Nombre del informe
Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información

Área(s) Auditada(s) - Responsable(s)	Dirección de Tecnologías de la Información y Comunicaciones

1. Objetivo

Hacer seguimiento al diseño e implementación del Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de Planeación, de conformidad con lo establecido en la normatividad vigente a nivel distrital y nacional, el Modelo Integrado de Planeación y Gestión y el estándar internacional NTCG ISO 27001:2013

2. Alcance

El seguimiento al Modelo de Seguridad y Privacidad comprende el análisis desde el segundo semestre de 2021 al 30 de septiembre de 2022.

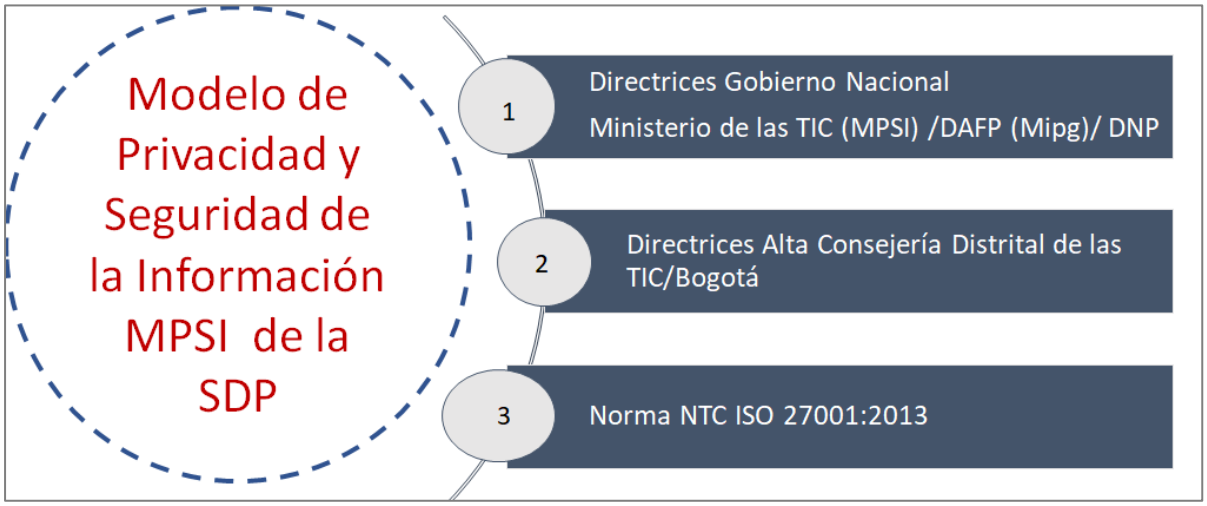
Para el desarrollo del seguimiento se utilizaron diferentes técnicas entre las cuales se encuentran:
1)Presentación por parte del líder del proceso y su equipo de trabajo.
2) Respuestas a los cuestionarios por parte de la Dirección de Tecnologías de la Información y las Comunicaciones.
3)Verificación y análisis de documentos y/o registros físicos y virtuales, la consulta en el Sistema de Información de procesos automáticos -SIPA y en la página web de la entidad, en cual fueron verificadas las diferentes Políticas y procedimientos establecidos, así como el mapa de riesgos vigente.
4)Entrevistas
5)Observación directa en reuniones y recorridos presenciales.
6) Revisión de planes de trabajo del MPSI, informes con destino a la Revisión por la Dirección y Revisión de Actas del Comité Institucional de Gestión y Desempeño

3. Criterios

- Decreto 1413 de 2017 (Título 17, parte 2, libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015 - Reglamenta la prestación de los Servicios Ciudadanos Digitales.
- Directiva presidencial 02 de 2019 - Simplificación de la interacción digital entre los ciudadanos y el Estado
- Resolución No. 500 de marzo 10 de 2021, y Anexo “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, del MinTIC
- Resolución 746 de 2022 “Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021” del MinTIC.
- Circular 036 de 2017. Alta Consejería Distrital de TIC de la Alcaldía Mayor de Bogotá.
- Modelo Integrado de Planeación y Gestión-MIPG. Marzo de 2021 -Versión 4
- Documentos del Modelo de seguridad y privacidad de la información de la Secretaría Distrital de Planeación, que se encuentran publicados en el Sistema de Información de Procesos Automáticos-SIPA.
- Planes de Mejoramiento asociados a los temas del MPSI de la SDP

4. Resultados del informe

La Oficina de Control Interno pudo evidenciar que la Dirección de Tecnologías de Información y las Comunicaciones de la Secretaría Distrital de Planeación, ha venido realizando múltiples esfuerzos para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, basado en el Modelo de Seguridad y Privacidad de la Información, bajo las directrices del Gobierno Nacional a través del Ministerio de las TIC, las Políticas Distritales recibidas de la Alta Consejería Distrital de TIC y también bajo los requisitos de la Norma NTC ISO 27001:2013.



Fuente: Elaboración propia

4.1 Políticas y Directrices Gobierno Nacional

De acuerdo con el Modelo Integrado de Planeación y Gestión, la **Política de Gobierno Digital** busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital; contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial).

La política de Gobierno Digital cuenta con cinco grandes propósitos que se pretenden alcanzar a través del uso y aprovechamiento de las TIC, por parte del Estado y de los actores de la Sociedad que se relacionan con este:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
- Tomar decisiones basadas en datos, a partir del aumento del uso y aprovechamiento de la información.
- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
- Impulsar el desarrollo de territorios y ciudades inteligentes, para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

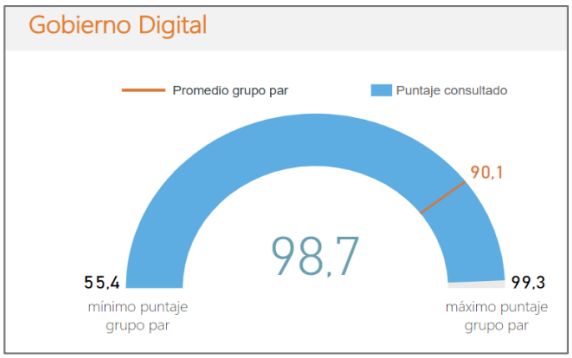
Así mismo, el CONPES 3920 incorpora en la Política de Gobierno Digital uno de los componentes esenciales para asegurar la transformación digital del Estado denominado como el Modelo de implementación de Explotación de Datos que permite que las entidades evalúen sus capacidades organizacionales y en recurso humano, tecnológico y financiero para la explotación de datos.

En concordancia con lo anterior, el Modelo Integrado de Planeación y Gestión describe que, entre los **Habilitadores Transversales del Gobierno Digital, se encuentra el de la Seguridad de la Información**, el cual busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del **Modelo de Seguridad y Privacidad de la Información**, que orienta la gestión e implementación de la seguridad de la información en el Estado.

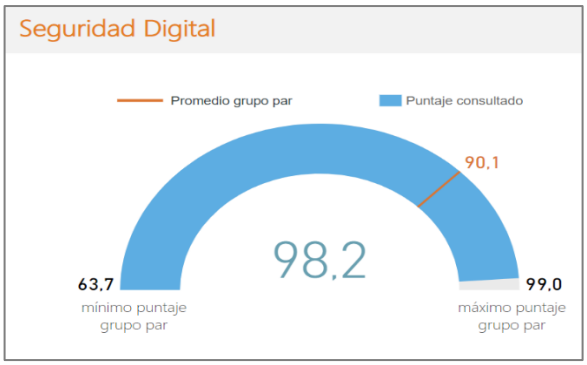
En cuanto a la Política de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades. La finalidad de esta Política consiste en fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

Resultados Formulario único de Reportes y Avances de - FURAG: De acuerdo con los resultados del FURAG 2021, se observa que las dos políticas de Gobierno Digital y de Seguridad Digital de la Secretaría Distrital de Planeación, obtuvieron puntajes altos en relación con entidades pares y con el promedio del Distrito Capital:

Política de Gobierno Digital



Política de Seguridad Digital



Fuente: DAFP-Resultados Medición Desempeño Institucional 2021/ https://app.powerbi.com/view?r=eyJrIjoiZTgwYTg4NGMtZGZhMy00YmE0LWI0ZWItN2FjYmUxMDQ1MWYyIiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9&pageName=ReportSection396d1cd03a850a004c59

Las principales recomendaciones del DAFP para la entidad, respecto a los resultados 2021 de las dos Políticas fueron las siguientes:

Recomendaciones Política de Gobierno Digital:

1. Utilizar técnicas de analítica de datos para predecir comportamientos o hechos de la entidad (analítica predictiva).
2. Diseñar y ejecutar un programa de desvinculación asistida por otras causales como actividad de la planeación del talento humano de la entidad.

3. Utilizar tecnologías emergentes de cuarta revolución industrial para mejorar la prestación de los servicios de la entidad, como tecnologías de desintermediación, DLT (Distributed Ledger Technology), cadena de bloques (Blockchain) o contratos inteligentes, entre otros.
4. Utilizar tecnologías emergentes de cuarta revolución industrial como el internet de las cosas (IoT) para mejorar la prestación de los servicios de la entidad.
5. Utilizar tecnologías emergentes de cuarta revolución industrial como la robótica para mejorar la prestación de los servicios de la entidad.
6. Utilizar tecnologías emergentes de cuarta revolución industrial como la automatización robótica de procesos para mejorar la prestación de los servicios de la entidad.
7. Mejorar los trámites en línea de la entidad teniendo en cuenta las necesidades de los usuarios, con el propósito de aumentar su nivel de satisfacción.
8. Disponer en línea todos los trámites de la entidad, que sean susceptibles de disponerse en línea.
9. Mejorar la solución de problemas a partir de la implementación de ejercicios de innovación abierta con la participación de los grupos de valor de la entidad.

Recomendaciones Política de seguridad Digital

1. Identificar los riesgos de seguridad y privacidad de la información de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, valorarlos y actualizarlos mediante un proceso de mejora continua.
2. Establecer objetivos específicos de seguridad de la información, aprobarlos mediante la alta dirección y medir su nivel de cumplimiento mediante los indicadores definidos para tal fin
3. Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.

4.2 Cumplimiento de las Directrices MinTIC y de la Alta Consejería Distrital de TIC

Como se mencionó anteriormente, el Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soporta el habilitador transversal de la Seguridad de la Información de la Secretaría Distrital de Planeación - SDP, que según el Manual de Gobierno Digital busca "que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos."

El Modelo de Seguridad y Privacidad de la Información - MSPI, contempla 6 niveles de madurez, de acuerdo con los instrumentos de medición del MinTIC, los cuales permiten identificar los niveles de evaluación aplicados a la seguridad de la información: Inexistente, Inicial, Repetible, Efectivo, Gestionado y Optimizado.

4.2.2 Servicios ciudadanos digitales.

La política de Gobierno Digital se implementa a través de dos líneas de acción que orientan su desarrollo: TIC para el Estado y TIC para la Sociedad; así como de tres habilitadores transversales, que son los elementos que proporcionan la base de la política: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

Los Servicios Ciudadanos Digitales buscan que los servicios ciudadanos digitales sean integrados a los procesos, servicios digitales, trámites digitales, sistemas de información y demás que lo requieran,

buscando racionalizar recursos, estandarizar y armonizar la administración pública en pro de mejorar los servicios del Estado.1

Sobre este tema se le solicitó a la Dirección de Tecnologías de la Información y Comunicaciones si se tienen identificados qué procesos, trámites y servicios de la entidad requieren interoperabilidad y si está documentada esta identificación.

La Dirección de Tecnologías de la Información y Comunicaciones respondió que la identificación de qué procesos, trámites y servicios de la entidad requieren interoperabilidad depende del proceso que presta el servicio y que la Dirección de TIC presta acompañamiento a lo requerido por los demás procesos en cuanto a soluciones con componente tecnológico. Así mismo esa Dirección remitió una relación de acciones encaminadas a apoyar la virtualización de servicios y trámites de la SDP entre las cuales se encuentran:

1. Se está trabajando en la primera fase para la implementación de soluciones de software para disponer a la ciudadanía servicios tecnológicos que les permitan realizar de manera virtual los trámites ante la SDP. De acuerdo con las prioridades en esta vigencia se está adelantando la fase precontractual para la Implementación de la solución de software para la virtualización de trámites de la SDP - **Estaciones Radioeléctricas .**

2. Servicios Ciudadanos Digitales:
(a) En proceso de implementación de una nueva versión del Web Service de Cámara de Comercio, la nueva versión incluye nuevas variables de acuerdo con el análisis realizado por la Dirección de Información y estadísticas hoy Dirección de Cartografía - El web Service permite el acceso a la información de registros mercantiles de las empresas y sociedades. A 09/11/2022 se finalizó la fase de construcción, se ejecutaron pruebas unitarias y se está adelantando la fase de pruebas funcionales por parte de la Cámara de Comercio.
(b) Revisión y ajustes a los servicios web de Curadurías Urbanas los cuales permiten la transferencia por parte de las Curadurías de la información de las licencias ejecutoriadas (mes vencido).
(c) Se está adelantando la fase precontractual para proveer los servicios comunicación de salida hacia los ciudadanos a través de medios virtuales, texto y voz para aumentar las interacciones de la SDP con la ciudadanía.

Esta Oficina considera que con ocasión de la expedición del Decreto 555 de 2021 y del rediseño institucional algunos trámites y servicios dejan de estar a cargo de la SDP, entre ellos el de estaciones Radioeléctricas, por lo que es importante evaluar la continuidad virtualización del tema en la SDP.

Compromiso de la Alta Dirección

La Alta Dirección de la Secretaría Distrital de Planeación ha demostrado su liderazgo con el sistema de gestión de seguridad de la información, asegurando el establecimiento de la Política y Objetivos de seguridad de la información. Es así como el Autodiagnóstico del MSPI con corte a 31 de diciembre de 2021, fue presentado por parte de la Dirección de Tecnologías de la Información y las Comunicaciones, conjuntamente con el Plan de Trabajo 2022 ante el Comité Institucional de Gestión y Desempeño para su aprobación.

El Plan de Seguridad y Privacidad de la Información 2022 **fue aprobado en enero de 2022** por el Comité Institucional de Gestión y Desempeño, Acta 01 de 2022, su objetivo consiste en definir las actividades para

[1] DAFP. Manual Operativo del Modelo Integrado de Planeación y Gestión. Consejo para la Gestión y Desempeño Institucional. Versión 4.Marzo de 2021

la implementación del Modelo de Seguridad y Privacidad de la información de la SDP, siguiendo la metodología de MINTIC; los principales cambios del plan respecto a la vigencia anterior fueron:

- Alineación con la nueva Plataforma Estratégica 2020-2024.
- Alineación con el Plan Operativo Anual 2022
- Aplicación del Decreto 500 de 2021, haciendo énfasis en el seguimiento y aplicación a los instrumentos creados para el funcionamiento del MSPI en la SDP.

Durante el seguimiento al Modelo de Seguridad y Privacidad de la Información de la SDP, por parte de la Oficina de Control Interno se pudo verificar que, desde la elaboración del Diagnóstico, así como del Plan de Trabajo, y la permanente actualización y mejora de los documentos e instrumentos que se desprenden del Modelo, han sido elaborados y actualizados **siguiendo las directrices del MINTIC** y de la ACDTIC. (**ver Anexo 1)**

De otra parte, la actualización del **Modelo de Seguridad y Privacidad de la Información** de la Secretaría Distrital de Planeación- **A-LE-373** fue aprobada por el Comité Institucional de Gestión y Desempeño-CIGD, en sesión del **11 de agosto de 2022**.

Este documento fue actualizado atendiendo las directrices de la Resolución No. 500 de marzo 10 de 2021, del MinTIC, “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

Se verificó que se encuentra establecida la Política General de Seguridad y Privacidad de la Información y que la misma atendió las recomendaciones de la “Guía - Elaboración de la política general de seguridad y privacidad de la información” generada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC – versión 2016

Roles y Responsabilidades

Se pudo evidenciar que existe un documento que define los “Roles y Responsabilidades de Seguridad de la Información”A-LE-009 requeridos para asegurar que el MSPI de la Secretaría Distrital de Planeación sea implementado, mantenido y mejorado continuamente en la entidad. En este documento se evidencia que existe un equipo conformado por 16 roles, conformados por representantes de las diferentes áreas como son:

Nº	Rol
1	Comité Institucional de Gestión y Desempeño de la SDP
2	Representante de la Alta Dirección
3	Líder de la Política de Seguridad Digital
4	Oficial de Seguridad y Privacidad de la Información
5	Líder de Seguridad Informática
6	Administrador de herramientas de colaboración
7	Líder de Seguridad Física y Gestión Documental
8	Líder Técnico del equipo de Desarrollo
9	Líder de Gestión Humana
10	Líder de Gestión Contractual
11	Asesor Legal
12	Dueño de la Información
13	Custodio de la Información
14	Usuario de la Información
15	Auditor-Control Interno
16	Líder y responsable del Control Disciplinario

Etapas Modelo de Seguridad y Privacidad de la Información

De acuerdo con las directrices del Ministerio de las Tecnologías de información y las Comunicaciones, establecidas en la Resolución 500 de 2021, las etapas para implementar el Modelo de Seguridad y Privacidad de la Información en las entidades públicas son las siguientes:

Ciclo del Modelo de Seguridad y Privacidad de la Información

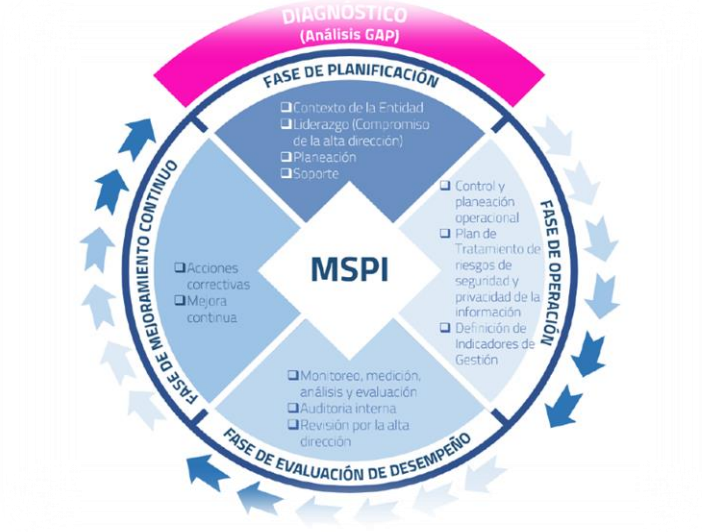


Figura 1. *Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información*
Fuente: *"Modelo de Seguridad y Privacidad de la Información"* - Anexo 1 de la Resolución 500 de 2021 de MinTIC

La Alta Consejería Distrital de TIC-ACDTIC sigue los lineamientos emitidos por Ministerio de las Tecnologías de la Información y las Comunicaciones -MINTIC y lidera y apoya la implementación del Modelo de Seguridad y Privacidad de la Información-MPSI de las entidades distritales a través de los instrumentos del MINTIC. Así mismo, el autodiagnóstico es utilizado por la ACDTIC para los informes del estado de implementación en las entidades distritales y adicionalmente se realizan sesiones de seguimiento virtuales desde el equipo de seguridad de esta Consejería.

Al revisar los documentos suministrados por el Director de Tecnologías de la Información y Comunicaciones, Ing. Dagoberto Rada, así como por parte de su equipo de trabajo, se pudo verificar que fueron desarrolladas las fases establecidas en el Modelo por el MINTIC y la ACDTIC, y que los principales documentos fueron aprobados por el Comité Institucional de Gestión y Desempeño-CIGD, de acuerdo con las siguientes consideraciones:

- **Fase de Diagnóstico:** En esta fase la SDP estableció el estado actual de la implementación de la seguridad y privacidad de la información de la entidad. Para tal fin la Dirección de Tecnologías de la Información y las Comunicaciones, utilizó el "instrumento de evaluación MSPI" con el fin de identificar de forma específica el estado de los controles implementados y faltantes. Esta fase se constituye en insumo para la fase de planificación.
- **Fase de Planificación:** Con base en los resultados del diagnóstico, se formuló el Plan de Seguridad y Privacidad de la Información.
- **Fase de Operación:** Comprende las actividades que permiten evidenciar la implementación de los controles para dar cumplimiento a los requisitos del MSPI. Los documentos que se generan de esta fase son: El Plan de implementación de controles de seguridad y privacidad de la información y la Evidencia de la implementación de los controles de seguridad y privacidad de la información.
- **Fase de Evaluación del Desempeño:** Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.
- **Fase de mejoramiento Continuo:** Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

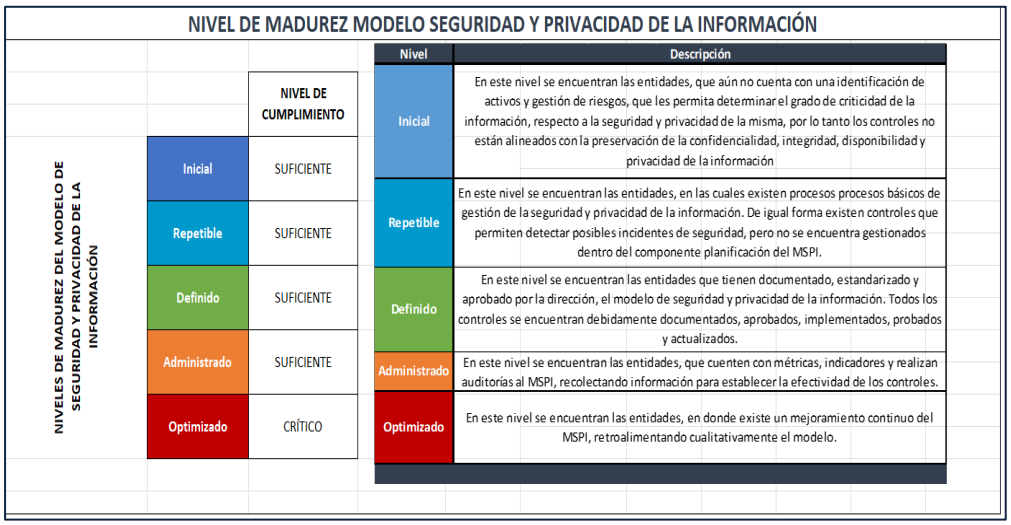
Se revisó el documento Autodiagnóstico 2021 del MPSI, realizado por la Dirección de Tecnologías de la Información y Comunicaciones de la Secretaría Distrital de Planeación con base en el instrumento del Ministerio de las TIC, encontrándose los siguientes porcentajes:

CUADRO AUTODIAGNÓSTICO 2021 DEL MPSI

COMPONENTE	ÍTEM	Nivel cumplimiento	%
PLANIFICACIÓN	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	100%	96%
	Políticas de seguridad y privacidad de la información	100%	
	Procedimientos de control documental del MSPI	100%	
	Roles y responsabilidades para seguridad de la información	100%	
	Inventario de Activos	100%	
	Identificación y valoración de riesgos	80%	
	Toma de conciencia, educación y formación en la seguridad de la información	100%	
IMPLEMENTACIÓN	Planificación y control operacional	100%	83.5%
	Implementación de controles	74%	
	Implementación del plan de tratamiento de riesgos	80%	
	Indicadores de gestión del MSPI	80%	
EVALUACIÓN DE DESEMPEÑO	Plan de seguimiento, evaluación y análisis del MSPI	100%	87%
	Auditoría Interna	80%	
	Evaluación del plan de tratamiento de riesgos	80%	
MEJORA CONTINUA	Plan de seguimiento, evaluación y análisis del MSPI	80%	80%
	Auditoría Interna	80%	
PROMEDIO			88%

Fuente: elaboración propia con base en el documento Autodiagnóstico 2021 elaborado por la Dirección de TIC de la SDP

Se observa que los ítems que obtuvieron autoevaluaciones con puntajes más bajos fueron los relacionados con la implementación de controles, la identificación y valoración de riesgos, la implementación del plan de tratamiento de riesgos e indicadores de gestión del MSPI, en las fases de planificación y de implementación:
De acuerdo con el autodiagnóstico realizado bajo la metodología del MinTIC, se tiene el nivel de madurez de la implementación del MSPI de la Secretaría Distrital de Planeación es "**Administrado**", que de acuerdo con la escala del MINTIC:



Fuente: Dirección de TIC-SDP. Autodiagnóstico2021_Diciembre_Final_Comite

4.3 Norma ISO 27001:2013

4.3.1 Declaración de Aplicabilidad y Políticas

Como se mencionó anteriormente, la Dirección de Tecnologías de la Información y las Comunicaciones-TIC, ha venido actualizando y fortalecimiento el Sistema de Gestión de Seguridad de la Información, así como el Modelo de Seguridad y Privacidad de la Información

Respecto a los documentos que soportan el Proceso y el Modelo de Seguridad y Privacidad de la Información de la entidad, a continuación, se presenta la relación de las Políticas, Guías, Instructivos y Procedimientos que contribuyen con el Modelo y sus fechas de actualización.

El Modelo de Seguridad y Privacidad de la Información de la SDP (A-LE-373), se encuentra alineado con la **Declaración de Aplicabilidad del Sistema de Gestión de Seguridad** de la Información-SGSI que incluye todos los controles del Anexo- A vinculado a la norma ISO/IEC 27001 versión 2013.

Para atender las directrices del Gobierno Nacional y Distrital, la SDP cuenta con el documento Políticas de Seguridad y Privacidad de la Información A-LE-429, a través del cual la SDP establece la intención de la alta dirección con el proceso responsable de la gestión y protección de la información, a fin de garantizar la integridad, la confidencialidad y la disponibilidad en los activos de información, conforme a la legislación vigente y a los estándares que le aplican. Las Políticas contenidas en este documento son:

Políticas de Protección de Datos Personales - A-LE-289: Dan a conocer las políticas de protección de datos personales establecidas en la SDP, con lo cual se preservan los derechos del titular de la información cuando suministra los datos a través de los diferentes canales habilitados para la respectiva captura.
Política para la Gestión de Copias de Respaldo y Recuperación de la Información Institucional - A-LE-297: Establece los lineamientos y directrices para la realización de las copias de respaldo de la información que está alojada en la infraestructura de la SDP, que permitan proteger la información de la entidad y restaurar de manera efectiva dicha información ante cualquier necesidad. Lo anterior permitirá mitigar el riesgo de pérdida de información ocasionada por eventos inesperados y no deseados.

Política de Control de acceso - A-LE-315: Para controlar el acceso a la información que gestiona la Entidad, estableciendo métodos para que sólo sea accesible a personal autorizado, siendo el responsable

y/o dueño de la información quien determine los privilegios para el acceso y las personas dependiendo del rol que les sea autorizado.

Política de Escritorio y Pantalla Limpios - A-LE-317: Con el fin de reducir los riesgos de acceso no autorizado, pérdida o daño de la información que reposa en los puestos de trabajo u oficinas o que es procesada en equipos de cómputo, durante y fuera del horario laboral de la SDP.

Política para el Uso de Dispositivos Móviles en la SDP - A-LE-321: establece las condiciones para el manejo de los dispositivos móviles institucionales o personales que acceden a información de la SDP y velar por el uso responsable de estos por parte de los usuarios.

Política de Desarrollo Seguro – A-LE-359: Define los parámetros y controles en materia de seguridad en los procesos de implementación, mantenimiento, adquisición y usos de aplicaciones/sistemas de información que adelante la Secretaría Distrital de Planeación, tanto a nivel interno como externo.

Política de Uso de Software de la SDP – A-LE-362: Establece los lineamientos mínimos necesarios, aplicables al interior de la entidad en el uso de software garantizando el cumplimiento del control de seguridad A.18.1.2 - Derechos de propiedad intelectual (DPI) y Directiva Presidencial 002 de 2002 -. Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de computador (software).

Política de Sensibilización y Comunicación en Seguridad de la Información en la SDP - A-LE-375: Establece e implementa estrategias de sensibilización, divulgación y concientización para la toma de conciencia apropiada de las políticas, procedimientos y demás instrumentos que hacen parte de la implementación del Modelo de Seguridad y Privacidad de la Información de la SDP, el cual se encuentra alineado a las disposiciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC y al Manual de Gobierno Digital, Implementación de Política de Gobierno Digital.

Política de Gestión de Carpetas Compartidas - A-LE-414:Documenta la gestión de las carpetas compartidas en la SDP a través de una política que permita una mejor administración de la información contenida en este tipo de recursos que la Dirección de Tecnologías de la Información y Comunicaciones pone a disposición de las áreas y usuarios internos de la Entidad.

Política de Seguridad Física y del Entorno - A-LE-452: Establece e implementa medidas efectivas en relación con el control de acceso físico a las áreas e infraestructura donde se custodia y administra información sensible de la Entidad.

Durante el desarrollo de este seguimiento, se pudo identificar que si bien en la Declaración de Aplicabilidad del SGSI se menciona que el Modelo de Seguridad y Privacidad de la información incluye todos los controles del Anexo- A vinculado a la norma ISO/IEC 27001 versión 2013, se identificó que se menciona que no se aplica el control «14.3.1Protección de datos de prueba dentro de la Política de seguridad de la información y en justificación». La Dirección de Tecnologías de la Información y las Comunicaciones, aclaró que la declaración de aplicabilidad se encuentra siendo ajustada en cumplimiento de la meta SG 4.4. del POA de la Dirección y que se trata de un error de forma, dado que no se tienen exclusiones de aplicabilidad de los controles para la entidad.

Para el caso del control 14.3.1. el cual establece que se deben proteger los datos de prueba que se estén utilizando, la Dirección de Tecnologías de la Información y Comunicaciones respondió que en la SDP se manejan tres ambientes a saber: de desarrollo, pruebas y producción y el ingreso a cada uno de ellos está dado por el procedimiento de control de acceso. A-PD-104 Gestión Cuentas de Usuario. En este marco sólo las personas autorizadas tienen permiso para acceder a los datos de cada uno de los ambientes de cada una de las aplicaciones. En este sentido a los datos utilizados en el ambiente de pruebas solo pueden acceder los servidores con privilegios previamente autorizados

Adicionalmente, durante el desarrollo de reuniones con la Dirección de Tecnologías de la Información y Comunicaciones de la SDP, se identificó que algunos documentos relacionados con el Modelo de Seguridad y Privacidad de la Información hacían referencia a normas que ya habían cambiado como, por ejemplo:

- En la **Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información - A-LE-334 ,** se menciona la Resolución 137 de 2018, "Por la cual se ajusta el Sistema Integrado de Gestión de la Secretaría Distrital de Planeación", actualmente se encuentra vigente la Resolución 998 de 2021.

- En el documento **Políticas de Seguridad y Privacidad de la Información- A-LE-429**, se menciona que se atienden las directrices del Artículo 20 "Directrices de Seguridad de los Datos y la Información" de la Resolución No. 305 de 2008 de la Comisión Distrital de Sistemas (CDS) . Pero este artículo fue derogado mediante el art. 18, Resolución Distrital 004 de 2017.

Sobre el particular la Dirección de Tecnologías de la Información y Comunicaciones presentó los ajustes en materia normativa que estaban trabajando para varios de los documentos.

Si bien es cierto la Declaración de aplicabilidad tiene fecha de actualización de Diciembre 23 de 2019, se pudo constatar por parte de los auditores de la Oficina de Control Interno, en reunión del 27 de octubre de 2022, que la misma se encuentra en proceso avanzado de actualización, al igual que los demás documentos que se relacionan con el MPSI**.(ver anexo1)**

La declaración de aplicabilidad de la SDP incluye el listado de todos los controles del Anexo-A de la ISO/IEC 27001 versión 2013 incluyendo sus 114 controles agrupados en 14 dominios y 35 objetivos de control y como se mencionó anteriormente **la SDP no tiene exclusiones respecto a la norma ISO 27001** relacionada con los controles implementados.

Dominios de la norma ISO 27001 y su naturaleza

Figura 2 Dominios de la norma ISO 27001 y su naturaleza
Fuente: DECLARACION DE APLICABILIDAD DEL SGSI EN LA SDP A-LE-334-SDP de diciembre 23 de 2019

4.3.2 Plan Operacional del Modelo de Privacidad y Seguridad de la Información y Recursos

Al revisar las actividades del Plan de Trabajo 2022, frente al audiagnóstico y al documento de efectividad de los controles se encontró:

- El Plan de trabajo 2022 del Modelo de Privacidad y Seguridad de la Información fue aprobado por el Comité Institucional de Gestión y Desempeño el **28 de enero de 2022**, mediante el Acta 01 de 2022. Como se mencionó anteriormente su objetivo consiste en definir las actividades para la implementación del Modelo de Seguridad y Privacidad de la información de la SDP.

- El Modelo de Seguridad y Privacidad de la Información se aprobó por el Comité Institucional de Gestión y Desempeño, el **11 de Agosto** de 2022.

4.3.2.1 Recursos Asociados al MPSI 2022 y 2023

De acuerdo con la información recibida de la Dirección de Tecnologías de la Información y Comunicaciones, se encontró que algunos temas asociados al MPSI se encuentran desfinanciados para la vigencia 2023:

Recursos asociados al MPSPI 2022-2023

OBJETO	2022	2023
Adquirir e implementar una herramienta de software para la realización de copias de seguridad de la información institucional de la entidad	$ 746.091.032	SIN
Realizar el monitoreo de la infraestructura tecnológica de la SDP	$ 183.000.000	$ 210.000.000
Renovación de garantías y soporte técnico de la solución integrada para la gestión de seguridad y protección de los sistemas de información y/o aplicaciones de la SDP	$ 218.250.000	$ 234.619.000
Realizar las actividades de la FASE I para la migración de servicios tecnológicos de la SDP a la nube y de la operacionalización del Plan de recuperación de desastres -DRP	$ 600.000.000	$ 458.000.000
Actualización del licenciamiento de la solución de antivirus de la SDP	$ 400.000.000	SIN
Renovar el servicio de certificados de firma digital para los servidores públicos de la SDP	SIN	$ 4.000.000
Adquirir el servicio para la gestión del programa de datos personales en la entidad	SIN	$ 26.954.000
Adquirir una herramienta para monitorear el rendimiento de la capa de aplicaciones de la infraestructura tecnológica de la SDP	SIN	$ 200.000.000
TOTAL	$ 2.147.341.032	$ 1.133.573.000

Fuente: Dirección de Tecnologías de la Información y las Comunicaciones de la SDP.2022

De acuerdo con la información recibida de la Dirección de Tecnologías de la Información y Comunicaciones de la SDP, se puede se puede observar la SDP para la vigencia 2023 no cuenta con recursos para la adquisición e implementación de herramientas de software para la realización de copias de seguridad de la información institucional, así como tampoco para la actualización del licenciamiento de la solución del antivirus.

De otra parte, se observa disminución de recursos significativos para realizar las actividades de la FASE I para la migración de servicios tecnológicos de la entidad a la nube y la operacionalización del Plan de Recuperación de Desastres.

4.3.3 Autoevaluación de la Efectividad de los controles

Tabla de Escala de Valoración de Controles Norma ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

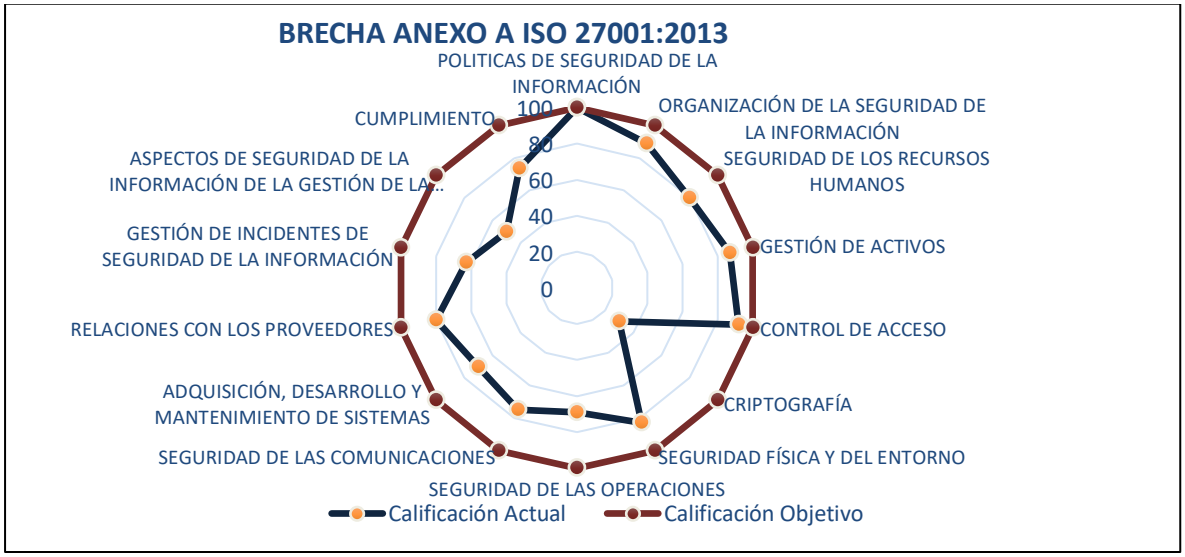
Fuente: Norma ISO 27001:2013 ANEXO A

De acuerdo con el autodiagnóstico realizado por la Dirección de Tecnologías de la Información y las Comunicaciones, siguiendo la metodología del MINTIC y la Norma ISO 27001:2013, se evaluaron los controles obteniendo la siguiente calificación de los controles:

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	89	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	87	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	92	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	30	100	**REPETIBLE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	83	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	69	100	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	75	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	70	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	**EFECTIVO**
A.18	CUMPLIMIENTO	73,5	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**74**	**100**	**GESTIONADO**

Fuente: Dirección de TIC-SDP. Autodiagnóstico2021_Diciembre_Final_Comite



Fuente: Dirección de TIC-SDP. Autodiagnóstico2021_Diciembre_Final_Comite

Como se puede observar las calificaciones más bajas se encuentran asociadas a los siguientes controles:

No	Control	Puntaje
A.10	CRIPTOGRAFÍA	30
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63
A.12	SEGURIDAD DE LAS OPERACIONES	69
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	70

Frente al Plan de trabajo 2022 del MSPI se indagó con el equipo de la Dirección de Tecnologías de la Información y Comunicaciones, cuáles fueron las acciones encaminadas a mejorar los resultados del autodiagnóstico y contribuir con el cierre de Brechas Nivel de Madurez por Dominios y controles en los temas de criptografía, seguridad de las comunicaciones, seguridad de las operaciones, gestión de continuidad del negocio y gestión de incidentes de seguridad de la información

Sobre el particular la Dirección de Tecnologías de la Información y Comunicaciones mencionó que desde la vigencia 2021 tomó la decisión de verificar el estado de la gran cantidad de instrumentos que se tenían elaborados en el marco de la implementación del MPSI, con el objetivo de mejorar lo ya implementado llegando a calificarlos como optimizados luego de realizar de forma aplicada el mejoramiento continuo.

Por lo anterior, la Dirección de Tecnologías de la Información y Comunicaciones aclara que el plan no se realizó teniendo en cuenta los controles con menor ejecución, aspecto que no fue el objetivo inicial y que el plan 2022 no está enfocado únicamente en subir el porcentaje de los dominios de control que tienen baja

calificación sino en optimizar los dominios ya implementados luego del seguimiento interno realizado a los mismos en la vigencia anterior.

Sin embargo, frente a cada uno de los controles seleccionados y preguntados por la Oficina de Control Interno, la Dirección de Tecnologías de la Información y Comunicaciones mencionó:

- ✓ La SDP cuenta con una política de criptografía encaminada a la gestión de certificados digitales A-LE-477 el cual fue aprobado con acta de mejoramiento 251 de Octubre de 2022.

- ✓ Seguridad de las comunicaciones y operaciones: Se optimizaron los instrumentos que se tienen definidos: se ajustó el documento dejándolo como «Política para el Aseguramiento de la Información y Servicios en la Red A-LE-481», en su Versión 2 Acta de Mejoramiento 242 de septiembre 30 de 2022 Proceso A-CA-007.

- ✓ Se revisaron los siguientes documentos y se decidió no hacerles modificaciones teniendo en cuenta que se ajustan a lo realizado actualmente:

  - A-PD-203 Transferencia de Información, Versión 1 acta de mejoramiento 340 de diciembre 31 de 2020
  - A-LE-453 Guía de Transferencia de Información, Versión 1 acta de mejoramiento 344 de diciembre 30 de 2019
  - Se encuentra en proceso de revisión el documento A-LE-452 Política de Seguridad Física y del Entorno

- ✓ En el tema de continuidad del negocio, la Dirección de Tecnologías de la Información y Comunicaciones menciona que es un proceso que debe ser liderado de forma estratégica, sin embargo, desde esta Dirección, bajo el tema de seguridad se está liderando la implementación del Plan de Recuperación de Desastres - DRP en la nube de Oracle, para tal fin fue radicado el proceso contractual 914.

- ✓ Gestión de Incidentes de seguridad: fue actualizado el procedimiento A-PD-187 GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA SDP Versión 5 acta de mejoramiento 282 de octubre 28 de 2022, el cual se encontraba como una acción para la vigencia 2022,

4.3.4 Riesgos de seguridad y privacidad de la información y controles

La Dirección de Tecnologías de la Información y Comunicaciones en las diferentes reuniones realizadas con ocasión de este seguimiento al MPSI, informó que **no se había detectado la materialización de ningún riesgo** del proceso y que, adicionalmente se estaba desarrollando conjuntamente con la Dirección de Planeación la definición de los riesgos de seguridad de la información con los 15 procesos de la entidad, para lo cual se habían venido realizando una serie de sesiones de capacitación y talleres con cada uno de ellos.

4.3.4.1 Plan para la Gestión de Vulnerabilidades.

Se encontró por parte de la Oficina de Control interno que la Dirección de Tecnologías de la Información y Comunicaciones había formulado un plan de mejoramiento asociado al Mapa de Riesgos del Proceso, Riesgo “Indisponibilidad no programada de servicios de TI”. Situación de mejora 1986 y la Acción 2781 consistente en Realizar las acciones que se establezcan en el plan de trabajo 2021 para mitigar las vulnerabilidades definidas, sobre la infraestructura tecnológica de la SDP (Da continuidad a la acción 2607). Tiene origen en una acción del 2019, “Realizar las acciones que se definan en el plan de trabajo **para remediar las vulnerabilidades detectadas en el diagnóstico realizado a la infraestructura tecnológica en el 2019**”. (subrayado nuestro).

Como causas se habían identificado 3-2020-02053:
- Falta de herramientas de monitoreo
- Deficiente verificación de las copias de respaldo realizadas sobre la plataforma tecnológica para asegurar la restauración de la información.
- Falta de gestión de logs de los servidores de aplicaciones , bases de datos y sistemas operativos.
- Obsolescencia tecnológica en parte critica de la infraestructura (servidores, Switches y software).
- Insuficiente tratamiento de vulnerabilidades detectadas

La acción **fue inactivada**, ampliándose el plazo de la acción 2781 a 31/12/2021, recogiendo en el informe de avance y soportes los resultados consolidados de las vigencias anteriores.

Se evidencia en la Matriz Todo extraída del Sistema de Información de procesos Automáticos-SIPA, que en la descripción del avance del plan de mejoramiento se menciona que la **intervención de las vulnerabilidades se abordaría para la vigencia 2022** a través de los planes de acción formulados para el seguimiento de los controles de seguridad de la información.

Adicionalmente, la Dirección de Tecnologías de la Información y Comunicaciones, consideró en su momento que no era apropiado seguir realizando las tareas de remediación de vulnerabilidades en el marco de un plan de un mejoramiento que fue propuesto inicialmente por el proceso, como acción de mitigación para el riesgo de indisponibilidad de la plataforma tecnológica de la SDP. La mitigación de vulnerabilidades es una tarea operacional del proceso, que se enmarca en el dominio de control de seguridad en las operaciones, objetivo del control A.12.6 gestión de la vulnerabilidad técnica.

Durante el desarrollo de este seguimiento, se solicitó por parte de la Oficina de Control Interno:

"Respecto al riesgo de Indisponibilidad no programada de servicios de TI de la SDP, en el documento «Avances y Logros a diciembre 31 de 2021, del Modelo de Seguridad y Privacidad de la Información de la SDP», como entrada de Revisión por la Dirección- marzo de 2022, se menciona que el proceso viene realizando mitigación de vulnerabilidades en el marco de 6 estrategias definidas para tal fin y donde adicionalmente se realizó la adquisición de una herramienta para la generación de escaneos de vulnerabilidades la cual quedó plenamente configurada en la vigencia 2022, por favor describir 1)Las seis estrategias desarrolladas 2) el nombre de la herramienta adquirida, adjuntar contrato 3)Si la herramienta ya se encuentra en uso y los resultados alcanzados"

Sobre el particular se recibió la siguiente respuesta de la Dirección de Tecnologías de la Información y Comunicaciones:

"En el tema de vulnerabilidades, en la vigencia 2021 la Dirección de TIC trabajó un plan que finalizó en Febrero de 2022, las 6 estrategias desarrolladas fueron:

Estrategia 1: Remediación vulnerabilidades servidores SO Windows
Estrategia 2: Remediación vulnerabilidades servidores SO Linux.
Estrategia 3: Remediación vulnerabilidades a nivel de aplicaciones y bases de datos.
Estrategia 4: Remediación vulnerabilidades a nivel de conectividad.
Estrategia 5: Remediación vulnerabilidades equipos de escritorio. Actualización SO.
Estrategia 6: Definición estrategias adicionales (adquisición y renovación de elementos de seguridad que permitan la mitigación de vulnerabilidades.

Para la vigencia 2022 se está trabajando desde el control seguridad de la información bajo el proyecto No. 2 de Infraestructura denominado Gestión de Vulnerabilidades el cual se encuentra ejecutado en un 78% con corte a 30 de septiembre.

La herramienta adquirida por la SDP se llama Tenable. En la vigencia 2022, se ha realizado la implementación y administración de la herramienta de vulnerabilidades adquirida en la vigencia 2021, con el Contrato 560 de 2021, dentro de las actividades realizadas se encuentra:

a) La implementación dentro de la infraestructura de la SDP de la herramienta de Tenable adquirida para el escaneo de vulnerabilidades,
b) Realización del primer escaneo de vulnerabilidades.

c) Generación de un Plan de Acción para gestionar las vulnerabilidades detectadas, que permita mitigar el top 13 de servidores más vulnerables, según el informe presentado en el escaneo."

Es importante mencionar que dentro del documento "Estrategias de Remediación de Vulnerabilidades detectadas en la Infraestructura Tecnológica de la SDP 2021", Seguimiento a 31 de diciembre de 2021, enviado por la Dirección de Tecnologías de la Información y Comunicaciones a esta Oficina, se identificó lo siguiente en relación con las 6 estrategias mencionadas anteriormente:

No Estrategia	ESTRATEGIA	ALCANCE	OBSERVACIONES
1.	Mitigación de vulnerabilidades de los servidores que tienen Sistema Operativo Windows	Enfocada a dar continuidad a la mitigación de vulnerabilidades de los servidores que tienen Sistema Operativo Windows; se planteó intervenir 7 servidores en ambiente de producción, así como definir tareas rutinarias para realizarlas con una periodicidad establecida	De conformidad con el alcance planteado para los 7 servidores en producción, de las **475 vulnerabilidades** se mitigarán al cierre de la Estrategia 1, un total de **71 vulnerabilidades a 31 de diciembre de 2021**
2.	Mitigación relacionada con servidores con Sistema Operativo Linux	Estrategia orientada a la mitigación relacionada con servidores con Sistema Operativo Linux, consistió en intervenir 27 servidores, alcance dentro del cual se realizó un proceso de validación para aplicar filtros y establecer los priorizados a intervenir sin sufrir alteraciones en la operación	De conformidad con el alcance planteado para los 27 servidores en producción, de las **475 vulnerabilidades** se mitigarán al cierre de la Estrategia 2, un total de **69 vulnerabilidades.** Del total de servidores con sistema operativo Linux, se cuenta con 102 servidores en los tres ambientes, de los cuales 64 fueron intervenidos a 31/12/2021

<table>
<tr><th>No Estrategia</th><th>ESTRATEGIA</th><th>ALCANCE</th><th>OBSERVACIONES</th></tr>
<tr><td>3.</td><td>Estrategia orientada a las vulnerabilidades de los servicios de aplicación y BD Oracle más críticas</td><td>El alcance estuvo dirigido a aplicar el último parche a los servidores de aplicaciones y BD, migración de servicios y pruebas funcionales del equipo de desarrollo, pruebas necesarias al incluir componentes que afectan servicios de aplicación, las pruebas con usuarios funcionales permiten validar que los cambios no hayan generados afectación en las capas de aplicación.

Resumen Aplicaciones Remediadas
<table><tr><th>Servidor de Aplicaciones</th><th>Aplicaciones/Sistemas de Información</th></tr><tr><td>Servidor de aplicaciones nginx con PHP 7</td><td>Portal Inventario Bogotá y Portal Regalías</td></tr><tr><td>Servidor de aplicaciones Web Logic</td><td>Gestor documental UCM</td></tr><tr><td>Servidor de aplicaciones Internet Information Server</td><td>SISBEN DNP</td></tr><tr><td>Servidor de aplicaciones Oracle Glassfish 4.2</td><td>SIAR Cargue curadurías, Web services Nomina SISE, Tablero de Mando.</td></tr></table></td><td>De conformidad con el alcance planteado para los servidores de aplicación y bases de datos en producción, de las 475 vulnerabilidades se mitigarán al cierre de la Estrategia 3, un total de 32 vulnerabilidades.

En el proceso de remediación algunas aplicaciones presentaron novedades técnicas y/o administrativas que no permitieron llevar a cabo las actividades de aseguramiento en los tiempos programados, es decir, que algunas aplicaciones no pudieron ser Remediadas en los tiempos establecidos:

Documanager, Sisbén - consulta WEB, Formación SDP - Moodle, Media WIKI y Metadatos, Página Web, Página Inventario Bogotá, SINUPOT, Sistema de Familias, Gestión de Usuarios, Intranet, Sisbén, SegPlan, SICapital, Planoteca, Plusvalía, Web Services, Sistema de requerimientos, SIAR.</td></tr>
<tr><td>4.</td><td>Estrategia enfocada en atacar las vulnerabilidades de servicios de conectividad dando continuidad a la implementación del certificado seguro</td><td>5 sistemas de información:
1. SIPA
2. SISBEN
3. Portal Web
4. Bogotá Solidaria
5. Inventario Bogotá
Dentro del alcance estaba intervenir componentes como el balanceador de cargas que participa dentro de toda la arquitectura dispuesta para proveer dichos servicios, implementar el certificado como buena práctica y también para mitigar posibles efectos validando que la aplicación de la remediación funciona sin posibles efectos, se empieza en ambiente de desarrollo, pruebas y finalmente en producción.</td><td>Herramientas de seguridad aplicadas en la estrategia
-FIREWALL: Este elemento protege de accesos no autorizados; igualmente se tiene habilitado las firmas de protección de IPS (Dentro de las cuales se gestiona firmas de protección contra ataques (sql injection, Xss, exploits); así mismo, se maneja la protección de web filtering y control de aplicaciones. La protección del firewall perimetral va dirigida a puertos a nivel de TCP.

WAF: Firewall de aplicaciones que se constituye en un elemento que protege contra ataques sobre las páginas web (http y https); dicha protección es contra ataques conocidos como:

Cross-Site Scripting (XSS), SQL Injection, Remote File Inclusion.
Local File Inclusion, OS Commands, Troyanos y virus.
Exploits, Información Sensible del servidor.
Firmas personalizadas, entre otros.</td></tr>
<tr><td>5.</td><td>Estrategia orientada a los temas de equipos de escritorio</td><td>Mitigar los riesgos de seguridad por obsolescencia, variedad de equipos y posibles fallas por la actualización de parches para los SO operativos Windows 10 de los equipos de escritorio, instalar los parches de seguridad, actualizar cada equipo en SO si eso es viable

Se realizó la actividad de actualización del sistema operativo Windows 10 Pro a la versión 1909, de acuerdo con el cronograma de actividades detallado. A la fecha se actualizó el</td><td>Se presentaron algunas dificultades con equipos que no respondieron al momento de la ejecución del proceso, por motivos asociados a que se encontraban apagados o por falta de espacio de almacenamiento en disco, igualmente porque el sistema alertaba sobre software que debía ser revisado o por falla en algún sector del disco, situación que en su momento, no permitía llevar completar la actividad;</td></tr>
</table>

No Estrategia	ESTRATEGIA	ALCANCE	OBSERVACIONES
		100% del total de equipos programados (417), interviniendo las siguientes dependencias (28): 1. Oficina del Despacho 2. Dirección de Sistemas 3. Planes Parciales 4. Taller del Espacio Público 5. Norma Urbana 6. Patrimonio y Renovación Urbana 7. Vías, Transporte y Servicios Públicos 8. Planes maestros y complementarios 9. Subsecretaría de Planeación Territorial 10. Confis 11. Subsecretaría Jurídica 12. Defensa Judicial 13. Análisis y Conceptos Jurídicos 14. Gestión Contractual 15. Gestión Financiera 16. Gestión Humana 17. Programación y Seguimiento a la Inversión 18. Planes de Desarrollo y Fortalecimiento Local 19. Subsecretaría de Planeación de la Inversión 20. Participación y Comunicación para la Planeación 21. Trámites Administrativos 22. Oficina Asesora de Prensa y Comunicaciones 23. Estratificación 24. Recursos Físicos y Gestión Documental 25. Servicio al Ciudadano 26. Legalización y Mejoramiento Integral de Barrios 27. Información Cartografía y Estadística 28. Subsecretaria de Gestión Corporativa	sin embargo, este tipo de inconsistencias se solucionaron y finalmente se reprocesaron hasta conseguir los resultados de la actualización a la versión 1909 de Windows 10 Prof. para la totalidad de equipos objetivo.
6.	Estrategia compuesta por tres procesos: 1)Renovación de Garantías y Soporte Técnico de la Solución Integrada para la Gestión de Seguridad y Protección de los Sistemas de Información y/o Aplicaciones de la SDP. 2)Adquirir e Implementar una Solución Integrada para la Gestión de Vulnerabilidades en la Infraestructura Tecnológica de la SDP.	Los elementos cubiertos son: 1)**Mantener la protección contra ataques** sobre **las páginas web (http y https**); dicha protección es contra ataques conocidos como: • Cross-Site Scripting (XSS), • SQL Injection, • Remote File Inclusion, • Local File Inclusion, • OS Commands, • Troyanos y virus, • Exploits, • Información Sensible del servidor, • Firmas personalizadas entre otros. 2) Permitirá a la SDP la gestión de vulnerabilidades en la infraestructura tecnológica de la SDP, a partir de la **detección y parametrización centralizada de las vulnerabilidades** que puedan presentarse en la infraestructura tecnológica de la SDP; obteniendo así una visión general continua de las vulnerabilidades, su entorno de TI y los riesgos asociados con ellas	

No Estrategia	ESTRATEGIA	ALCANCE	OBSERVACIONES
	3)Ampliar la Capacidad de Gestión de Copias de Seguridad de la Librería LTO-8.	3) Para potenciar y fortalecer la librería HPE MSL4048- Drive Tape Library que **soporta la gestión de las copias de respaldo desde su programación hasta la restauración y disposición de la información**; con el fin de ofrecer mayor oportunidad en los respaldos de información, tanto programados como por demanda, se considera necesario robustecer dicha librería con dos drives adicionales y otros elementos necesarios para que dichos drives operen, justificado principalmente en el crecimiento en términos de volumen de información institucional y cantidad de servicios a respaldar.	
	4) Renovación de Garantías y Soporte Técnico para los Equipos de Seguridad Perimetral Firewall.	4)Permite garantizar la protección de accesos no autorizados; igualmente se tiene habilitado las firmas de protección de IPS (Dentro de las cuales se gestiona firmas de protección contra ataques (sql injection, Xss, exploits); igualmente se maneja la protección de web filtering y control de aplicaciones. La protección del firewall perimetral. Esta protección va dirigida a puertos a nivel de TCP	

Fuente: Elaboración propia a partir del documento Estrategias de Remediación de Vulnerabilidades detectadas en la Infraestructura Tecnológica de la SDP 2021 de la Dirección de TIC de la SDP.

Se puede observar que:

- En la vigencia 2021 no fueran resueltas la totalidad de vulnerabilidades (475) identificadas en la vigencia anterior.
- Algunas aplicaciones no pudieron ser Remediadas en los tiempos establecidos.
- Se presentaron algunas dificultades por obsolescencia, con equipos de escritorio que no respondieron al momento de la ejecución del proceso, por motivos asociados a que se encontraban apagados o por falta de espacio de almacenamiento en disco, igualmente porque el sistema alertaba sobre software que debía ser revisado o por falla en algún sector del disco

De otra parte, la Oficina de Control Interno recibió dentro de los soportes y respuestas solicitados un **Plan de acción 2022 de "Gestión de Vulnerabilidades**", con el cual se busca responder a uno de los requisitos de Implementación de la Política de Gobierno Digital, según el Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2), como parte del cumplimiento del Anexo 2 - Segmentación Elementos Habilitadores: Arquitectura - Dominio de Servicios Tecnológicos.

Se pudo evidenciar por parte de la Oficina de Control Interno que de las 18 actividades formuladas para la vigencia 2022, siete actividades (el 33% del Plan), quedaron pospuestas para ser programadas en la vigencia 2023, como se muestra a continuación:

Plan de acción 2022 de "Gestión de Vulnerabilidades"

Plan de Trabajo						Seguimiento
Actividad	Ejecutor - Responsable	Fecha Inicio	Fecha Final	Peso Porcentual Programado	Peso Porcentual Ejecutado	Observaciones
1. Implementación herramienta Tenable para escaneo de vulnerabilidades	Ing. Ángel María Pérez Proveedor PC Micros	3/1/2022	10/2/2022	6%	6%	Se implementó la herramienta de Tenable, adquirida por la SDP para el escaneo de vulnerabilidades

Plan de Trabajo						Seguimiento
Actividad	Ejecutor - Responsable	Fecha Inicio	Fecha Final	Peso Porcentual Programado	Peso Porcentual Ejecutado	Observaciones
2. Primer escaneo de vulnerabilidades a nivel de host	Ing. Ángel María Pérez Proveedor PC Micros	9/2/2022	10/2/2022	2%	2%	Se realizó el primer escaneo de vulnerabilidades. Ver Carpeta *PrimerEscaneo*
3. Identificación de Servidores a intervenir	Equipo Infraestructura	7/3/2022	7/3/2022	2%	2%	A partir del informe del primer escaneo, se toma la decisión de realizar actividades de mitigación sobre el top 13 de servidores que presenten mayor cantidad de vulnerabilidades. Ver Archivo *Top13_Vulnerabilidades.xls* - Finalmente la lista es de 14 servidores por cuanto dos servidores presentan el mismo número de vulnerabilidades.
4. Generación Plan de Acción Top 13 de servidores vulnerables - Propuesto	Equipo Infraestructura	7/3/2022	31/3/2022	6%	6%	Se genera una propuesta general a ser presentada ante el equipo de infraestructura. *PlanDetalladoTop13_Propuesta.xls*
5. Aseguramiento Servidores Linux Nuevos y en operación	Winston Ropero	1/3/2022	15/12/2022	10%	10%	01/08/2022: Se crearon 37 máquinas linux y 5 máquina Windows en la infraestructura de hiperconvergencia, configurando las acciones de aseguramiento sobre cada uno. De igual forma se han asegurado 87 máquinas Linux de infraestructura ya existente. *Ver DetalleActividad5_AseguramientoLinux.xls* 01/09/2022: Se crearon 41 máquinas linux y 5 máquina Windows en la infraestructura de hiperconvergencia, configurando las acciones de aseguramiento sobre cada uno. De igual forma se han asegurado 92 máquinas Linux de infraestructura ya existente.
6. Presentación del plan y estrategia de mitigación DS	Equipo DS	4/4/2022	4/4/2022	2%	2%	Se realizó la reunión de presentación del plan al grupo de la Dirección en la fecha programada y el mismo fue aprobado por los participantes.
7. Validación de los tiempos por parte de los participantes en las acciones de Mitigación	Equipo Software	5/4/2022	21/4/2022	1%	1%	En reunión del 21/04/2022 se confirmaron fechas generales con la Ing. María Teresa.
8. Generación Plan de Acción Top 13 de servidores - Definitivo	Equipo Infraestructura	22/4/2022	22/4/2022	1%	1%	Se conforma el Plan Definitivo con fecha del 21/04/2022 Ver archivo 20220516_Plan_Vulnerabilidades.xls
9. Ejecución Plan de Acción Top 13 de servidores - Definitivo	Equipo Infraestructura	11/4/2022	18/11/2022	55%	48%	En resumen, se aseguraron 6 servidores del ambiente de producción y sus correspondientes en pruebas y desarrollo. \\sdpatlas08\Dir_sistemas\GrupoInfraestructura\12_Proyectos\2022\Proyecto2_GestionVulnerabilidades\Seguimiento Ver 20220801_PlanDetalladoTop13_Aprobado_Seguimiento.xls 20220928_PlanDetalladoTop13_Aprobado_Seguimiento.xls Se reprograma esta actividad y todas las siguientes, de acuerdo con el avance del seguimiento al Top13.
10. Segundo escaneo de vulnerabilidades a nivel de host	Ing. Ángel María Pérez Ing. Sandra Palacios	21/11/2022	22/11/2022	5%	0%	Se reprograma actividad, a partir de la fecha de finalización de remediación Top 13
11. Generación informe resultados	Ing. Ángel María Pérez Ing. Sandra Palacios	23/11/2022	15/12/2022	10%	0%	Se reprograma actividad, a partir de la fecha de finalización de remediación Top 13
12. Identificación de Servidores a extender la estrategia de mitigación	Equipo Infraestructura	16/11/2022	15/12/2022	0%	0%	Se reprograma actividad, a partir de la fecha de finalización de remediación Top 13. Se toma decisión de eliminar la segunda fase de migración programada para el segundo semestre del 2022 dado que la complejidad del Top 13 requirió reprogramación y corrimiento de actividades; por lo anterior se eliminan actividades 12 a 18 y se reasignan los pesos porcentuales.
13. Generación Plan de Acción Segundo Grupo de Servidores - Propuesto	Equipo Infraestructura	12/9/2022	23/9/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.

Plan de Trabajo						Seguimiento
Actividad	Ejecutor - Responsable	Fecha Inicio	Fecha Final	Peso Porcentual Programado	Peso Porcentual Ejecutado	Observaciones
14. Presentación del plan y estrategia de mitigación DS	Equipo DS	26/9/2022	26/9/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.
15. Generación Plan de Acción Segundo Grupo de Servidores - Definitivo	Equipo Infraestructura	27/9/2022	28/9/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.
16. Ejecución Plan de Acción Segundo Grupo de Servidores - Definitivo	Equipo Infraestructura	29/9/2022	30/11/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.
17. Tercer escaneo de vulnerabilidades a nivel de host	Ing. Ángel María Pérez Ing. Sandra Palacios	1/12/2022	1/12/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.
18. Generación informe resultados	Ing. Ángel María Pérez Ing. Sandra Palacios	5/12/2022	15/12/2022	0%	0%	Se elimina actividad; determinando que la segunda etapa de remediación se deberá realizar la siguiente vigencia.
TOTALES				**100%**	**78%**	

Fuente: Dirección de TIC-SDP. Plan de acción 2022 de “Gestión de Vulnerabilidades”

El MinTIC en el tema de Arquitectura, establece como lineamiento que "La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información."

Finalmente, teniendo en cuenta la guía metodológica de pruebas de efectividad de MinTIC, frente a los requerimientos para implementación de la norma ISO 27000, Objetivo de Control A.12.6 - Gestión de la vulnerabilidad técnica, la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC, la Secretaría Distrital de Planeación requiere gestionar las vulnerabilidades **de manera continua** sobre la infraestructura tecnológica y los sistemas de información expuestos en internet que le permita mitigar y/o cerrar brechas de seguridad que sean detectados en la fase de análisis de vulnerabilidades.

4.3.4.2 Incidentes de seguridad de la información en GLPI

De otra parte, esta Oficina revisó el documento word «Avances y Logros a diciembre 31 de 2021 Modelo de Seguridad y Privacidad de la Información de la SDP», presentado por la Dirección de Tecnologías de la Información y Comunicaciones como insumo para el Comité Institucional de Gestión y Desempeño en el mes de marzo de 2022, en el capítulo «1.3 Cumplimiento Indicadores De Gestión MSPI 2021».

En este documento se presentó el indicador «**Porcentaje de atención de incidencias de seguridad realizadas por los usuarios de la SDP**», con una meta del 92% y una ejecución de cero y una observación: **«no se presentaron incidentes de seguridad de la información en GLPI»** para la vigencia en estudio.

Al cruzar la información y revisar aleatoriamente frente a las estadísticas de las encuestas de satisfacción de ese mismo periodo (a 2021), se identificó la incidencia 58814 relacionada con Seguridad y Privacidad de la información: “Hacker del DANE”. Por lo que la Oficina de Control Interno solicitó aclaración a la Dirección de Tecnologías de la Información y Comunicaciones.

Sobre este particular, la Dirección de Tecnologías de la Información y Comunicaciones mencionó que *"efectivamente, revisada la incidencia corresponde a un correo malicioso enviado a un servidor de la SDP el cual fue gestionado por el administrador de colaboración sin ser escalado a seguridad y que teniendo en cuenta que desde seguridad no se recibió la incidencia no se reportó como tal, aunque fue atendida en su momento y gestionada."*

Esta Oficina considera que:

1)Al contrastar el indicador «**Porcentaje de atención de incidencias de seguridad realizadas por los usuarios de la SDP**» con las estadísticas de incidencias que maneja la misma Dirección de Tecnologías de la Información y Comunicaciones, existe una contradicción respecto a los resultados, lo que no quiere decir que en la entidad se hayan materializado los riesgos de seguridad
2) Se dificulta valorar con objetividad el indicador al dejarse su resultado en cero, aspecto que tampoco permite evaluar el volumen de las incidencias relacionadas con la seguridad en la SDP y determinar con exactitud si los controles son efectivos.
3) Se evidencia una debilidad en la comunicación entre la mesa de ayuda y el área de seguridad de la Dirección de Tecnologías de la Información y Comunicaciones con respecto a la información que se maneja relacionada con las incidencias de seguridad.

De otra parte, se encontró por parte de esta Oficina, durante el desarrollo de este seguimiento que en el documento "PlandeAccionControles2022_Seguimiento", (documento Excel) se tienen avances del 0% para el control A.6.1.2 Separación de deberes, frente a lo cual la Dirección de Tecnologías de la Información y Comunicaciones explicó lo siguiente:

"Se encuentra en cero porque corresponde la ejecución de lo programado que para la vigencia es 0, no se programaron actividades para este control en el 2022, lo cual se puede ver también en el plan para la vigencia no hay nada programado en 2022. Lo anterior no significa que el control se encuentre implementado en 0, se encuentra con porcentaje de implementación del 100% se ha venido cumpliendo con:
A-LE-009_2022: ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP.
A-LE-315_2022 POLÍTICA DE CONTROL DE ACCESO.
A-LE-474_2022: POLITICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Estos documentos son revisados y ajustados anualmente (si se requiere) y dictan los lineamientos en separación de deberes."

Esta Oficina corroboró que los documentos relacionados con la separación de deberes fueron revisados y actualizados por parte de la Dirección de Tecnologías de la Información y Comunicaciones de la entidad. (ver anexo1)

4.3.4.3 Implementación del Protocolo IPv6 como un componente del Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de Planeación

Al indagar si se establecieron nuevas políticas de seguridad en la SDP o se modificaron las existentes frente a la adopción e implementación de IPV6, teniendo en cuenta que este protocolo juega un papel fundamental en la infraestructura para la transformación digital de la SDP y que hace parte del MSPI, la respuesta recibida de la Dirección de Tecnologías de la Información y Comunicaciones fue la siguiente:

"El tema de IPV6 no se encuentra incluido en el modelo de seguridad y privacidad de la información, sin embargo, la entidad viene trabajando: Se realizó la renovación de los prefijos de ipv6; igualmente se realizó configuración de segmentación por plan para ipv6; igualmente se realizó la configuración en servidores linux

y windows. asi como la implementación de políticas en firewall y balanceadores de carga. se realizó configuración de los diferentes scope de IPV6 en DHCP. De igual manera en el plan de implementación de los componentes de infraestructura para la vigencia 2022 en el proyecto 4 Implementación IPV6 sobre elementos de waf, firewall y balanceadores de carga F5 se han realizado las acciones a corte 30 de septiembre en un 50.5% dejando las evidencias "

Es importante recordar que:

"..para navegar en la web, enviar un correo electrónico, descargar un archivo y realizar cualquier actividad en línea *se necesita una comunicación entre los elementos de la red y el dispositivo desde el cual se intentan realizar las acciones. A esto se le denomina Protocolo de Internet, mejor conocido como IP (por sus siglas en inglés). Y es por esta razón que todo equipo electrónico que se conecte a Internet requiere de una dirección IP.*

El IPv6, que obedece a la sexta y más reciente versión del Protocolo de Internet, pretende reemplazar la escasez de direcciones que tiene el actual IPv4 (cuarta versión). Por este motivo, las entidades del orden territorial deben priorizar su implementación en 2020, pues este protocolo juega un papel fundamental en la infraestructura para la transformación digital del Estado.

El nuevo protocolo dará la posibilidad de tener un mayor número de equipos conectados a la red de las entidades e incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad. Además, facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas así como el crecimiento de ciudades inteligentes y nuevas tecnologías como el Internet de las Cosas, Blockchain, redes de sensores, entre otros."[2]

De acuerdo con la **Resolución 2710 de 2017 de MinTIC** "Por la cual se establecen lineamientos para la adopción del protocolo IPv6." en su Artículo 2o. Ámbito de Aplicación: Son sujetos obligados de las disposiciones contenidas en la presente Resolución las entidades de que trata el artículo 2.2.9.1.1.2 del Decreto número 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, en todas sus infraestructuras de TIC con soporte IPv6, entendidas dichas infraestructuras como las redes de telecomunicaciones, programas y/o aplicaciones, sitios web, sistemas de almacenamiento, seguridad, sistemas de cómputo y en general toda tecnología que utilice el protocolo de internet IP que soporte IPv6, acorde al diagnóstico de cada entidad. Lo anterior sin perjuicio de la coexistencia con el Protocolo IP versión 4-IPv4.

Así mismo, se tiene establecido en su Artículo 6, que el incumplimiento de las disposiciones de la norma dará lugar a las sanciones establecidas en el marco de la Ley 1341 de 2009. En todo caso, las entidades tendrán la posibilidad de continuar el proceso de adopción de IPv6, de conformidad con el plan de diagnóstico de las infraestructuras de TI que se hayan realizado y, por otro lado, iniciar el registro del avance en la herramienta de seguimiento.

En concordancia con las normas del nivel nacional, desde la Alta Consejería Distrital de TIC de la Alcaldía Mayor de Bogotá, expidió la **Circular 036 de 2017** mediante la cual se dieron **lineamientos** a los Secretarios de Despacho del Distrito Capital, para el **Avance en la Implementación del Modelo de Seguridad y Privacidad de la Información-MPSI,** describiendo como un componente de la **Fase de Planificación del MPSI**, Numeral 9. Inventario de Activos de IPV6 y en la **Fase de Implementación del MPSI** el numeral 3 el Plan de Transición de IPV4 a IPV6, y la necesidad de atender los lineamientos establecidos en la Resolución 2710 de 2017 de MinTIC.

[2] Ministerio de las TIC. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126452:Que-es-el-protocolo-IPv6-y-por-que-es-importante-entender-la-urgencia-de-su-implementacion

Así mismo, vale la pena recordar algunos de los beneficios de la transición de IPV 4 a IPV 6[3]:

- La posibilidad de tener un mayor número de equipos conectados a la red de las entidades al ser implementada esta solución.
- La posibilidad de incrementar la movilidad de los usuarios al tener un número mayor de direcciones IP para la conectividad.
- Mejora de la seguridad a nivel de direccionamiento IP de la red en virtud de la arquitectura del nuevo protocolo y sus servicios.
- Reducción de los costos al implementar la solución de IPv6, en este sentido los costos podrían ser mayores de no implementarse el nuevo protocolo en las entidades.
- Se facilitará la aparición de nuevas aplicaciones y servicios sobre una gran variedad de plataformas.
- Gran número de direcciones IP para conexiones a Internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.

En conclusión, la Oficina de Control Interno recomienda que, de acuerdo con las directrices del MinTIC y de la Alta Consejería Distrital de TIC, se debe implementar el protocolo IPv6 **como un componente del Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de Planeación**, aspecto que implica establecer nuevas políticas de seguridad frente a su adopción.

4.3.4.4 Cumplimiento de normatividad Nacional en materia de Derecho de Autor 2021.

La Oficina de Control Interno solicitó información con el fin de identificar el cumplimiento de la normatividad relacionada con Derecho de Autor, para lo cual envió cuestionario que fue igualmente respondido por la Dirección de Tecnologías de la Información y Comunicaciones de la SDP. A continuación, se describen los principales aspectos:

Equipos de la Secretaría Distrital de Planeación

EQUIPOS	Activos	Inactivos	En trámite para Baja	Total
EQUIPOS DE CÓMPUTO	771	0	26	797
PORTÁTILES	65	0	1	66
TOTAL EQUIPOS Y PORTÁTILES	**836**	**0**	**27**	**863**
SERVIDORES	54	0	3	57
TOTAL SERVIDORES	**54**	**0**	**3**	**57**

Fuente: Dirección de TIC-SDP

La Entidad para la vigencia 2021 contaba con un total de 863 equipos, incluidos portátiles (836 activos y 27 en trámite para baja). Lo anterior corresponde a equipos de escritorio y portátiles asignados a los puestos de trabajo. En lo referente a servidores, la Entidad cuenta con un total de 57 servidores (54 activos y 3 en trámite para baja). Para la vigencia 2022. Pasó a tener 777 Equipos de escritorio y 78 Equipos portátiles.

Así mismo, respecto al software instalado en los equipos de cómputo propiedad de la Secretaría Distrital de Planeación - SDP, **se encuentra debidamente licenciado y de conformidad con las políticas de seguridad implementadas en la entidad**, se controla la instalación de software a través de los perfiles de usuario, actividad que solo puede ser realizada por los usuarios con perfil administrador, los demás usuarios tienen acceso restringido para instalación. Un ejemplo de esto es el manejo al software ofimático:

[3] Ministerio de las TIC .Guía No 20 de Transición de IPv4 a IPv6 para Colombia

Software Ofimático en la SDP 2022

Tipo_office	Cuenta de Tipo_office
Microsoft Office 2011	4
Microsoft Office LTSC Professional Plus 2021 - en-us	4
Microsoft Office Profesional Plus 2019 - es-es	134
Microsoft Office Professional Plus 2007	19
Microsoft Office Professional Plus 2010	3
Microsoft Office Professional Plus 2013	183
Microsoft Office Professional Plus 2016	570
Microsoft Office Standard 2019 - es-es	10
Suma total	**927**

Fuente: Dirección de TIC-SDP

De igual manera, le fue proporcionado a esta Oficina el inventario intangibles - corte septiembre de 2022.

Respecto a la Privacidad y protección de información de datos personales, se cuenta con la Política de Datos Personales y para la vigencia se realizó la revisión y ajuste de esta, en el momento se encuentra en revisión de la Dirección de servicio al ciudadano en el respectivo ciclo documental en SIPA proceso 2007910.

La Dirección de Tecnologías de la Información y Comunicaciones realiza actividades orientadas al control de instalación de software, así:

- El procedimiento A-PD-089 Soporte y atención a la mesa de ayuda, establece para el caso de instalación de software lo siguiente:

  "Instalación/desinstalación de software (incluye aplicaciones de software): *La instalación de software y de programas utilitarios está restringida y sólo podrá ser ejecutada por los usuarios de la Dirección de TIC con perfil de administrador. Lo anterior para controlar la instalación de software que pueda tener la capacidad de limitar los controles de seguridad configurados en el sistema operativo o en el software instalado. Por lo anterior, las solicitudes de instalación de software para un área deben ser realizadas únicamente por el Directivo de esta, con la respectiva justificación de su uso; esta responsabilidad no podrá ser delegada a un tercero. Dicho requerimiento deberá ser aprobado por la Dirección de TIC, quien previamente validará si posee una licencia disponible. Si se trata de software libre, la Dirección de TIC evaluará que dicho software no genere vulnerabilidades sobre la infraestructura tecnológica de la SDP. En caso de que dicho software represente un riesgo para la Entidad, su instalación no será aprobada, todo esto en cumplimiento de lo establecido en la Política de Usos de Software A-LE-362 y el Procedimiento A-PD-198 Instalación y Administración de Software vigentes en la entidad."*

- Se cuenta con el procedimiento A-PD-198 Instalación y administración de software cuyo objetivo es "establecer las actividades requeridas para la instalación y administración del licenciamiento administrado por la Dirección de Tecnologías de la Información y Comunicaciones, con el fin de optimizar los recursos informáticos, reducir el riesgo de incumplimiento a la normatividad vigente en derechos de autor".

- Se aplica el concepto de aprobación para instalación de software libre, mediante el Formato A-FO-352, con el fin de realizar el análisis del software libre solicitado por los usuarios de la entidad y garantizar que las instalaciones que se realicen estén controladas, no se instala software que requiera licencia y

no haya sido adquirido (el instrumento se incluyó en el procedimiento A-PD-198 Instalación y administración de software, para su realización permanente).

Como insumo al procedimiento se elaboró el inventario de software base; es decir, el software que se instala por defecto en cada uno de los equipos de la SDP. Este software no requiere autorización especial para su instalación pues es el necesario para la operación, ya que incluye lo requerido para garantizar que las aplicaciones de la entidad funcionen sin ningún inconveniente (el instrumento se incluyó en el procedimiento A-PD-198 Instalación y administración de software, para su realización permanente).

- Utilización del A-FO-329 Lista de chequeo, traslado, movimiento o instalación de PC. Se aplica este instrumento, el cual hace parte del procedimiento A-PD-089, donde se registra no solo la entrega, asignación o traslado de equipos, sino el software que se le instala al mismo. Como parte de la mejora del procedimiento, se carga una imagen a cada una de las placas del elemento en el inventario de GLPI, reportando finalmente estas modificaciones en radicados enviados a la Dirección Administrativa para los respectivos controles de inventario que se realizan en la Entidad.

  Como complemento, cualquier instalación de software es realizada en el control de inventario de intangibles de la Dirección de Tecnologías de la Información y Comunicaciones con el cual se controla la instalación de todos los productos de software con que cuenta la Entidad.

- La Secretaría Distrital de Planeación cuenta con el documento de política de uso de software de la SDP formalizado con documento A-LE-362, siendo esta una herramienta fundamental para garantizar el cumplimiento de las normas de derechos de autor, el cual hace parte del plan de acción anual para la revisión documental, actividades en las que participan los profesionales que realizan los procesos de adquisición de software en la Entidad.

Destino final que se le da al software dado de baja en la SDP

El destino final corresponde al NO USO del software. Según Resolución No. 1 del 2001 de la Secretaría Distrital de Hacienda, se emitió por parte de la Subsecretaría de Gestión Corporativa la Resolución Interna No. 507 de 2007 y el procedimiento A-PD-045, que establecen las bases para la realización de las bajas de software.

En ese marco, la Dirección de Tecnologías de la Información y Comunicaciones emite un concepto técnico de obsolescencia o actualización del software, con base en el cual y siguiendo lo establecido en el procedimiento mencionado, se realiza la actualización o la baja del mismo.

En la vigencia 2021 y como parte del seguimiento realizado a los instrumentos creados en cumplimiento de lo establecido en el plan de controles de seguridad de la información y con la participación del equipo de la entidad encargado de las adquisiciones del software se realizó seguimiento por parte de la Dirección de Tecnologías de la Información y Comunicaciones a cada una de las actividades realizadas en el marco del procedimiento A-PD-198 Instalación y Administración de Software.

De acuerdo con la evidencia aportada por la Dirección de Tecnologías de la Información y Comunicaciones se observa que efectuaron sesión de trabajo, y mencionan que no se encontraron modificaciones de fondo al procedimiento y únicamente se realizarán correcciones de forma al procedimiento. ***Evidencia 5.*** *A-FO-184 Reunión de Seguimiento Procedimiento A-PD-198.*

En la verificación realizada se revisaron de forma secuencial la ejecución de tareas a realizar para garantizar el cumplimiento de la política de uso de software A-LE-362 la cual es fundamental para el cumplimiento de la Directiva 2 de 2002 sobre Derechos de Autor:

- ✓ La forma como se autoriza la instalación y desinstalación del software solicitado.
- ✓ Las tareas a realizar en la administración del software a cargo de la Dirección de Tecnologías de la Información y Comunicaciones.
- ✓ Las tareas a realizar en el procedimiento para la autorización del software libre y el software base.
- ✓ Las tareas a realizar para los conceptos de baja e ingreso de software al inventario de intangibles y;
- ✓ En general toda la acción a realizar para garantizar la no instalación de software no licenciado o no autorizado.

Titularidad del derecho de autor para las soluciones de software

La titularidad del derecho de autor para las soluciones de software (sistemas de información o aplicaciones de software) que demanda la Secretaría Distrital de Planeación, se viene tratando de la siguiente manera:

a. Soluciones de software desarrollados por terceros

Para los procesos de desarrollo de soluciones de software que se adelantan por terceros, la Secretaría Distrital de Planeación dentro de la minuta del contrato o convenio y de manera específica en la Cláusula **OBLIGACIONES DEL CONTRATISTA,** literal **Obligaciones Específicas** incluye entre otras las siguientes obligaciones. ***Evidencia 6.*** *Minuta Contrato 332 de 2019 que a 31/12/2021 se encontraba en ejecución*:

- Realizar el trámite de registro de Soporte Lógico (Software) ante el Ministerio del Interior - Dirección Nacional de Derechos de Autor - Unidad Administrativa Especial - Oficina de Registro, previa celebración del "Contrato de Cesión de Derechos Patrimoniales de Autor" a favor del Distrito Capital - Secretaría Distrital de Planeación, dicho Contrato de Cesión debe ser reconocido ante notario (reconocimiento de contenido y firma por parte de los intervinientes).
- Entregar a la SDP el "Certificado de Registro de Soporte Lógico - Software", expedido por el Ministerio del Interior - Dirección Nacional de Derechos de Autor - Unidad Administrativa Especial - Oficina de Registro, en el cual conste que el Distrito Capital - Secretaría Distrital de Planeación posee los derechos patrimoniales sobre el software implementado.

b. Soluciones de software desarrollados por servidores públicos de la SDP

Para los procesos de desarrollo de soluciones de software que adelanten los servidores públicos de la SDP, se aplica lo estipulado en la Ley 23 de 1982, Artículo 92. Las obras colectivas creadas dentro de un contrato laboral o de arrendamiento de servicios, en las que sea imposible identificar el aporte individual de cada una de las personas naturales que en ellas contribuyen, tendrán por titular de los derechos de autor al editor o persona jurídica o natural por cuya cuenta y riesgo ellas se realizan.

Es de señalar que la Ley 23 de 1982 fue modificada por la Ley 44 – 1993 “Por la cual se modifica y adiciona la Ley 23 de 1983 y se modifica la Ley 29 de 1944”, no obstante, lo anterior el Artículo 92 no tuvo modificaciones.

Capacitación para los funcionarios sobre el derecho de autor y los derechos conexos en materia de programas de computador

En la vigencia 2021 y específicamente el 23 de abril de 2021, en actividad coordinada por la Dirección de Gestión Humana, se llevó a cabo el "Tercer seminario virtual: Derechos de Autor, tecnologías emergentes y nuevas dinámicas" actividad que fue coordinada por la Dirección de Gestión Humana de la SDP, de lo

cual se cuenta con las evidencias de los Correos Gestión Humana Invitación Seminario Virtual Derechos de Autor y Lista de Asistencia.

4.3.4.5 Toma de conciencia, Educación y Formación en la seguridad de la Información

De acuerdo con la Resolución 500 de 2021 de MINTIC. Modelo de Seguridad y Privacidad de la Información. Anexo 1. Control A.7.2.2 "Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

Respecto a este control y en el marco de la implementación del plan de seguridad de la información proyectado por la Dirección de Tecnologías de la Información y Comunicaciones y aprobado por parte del Comité Institucional de Gestión y Desempeño, el plan de sensibilización en seguridad, el cual se ha venido gestionando. A 31 de Octubre se encontraba ejecutado un 77% del plan (programado 74%).

Se destaca la labor realizada por la Dirección de Tecnologías de la Información y Comunicaciones de la SDP frente a este control, se evidencia con suficiencia las actividades realizadas a través de 6 estrategias a saber:

Estrategia 1 - Sesiones de sensibilización. Realización de sesiones donde se exponen temas de seguridad de la información, políticas institucionales, normas y buenas prácticas a todos los servidores y contratistas de la SDP.

Estrategia 2 - Campañas de Seguridad y Privacidad de la Información. Campaña de seguridad y privacidad de la información con piezas informativas denominadas TIPs que desarrolle aspectos puntuales de seguridad y privacidad que deben tener en cuenta los servidores y contratistas de la SDP en su gestión diaria, con el objetivo de garantizar su apropiación y aplicación.

Estrategia 3 - Píldoras de Seguridad y Privacidad de la Información. Generar piezas de comunicación dirigidas a los directivos, que contengan información concreta de seguridad y privacidad de la información, a tener en cuenta tanto en su gestión diaria como en la gestión de sus equipos de trabajo.

Estrategia 4 - Encuesta en Seguridad y Privacidad de la Información. Diseño y aplicación de Encuesta en Seguridad y Privacidad de la Información de forma virtual, que permita medir el grado de conocimiento y la satisfacción .

Estrategia 5 - Socialización Políticas, Guías e Instrumentos que componen el SGSI. Realizar la socialización en cada una de las dependencias de la SDP de los diferentes instrumentos que componen el SGSI, entre los que se encuentran políticas, guías, instructivos, directrices, circulares, procedimientos, formatos, etc.

Estrategia 6 - Boletines con temas de actualidad en Seguridad y Privacidad de la Información. Enviar boletines virtuales con contenidos actualizados, relacionados con la seguridad de la información y privacidad de la información en temas de seguridad de la información a todos los servidores de la SDP.

4.3.4.6 Acciones frente a la implementación del rediseño institucional

En el marco del rediseño las actividades planeadas y desarrolladas corresponden a:

- ✓ Información remitida a las áreas administradoras funcionales, informando lo que se debía considerar y realizar en los sistemas con afectación o cambio por el rediseño (SIPA, PERNO, SISCO, Portal SDP) para la implementación de la nueva estructura derivada del rediseño. (soportes radicados).

- ✓ Reuniones con las áreas funcionales para la coordinación y ejecución de actividades tanto a nivel de sistemas información, como para lo pertinente a actualización en Directorio Activo, accesos red, VPN (soporte reuniones y actas de las reuniones)

- ✓ Ejecución de actividades entre Oct-28 a oct-31 de 2022 (soporte relación de actividades realizadas, check list) Igualmente se realizaron actividades como

    - Se realizó el rediseño de unidades organizacionales en el directorio activo
    - Implementación de las políticas para las nuevas unidades organizacionales
    - Traslado de los servidores de acuerdo con las unidades organizaciones siguiendo lo establecido en la resolución
    - De igual manera se ejecutará plan para la asignación de permisos a los recursos compartidos

4.3.4.7 Incidentes de seguridad de la Información y aprendizajes obtenidos

Esta Oficina solicitó en el cuestionario enviado a la Dirección de Tecnologías de la Información y Comunicaciones si en el periodo comprendido entre el 2021 y 2022 se tuvieron incidentes de seguridad de la información-SI y de ser positiva la respuesta, **cuáles fueron los aprendizajes obtenidos**. Control A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información. Norma ISO 27001:2013

Dirección de Tecnologías de la Información y Comunicaciones mencionó que :

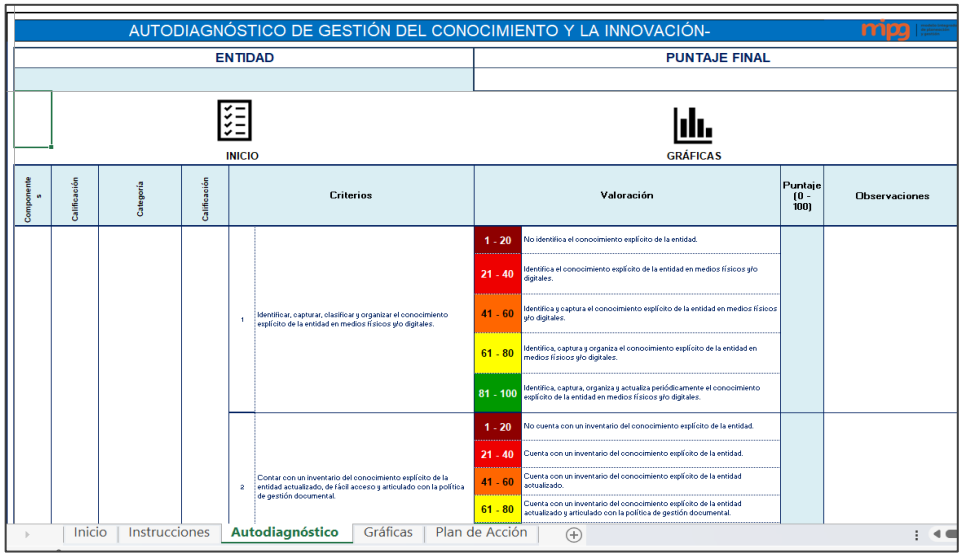
"…se recibieron incidencias de seguridad y que teniendo en cuenta que en el momento no se dejan las lecciones aprendidas, tema que se identificó en la entidad no sólo en estos procesos sino en todos los de la Secretaria: En el marco de plan de acción de gestión del conocimiento y la innovación como resultado de su autodiagnóstico 2022 se formularon actividades para fortalecer el componente de lecciones aprendidas para toda la entidad las cuales se tiene programado ejecutar en la vigencia 2023:

1. Identificar y clasificar la información para publicar como lecciones aprendidas a nivel general (Equipo interdisciplinario con prensa y comunicaciones).
2. Identificar la ubicación del repositorio para la publicación de la información sobre lecciones aprendidas - I Semestre 2023.
3. Proyectar, adoptar, implementar y divulgar el protocolo y su instrumento (formato) que guie la documentación de lecciones aprendidas en la SDP.
4. Gestionar propuesta de lineamiento para que se realice socialización de los proyectos asociados a lecciones aprendidas, como parte de los entregables de los procesos contractuales (Equipo Interdisciplinario con Gestión Contractual).
5. Capacitar al personal de la Entidad en el manejo de la Wiki y el protocolo de publicación - I Semestre 2023"

Sobre el particular la Oficina de Control Interno revisó el "Plan de Gestión del Conocimiento y la Innovación", aportado por la Dirección de Tecnologías de la Información y Comunicaciones, encontrándose los siguiente:

- En el autodiagnóstico no se encuentra diligenciada la columna puntaje o calificación, ni la columna de observaciones que permita identificar dentro de la escala de la autoevaluación para cada uno de los 37

criterios cuál fue el resultado a partir del cual se debían formular las acciones a realizar en la vigencia 2022 o 2023.



AUTODIAGNÓSTICO DE GESTIÓN DEL CONOCIMIENTO Y LA INNOVACIÓN-

ENTIDAD	PUNTAJE FINAL

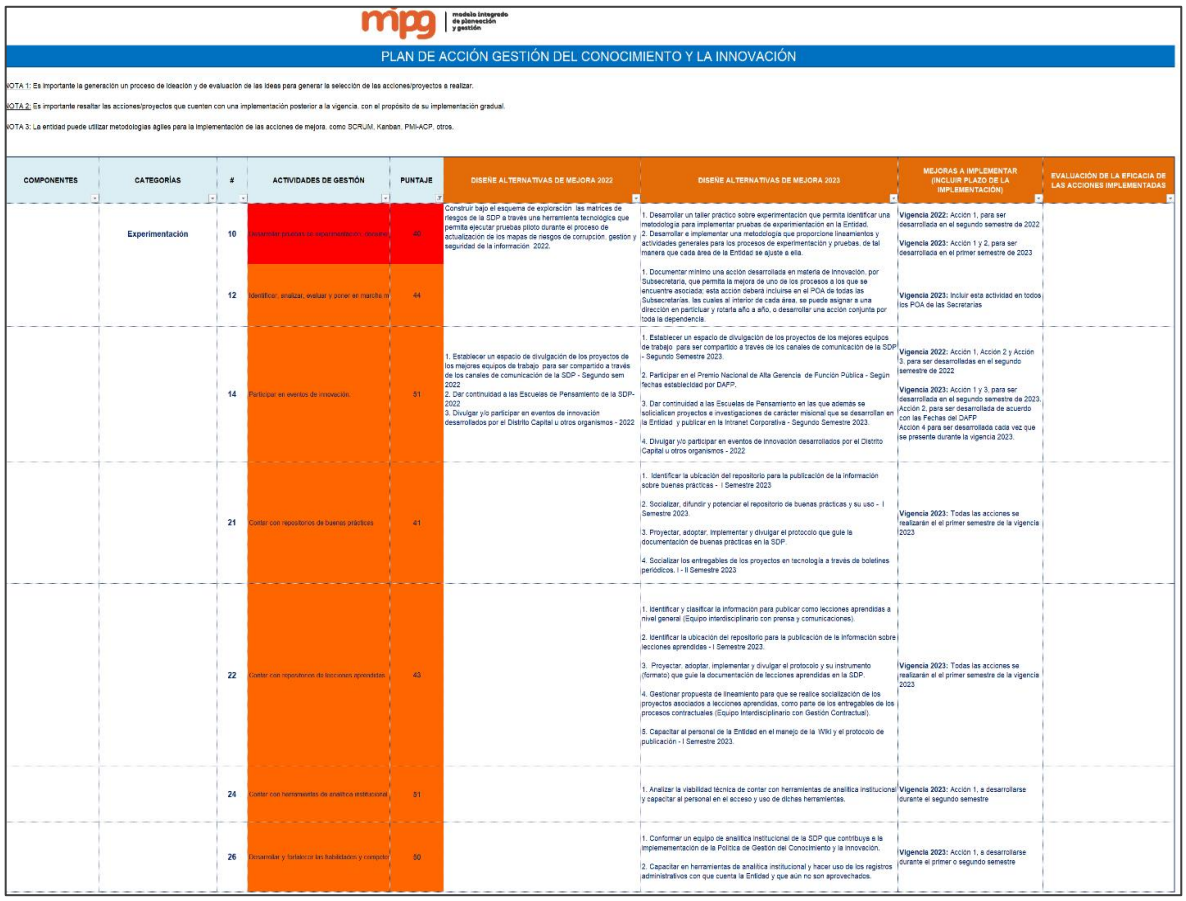
INICIO GRÁFICAS

Componentes	Calificación	Categoría	Calificación		Criterios	Valoración		Puntaje (0 - 100)	Observaciones
				1	Identificar, capturar, clasificar y organizar el conocimiento explícito de la entidad en medios físicos y/o digitales.	1 - 20	No identifica el conocimiento explícito de la entidad.		
						21 - 40	Identifica el conocimiento explícito de la entidad en medios físicos y/o digitales.		
						41 - 60	Identifica y captura el conocimiento explícito de la entidad en medios físicos y/o digitales.		
						61 - 80	Identifica, captura y organiza el conocimiento explícito de la entidad en medios físicos y/o digitales.		
						81 - 100	Identifica, captura, organiza y actualiza periódicamente el conocimiento explícito de la entidad en medios físicos y/o digitales.		
				2	Contar con un inventario del conocimiento explícito de la entidad actualizado, de fácil acceso y articulado con la política de gestión documental.	1 - 20	No cuenta con un inventario del conocimiento explícito de la entidad.		
						21 - 40	Cuenta con un inventario del conocimiento explícito de la entidad.		
						41 - 60	Cuenta con un inventario del conocimiento explícito de la entidad actualizado.		
						61 - 80	Cuenta con un inventario del conocimiento explícito de la entidad actualizado y articulado con la política de gestión documental.		

Inicio | Instrucciones | Autodiagnóstico | Gráficas | Plan de Acción

Fuente: Dirección de TIC. Documento V6_PlanAccionGesKtoSDP_09092022

- En el Plan de Acción no se encuentra diligenciada la columna de “Evaluación de la Eficacia de las Acciones Implementadas”, de tal manera que se pueda identificar el cumplimiento de las acciones 2022 y cuáles se debían reprogramar para el 2023. Así mismo, se observa que la mayoría de las acciones están para ser ejecutadas en el 2023:



PLAN DE ACCIÓN GESTIÓN DEL CONOCIMIENTO Y LA INNOVACIÓN

NOTA 1: Es importante la generación un proceso de ideación y de evaluación de las ideas para generar la selección de las acciones/proyectos a realizar.

NOTA 2: Es importante resaltar las acciones/proyectos que cuenten con una implementación posterior a la vigencia, con el propósito de su implementación gradual.

NOTA 3: La entidad puede utilizar metodologías ágiles para la implementación de las acciones de mejora, como SCRUM, Kanban, PMI-ACP, otros.

COMPONENTES	CATEGORÍAS	#	ACTIVIDADES DE GESTIÓN	PUNTAJE	DISEÑE ALTERNATIVAS DE MEJORA 2022	DISEÑE ALTERNATIVAS DE MEJORA 2023	MEJORAS A IMPLEMENTAR (INCLUIR PLAZO DE LA IMPLEMENTACIÓN)	EVALUACIÓN DE LA EFICACIA DE LAS ACCIONES IMPLEMENTADAS
	Experimentación	10	Desarrollar pruebas de experimentación (Gestión	40	Construir bajo el esquema de exploración las matrices de riesgos de la SDP a través una herramienta tecnológica que permita ejecutar pruebas piloto durante el proceso de actualización de los mapas de riesgos de corrupción, gestión y seguridad de la información 2022.	1. Desarrollar un taller practico sobre experimentación que permita identificar una metodología para implementar pruebas de experimentación en la Entidad. 2. Desarrollar e implementar una metodología que proporcione lineamientos y actividades generales para los procesos de experimentación y pruebas, de tal manera que cada área de la Entidad se ajuste a ella.	**Vigencia 2022:** Acción 1, para ser desarrollada en el segundo semestre de 2022. **Vigencia 2023:** Acción 1 y 2, para ser desarrollada en el primer semestre de 2023	
		12	Identificar, analizar, evaluar y poner en marcha m	44		1. Documentar mínimo una acción desarrollada en materia de innovación, por Subsecretaría, que permita la mejora de uno de los procesos a los que se encuentre asociada; esta acción deberá incluirse en el POA de todas las Subsecretarías, las cuales al interior de cada área, se puede asignar a una dirección en particular y rotarla año a año, o desarrollar una acción conjunta por toda la dependencia.	**Vigencia 2023:** Incluir esta actividad en todos los POA de las Secretarías	
		14	Participar en eventos de innovación.	51	1. Establecer un espacio de divulgación de los proyectos de los mejores equipos de trabajo para ser compartido a través de los canales de comunicación de la SDP - Segundo sem 2022 2. Dar continuidad a las Escuelas de Pensamiento de la SDP-2022 3. Divulgar y/o participar en eventos de innovación desarrollados por el Distrito Capital u otros organismos - 2022	1. Establecer un espacio de divulgación de los proyectos de los mejores equipos de trabajo para ser compartido a través de los canales de comunicación de la SDP - Segundo Semestre 2023. 2. Participar en el Premio Nacional de Alta Gerencia de Función Pública - Según fechas establecidad por DAFP. 3. Dar continuidad a las Escuelas de Pensamiento en las que además se soliciaiten proyectos e investigaciones de carácter misional que se desarrollan en la Entidad y publicar en la Intranet Corporativa - Segundo Semestre 2023. 4. Divulgar y/o participar en eventos de innovación desarrollados por el Distrito Capital u otros organismos - 2022	**Vigencia 2022:** Acción 1, Acción 2 y Acción 3, para ser desarrolladas en el segundo semestre de 2022 **Vigencia 2023:** Acción 1 y 3, para ser desarrollada en el segundo semestre de 2023, Acción 2, para ser desarrollada de acuerdo con las Fechas del DAFP. Accion 4 para ser desarrollada cada vez que se presente durante la vigencia 2023.	
		21	Contar con repositorios de buenas prácticas	41		1. Identificar la ubicación del repositorio para la publicación de la información sobre buenas prácticas - I Semestre 2023 2. Socializar, difundir y potenciar el repositorio de buenas prácticas y su uso - I Semestre 2023. 3. Proyectar, adoptar, implementar y divulgar el protocolo que guíe la documentación de buenas prácticas en la SDP. 4. Socializar los entregables de los proyectos en tecnología a través de boletines periódicos. I - II Semestre 2023	**Vigencia 2023:** Todas las acciones se realizarán el el primer semestre de la vigencia 2023	
		22	Contar con repositorios de lecciones aprendidas	43		1. Identificar y clasificar la información para publicar como lecciones aprendidas a nivel general (Equipo interdisciplinario con prensa y comunicaciones). 2. Identificar la ubicación del repositorio para la publicación de la información sobre lecciones aprendidas - I Semestre 2023. 3. Proyectar, adoptar, implementar y divulgar el protocolo y su instrumento (formato) que guíe la documentación de lecciones aprendidas en la SDP. 4. Gestionar propuesta de lineamiento para que se realice socialización de los proyectos asociados a lecciones aprendidas, como parte de los entregables de los procesos contractuales (Equipo Interdisciplinario con Gestión Contractual). 5. Capacitar al personal de la Entidad en el manejo de la Wiki y el protocolo de publicación - I Semestre 2023.	**Vigencia 2023:** Todas las acciones se realizarán el el primer semestre de la vigencia 2023	
		24	Contar con herramientas de analítica institucional	51		1. Analizar la viabilidad técnica de contar con herramientas de analítica institucional y capacitar al personal en el acceso y uso de dichas herramientas.	**Vigencia 2023:** Acción 1, a desarrollarse durante el segundo semestre	
		26	Desarrollar y fortalecer las habilidades y competer	50		1. Conformar un equipo de analítica institucional de la SDP que contribuya a la implementación de la Política de Gestión del Conocimiento y la Innovación. 2. Capacitar en herramientas de analítica institucional y hacer uso de los registros administrativos con que cuenta la Entidad y que aún no son aprovechados.	**Vigencia 2023:** Acción 1, a desarrollarse durante el primer o segundo semestre	

Fuente: Dirección de TIC. Documento V6_PlanAccionGesKtoSDP_09092022

4.3.4.8 Copias de Respaldo. Resolución 500 de 2021 de MinTIC. Anexo 1 MPSI Control A.12.3 Copias de respaldo

En respuesta al cuestionario enviado por esta Oficina, la Dirección de Tecnologías de la Información y Comunicaciones informó que las copias de respaldo se realizan y almacenan en medios magnéticos (Cintas LTO), las cuales se manejan por medio de políticas (Por demanda, Diarias, Semanales, Mensuales y Anuales) y estas mismas tienen 3 lugares de almacenamiento dependiendo de la protección que tengan (Empresa de Guarda custodia actualmente "tiedot", Cintoteca SHD, Cintoteca SDP).

Backups por demanda: esta actividad se apoya Para el tema de la elección aleatoria de la información que se respalda mediante políticas definidas en la solución de copias de respaldo, de acuerdo con el documento A-FO-298 Inventario Políticas de Respaldo y a su vez usan un aplicativo de elección aleatorio vía web llamado sortea2 https://www.sortea2.com/sortear/numeros , el cual funciona de la misma manera que la aplicación appsorteos.

Políticas de Respaldo: Para el tema de la elección aleatoria de la información que se respalda mediante políticas definidas en la solución de copias de respaldo, la Dirección de Tecnologías de la Información y Comunicaciones se basa en el documento A-FO-298 Inventario Políticas de Respaldo y a su vez usan un aplicativo de elección aleatorio vía web llamado sortea2 https://www.sortea2.com/sortear/numeros , el cual funciona de la misma manera que la aplicación appsorteos

Por un tema de capacidad de espacio disponible, para el ejercicio, la Dirección de Tecnologías de la Información y Comunicaciones va a tomar un solo servidor por política. Respecto a las pruebas de restauración, en el año 2022 se llevó a cabo un plan de restauración y se dejó como evidencia documento con la descripción de todo el proceso realizado.

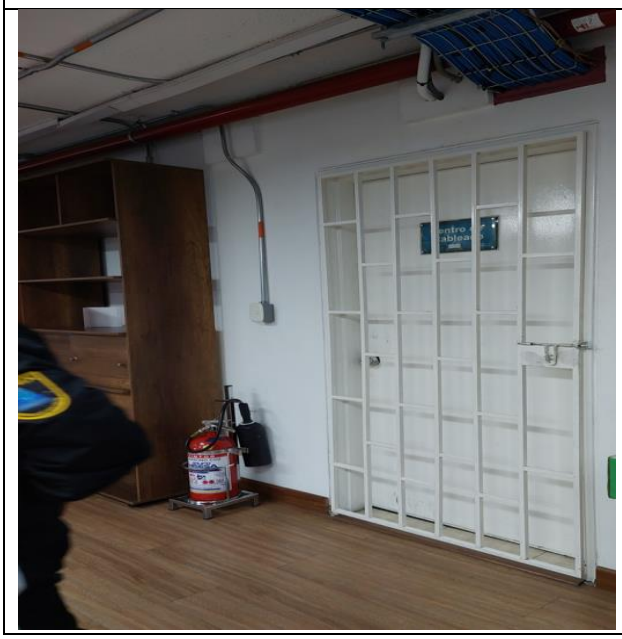
4.3.5 Prueba de recorrido -Centros de Comunicaciones SDP. Pisos 2, 5,8 y 13 y Planoteca Primer Piso SuperCade

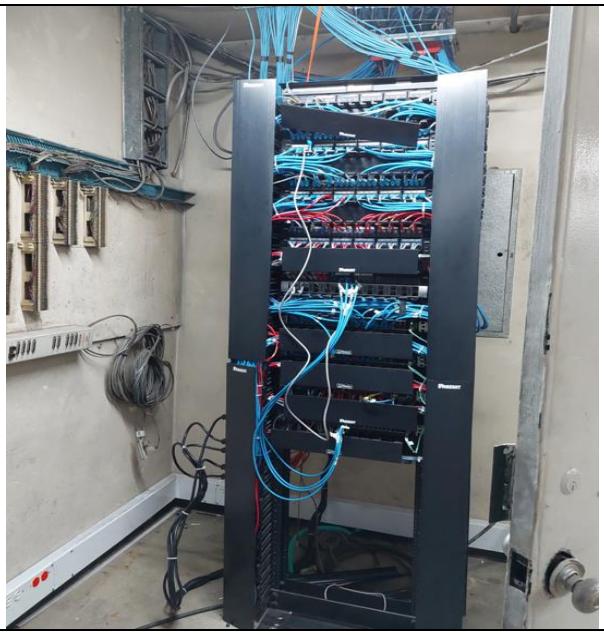
Durante la prueba de recorrido por los cuartos de telecomunicaciones de la Secretaría Distrital de Planeación y Primer piso Planoteca, se hizo prueba de acceso a los mismos, encontrándose que la clave de acceso a estos espacios de una de las personas del equipo auditor de la Oficina de Control Interno cuando ejerció como brigadista aún estaba habilitada para acceder.

Es decir que para la fecha del recorrido aun no se le habían deshabilitado los permisos, evidenciándose incumplimiento del control A.9.2.6 Retiro o ajuste de los derechos de acceso de la ISO 27001:2013. Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.

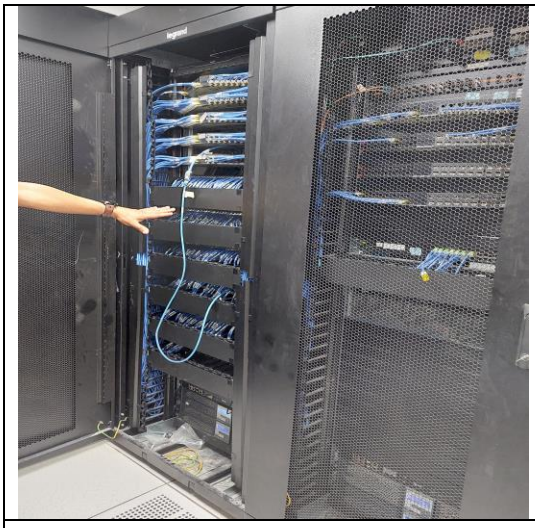
Así mismo, se encontró durante el recorrido:

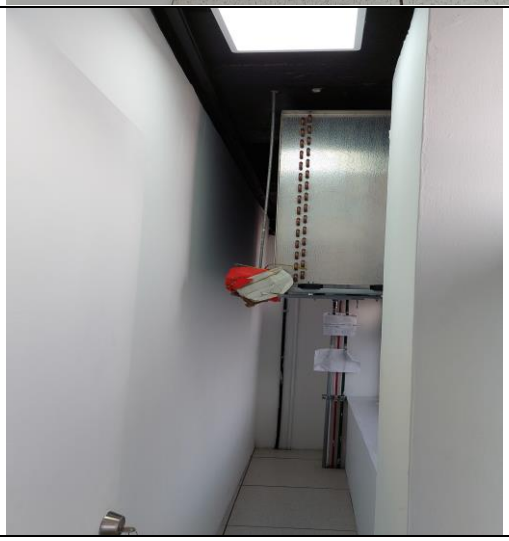
Piso 2: Centro de telecomunicaciones con doble puerta metálica

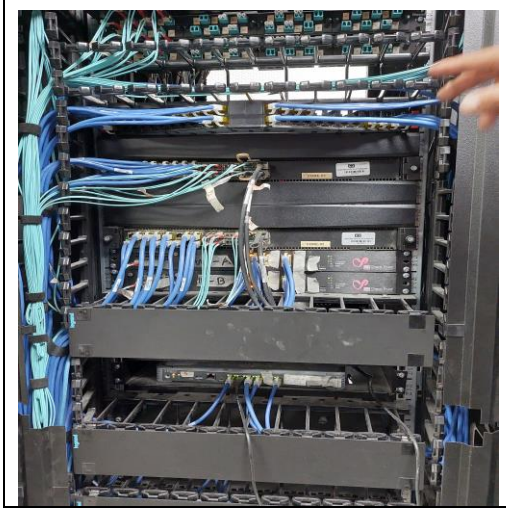


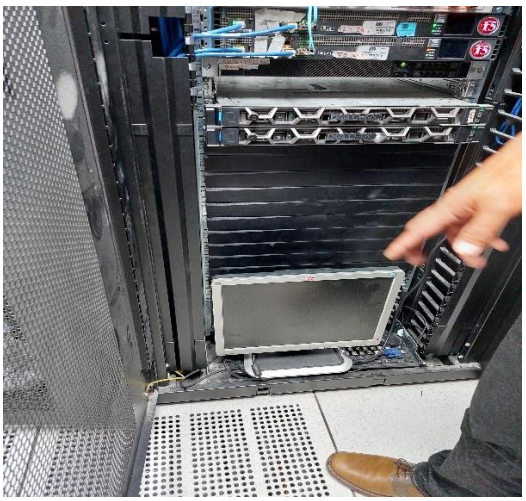


Piso 5: El centro de telecomunicaciones se estaba adecuando y remodelando para la fecha de la visita, encontrándose elementos ajenos al mismo.

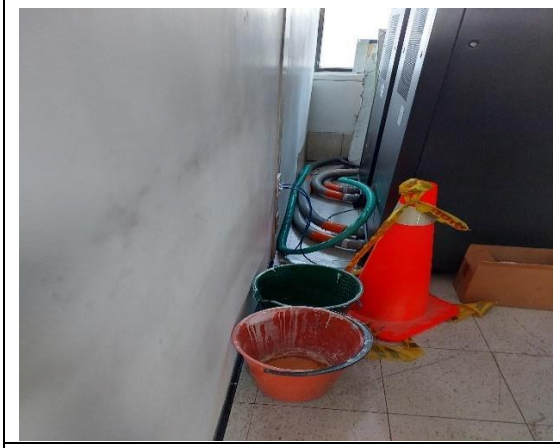








Piso 8: Se encontraron en el centro de comunicaciones elementos como baldes, traperos, escaleras, cajas de cartón y elementos inflamables como pinturas, tíner, muñecos de felpa



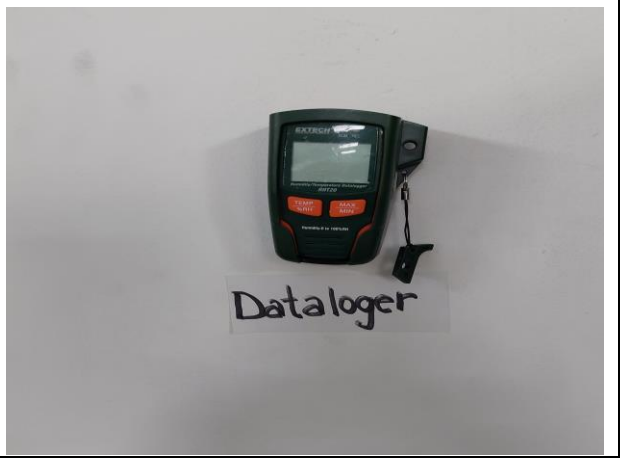
	

Piso 13: se encontraron cajas de cartón y elementos tecnológicos sobrantes o sin utilizar.

Piso 1-Área de Planoteca: al continuar con el recorrido por los espacios de la planoteca primer piso y de atención al ciudadano, se pudo verificar por parte de esta Oficina, que el datalogger **no estaba funcionando** para la fecha de la visita 28 de septiembre de 2022:

De acuerdo con la "Guía práctica para las entidades del Distrito Capital, del Programa del Sistema Integrado de Conservación del Archivo de Bogotá y el Acuerdo del AGN No.049 de 2000 en su artículo quinto, existen parámetros y mecanismos de prevención que permitan realizar mediciones para conocer, registrar y monitorear los niveles de humedad relativa y temperatura de un espacio. «*Para ello, se recomiendan los equipos que utilizan sistemas digitales para la captura y registro de los datos, como es el caso de termohigrómetros digitales conocidos como dataloggers o compiladores de datos. Se trata de equipos electrónicos que registran datos digitales y "funcionan recogiendo y procesando las señales procedentes de varios sensores a los que se encuentran conectados, las señales son digitalizadas y almacenadas en la memoria para luego traducirse e interpretarse por medio de programas de ordenador. El intervalo de tiempo para la recolección de datos se programa antes de comenzar el registro" [García, 1999, p.87]. Los dataloggers necesitan de calibración regular y atención para el cambio de las baterías.*»

4.4 Anexos

Anexo 1

Documentos del Proceso que lidera la Dirección de Tecnologías de la Información y Comunicaciones de la Secretaría Distrital de Planeación y fechas de actualización

CÓDIGO	NOMBRE	VERSIÓN	ACTA	FECHA ACTA
A-LE-433	GUÍA DEL USUARIO FINAL MÓDULO DE CORRESPONDENCIA INTERNA Y EXTERNA EN EL SIPA	1	88	April 25, 2019
A-LE-334	DECLARACIÓN DE APLICABILIDAD DEL SGSI EN LA SDP	2	324	December 24, 2019
A-LE-453	GUÍA DE TRANSFERENCIA DE INFORMACIÓN	1	344	December 31, 2019
A-LE-303	MAPA DE RIESGOS DEL PROCESO SOPORTE TECNOLÓGICO	7	45	January 31, 2020
A-FO-298	INVENTARIO POLÍTICAS COPIAS DE RESPALDO	3	154	July 21, 2020
A-FO-479	BITACORA GESTION DEL CAMBIO INFORMATICO	1	303	December 19, 2020
A-LE-015	PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PETI	9	311	December 28, 2020
A-PD-198	INSTALACIÓN Y ADMINISTRACIÓN DE SOFTWARE	2	336	December 30, 2020
A-FO-467	CONTROL INVENTARIO DE SOFTWARE LICENCIADO	1	334	December 30, 2020
A-PD-089	SOPORTE Y ATENCIÓN DE LA MESA DE AYUDA	15	333	December 30, 2020
A-PD-069	DESARROLLO, INSTALACIÓN Y MANTENIMIENTO DE APLICACIONES	11	344	December 31, 2020
A-PD-204	GESTION DEL CAMBIO INFORMATICO	1	345	December 31, 2020
A-PD-203	TRANSFERENCIA DE INFORMACIÓN	1	340	December 31, 2020
A-LE-327	GUÍA GESTIÓN DEL CAMBIO INFORMÁTICO	3	343	December 31, 2020
A-LE-289	POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES	6	218	December 9, 2021
A-LE-429	POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	3	241	December 30, 2021
A-PD-192	MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA	4	8	January 25, 2022
A-LE-389	PLAN DE MANTENIMIENTO DE INFRAESTRUCTURA TECNOLÓGICA DE LA SDP	4	13	January 28, 2022
A-FO-334	LISTA DE CHEQUEO DE ELEMENTOS DE INFRAESTRUCTURA TECNOLÓGICA	4	15	January 31, 2022

CÓDIGO	NOMBRE	VERSIÓN	ACTA	FECHA ACTA
A-LE-445	CATÁLOGO DE SISTEMAS DE INFORMACIÓN DE LA SDP (ANEXO 3 PETI)	3	121	May 25, 2022
A-FO-296	BITÁCORA CINTOTECA	4	134	June 6, 2022
A-PD-092	COPIAS DE SEGURIDAD Y RECUPERACIÓN DE INFORMACIÓN	12	142	June 9, 2022
A-IN-016	GUÍA PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN DE LA SDP	10	154	June 16, 2022
A-LE-362	POLÍTICA DE USO DE SOFTWARE	3	155	June 17, 2022
A-LE-359	POLÍTICA DE DESARROLLO SEGURO	3	156	June 17, 2022
A-LE-321	POLÍTICA PARA EL USO DE DISPOSITIVOS MÓVILES EN LA SDP	4	157	June 17, 2022
A-LE-315	POLÍTICA DE CONTROL DE ACCESO	6	159	June 17, 2022
A-LE-297	POLÍTICA PARA LA GESTIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN INSTITUCIONAL	5	158	June 17, 2022
A-FO-209	FORMATO REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI)	13	174	July 15, 2022
A-LE-016	PLAN DE CONTINGENCIA INFORMÁTICO	4	188	July 28, 2022
A-LE-505	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	190	July 29, 2022
A-LE-474	POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN	2	205	August 12, 2022
A-LE-320	POLÍTICA DE USO DE MEDIOS REMOVIBLES	4	206	August 12, 2022
A-LE-317	POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS	5	208	August 16, 2022
A-LE-373	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SDP	4	207	August 22, 2022
A-CA-007	CARACTERIZACIÓN SOPORTE TECNOLÓGICO	6	222	September 9, 2022
A-FO-400	FORMATO CONCEPTO TÉCNICO	2	220	September 9, 2022
A-FO-329	LISTA DE CHEQUEO, TRASLADO, MOVIMIENTO O INSTALACIÓN DE PC	5	221	September 9, 2022
A-LE-398	LINEAMIENTOS OPERACIONALES TIC	3	229	September 15, 2022

CÓDIGO	NOMBRE	VERSIÓN	ACTA	FECHA ACTA
A-FO-352	CONCEPTO APROBACIÓN PARA INSTALACIÓN DE SOFTWARE LIBRE	3	232	September 19, 2022
A-LE-446	CATÁLOGO DE SERVICIOS DE TI SDP (ANEXO 4 PETI)	3	230	September 19, 2022
A-PD-107	INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES DE LA SDP	6	240	September 27, 2022
A-FO-300	ACTA DE COMPROMISO PARA ADMINISTRADORES DE APLICACIONES DE LA SDP	3	237	September 27, 2022
A-FO-299	ACTA DE COMPROMISO PARA USUARIOS PRIVILEGIADOS	6	238	September 28, 2022
A-FO-478	CONTROL DE CAMBIO INFORMÁTICO	2	239	September 28, 2022
A-IN-422	GUÍA ESTÁNDAR PARA LA CREACIÓN DE USUARIOS EN LA SDP	2	243	September 30, 2022
A-LE-285	DIRECTRICES GENERALES PARA LA FORMULACIÓN DE PROYECTOS INFORMÁTICOS DE LA SDP	5	245	September 30, 2022
A-LE-284	METODOLOGÍA GERENCIA DE PROYECTOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE LA SDP	5	246	September 30, 2022
A-IN-412	MANUAL PARA EL MANEJO DEL MÓDULO DE PLANES DE MEJORAMIENTO DEL SISTEMA DE INFORMACIÓN DE PROCESOS AUTOMÁTICOS - SIPA	4	250	October 6, 2022
A-LE-477	POLÍTICA DE CRIPTOGRAFÍA ENFOCADA A LOS CERTIFICADOS DE FIRMA DIGITAL	2	251	October 12, 2022
A-LE-480	LINEAMIENTOS PARA EL TRATAMIENTO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LOS ACUERDOS CON LOS PROVEEDORES	2	252	October 14, 2022
A-FO-295	BITÁCORA DE COPIAS DE RESPALDO POR DEMANDA Y RESTAURACIONES SOBRE EQUIPOS DE CÓMPUTO O SERVIDORES	3	253	October 21, 2022
A-LE-375	POLÍTICA DE SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN EN LA SDP	4	255	October 24, 2022
A-LE-414	POLÍTICA PARA LA GESTIÓN DE CARPETAS COMPARTIDAS	3	260	October 25, 2022
A-LE-009	ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP	8	261	October 25, 2022
A-LE-481	POLÍTICA PARA EL ASEGURAMIENTO DE LA INFORMACIÓN Y SERVICIOS EN LA RED	3	268	October 27, 2022
A-LE-465	ALCANCE Y LÍMITES DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - SGSI	3	269	October 27, 2022

CÓDIGO	NOMBRE	VERSIÓN	ACTA	FECHA ACTA
A-PD-104	GESTIÓN CUENTAS DE USUARIO	12	289	October 28, 2022
A-PD-187	GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA SDP	5	282	October 28, 2022
A-LE-283	REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI)	11	287	October 28, 2022
A-FO-010	SOLICITUD GESTIÓN CUENTAS DE USUARIO	16	296	November 23, 2022
A-FO-212	ACTA DE COMPROMISO PARA EL USO DE RECURSOS INFORMÁTICOS	10	299	November 30, 2022

5. Fortalezas

La Oficina de Control Interno destaca de la Dirección de Tecnologías de la Información y las Comunicaciones:

- Los buenos resultados obtenidos en el Reporte de Avances de la Gestión – FURAG, con un puntaje sobresaliente en cuanto a los avances sectoriales e institucionales en la implementación de las políticas de Gobierno Digital y Seguridad Digital.

- La Dirección de Tecnologías de la Información y las Comunicaciones, viene realizando una labor sobresaliente y comprometida de mejoramiento continuo desde la vigencia 2021, cuando tomó la decisión de verificar, racionalizar y mejorar las Políticas TIC y sus diferentes instrumentos.

- La alineación del Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de Planeación con la Metodología y Políticas establecidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones, y por la Alta Consejería TIC de Bogotá.

- La información completa, organizada y disponible del Modelo de Privacidad y Seguridad de la Información, que lidera la Dirección de Tecnologías de Información y Comunicaciones desde el diagnostico, los planes de trabajo y los seguimientos que ha presentado ante el Comité Institucional de Gestión y Desempeño, que demuestran el gran esfuerzo y compromiso realizado por los profesionales de la Dirección de TIC por establecer, implementar, mantener y mejorar continuamente el MPSI.

- Se resalta la actividad realizada por la Dirección de TIC, para la actualización de los activos de información de la SDP.

- En el tema de Riesgos, se destaca la actividad que viene realizando la Dirección de Tecnologías de la Información y las Comunicaciones capacitando y asesorando a los procesos y dependencias de la entidad en la actualización y mejora de los riesgos de seguridad de la información.

- De acuerdo con las evidencias, sobresalen las actividades de sensibilización y capacitación desarrolladas a través de 6 estrategias por la Dirección de TIC de la SDP, frente al Control A.7.2.2 del Anexo 1 Modelo de Seguridad y Privacidad de la Información de la Resolución 500 de 2021 de MINTIC.

- Se resalta que en la entidad las Direcciones de Talento Humano, Planeación Institucional y de Tecnologías de la Información y las Comunicaciones, realicen trabajo articulado en la Política de Gestión del Conocimiento y la Innovación.

6. Situaciones susceptibles de mejora / oportunidades (observaciones)

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
1.	Al contrastar el indicador «**Porcentaje de atención de incidencias de seguridad realizadas por los usuarios de la SDP**» del documento «Avances y Logros a diciembre 31 de 2021 Modelo de Seguridad y Privacidad de la Información de la SDP», (presentado por la Dirección de TIC como insumo para el Comité Institucional de Gestión y Desempeño en el mes de marzo de 2022), contra las estadísticas de incidencias que maneja la misma Dirección de TIC, se encontraron diferencias respecto a los resultados, lo que denota debilidad en la formulación y seguimiento de indicadores.	4.3.4	Dirección de Tecnologías de la Información y las Comunicaciones
2.	Debilidades en la comunicación entre la mesa de ayuda y el área de seguridad de la Dirección de TIC con respecto a la información que se maneja, relacionada con las incidencias de seguridad.	4.3.4	Dirección de Tecnologías de la Información y las Comunicaciones
3.	Insuficiente tratamiento de vulnerabilidades detectadas: • En el Plan de Gestión de Vulnerabilidades 2021, no fueron resueltas la totalidad de vulnerabilidades identificadas en la vigencia anterior (475). • En el proceso de remediación algunas aplicaciones presentaron novedades técnicas y/o administrativas que no permitieron llevar a cabo las actividades de aseguramiento en los tiempos programados, es decir, que algunas aplicaciones no pudieron ser Remediadas en los tiempos establecidos, por ejemplo: Documanager, Sisbén - consulta WEB, Formación SDP - Moodle, Media WIKI y Metadatos, Página Web, Página Inventario Bogotá, SINUPOT, Sistema de Familias, Gestión de Usuarios, Intranet, Sisbén, SegPlan, SICapital, Planoteca, Plusvalía, Web Services, Sistema de requerimientos, SIAR. • Se presentaron algunas dificultades por obsolescencia, con equipos de escritorio que no respondieron al momento de la ejecución del proceso, por motivos asociados a que se encontraban apagados o por falta de espacio de almacenamiento en disco, igualmente porque el sistema alertaba sobre software que debía ser revisado o por falla en algún sector del disco.	4.3.4.1	Dirección de Tecnologías de la Información y las Comunicaciones

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
4.	La obsolescencia en la infraestructura tecnológica de la SDP, pero especialmente en servidores y equipos de escritorio generan riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP.	4.3.4.1	Dirección de Tecnologías de la Información y las Comunicaciones
5.	En el documento aportado por la Dirección de TIC, relacionado con el Plan de Acción de Gestión del Conocimiento y la Innovación, se observó que el autodiagnóstico no tiene diligenciada la columna puntaje o calificación para cada uno de los 37 criterios que permita identificar los resultados a partir de los cuales se formularon las acciones a realizar tanto para la vigencia 2022 como la vigencia 2023. Así mismo, en el Plan de Acción, no está diligenciada la columna de Evaluación de la eficacia de las acciones y no se cuenta con información sobre el avance de estas.	4.3.4.7	Dirección de Tecnologías de la Información y las Comunicaciones Dirección de Planeación Institucional Dirección de Talento Humano
La formulación de planes de mejoramiento es opcional para las situaciones de mejora identificadas, no obstante, la Oficina de Control Interno - OCI revisará las medidas adoptadas en la próxima auditoría y/o seguimiento.			

7. Situaciones críticas

N°	1.	Reincidente (si/no)	NO
Descripción de la situación crítica	El protocolo IPv6 no fue identificado como un entregable del Modelo de Seguridad y Privacidad de la Información-MPSI de la Secretaría Distrital de Planeación, de acuerdo con lo establecido en la Circular 036 de 2017 de la Alta Consejería Distrital de TIC, tanto para la fase de planeación, como para la fase de implementación del MPSI.		
Criterio Incumplido (Estándar/norma/reglamento)	Circular 036 de 2017 “Lineamientos de Avance Implementación Modelo de Seguridad y Privacidad de la Información” de la Alta Consejería Distrital de TIC, de la Alcaldía Mayor de Bogotá.		
Numeral del informe (capítulo 4)	4.3.4.3		
Responsable	Dirección de Tecnologías de la Información y las Comunicaciones		
Posible efecto	Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP		
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Protocolo IPv6, MPSI		

N°	2	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Para la vigencia 2023, la SDP no cuenta con recursos para la adquisición e implementación de herramientas de software para la realización de copias de seguridad de la información institucional, así como tampoco para la actualización del licenciamiento de la solución del antivirus.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021 de MinTIC. Anexo 1 MPSI **Control A.12.3 Copias de respaldo**		
Numeral del informe (capítulo 4)	4.3.2.1 y 4.3.4.8		
Responsable	Subsecretaría de Gestión Institucional Dirección de Tecnologías de la Información y las Comunicaciones		
Posible efecto	Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP		
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Copias seguridad de la información institucional		

N°	3	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Para la vigencia 2023 se observa disminución de recursos significativos para realizar las actividades de la «FASE I para la Migración de servicios tecnológicos de la entidad a la nube» y la «Operacionalización del Plan de Recuperación de Desastres.» En el tema de continuidad del negocio o de la organización, se requiere que se aborde el tema de forma estratégica por parte de la SDP.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021 de MinTIC. Anexo 1 MPSI . **Control A.17 Continuidad de la seguridad de la Información**		
Numeral del informe (capítulo 4)	4.3.2.1 y 4.3.3		
Responsable	Subsecretaría de Gestión Institucional Dirección de Tecnologías de la Información y las Comunicaciones		
Posible efecto	Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP		
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Riesgos Continuidad Negocio ; MPSI		

N°	4	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Durante la prueba de recorrido por los cuartos de telecomunicaciones de la Secretaría Distrital de Planeación y Primer piso Planoteca, se hizo prueba de acceso a los mismos. Se encontró que la clave de acceso a estos espacios por parte de una de las personas del equipo auditor de la Oficina de Control Interno aún estaba habilitada para acceder, desde cuando ejerció como brigadista (ya no lo es).		

Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021 de MinTIC. Anexo 1 MPSI **Control A.9.2.6 Retiro o ajuste de los derechos de acceso**
Numeral del informe (capítulo 4)	4.3.5
Responsable	Dirección de Tecnologías de la Información y las Comunicaciones
Posible efecto	Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Retiro o ajuste derechos acceso MPSI

N°5	5	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Al hacer el recorrido por los cuartos de comunicaciones de la entidad, se encontraron elementos ajenos a los mismos, algunos incluso son inflamables, encontrados en el piso 8.(Tarros de pintura y thinner, junto a bolsas y muñecos de felpa).		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021 de MINTIC. Modelo de Seguridad y Privacidad de la Información. Anexo 1. **Control A.11. Seguridad Física y del entorno**		
Numeral del informe (capítulo 4)	4.3.5		
Responsable	Dirección de Tecnologías de la Información y las Comunicaciones		
Posible efecto	Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP		
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Modelo Seguridad y Privacidad de la Información		

N°	6	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Se encontró en el espacio de atención al ciudadano, al interior de la planoteca, primer piso, que el datalogger no estaba funcionando para la fecha de la visita.		
Criterio Incumplido (Estándar/norma/reglamento)	- Acuerdo No.049 de 2000, Artículo 5°, Archivo General de la Nación-AGN -Guía práctica para las entidades del Distrito Capital, Programa del Sistema Integrado de Conservación del Archivo de Bogotá. Resolución 500 de 2021 de MINTIC. Modelo de Seguridad y Privacidad de la Información. Anexo 1. **Control A.11.2.4 Mantenimiento de equipos**.		
Numeral del informe (capítulo 4)	4.3.5		
Responsable	Dirección Administrativa Dirección de Tecnologías de la Información y las Comunicaciones		
Posible efecto	Riesgos para la conservación adecuada de los planos que reposan en este espacio al no realizarse el monitoreo de humedad relativa y		

	temperatura. Posibilidad de deterioro de planos y rasgos de pérdida de información de la ciudad. Riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	**Mantenimiento equipos, MPSI**

- Con el fin de eliminar las causas que los procesos identifiquen en cada situación crítica, se deben identificar y formular acciones atendiendo lo establecido en el procedimiento S-PD-005 - Gestión del Plan de Mejoramiento.
- La Oficina de Control Interno efectuará el análisis y verificación de la efectividad alcanzada.

8. Recomendaciones

- Con ocasión de la expedición del Decreto 555 de 2021 y del rediseño institucional algunos trámites y servicios dejan de estar a cargo de la SDP, entre ellos el de estaciones Radioeléctricas, por lo que es importante evaluar la continuidad de procesos contractuales para la virtualización de este trámite en la SDP.

- Se pudo evidenciar por parte de la Oficina de Control Interno que de las 18 actividades formuladas para la vigencia 2022 en el Plan para la Gestión de Vulnerabilidades , siete actividades (el 33% del Plan), quedaron pospuestas para ser programadas en la vigencia 2023, lo que puede estar generando riesgos de confiabilidad, integridad y disponibilidad de la información de la SDP.

- A pesar de que la Dirección de TIC informa que en anteriores vigencias ha solicitado capacitaciones, pero por restricciones presupuestales no ha sido posible acceder a diferentes temas que son estratégicos para asegurar la confiabilidad, disponibilidad e integridad de la Información de la SDP, se recomienda gestionar nuevamente con la Dirección de Talento Humano la programación de una ruta de capacitación encaminada a fortalecer al equipo humano de la Dirección de TIC en temas como son seguridad de la información, en seguridad informática, programación y en las nuevas herramientas de la Cuarta Revolución Industrial, entre otros aspectos.

Nombres / Equipo Auditor	
Auditor líder	Lucy Divanelly Muñoz Rodríguez
Auditor(es)	Fernando Tunjano Reyes

Denis Parra Suárez
Jefe Oficina de Control Interno