estos y se ajustaron de acuerdo con la metodología aplicable a la SDHT, que a continuación se relacionan:

Riesgo	Causas	Consecuencias	Controles
R186. Posibilidad de afectación reputacional durante la gestión del ciclo de vida de la infraestructura tecnológica por problemas en su manejo, mantenimiento y seguridad.	Causa raíz: Problemas en su manejo, mantenimiento y seguridad. Inadecuada gestión de vulnerabilidades (identificación, remediación y seguimiento) Tecnológica- Falta de implementación de los lineamientos de seguridad de la información dados por MinTIC	Fallas o pérdida en los niveles de integridad, confidencialidad y disponibilidad de la información de la entidad para el cumplimiento de su misión. Interrupción en los servicios al interior de la entidad y a la ciudadanía	Se establecieron los controles de acuerdo con el procedimiento de Monitoreo de los Recursos de Procesamiento y Almacenamiento de Información, Gestión de Incidentes, Gestión de cuentas de usuario y Control de Cambios. Por tanto, se determinaron los siguientes: C186: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento al funcionamiento de los sistemas de almacenamiento y las copias de respaldo, mensualmente, con el propósito de evidenciar el suficiente espacio para garantizar su funcionamiento Evidencia: Informes y reportes del estado de los backups y sistemas de almacenamiento. C187: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica verifica el estado de la seguridad informática

Riesgo	Causas	Consecuencias	Controles
			(Firewall y Antivirus), mensualmente, con el propósito de validar la seguridad de la información y su actualización frente a las políticas Evidencia: Informe de revisión de firewall y antivirus Desviación: En caso de detectarse alguna vulnerabilidad o ataque se toman las medidas preventivas y correctivas según sea el caso. C188: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento al control en la asignación de permisos a usuarios, mensualmente, con el propósito de depurar la base de datos de usuarios y la asignación de los mismos. Evidencia: Reporte de casos de creación de usuarios reportados en la mesa de ayuda. Desviación: En caso de que no se realice la asignación de permisos, se analizan las causales que generan demora en la asignación del usuario
R187. Posibilidad de afectación reputacional durante la gestión del	Causa raíz: problemas en su manejo,	Se realizó el análisis de las consecuencias del riesgo y se	Se establecieron los controles de acuerdo con el procedimiento

Riesgo	Causas	Consecuencias	Controles
ciclo de vida, interoperabilidad y bases de datos de los sistemas de información bajo dominio del proceso de Gestión Tecnológica por problemas en su manejo, mantenimiento y seguridad.	mantenimiento y seguridad. Inadecuadas medidas de seguridad para el acceso a archivos de información almacenada en medios digitales. Capacidad de almacenamiento insuficiente y/o inadecuada para la custodia de la información. Vulnerabilidad de seguridad de los sistemas de información. Existencia de obsolescencia tecnológica	determinaron las siguientes: Pérdida de información Interrupción en los servicios al interior de la entidad y a la ciudadanía Pérdida de credibilidad de la ciudadanía	de Monitoreo de los Recursos de Procesamiento y Almacenamiento de Información, Gestión de Incidentes y Gestión cuentas de usuario. Por tanto, se determinaron los siguientes: C190: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento al funcionamiento de los sistemas de almacenamiento y las copias de respaldo, mensualmente, con el propósito de evidenciar el suficiente espacio para garantizar su funcionamiento. Evidencia: Informes y reportes del estado de los backups y sistemas de almacenamiento Desviación: En caso de que no se haga el seguimiento, el sistema de información genera la alerta de poco espacio C191: Profesional de la Subsecretaria de Gestión Corporativa-Gestión tecnológica verifica el estado de la seguridad informática (Firewall y Antivirus), mensualmente, con el propósito de validar la seguridad de la

Riesgo	Causas	Consecuencias	Controles
			información y su actualización frente a las políticas mensualmente Evidencia: Informe de revisión de firewall y antivirus Desviación: En caso de detectarse alguna vulnerabilidad o ataque se toman las medidas preventivas y correctivas según sea el caso. C192: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento al control en la asignación de permisos a usuarios, mensualmente, con el propósito de depurar la base de datos de usuarios y la asignación de los mismos mensualmente Evidencia: Reporte de casos de creación de usuarios reportados en la mesa de ayuda. Desviación: En caso de que no se realice la asignación de permisos, se analizan las causales que generan demora en la asignación del usuario.
R188. Posibilidad de afectación reputacional durante la implementación efectiva	Causa raíz: fallas en la infraestructura de TI o vulnerabilidades	Se realizó el análisis de las consecuencias del riesgo y se determinaron las	Se establecieron los controles de acuerdo con el de la caracterización del

Riesgo	Causas	Consecuencias	Controles
de los proyectos relacionados con la arquitectura misional y tecnológica por fallas en la infraestructura de TI o vulnerabilidades de seguridad no gestionadas.	de seguridad no gestionadas. Inadecuados controles de seguridad para el acceso a la información (definición de los roles y responsabilidades del uso de la información). Ausencia de políticas claras para gestionar vulnerabilidades y proteger la infraestructura tecnológica deja la entidad expuesta a ataques cibernéticos. Ausencia de procesos formales para el diseño y actualización del PETI y las arquitecturas misional y tecnológica.	siguientes: Incumplimientos por no aplicación de políticas nacionales y distritales. Perder la confianza en la Entidad si se producen incidentes de seguridad o fallas en los sistemas que afecten la disponibilidad o integridad de la información.	proceso. Por tanto, se determinaron los siguientes: C193: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento a las necesidades de desarrollo tecnológico de las áreas de la entidad, semestralmente, alineándose con los motivadores estratégicos definidos en el PETI, para diagnosticar los elementos requeridos en la renovación de infraestructura tecnológica. Evidencia: Plan Estratégico de Tecnologías de la Información (PETI) Desviación: En caso de que no se haga seguimiento a las necesidades de desarrollo tecnológico, estas se presentan a la Subsecretaria de Gestión Corporativa para su revisión C194: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica realiza seguimiento al desarrollo del proyecto, semestralmente, siguiendo las buenas prácticas de gestión

Riesgo	Causas	Consecuencias	Controles
			de proyectos y satisfacer la necesidad que tiene la entidad Evidencia: Actas de reunión de seguimiento Desviación: En caso de que se presenten retrasos en la ejecución de los proyectos, se generan las alertas internas en el proceso C195: Profesional o apoyo designado por la SDHT para el proceso de Gestión Tecnológica valida el cumplimiento de los objetivos del proyecto, cada vez que se requiera, con el propósito de documentar los resultados obtenidos Evidencia: Actas de cierre del proyecto. Desviación: En caso de que se presenten retrasos en la ejecución de los proyectos, se generan las alertas internas en el proceso.

Identificación servicios y procesos críticos

La evaluación de riesgos y su impacto se lleva a cabo por dependencias o procesos institucionales, permitiendo identificar la criticidad de los procesos, servicios, actividades y activos de la entidad, con el fin de determinar los mecanismos más adecuados para su recuperación.

El escenario ideal es tener una contingencia que cubra cualquier necesidad de las dependencias, pero el tener un escenario como estos no es viable por los costos de implementación operación y mantenimiento. Debido a esto, la mejor práctica es identificar los servicios y procesos críticos y de acuerdo con su naturaleza establecer los mecanismos de contingencia apropiados. Por ejemplo, en casos de fallas tecnológicas, se establecen mecanismos como las copias de respaldo

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co



de la información o mantener infraestructura tecnológica duplicada para servicios específicos, en el caso de personas se busca tener un conocimiento distribuido en dos o más personas.

Determinar las medidas y estrategias

Como se mencionó anteriormente la identificación de las medidas y estrategias para la continuidad, varían de acuerdo con el servicio, proceso o actividad que requiera contingencia. Las medidas de contingencia para los elementos tecnológicos están basadas en la tecnología; y las medidas de contingencia para personas, o para procesos, están basadas en conocimiento o en prácticas. Sin embargo, en ambos casos la tecnología y los procesos son complementarios para tener un escenario de contingencia completo.

Implementar y evaluar

Una vez implementadas las medidas y estrategias de contingencia para la tecnología, los procesos y las actividades, es necesario realizar una evaluación continua y tomar acciones correctivas para asegurar que las actividades de contingencia cumplan su objetivo.

Acciones realizadas durante la vigencia 2024

Respecto a la contingencia tecnológica, se realizó la revisión del Plan de Recuperación de Desastres (DRP) como medida estratégica para la preservación de la información y la disponibilidad de los servicios de los sistemas de información críticos ante situaciones disruptivas (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio), permitiendo minimizar el impacto y recuperación por pérdida de activos de información de la entidad, hasta un nivel aceptable, mediante la combinación de controles preventivos y de recuperación.

Como resultado de la gestión de contingencia, el Grupo de Gestión tecnológica de la SDHT, identificó puntos clave y acciones necesarias para mejorar el nivel de contingencia y minimizar los riesgos de pérdida de datos e indisponibilidad de los servicios tecnológicos de la entidad.

En cuanto a la Infraestructura Tecnológica representada en las siguientes imágenes, se relacionan las acciones requeridas por cada uno de los tipos de infraestructura, a saber:



ILUSTRACIÓN 2 INFRAESTRUCTURA TECNOLÓGICA ACTUAL SDHT, ALMACENAMIENTO, RESPALDO Y PROCESAMIENTO

Acciones Requeridas:

- Renovar soporte infraestructura
 - Renovar soporte almacenamiento
 - Generar concepto de almacenamiento obsoleto
 - Depurar Sharepoint
 - Administrar y optimizar infraestructura OCI
- Estabilizar infraestructura
- Recuperar 2 Host Cisco en desuso
 - Renovar licenciamiento Vcenter
 - Renovar soporte Blade Cisco
- Implementar procedimiento de Backup
 - Habilitar solución de cintas para backup
 - Renovar licenciamiento de Veeam
- Migrar Paz y Salvos, página web a OCI
- Reportar y programar updates de SO obsoletos.

Como medida adicional, se requiere identificar y valorar el uso de mecanismos adicionales de renovación de infraestructura y licenciamiento.



ILUSTRACIÓN 3 INFRAESTRUCTURA TECNOLÓGICA ACTUAL SDHT, SEGURIDAD, COMUNICACIONES, MONITOREO

Acciones Requeridas:

- Firewall – Seguridad
 - Retirar FW Palo Alto obsoletos
 - Renovar licenciamiento FW Fortinet
 - Ajustar configurar correlacionador de eventos SolarWinds
- Networking
 - Ajustar topología switches eXtreme sobre utilizados
 - Generar topología de datacenter, sedes y topologías
 - Generar pruebas de conmutación y saturación de canales
 - Renovar ecosistema de Networking
- Monitoreo
 - Recuperar acceso herramienta monitoreo
 - Configurar agentes reales de la monitorización (On-Premise, OCI)
 - Configurar alertas con umbrales
 - Apoyar plan de capacidades con Solarwinds

Medidas adicionales de contingencia

En complemento de lo anterior, el Grupo de Gestión Tecnológica realizó diferentes actividades con el propósito de cumplir el plan de contingencia, que a continuación se relacionan:

- Habilitación de una plataforma alterna de backupss para la toma de respaldos de la información de la entidad y tener un punto de recuperación en caso de falla, sin embargo, se hace necesario contar con una copia adicional que se aloje en una ubicación externa.
- Habilitación y ajustes de las plataformas de monitoreo para mejorar el nivel de observabilidad de la infraestructura tecnológica y tomar acciones preventivas o correctivas previas a la suspensión de los servicios, e implementar medidas de contingencia con tiempos aceptables con la criticidad de los servicios institucionales.
- Fortalecimiento de las políticas de seguridad perimetral que minimicen los riesgos de ataque o acceso no autorizado de usuarios externos y acceso malintencionados dirigidos a robos de información.
- Gestión sobre los proveedores del centro de datos y comunicaciones y la planeación de la migración a la nueva ubicación, mejorando las prestaciones de los facilities (ubicación física del centro de datos que incluye los sistemas de acceso, video vigilancia, control anti-incendio, aire acondicionado y redundancia de red y alimentación eléctrica).

Como medida adicional, de contingencia para los canales de comunicación, se tiene dispuesta la siguiente topología, en la cual se cuenta en diferentes puntos con equipos redundantes o con una disposición que permite la recuperación de los servicios de conectividad con conexiones o líneas de respaldo.

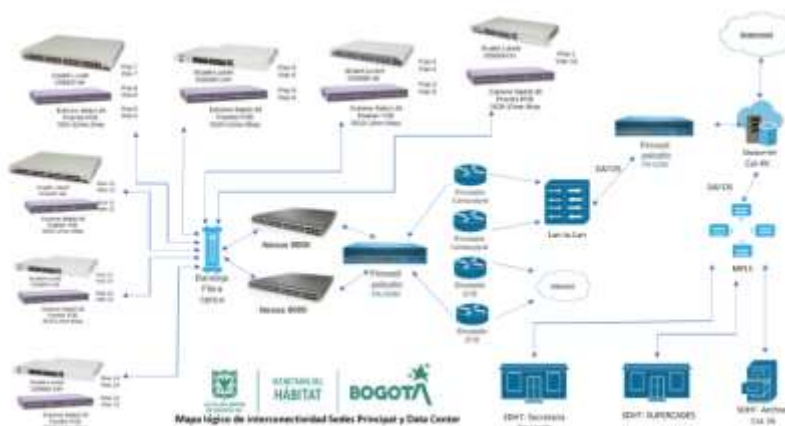


ILUSTRACIÓN 4 DIAGRAMA DE RED SDHT.

Entre los activos de infraestructura de red de la SDHT, podemos destacar que las diferentes sedes, como son el centro de datos, el archivo documental sede carrea 16, Supercades y la sede de la Secretaría de Hacienda y la sede principal de SDHT de la calle 52, se encuentran

interconectadas a través de una red MPLS, la cual cuenta con activos de telecomunicaciones como son router centurylink, router Cisco, firewall Palo Alto, switches Alcatel, switches Lexus, y dispositivos eléctricos como la UPS PowerSUN y con medidas de contingencia previstas por el proveedor de los servicios de conectividad. Estos activos tecnológicos están administrados por el grupo de Gestión Tecnológica de la entidad.

Inventario de equipos

A continuación, se relaciona la infraestructura tecnológica de la entidad:

No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietario	¿Está en Garantía?	Tiene Contrato de soporte y/o mantenimiento?	Criticidad	Tiene Contingencia	Producción / Pruebas / Respaldo
1	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
2	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
3	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
4	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
5	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
6	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
7	Físico	Centro de datos externo	Virtualizador Vm Ware 6.0	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
8	Virtu al	Centro de datos externo	Directorio Activo	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
9	Virtu al	Centro de datos externo	Directorio Activo	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
10	Virtu al	Centro de datos externo	VUC	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
11	Virtu al	Centro de datos externo	Argis	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
12	Virtu al	Centro de datos externo	Aula Virtual	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
13	Virtu al	Centro de datos externo	Centos Pruebas	Aplicación	SDHT	NO	NO	ALTA	NO	Pruebas
14	Virtu al	Centro de datos externo	SIDICIC	Aplicación	SDHT	NO	NO	ALTA	NO	Producción
15	Virtu al	Centro de datos externo	SIDIVIC	Aplicación	SDHT	NO	NO	ALTA	NO	Producción

No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietar io	¿Está en Garantí a?	Tiene Contrato de soporte y/o mantenimient o?	Criticid ad	Tiene Contingen cia	Producción / Pruebas / Respaldo
16	Virtu al	Centro de datos externo	SIDIVIC	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
17	Virtu al	Centro de datos externo	VUC	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
18	Virtu al	Centro de datos externo	DIGITURNO	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
19	Virtu al	Centro de datos externo	Expedientes	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
20	Virtu al	Centro de datos externo	Expedientes	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
21	Virtu al	Centro de datos externo	File Server	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
22	Virtu al	Centro de datos externo	Forest	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
23	Virtu al	Centro de datos externo	Forest	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
24	Virtu al	Centro de datos externo	Forest	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
25	Virtu al	Centro de datos externo	GLPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
26	Virtu al	Centro de datos externo	GLPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
27	Virtu al	Centro de datos externo	Habitat a la vista	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
28	Virtu al	Centro de datos externo	Habitat a la vista	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
29	Virtu al	Centro de datos externo	Historico	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
30	Virtu al	Centro de datos externo	Almacenamiento	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
31	Virtu al	Centro de datos externo	Intranet	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
32	Virtu al	Centro de datos externo	JSP7	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
33	Virtu al	Centro de datos externo	JSP7	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
34	Virtu al	Centro de datos externo	Consola de administración VMWARE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
35	Virtu al	Centro de datos externo	MAPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co



No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietar io	¿Está en Garantí a?	Tiene Contrato de soporte y/o mantenimient o?	Criticid ad	Tiene Contingen cia	Producción / Pruebas / Respaldo
36	Virtu al	Centro de datos externo	Ocupaciones	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
37	Virtu al	Centro de datos externo	Ocupaciones	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
38	Virtu al	Centro de datos externo	Base de datos potsgresql RHEL	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
39	Virtu al	Centro de datos externo	Base de datos potsgresql RHEL	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
40	Virtu al	Centro de datos externo	Relays Base de Datos	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
41	Virtu al	Centro de datos externo	Directorio Activo	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
42	Virtu al	Centro de datos externo	Base de Datos ETB	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
43	Virtu al	Centro de datos externo	SIDEC	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
44	Virtu al	Centro de datos externo	SIDEC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
45	Virtu al	Centro de datos externo	SIG	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
46	Virtu al	Centro de datos externo	SIG	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
47	Virtu al	Centro de datos externo	SIG	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
48	Virtu al	Centro de datos externo	SIG	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
49	Virtu al	Centro de datos externo	SIHAB - 2020	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
50	Virtu al	Centro de datos externo	SIPIVE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
51	Virtu al	Centro de datos externo	SIPIVE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
52	Virtu al	Centro de datos externo	SOLARWINDS (SEM)	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
53	Virtu al	Centro de datos externo	SPSS SISTEMA ESTADISTICO	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
54	Virtu al	Centro de datos externo	ARGIS	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
55	Virtu al	Centro de datos externo	Directorio Activo	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co



No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietar io	¿Está en Garantí a?	Tiene Contrato de soporte y/o mantenimient o?	Criticid ad	Tiene Contingen cia	Producción / Pruebas / Respaldo
56	Virtu al	Centro de datos externo	ARGIS	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
57	Virtu al	Centro de datos externo	Escuela Virtual	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
58	Virtu al	Centro de datos externo	Escuela Virtual	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
59	Virtu al	Centro de datos externo	Escuela Virtual	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
60	Virtu al	Centro de datos externo	Gitlab	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
61	Virtu al	Centro de datos externo	JENKINS	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
62	Virtu al	Centro de datos externo	JSP7	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
63	Virtu al	Centro de datos externo	MAPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
64	Virtu al	Centro de datos externo	MAPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
65	Virtu al	Centro de datos externo	Monitoreo	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
66	Virtu al	Centro de datos externo	Monitoreo	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
67	Virtu al	Centro de datos externo	Observatorio	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
68	Virtu al	Centro de datos externo	SRVAPPPCONT	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
69	Virtu al	Centro de datos externo	Impresión	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
70	Virtu al	Centro de datos externo	Proxy	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
71	Virtu al	Centro de datos externo	Restauración Windows	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
72	Virtu al	Centro de datos externo	Restauración Linux	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
73	Virtu al	Centro de datos externo	Reportes	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
74	Virtu al	Centro de datos externo	Sistema de Gestión Financiera	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
75	Virtu al	Centro de datos externo	Sistema de Gestión Financiera	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co



No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietar io	¿Está en Garantí a?	Tiene Contrato de soporte y/o mantenimient o?	Criticid ad	Tiene Contingen cia	Producción / Pruebas / Respaldo
76	Virtu al	Centro de datos externo	SIDEC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
77	Virtu al	Centro de datos externo	SIDIVIC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
78	Virtu al	Centro de datos externo	TABLEU	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
79	Virtu al	Centro de datos externo	SRVAPPTMX	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
80	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
81	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
82	Virtu al	Centro de datos externo	WEB	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
83	Virtu al	Centro de datos externo	WEB	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
84	Virtu al	Centro de datos externo	XROAD	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
85	Virtu al	Centro de datos externo	XROAD	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
86	Virtu al	Centro de datos externo	Chat Web	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
87	Virtu al	Centro de datos externo	Escuela Virtual	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
88	Virtu al	Centro de datos externo	Escuela Virtual	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
89	Virtu al	Centro de datos externo	MAPI	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
90	Virtu al	Centro de datos externo	MAPI	Base de Datos	SDHT	NO	NO	ALTA	NO	Pruebas
91	Virtu al	Centro de datos externo	SIDIVIC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
92	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
93	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Pruebas
94	Virtu al	Centro de datos externo	WEB	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
95	Virtu al	Centro de datos externo	DHCP	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción

Secretaría Distrital del Hábitat

Servicio al ciudadano: Carrera 13 No. 52-13

Sede Principal: Calle 52 No. 13-64

Teléfono: 601-3581600

Código Postal: 110231

www.habitatbogota.gov.co

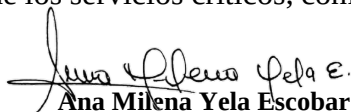


No.	Virtu al o Físico	Ubicación	Servicio que Provee	App/DB	Propietar io	¿Está en Garantí a?	Tiene Contrato de soporte y/o mantenimient o?	Criticid ad	Tiene Contingen cia	Producción / Pruebas / Respaldo
96	Virtu al	Centro de datos externo	File Server	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
97	Virtu al	Centro de datos externo	GLPI Bienes y Servicios	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
98	Virtu al	Centro de datos externo	MEMCACHEDWE B	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
99	Virtu al	Centro de datos externo	RADIUS	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
100	Virtu al	Centro de datos externo	Monitoreo	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
101	Virtu al	Centro de datos externo	vCenter_6U2	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
102	Virtu al	Centro de datos externo	Aplicación	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción - Respaldo
103	Virtu al	Centro de datos externo	Producción	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción - Respaldo
104	Virtu al	Centro de datos externo	VMWARE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
105	Virtu al	Centro de datos externo	VMWARE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
106	Virtu al	Centro de datos externo	VMWARE	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
107	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
108	Virtu al	Centro de datos externo	VUC	Base de Datos	SDHT	NO	NO	ALTA	NO	Producción
109	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
110	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
111	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
112	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
113	Virtu al	Centro de datos externo	VUC	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
114	Virtu al	Centro de datos externo	Website SDHT	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción
115	Virtu al	Centro de datos externo	WSUS	Aplicaci ón	SDHT	NO	NO	ALTA	NO	Producción

TABLA 1 INVENTARIO SERVIDORES SDHT

La Entidad ha estado llevando a cabo procesos continuos de renovación y migración de su infraestructura tecnológica, con el objetivo de actualizar y fortalecer sus capacidades para enfrentar los desafíos del entorno digital. Este proceso se alinearán con las directrices del nuevo Plan Estratégico de Tecnologías de la Información (PETI), el cual guiará los esfuerzos y las iniciativas para optimizar, actualizar y corregir los diversos entornos tecnológicos que soportan las operaciones de la entidad. Es fundamental resaltar, como se muestra en el desarrollo del documento, los aspectos clave del estado actual de la infraestructura, los cuales incluyen los avances logrados hasta la fecha, así como los puntos críticos que requieren atención para asegurar la sostenibilidad, la eficiencia operativa y la seguridad de los sistemas a largo plazo.

De acuerdo con lo anterior, es necesario continuar con los procesos de modernización tecnológica, priorizando la actualización de hardware, la contratación de soporte especializado y la implementación de soluciones de contingencia que garanticen la alta disponibilidad y continuidad de los servicios críticos, conforme a los lineamientos del nuevo PETI.



Ana Milena Yela Escobar

Subsecretaria de Gestión Corporativa

Proyectó: José Luis Daza Pérez – Contratista Subsecretaría de Gestión Corporativa

Revisó: Claudia Patricia Ceballos García – Contratista Subdirección Administrativa