Nombre del informe
Informe Definitivo 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 de la vigencia 2023.

En el alcance fueron revisadas las Políticas del MSPI y la aplicabilidad de cada uno de los 14 dominios y 114 controles bajo las directrices del MSPI -Resolución 500 de 2021 bajo la ISO 27001:2013, teniendo en cuenta que aún no se ha realizado la transición hacia la versión 2022.

3. Criterios

- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales.”
- Decreto 1377 de 2013, “Por el cual se reglamenta parcialmente la Ley 1581 de 2012.”
- 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.
- Decreto Nacional 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Directiva Presidencial 002 de 2022. “Reiteración de la Política Pública en Materia de Seguridad Digital”.

- 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, publicados en el Sistema de Información de Procesos Automáticos-SIPA.
- Planes de Mejoramiento asociados a los temas del MPSI de la SDP

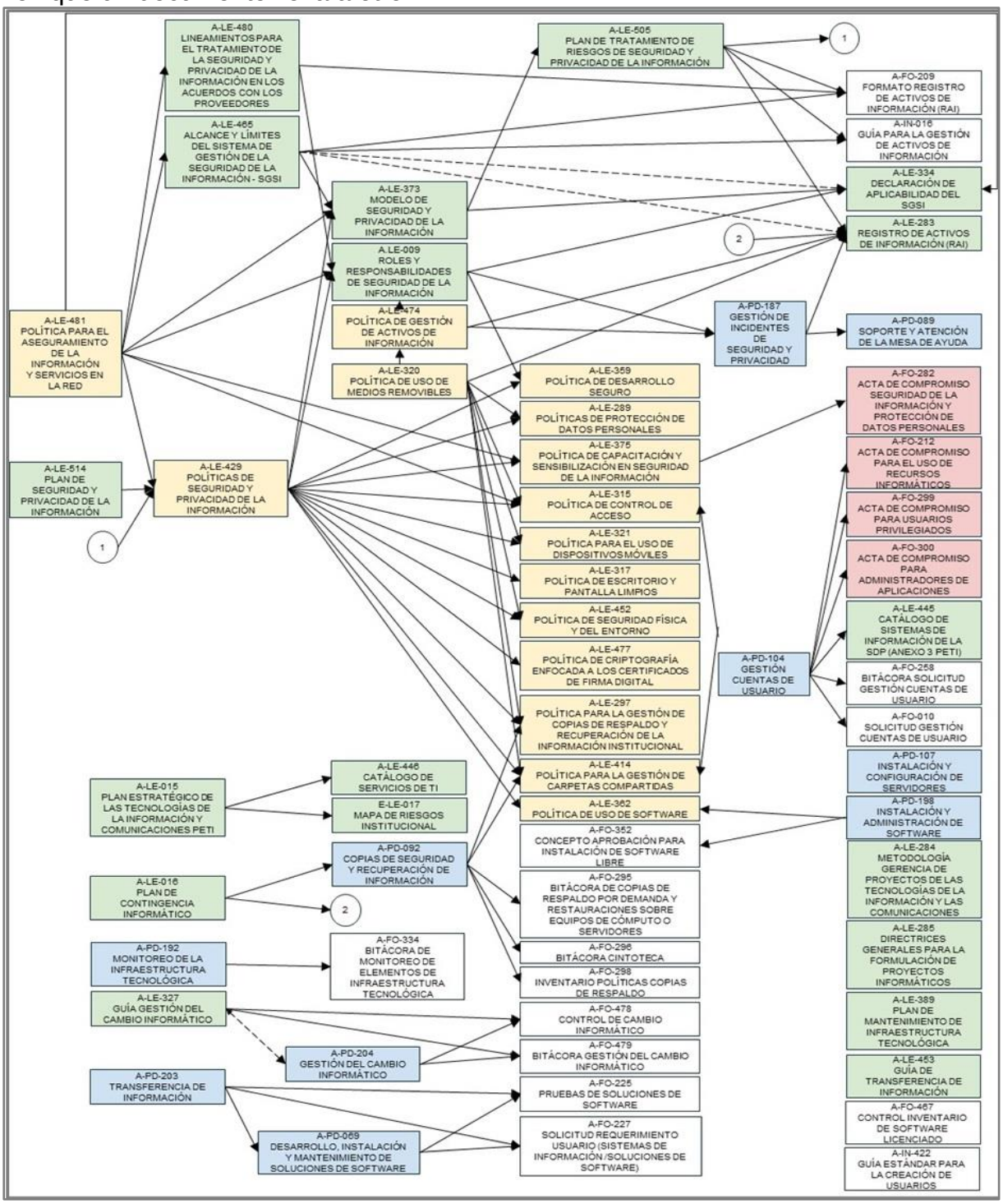
4. Resultados del informe

Para el desarrollo del seguimiento al MSPI se utilizaron diferentes técnicas de auditoría:

1. Solicitud de información a través de dos cuestionarios enviados a la Dirección de TIC de la SDP, y revisión de las respuestas y registros de evidencias recibidas en 44 carpetas que envió esta Dirección.
2. Verificación del cumplimiento normativo y de las Políticas a través del análisis de documentos y/o registros físicos y virtuales, 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, así como se consultó en el Sistema de Información de procesos automáticos -SIPA y en la página web de la entidad, las diferentes Políticas y procedimientos establecidos, así como el mapa de riesgos vigente.
3. Se realizaron tres reuniones con el Director TIC y su equipo
4. Se realizó visita al Datacenter de la entidad el cual se tiene a través de un convenio con la Secretaría Distrital de Hacienda.
5. Recorrido por todos los centros de cómputo ubicados en todos los pisos.
6. Recorridos para verificar de forma aleatoria hardware y software de la entidad.
7. Se efectuó prueba de verificación y recuperación de Backups
8. Muestreo en el Sistema de Información de procesos automáticos para verificar aplicabilidad de protección de datos personales.
9. Revisión de aplicabilidad de los 114 controles en la entidad del MSPI.

4.1 Políticas y Directrices Gobierno Nacional y Distrital

Los asuntos de la seguridad de la información están ampliamente documentados en el sistema de gestión de la entidad, al punto que generan una gigante red de consulta, toda vez que un documento lleva a otro.



Fuente: aplicativo SIPA

En la construcción de esta imagen, se encontró que el documento Gestión Cuentas de Usuario A-PD-104 Versión 12 acta de mejoramiento 289 de octubre 28 de 2022, vigente a la fecha, hace referencia en las observaciones generales a Lineamientos Operacionales TIC A-LE-398, el cual fue retirado del sistema de gestión mediante Acta de mejoramiento 409 de 30-Oct-2023

En la página 19 del Modelo De Seguridad y Privacidad de la Información de la SDP, A-LE-373, Versión 5 Acta de Mejoramiento 257 de Julio 27 de 2023, para el Plan de tratamiento de riesgos de seguridad de la información lo identifican con el código A-LE-515, pero en realidad se trata de A-LE-505

En el documento Plan de Seguridad y Privacidad de la Información de la SDP, A-LE-514 se estableció la tarea de actualizar el documento A-LE-283 / Registro de Activos de Información (RAI) a septiembre de 2023, no obstante, a la fecha de hoy sigue vigente el de octubre de 2022.

Si bien es cierto se destaca la permanente revisión y actualización de los documentos del MSPI, se recomienda analizar la posibilidad de reducir los documentos a) Unir los documentos de políticas para hacer uno solo de políticas TIC, en donde cada una de las actuales constituya un capítulo y B) Reducir los formatos en que se hacen compromisos, para que en uno solo la persona se comprometa con lo que haya a lugar en materia TIC.

Control A.5.1.1 Políticas de seguridad de la información

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 se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo.

Es así como la Seguridad y Privacidad de la Información es un habilitador de la Política de Gobierno Digital que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad 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.[1] Este habilitador se desarrolla a través

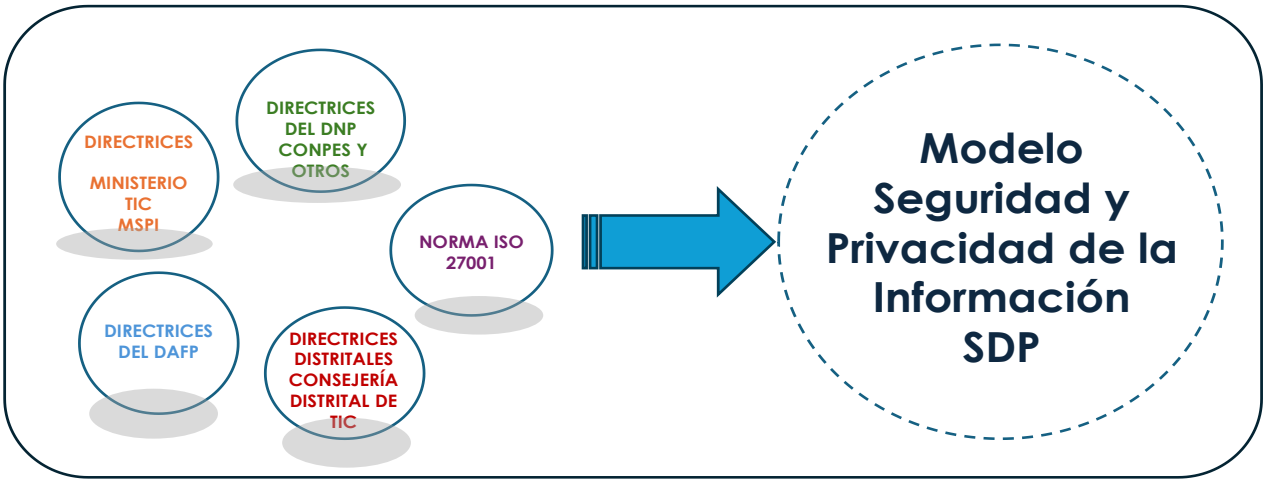
[1] Decreto 767 de 2022. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

del **Modelo de Seguridad y Privacidad de la Información**, que orienta la gestión e implementación de la seguridad de la información en el Estado.

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 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.

Se destaca que la Dirección de Tecnologías de Información y las Comunicaciones de la Secretaría Distrital de Planeación, viene 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

4.2 Resultados de la Medición del Desempeño Institucional MDI a través del reporte anual de información del Formulario Único de Reporte y Avance de Gestión FURAG

4.2.1Acciones en el 2023 frente a Resultados FURAG 2022

Se preguntó a la Dirección TIC si fueron tenidas en cuenta las sugerencias del DAFP sobre los resultados de la medición del desempeño 2022, frente a aquellos puntajes más bajos en la Política de Seguridad Digita y cuyos resultados fueron publicados en la evaluación FURAG de 2023:

Con el fin de contextualizar los resultados obtenidos en la medición del año 2022, realizada en la vigencia 2023, se detallan los resultados obtenidos por la Secretaría Distrital de Planeación en la Política de Seguridad Digital a continuación:

Política 08. Seguridad Digital: 82.7
Índices evaluados en la política:

No. Índice	POLÍTICA 8 Seguridad Digital	Puntaje
I21	Asiganción de Recursos	**76,04**
I22	Implementación Lineamientos de Política	**85,33**
I23	Despliegue de Controles	**80**

Frente a estos resultados la Dirección adelantó las siguientes acciones:

I21- Asignación de Recursos: Mide la capacidad de la entidad pública de asignar recursos para el despliegue de la Política de Seguridad Digital con el fin de proteger la información bajo su custodia.

En la vigencia 2023 se asignaron $5.474.855.473 equivalente al **7.40%** del presupuesto total de la entidad $74.005.092.765. La distribución de los recursos se dio en el marco del plan estratégico de Tecnologías de la Información y las Comunicaciones y el plan anual de adquisiciones.

I22 - Implementación Lineamientos de Política: Mide el cumplimiento de la entidad pública frente a la implementación de los lineamientos de política pública en materia de seguridad digital.

En Colombia, la política pública en materia de seguridad digital se encuentra enmarcada en el Decreto 1078 de 2015, también conocido como "Estrategia Nacional de Seguridad Digital". Este decreto establece los lineamientos generales para la creación de una cultura de seguridad digital en el país, con el objetivo de proteger la información y los sistemas de información de las entidades públicas y privadas contra amenazas internas y externas.

Los lineamientos de la Estrategia Nacional de Seguridad Digital se basan en los siguientes principios:

- Prevención: Enfocarse en prevenir las amenazas a la seguridad digital antes de que ocurran.
- Protección: Implementar medidas para proteger la información y los sistemas de información contra ataques.
- Detección: Identificar y detectar oportunamente las amenazas y los ataques a la seguridad digital.
- Respuesta: Responder de manera efectiva a los incidentes de seguridad digital.
- Recuperación: Restaurar la información y los sistemas de información afectados por incidentes de seguridad digital.

Para implementar estos principios, en la Secretaría Distrital de Planeación se realizaron las siguientes acciones:

- Inclusión de los temas de seguridad digital en el Comité Institucional de Gestión y desempeño logrando que esta instancia como representante de la Alta Dirección este comprometida con la gestión de la seguridad digital.
- Se fortalecieron las capacidades técnicas y humanas para enfrentar las amenazas a la seguridad digital.
- Se promovió la cultura de seguridad digital mediante sesiones de sensibilización a todos los servidores públicos, contratista y pasantes activos del Entidad sobre la importancia de la seguridad digital y promover buenas prácticas en el uso de las tecnologías de la información y la comunicación.
- Se destinaron recursos importantes para modernizar la infraestructura de seguridad digital necesaria para proteger los sistemas de información.
- Constante y fluida comunicación con la Alta Consejería de Transformación Digital Bogotá como aliado de la SDP para enfrentar las amenazas a la seguridad digital de manera conjunta.
- Se atienden los lineamientos formulados en las Normas que rige la seguridad digital en Colombia, entre ellos:

  Ley 1235 de 2008, también conocida como "Ley Anti-phishing y Anti-spam". Esta ley tiene como objetivo proteger a los usuarios de las tecnologías de la información y la comunicación contra prácticas abusivas, como el phishing, el spam y el malware. Establece las siguientes obligaciones para las entidades públicas y privadas:

  - Implementar medidas de seguridad para proteger la información de sus usuarios.
  - Notificar a las autoridades competentes sobre cualquier incidente de seguridad que afecte a sus usuarios.
  - Capacitar a sus empleados sobre seguridad digital.

Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Código Penal: Tipifica delitos informáticos como el acceso no autorizado a sistemas de información, la interceptación de datos y el fraude informático.

I23 - Despliegue de Controles: Mide las capacidades de la entidad para establecer e implementar puntos de control básicos para mitigar los riesgos de seguridad digital.

Con relación a este índice, realizó la identificación y valoración de riesgos, permitiendo determinar los controles que se aplican a cada riesgo asociando un plan de trabajo en el caso que los controles aplicados no logren mitigar o reducir el riesgo.

De acuerdo con lo descrito anteriormente, la SDP tuvo en cuenta las sugerencias del DAFP sobre los resultados de la medición del desempeño 2022, (evaluación FURAG de 2023), relacionados con la Política de Seguridad Digital. Así mismo, se incluyó en el plan de adquisiciones los bienes y servicios que permite mejorar y fortalecer la postura de seguridad de la entidad de acuerdo con las capacidades institucionales.

4.2.2. Resultados FURAG 2023

Las políticas de Gobierno Digital y de Seguridad Digital de la Secretaría Distrital de Planeación, para la vigencia 2023 obtuvieron los siguientes puntajes de acuerdo a la medición del Desempeño Institucional:

Resultados FURAG		
Política	**2022**	**2023**
POLÍTICA 7 Gobierno Digital	83,5	87,1
POLÍTICA 8 Seguridad Digital	82,7	82.3

Política de Gobierno Digital

La Política de Gobierno Digital busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TIC.[2]

[2] https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

POLÍTICA 7 Gobierno Digital	87,1	**i11.Gobernanza**	88,9
		i12.Innovación Pública Digital	88,9
		i13.Arquitectura	95,1
		i14.Seguridad y Privacidad de la información	69,6
		i15.Servicios Ciudadanos Digitales	0,0
		i16.Cultura y apropiación	100,0
		i17.Servicios y Procesos Inteligentes	42,9
		i18.Estado abierto	95,3
		i19.Decisiones basadas en datos	91,4
		i20.Proyectos de Transformación Digital	100,0
		i21.Estrategias de Ciudades y Territorios Inteligentes	100,0

Respecto a las 32 recomendaciones del DAFP sobre la Política de Gobierno Digital, se observa que algunas de ellas deben ser objeto de análisis por parte de la Dirección de TIC, pero de igual forma existen recomendaciones que son de resorte de otras Direcciones de la entidad.

Recomendaciones Política de Gobierno Digital

1. Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y tomar las medidas necesarias para evitar que se vuelvan a presentar
2. Aprobar y publicar la licencia de datos abiertos de la entidad, mediante la cual se determina el alcance, uso y aprovechamiento que los particulares o terceros interesados puedan efectuar sobre los mismos.
3. Aprobar, clasificar y actualizar mediante un proceso de mejora continua el inventario de activos de seguridad y privacidad de la información de la entidad.
4. Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).
5. Caracterizar los usuarios de los Otros Procedimientos Administrativos (OPAS) total o parcialmente en línea de la entidad.
6. Desarrollar conjuntos de datos abiertos estratégicos de la entidad en procesos de cocreación o consulta pública.
7. Digitalizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).
8. Disponer de un servidor con las características establecidas en el anexo 2 del Decreto 620 de 2020 para vincularse al servicio de interoperabilidad.
9. Disponer en línea los Otros Procedimientos Administrativos (OPAS) de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).
10. Disponer en línea los trámites de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).

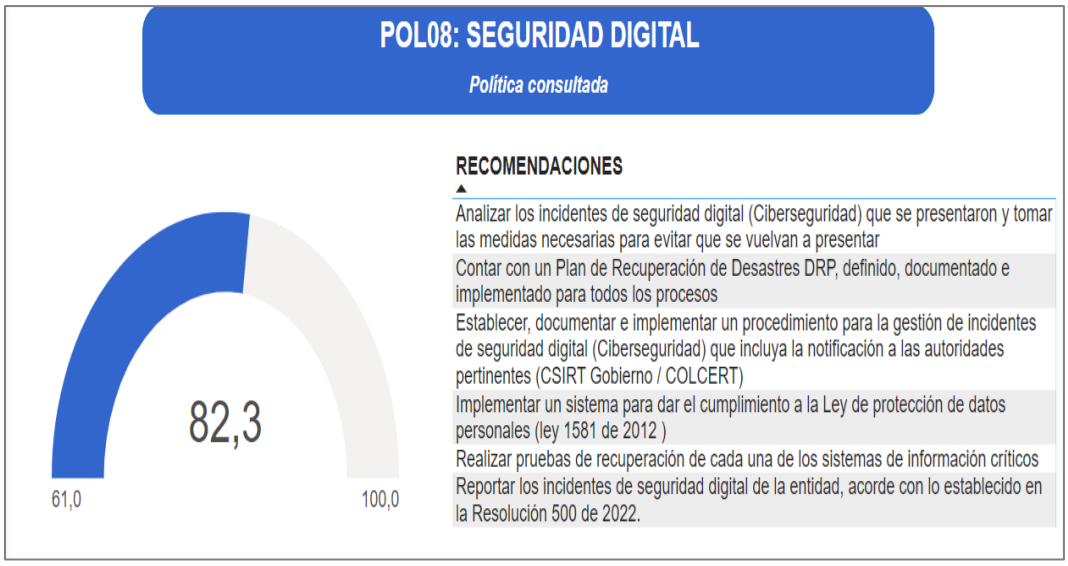
11. Disponer todos los documentos resultantes de los trámites de la entidad en la Carpeta Ciudadana Digital.
12. Ejecutar el proceso de Arquitectura Empresarial en la entidad.
13. Establecer instancias/dependencias de toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad, tales como el Comité de Gestión y Desempeño Institucional, la Oficina de Tecnologías de Información, la Oficina de Planeación, entre otras.
14. Evaluar la implementación de lineamientos en materia de datos en la entidad.
15. Evaluar las capacidades y competencias de la entidad con relación al uso y explotación de datos.
16. Habilitar funcionalidades que permitan a los usuarios hacer seguimiento en línea del estado de los Otros Procedimientos Administrativos (OPAS) total o parcialmente en línea de la entidad.
17. Implementar acciones para que los Otros Procedimientos Administrativos (OPAS) total o parcialmente en línea de la entidad cumplan con todos los criterios de usabilidad web.
18. Implementar acciones para que los Otros Procedimientos Administrativos (OPAS) total o parcialmente en línea de la entidad, cumplan con todos los criterios de accesibilidad web definidos en el anexo 1 de la Resolución 1519 de 2020.
19. Implementar el criterio de accesibilidad web 'CC3. Guion para solo video y solo audio' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.
20. Implementar el servicio de autenticación digital de los Servicios Ciudadanos Digitales en todos los trámites de la entidad que requieran verificar la identidad de sus usuarios.
21. Implementar estrategias de mejora de los conjuntos de datos publicados por la entidad para aumentar el número de usuarios satisfechos con su uso.
22. Implementar la técnica de 'análisis prescriptivo' para el análisis de datos de la entidad. El uso de esta técnica permite establecer cuál es la mejor acción a tomar bajo un contexto específico.
23. Realizar auditorías internas, externas y de certificación o recertificación respecto al estándar ISO 27001 en la entidad.
24. Realizar el reporte de la entidad en la herramienta habilitada por el Ministerio TIC para el seguimiento del avance en la adopción de IPv6.
25. Realizar pruebas de recuperación de cada uno de los sistemas de información críticos
26. Reportar los incidentes de seguridad digital de la entidad, acorde con lo establecido en la Resolución 500 de 2022.
27. Usar el servicio de Carpeta Ciudadana Digital para que la entidad reduzca el número de PQRSD, reduzca los tiempos de respuesta de los trámites, reduzca el consumo de papel necesario para dar respuesta a los trámites, entre otros.
28. Utilizar tecnologías emergentes de la cuarta revolución industrial para desarrollar procesos de innovación pública digital en la entidad, tales como tecnologías de desintermediación, DLT (Distributed Ledger Technology) como cadena de bloques (Blockchain) o contratos inteligentes; análisis masivo de datos (Big data); Inteligencia Artificial (AI); Internet de las Cosas (IoT); robótica y similares; realidad aumentada o realidad virtual; automatización robótica de procesos; entre otras.

29. Vincular a X-ROAD todos los servicios de intercambio de información requeridos para la realización de Otros Procedimientos Administrativos (OPAS) de la entidad.
30. Vincular a X-ROAD todos los servicios de intercambio de información requeridos para la realización de trámites de la entidad.

Política de Seguridad Digital

POLÍTICA 8 Seguridad Digital	82.3	**i22.Asiganción de Recursos**	80,0
		i23.Implementación Lineamientos de Política	78,1
		i24.Despliegue de Controles	100,0

Recomendaciones Política de Seguridad Digital



4.3 Nueva versión de la Norma ISO 27001:2022

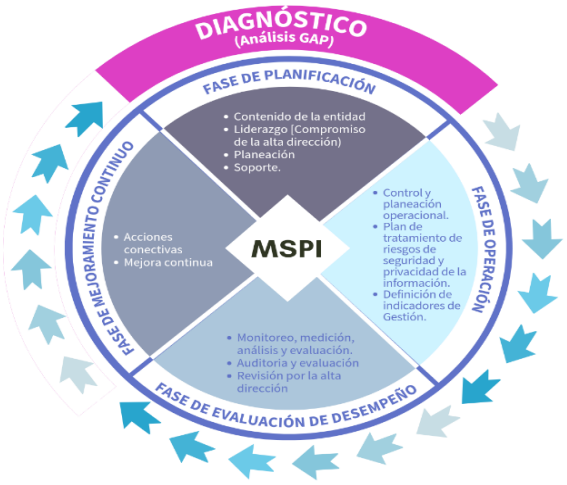
Respecto a la transición de la norma ISO 27001 hacia la versión 2022 la Dirección de TIC informó al equipo auditor que a partir del mes de abril de 2023 inició con la revisión de los cambios que presenta la nueva versión de la ISO 27001, fecha del primer seguimiento del Plan Operativo Anual (POA) 2023, Meta 5 Gobierno Digital, Actividad 5.3. Formular el Plan de Controles SGSI vigencia 2023, ejecutar y hacer seguimiento.

Así mismo, se observó que la Dirección TIC respecto a la implementación de la norma ISO 27001 no realizó ninguna exclusión y cuenta con el documento Declaración de Aplicabilidad del SGSI en la SDP, la cual incluye el listado de los 114 controles del Anexo-A de la ISO/IEC 27001 versión 2013 agrupados en 14 dominios y 35 objetivos de control, sobre el cual se relacionan los controles aplicables a la Entidad.

4.4 CICLO DE OPERACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El ciclo de operación del Modelo de Seguridad y Privacidad de la Información-MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC comprende cuatro etapas a saber: Planificación, Operación, Evaluación Del Desempeño y Mejora Continua

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

4.4.1 FASE DE DIAGNÓSTICO- Resolución 500 de 2021 de MINTIC

Se evidenció por parte del equipo auditor que la Dirección TIC realizó dos diagnósticos en la vigencia 2023, uno en el mes de junio y otro en el mes de diciembre.

Autodiagnóstico Controles Primer semestre de 2023

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	91	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	89	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	89	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	92	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	92	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	73	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	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	66	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFECTIVO
A.18	CUMPLIMIENTO	76,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**78**	**100**	GESTIONADO

Fuente: Dirección de TIC. Instrumento de Identificación de la Línea Base MSPI. 2023

Autodiagnóstico Controles segundo semestre de 2023

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	91	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	86	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	91	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	92	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	92	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	68	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	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	71	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	73,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**79**	**100**	GESTIONADO

Fuente: Dirección de TIC. Instrumento de Identificación de la Línea Base MSPI. 2023

Se observó que los aspectos que obtuvieron **menos puntaje fueron: Criptografía, Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio, y Gestión de Incidentes de Seguridad de la Información.**

En el instrumento de evaluación del MPSI presentado por la Dirección de TIC como único documento del autodiagnóstico a diciembre de 2023, se encuentra un Excel que tiene por encabezado “Instrumento de Identificación de la Línea Base de Seguridad Administrativa y Técnica”. Allí hay una hoja dedicada al análisis de la madurez de los diferentes requisitos a partir de su clasificación en los siguientes niveles:

Nivel 1: Inicial
Nivel 2: Gestionado
Nivel 3: Definido
Nivel 4: Gestionado Cuantitativamente
Nivel 5: Optimizado

En dicho análisis se observa que los requisitos avanzan de la siguiente manera:

- 16 cumplen (R1, R2, R3, R4, R6, R7, R8, R13, R23, R24, R25, R28, R45, R46, R47, R53)
- 04 en avance mayor (R41, R42, R48, R55)
- 34 en avance menor (R5, R9, R10, R11, R12, R14, R15, R16, R17, R18, R19, R20, R21, R22, R26, R27, R29, R30, R31, R32, R33, R34, R35, R36, R37, R38, R39, R40, R43, R44, R49, R50, R51, R52)
- 1 con avance sin clasificar

En el que se clasifica el CUMPLIMIENTO del NIVEL 5 OPTIMIZADO como “menor”, hay 28 que están calificados con 100 (R5, R9, R10, R11, R12, R14, R15, R16, R17, R18, R19, R20, R21, R22, R26, R27, R29, R30, R31, R32, R33, R34, R35, R36, R37, R38,

R39, R40), razón por la cual no es claro la razón por la que se clasificó como avance menor, igual que los que obtuvieron calificación de 80.

Del mismo modo, no se hizo la clasificación del R41, pese a que en el nivel 5 logró una calificación de 80.

De otro lado, los niveles fueron clasificados así:

- Nivel 1: Inicial……..Menor
- Nivel 2: Gestionado…… Menor
- Nivel 3: Definido…… Menor
- Nivel 4: Gestionado Cuantitativamente… Menor
- Nivel 5: Optimizado……Cumple

Se observa una imprecisión ya que no es claro cómo el último nivel se haya cumplido si los niveles anteriores no.

Dentro del avance de las fases del Modelo de Seguridad y Privacidad, se tiene el siguiente avance en la entidad:

Año	AVANCE PHVA		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2023	Planificación	37%	40%
	Implementación	17%	20%
	Evaluación de desempeño	17%	20%
	Mejora continua	16%	20%
TOTAL		**88%**	**100%**

Fuente: Dirección de TIC 2023

Respecto a los temas de Ciberseguridad la entidad atiende de igual forma el Modelo framework ciberseguridad NIST (Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de EE. UU.), el cual es un marco de referencia que las entidades públicas están adoptando de forma voluntaria. Los resultados del autodiagnóstico arrojaron los siguientes resultados:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	79	100
DETECTAR	69	100
RESPONDER	78	100
RECUPERAR	80	100
PROTEGER	82	100

Fuente: SDP-Dirección TIC 2023

Nivel de madurez MSPI a Diciembre 2023

De conformidad con el resultado final del Autodiagnóstico del MSPI a Diciembre 2023, el nivel de madurez se encuentra en el nivel **Gestionado**, de acuerdo a la valoración de los controles, Anexo A de la norma ISO 27001.

Lo anterior significa que los controles definidos permiten monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción de mejora continua.

Tabla de Escala de Valoración de Controles		
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.

4.4.2 FASE DE PLANIFICACIÓN

4.4.2.1 Liderazgo y Compromiso

Se evidenció por parte del equipo auditor que la Dirección de Tecnologías de la Información y las Comunicaciones de la Secretaría Distrital de Planeación elaboró y/o actualizó los documentos necesarios que exige el Modelo de Seguridad y Privacidad de la información que dan cuenta de:

- El Alcance del Modelo de Seguridad y Privacidad de la Información- MSPI
- El acto administrativo con las funciones de seguridad y privacidad de la información.
- La Política de seguridad y privacidad de la información.

- El documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.
- El procedimiento de inventario y clasificación de la Información e infraestructura crítica.
- El inventario y clasificación de la información e infraestructura crítica.
- El procedimiento de gestión de riesgos de seguridad de la información.
- El plan de tratamiento de riesgos de seguridad de la información.
- La Declaración de aplicabilidad.
- El Manual de políticas de Seguridad de la Información.
- El Plan de capacitación y sensibilización en seguridad de la información.

4.4.2.2 Políticas relacionadas con el Modelo de seguridad y privacidad de la información

Control A. 5.1.1

De igual manera, se evidenció que como compromiso de la Alta Dirección fue aprobada la actualización de las políticas que hacen parte del Modelo de Seguridad y Privacidad de la Información en Comités de Gestión y Desempeño-CIGD, cuyas actas fueron revisadas por el equipo auditor:

Sesión CIGD del 22 de septiembre de 2023:

A-LE-465 Alcance y Límites del Sistema de Gestión de la Seguridad de la Información – SGSI
A-LE-315 Política de Control de Acceso.
A-LE-317 Política de Escritorio y Pantalla Limpios.
A-LE-334 Declaración de Aplicabilidad del SGSI en la SDP.
A-LE-362 Política de uso de software
A-LE-320 Política de uso de medios removibles

Sesión CIGD del 22 de septiembre y 15 de noviembre de 2023:

A-LE-321 Política para el uso de dispositivos móviles en la SDP
A-LE-375 Política de capacitación y sensibilización en seguridad de la información en la SDP
A-LE-429 Políticas de seguridad y privacidad de la información
A-LE-474 Política de gestión de activos de información

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

De acuerdo con lo expuesto anteriormente, se evidenció que la Secretaría Distrital de Planeación durante la vigencia 2023 en cumplimiento de las directrices del Gobierno Nacional y Distrital:

1. Elaboró autodiagnósticos del Modelo con corte junio y diciembre de 2023, los cuales fueron revisados, socializados y aprobados por el Comité Institucional de Gestión y Desempeño.
2. Aplicó lo establecido en la Resolución 500 de 2021, en cuanto a la construcción y/o actualización de las políticas e instrumentos del Sistema de Gestión de Seguridad de la Información SGSI . Base para la operación del Modelo de Seguridad y Privacidad de la Información.
3. En cumplimiento del Decreto 612 de 2018 del 2023, elaboró y publicó los documentos exigidos por esta norma.

4.4.2.4 Soporte/Recursos necesarios

4.4.2.4.1 Control A.12.1.3 Gestión de capacidad

De acuerdo con los lineamientos del Ministerio de las TIC a través del Manual del MPSI (basado en la norma 27001) y la Resolución 500 de 2021; *"(…)se deben determinar y proporcionar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información"*.[3]

La implementación del Modelo de Seguridad y Privacidad de la Información MSPI, es un tema transversal y de alto impacto para la Secretaría Distrital de Planeación, máxime cuando es la entidad distrital que maneja información de impacto para la planeación territorial, económica y social de la ciudad.

El tema de asignación de recursos tuvo una alta incidencia en la evaluación y calificación de la Política de Seguridad Digital realizada a través del instrumento FURAG.

Se pudo evidenciar por parte del equipo auditor que, como compromiso de la Alta Dirección, hubo una mejora significativa en la asignación de los recursos para el Sistema de Gestión de la Seguridad de la Información – SGSI, en comparación con la vigencia 2022.

Es así como para la vigencia 2023, fueron asignados $ 5.474.852.226,50 recursos a los temas de seguridad digital, los cuales representaron el 7.40% del total del presupuesto de la entidad.

[3] Ministerio de las TIC. Resolución 500 de 2021

Recursos asignados al SGSI en la vigencia 2023

CONTRATOS 2023	OBJETO		Valor Principal	Valor Adición 1	Valor Adición 2	Total
CTO 72	PRESTAR SERVICIOS PROFESIONALES DE APOYO A LA DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES EN LAS ACTIVIDADES REQUERIDAS PARA EL MANTENIMIENTO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMPLEMENTADO EN LA SDP.	Yadir Molina	98.900.000,00			98.900.000,00
CTO 759	RENOVAR EL SERVICIO DE CERTIFICADOS DE SERVIDOR SEGURO	CERTICAMARA S.A.	69.998.767,00			69.998.767,00
CTO 764	ADQUISICION DE CERTIFICADOS DE FIRMA DIGITAL PARA LOS SERVIDORES PUBLICOS DE LA SDP.	GESTION DE SEGURIDAD ELECTRONICA SA	11.888.100,00			11.888.100,00
CTO 603	RENOVACION DE GARANTIAS Y SOPORTE TECNICO PARA LOS EQUIPOS DE SEGURIDAD PERIMETRAL FIREWALL	SAFETY IN DEEP SAS	126.090.300,00			126.090.300,00
CTO 71	PRESTAR SERVICIOS PROFESIONALES DE APOYO A LA DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PARA LA OPERACIÓN DE LAS HERRAMIENTAS DE ADMINISTRACION DE SEGURIDAD INFORMATICA Y ACTIVIDADES DE ASEGURAMIENTO DE LA CONECTIVIDAD DE LA SDP.	Henry Cepeda	84.900.000,00	8.490.000,00	8.490.000,00	101.880.000,00
CTO 760	RENOVACION DE GARANTIAS Y SOPORTE TECNICO DE LA SOLUCIÓN INTEGRADA PARA LA GESTION DE SEGURIDAD Y PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN Y/O APLICACIONES DE LA SDP	GAMMA INGENIEROS S.A.S.	208.218.000,00			208.218.000,00
CTO 148	PRESTAR SERVICIOS PROFESIONALES A LA DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PARA APOYAR EN LAS ACTIVIDADES TECNICAS DE GESTIÒN Y CONTROL DE LOS SISTEMAS OPERATIVOS DE LA INFRAESTRUCTURA TECNOLOGICA DE LA SDP.	Fredy Salinas	81.366.000,00			81.366.000,00
CTO 70	PRESTAR SERVICIOS PROFESIONALES A LA DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES PARA APOYAR EN LAS ACTIVIDADES TECNICAS DE GESTIÒN Y CONTROL DE LAS BASES DE DATOS SQLSERVER DE LA INFRAESTRUCTURA TECNOLOGICA DE LA SDP.	HECTOR MILLER PATIÑO GARZON	92.000.000,00			92.000.000,00
CTO 721-2023	PRESTAR SERVICIOSESPECIALIZADOS ACS DE LOS PRODUCTOSORACLE DE PROPIEDAD DE LA SDP	IAD Software I - Oracle	40.232.688,33			40.232.688,33
OC 119578 CTO 744-2023 (2)	REALIZAR LAS ACTIVIDADES DEMIGRACIÓN DE SERVICIOS DE LA SDP A LA NUBEY DE LA OPERACIONALIZACION DEL PLAN DERECUPERACION DE DESASTRES - DRP -PROCESO 42	Oracle	438.713.657,85			438.713.657,85
Orden de Compr_381-2023	PRESTAR EL SERVICIO DEACTUALIZACIÓN Y SOPORTE TÉCNICO DE LOSPRODUCTOS ORACLE PROPIEDAD DE LA SDPPROCESO 167. Propuesta No. SPS-FY23-022 (Cap.1 – 3192316, Cap. 2 – 17538982)	ORACLE	1.221.853.536,00			1.221.853.536,00
Cto_589_SystemDigital	PRESTAR EL SERVICIO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS DE CÓMPUTO PROPIEDAD DE LA SDP, CON REPOSICIÓN DE ELEMENTOS	SystemDigital	500.000.000,00			500.000.000,00
CTO 698 DE 2023	SOPORTE TECNICO PARA LOS SERVIDORES, LIBRERIA Y EQUIPOS DE CONECTIVIDAD DE LA SDP.	UT PENTATEK-SOPORTCOL	233.178.688,00			233.178.688,00
542 DE 2023	RENOVACION DE GARANTIAS Y SOPORTE TECNICO DEL SISTEMA DE ALMACENAMIENTO DE LA SDP	REDCOMPUTO LTDA.	103.069.938,00			103.069.938,00
CONTRATO 712-2023	SERVICIO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DEL SISTEMA DE CONTROL DE ACCESO CON REPUESTOS	IDEAS CONTROL EQUIPOS Y SOLUCIONES S.A.S.	25.807.000,00			25.807.000,00
CONTRATO No. 680 DE 2023	PRESTAR EL SERVICIO DE MANTENIMIENTO PREVENTIVO CORRECTIVO CON SUMINISTRO DE REPUESTOS A LOS EQUIPOS DE AIRE ACONDICIONADO PROPIEDAD DE LA SDP.	TERMEC LIMITADA	10.423.000,00			10.423.000,00
CONTRATO No. 713 DE 2023	PRESTACIÓN DE SERVICIOS OBJETO: PRESTAR EL SERVICIO DE GUARDA CUSTODIA Y TRANSPORTE DE MEDIOS MAGNÉTICOS Y DOCUMENTOS DE LA SDP.	GRUPO TIEDOT SAS	5.997.788,00			5.997.788,00
CONTRATO 724-2023	PRESTAR EL SERVICIO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO AL SISTEMA DE	GRUPO CONEXION COLOMBIA	7.185.402,00			7.185.402,00
CONTRATO No. 730 _DE 2023	RENOVACIÓN DE GARANTÍAS Y SOPORTE TÉCNICO PARA LOS EQUIPOS DE BALANCEO DE	GAMMA INGENIEROS SAS	67.398.510,00			67.398.510,00
CONTRATO Nº 762 de 2023	ADQUIRIR, IMPLEMENTAR Y PONER EN OPERACIÓN EL SOFTWARE PARA SOPORTAR Y	ISOLUCION SISTEMAS	197.999.999,00			197.999.999,00
CTO No. 740 DE 2023	ADQUIRIR LICENCIAMIENTOBASE PARA SOPORTAR LA INFRAESTRUCTURATECNOLÓGICA DE	NOVENTIQ	226.497.980,32			226.497.980,32
CTO INTERADMINISTRATIVO 536-2023-Minuta CI SDP-V2 (1)	PROVEER LOS SERVICIOS INTEGRADOS DE COMUNICACIONES PARA LA SDP	EMPRESA DE TELECOMUNICACIONES DE BOGOTA S.A. E.S.P. – ETB S.A. E.S.P.	644.172.872,00			644.172.872,00
CTO-692-2023	SOLUCIÓN DE ALMACENAMIENTO NAS- SAN (20T), el presupuesto oficial para este ITEM 1, es de SEISCIENTOS SETENTA Y TRES MILLONES NOVECIENTOS NOVENTA MIL PESOS MONEDA CORRIENTE ($673.990.000) incluido IVA. ITEM 2: SOLUCIÓN DE COMUNICACIONES – RED FIBER CHANNEL, el presupuesto oficial para este ITEM 2, es de DOSCIENTOS OCHENTA Y SIETE MILLONES NOVECIENTOS NOVENTA MIL PESOS MONEDA CORRIENTE ($287.990.000) incluido IVA.	REDCOMPUTO LIMITADA	961.980.000,00			961.980.000,00
TOTAL			5.457.872.226,50	8.490.000,00	8.490.000,00	5.474.852.226,50

Fuente: Dirección de TIC 2023

4.4.2.4 .2 Talento Humano

Respecto al Talento Humano, para la seguridad de información, el equipo auditor preguntó a la Dirección de TIC cuáles fueron las acciones adelantadas en la vigencia 2023 para mejorar los perfiles y/o contar con expertos en seguridad de la información, seguridad informática, en programación, analítica de datos, innovación pública y en las nuevas herramientas de la Cuarta Revolución Industrial (big data, blockchain, inteligencia artificial, entre otras), encaminados a mejorar los servicios que presta la entidad y lograr y avanzar en la transformación digital de la entidad.

En respuesta al cuestionario enviado por el equipo auditor, la Dirección TIC envió una relación de contratos suscritos con los siguientes perfiles:

Relación de contratos para fortalecer temas del Sistema de Gestión de la Seguridad de la Información

No.	Contrato #	Experticia
1	180/2023	Programación
2	181/2023	Programación
3	147/2023	Programación
4	71/2023	Seguridad Informática
5	342/2023	Programación
6	70/2023	Seguridad Informática
7	72/2023	Seguridad de la Información
8	148/2023	Seguridad Informática
9	810/2022 Ejecutado 2023	Nube Pública

Fuente: Dirección de TIC en respuesta al cuestionario enviado por el equipo auditor.

No obstante lo anterior, **se recalca la necesidad de capacitar al equipo de planta de la Dirección TIC** en los temas propios de su misionalidad, entre los cuales se encuentran seguridad de la información, seguridad informática, programación, analítica de datos, innovación pública y en las nuevas herramientas de la Cuarta Revolución Industrial, así como en las aplicaciones ofimáticas que incluyen desde los procesadores de texto y software para generar y administrar bases de datos, hasta los sistemas informáticos y dispositivos inteligentes que automatizan los procesos de la entidad. Esto en concordancia con la nueva Política de Gobierno Digital Decreto Nacional 767 de 2022.

Se identificó por parte del equipo auditor, que ante el cambio de la plataforma Gmail a Outlook, el equipo humano de la Dirección TIC no contó con la capacitación previa necesaria para atender una adecuada gestión del cambio en el tema y los requerimientos propios de las dependencias y funcionarios, a pesar de haberlo solicitado mediante la encuesta que hace anualmente la Dirección de Talento Humano para la formulación del Plan Institucional de Capacitación (PIC), este último orientado a fortalecer los saberes, actitudes, habilidades, destrezas y conocimientos de los servidores públicos.

4.4.2.5 Roles y responsabilidades MSPI

Control A.6.1.1

El equipo auditor verificó que los roles y responsabilidades de seguridad de la información se encuentran establecidos entre otros documentos en:

- La Resolución 1923 de 2022, “Por la cual se dictan otras disposiciones relacionadas con el Sistema de Gestión SG-MIPG de la Secretaría Distrital de Planeación y se deroga la Resolución 0998 de 2021”, Artículo 7en la cual se encuentran establecidas las responsabilidades del Comité relacionadas con la política de Seguridad Digital de la Entidad.

- La Resolución 1771 de 2018, expedida por la SDP, "*por la cual se establecen los responsables de la Política de Gobierno Digital"*

- Documento Roles y Responsabilidades de Seguridad de la Información en la SDP (A-LE-009), actualizado en agosto de 2023, en el cual se encuentran asignadas las responsabilidades a los siguientes actores: Comité Institucional de Gestión y Desempeño de la SDP, Representante de la Alta Dirección, Líder de la Política de Seguridad Digital, Oficial de Seguridad y Privacidad de la Información, Líder de Seguridad Informática, Administrador de herramientas de colaboración, Líder de Seguridad Física y Gestión Documental, Líder Técnico del equipo de Desarrollo, Líder de Talento Humano, Líder de Contratación, Asesor Legal, Dueños de la Información, Usuario de la Información, Auditor, Líder y responsable del Control Disciplinario.

4.4.2.6 Competencia, toma de conciencia y comunicación Control A.7.2.2

El artículo 5 de la estrategia de seguridad digital de la Resolución 500 de 2021 en su numeral 4 menciona que se debe "Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces"

Y en el Modelo de Seguridad y Privacidad de la Información. Dominio A7 Seguridad De Los Recursos Humanos 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."

Se pudo verificar que la Dirección de Tecnologías de la Información y Comunicaciones de la SDP, ha venido ejecutando anualmente la Política de Capacitación y Sensibilización en Seguridad de la Información en la SDP A-LE-375, y en la vigencia 2023 fue aprobada su actualización mediante Acta 435 del 16 de noviembre de 2023.

De otra parte, la Declaración de Aplicabilidad del SGSI en la SDP se interrelaciona con la aplicación del control, especificando que se ejecuta a través del plan de sensibilización y capacitación.

En el marco de la implementación del Plan de Seguridad de la Información, en el Plan de Sensibilización y Capacitación fueron incluidas y ejecutadas seis estrategias a saber:

Estrategia 1 - Sesiones de sensibilización.
Estrategia 2 - Campañas de Seguridad y Privacidad de la Información.
Estrategia 3 - Píldoras de Seguridad y Privacidad de la Información.

Estrategia 4 - Encuesta en Seguridad y Privacidad de la Información.
Estrategia 5 - Socialización Políticas, Guías e Instrumentos que componen el SGSI.
Estrategia 6 - Boletines con temas de actualidad en Seguridad y Privacidad de la Información.

Se destaca por parte del equipo auditor, que la Dirección de TIC ejecutó al 100% el Plan de sensibilización en seguridad de la información a 31 de diciembre de 2023.

4.4.3 FASE OPERACIÓN

El MSPI establecido a través de la Resolución 500 de 2021, establece que la Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Y se debe contar con:

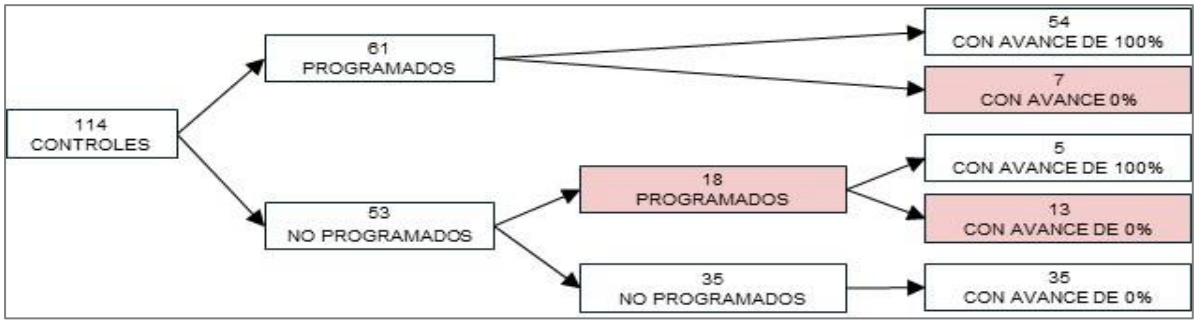
- Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto.
- Evidencia de la implementación de los controles de seguridad y privacidad de la información.

4.4.3.1 PLAN DE ACCIÓN IMPLEMENTACIÓN DE CONTROLES DEL MSPI 2023

De acuerdo con la información proporcionada por la Dirección de TIC, en la vigencia 2023 la ejecución del plan de acción de controles del MSPI alcanzó el 100%, y ningún control de la norma 27001 base del Modelo de Seguridad y Privacidad de la Información fue excluido.

<u>Situación crítica:</u>

Sin embargo, se identificó por parte del equipo auditor que en el documento Excel Plan de acción de controles del MSPI, con título implementación de controles 2023, existe dificultad para conocer con precisión el nivel de implementación de controles del MPSI para la vigencia 2023.



Fuente: Análisis propio a partir de los datos entregados por la Dirección de TIC en el documento de Implementación de Controles 2023

Se observó que no hay coherencia entre algunas de las actividades programadas, las fechas programadas, y el porcentaje de avance. Así mismo, se encontró que:

- Cincuenta y cuatro(54) controles tienen en la columna de avance una calificación de 0%. Dentro de las actividades en este grupo se encuentra: *"Actualizar el inventario de activos de información en los 15 procesos de la SDP para la vigencia 2023".*
- El control de "Seguridad en los procesos de desarrollo y soporte", tiene ejecución del 11%.
- El control "Responsabilidad por los activos" tiene ejecución del 25%.
- El control "Registro y seguimiento" encaminado a Registrar eventos y generar evidencia, tiene ejecución del 33%.
- El control "Gestión de la vulnerabilidad técnica" tiene ejecución del 50%.
- El control de "Equipos" encaminado a Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización tiene ejecución del 56%.
- Los controles "Organización interna" (Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización) y "Áreas seguras" (Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización), presentaron cada uno una ejecución del 60%.
- Los controles "Clasificación de la información" y "Procedimientos operacionales y responsabilidades" presentaron ejecución del 67%
- 53 controles de 114 tienen la observación "no se programa para la vigencia 2023. En otros casos la acción está prevista para la vigencia 2024 pero con ejecución 100% en el 2023 , por ejemplo:

  "*GENERAR ACCION Para la vigencia 2024*" y con ejecución del 100%. *"Revisar en 2024 que en el procedimiento para dar de baja o reutilización de los equipos se realice borrado seguro*": ejecución 100%

  "GENERAR ACCIONES. Para 2024 revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información" ejecución 100%

  "Para el 2024, revisar controles para protegerse contra códigos maliciosos" Ejecución 100%

- En algunas actividades no son claras las observaciones que menciona que no se programan, pero que se ejecutan en la entidad. Por ejemplo:

  Control A.12.1.1 Procedimientos de operación documentados: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
  Observación de la DTIC: ***No Se Programan Actividades*** Subrayado y resaltado nuestro.

Control A.12.1.3 Gestión de capacidad: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura
Observación de la DTIC: ***No se programa para 2023*** Subrayado y resaltado nuestro.

La Dirección TIC debe hacer seguimiento en cada vigencia del Plan de Controles, además con la realización del anteproyecto de presupuesto compuesto por metas, actividades, recursos e indicadores necesariamente se debe hacer seguimiento a la ejecución de los recursos y al logro de los objetivos; adicionalmente se cuenta con el PETI como Hoja de Ruta y Alineación 2020-2024, documento en el cual se hace análisis de la capacidad y se hacen proyecciones. Como se puede evidenciar es un control que, si se ejecuta, prueba de ello es el incremento del presupuesto para mejorar la capacidad de la seguridad de la información de la entidad.

Frente a la Situación Crítica No 3 identificada en la Auditoria, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Reconocemos la importancia de la claridad y precisión en la presentación de los datos relacionados con la implementación de los controles de seguridad. Entendemos que las inconsistencias identificadas puedan generar inquietudes sobre el avance real de nuestro plan. Sin embargo, consideramos que la calificación de "0%" asignada a los controles sin actividades programadas en la vigencia 2023, así como la programación de algunas actividades para el año siguiente, se realizó de manera intencional y con base en una evaluación rigurosa de las prioridades y recursos disponibles.

La priorización de los controles en nuestro Plan de Acción se basa en una evaluación integral que considera factores como el nivel de madurez de cada control y se priorizan aquellos que requieren mayor atención o implementación.

Los controles que fueron asignados con un porcentaje de ejecución de 0% corresponde a que no se programaron actividades específicas para ellos en la vigencia 2023. Sin embargo, esto no implica que no se estén llevando a cabo acciones relacionadas con estos controles. Por ejemplo, algunos controles pueden estar integrados en otros procesos o pueden ser abordados de manera continua a través de actividades de mantenimiento.

La programación de algunas actividades para el año 2024 se realizó considerando la disponibilidad de recursos y la complejidad de las mismas. Además, se busca garantizar una implementación gradual y sostenible de los controles.

En relación con la observación planteada sobre los controles programados para la vigencia 2024 pero con una ejecución reportada del 100% en 2023, la Dirección de TIC presenta la siguiente aclaración:

La aparente inconsistencia se debe a la forma en que se interpretan las acciones programadas para el año siguiente. Al indicar que una acción se "generará" o se "revisará" en 2024, lo que se está comunicando es que la definición detallada de las actividades específicas y los plazos para su ejecución se establecerán durante ese año. Al programar acciones para el año siguiente, estamos adoptando una perspectiva estratégica que nos permite alinear nuestros esfuerzos con los objetivos a largo plazo de la entidad y con los recursos disponibles, permitiendo adaptar las acciones a las necesidades cambiantes y a los nuevos desafíos que puedan surgir.

En el caso del control "Generar acciones para el 2024", lo que se ha hecho es identificar la necesidad de realizar ciertas acciones en el futuro, pero aún no se han definido los pasos específicos a seguir. Al indicar

un avance del 100%, estamos señalando que la necesidad ha sido reconocida y que se ha incluido en la planificación estratégica, el hecho de que una acción esté programada para el 2024 y tenga un avance del 100% en ese mismo año significa que:

- *Se ha identificado la necesidad de realizar la acción.*
- *Se ha incluido la acción en el plan de trabajo.*
- *La definición detallada de las actividades y los plazos se realizará durante el año 2024.*

En relación con la observación sobre los controles A.12.1.1 y A.12.1.3, donde se indica que no se programaron actividades específicas, pero que se ejecutan acciones relacionadas dentro de la gestión de la Dirección de TIC, presentamos la siguiente aclaración:

Es cierto que para estos controles no se definieron actividades puntuales en el plan de acción de 2023. Sin embargo, es importante destacar que muchas de las acciones relacionadas con estos controles se llevan a cabo como parte de las operaciones diarias de la Dirección de TIC y están integradas en otros procesos. Actividades como la documentación de procedimientos y la gestión de la capacidad son procesos continuos que se realizan de manera regular como parte de las operaciones normales de la Dirección de TIC. Aunque no se hayan definido proyectos específicos para estos controles en el plan de acción, se realizan acciones para mantenerlos actualizados y garantizar el cumplimiento de los requisitos; así mismo, muchas de las actividades relacionadas con estos controles están integradas en otros procesos de la Dirección de TIC, como la gestión de cambios, la resolución de incidentes y el mantenimiento de sistemas.

Es de resaltar que la Dirección de TIC prioriza la atención a los riesgos más críticos y asigna recursos en función de su impacto potencial. En algunos casos, los controles que no presentan un riesgo inmediato pueden no ser priorizados para acciones específicas en un año determinado, pero se mantienen bajo vigilancia, por ejemplo:

- *Control A.12.1.1 Procedimientos de operación documentados: Si bien no existe un proyecto específico para documentar todos los procedimientos de operación en un año determinado, la Dirección de TIC se asegura de que los procedimientos críticos estén documentados y actualizados a medida que se realizan cambios en los sistemas o procesos.*

- *Control A.12.1.3 Gestión de capacidad: La gestión de la capacidad es una actividad continua que se realiza como parte de la administración de los sistemas. La Dirección de TIC monitorea el uso de los recursos, realiza ajustes cuando es necesario y planifica futuras ampliaciones de capacidad.*

Si bien es cierto que no se programó una actividad específica en el plan de acción para actualizar el inventario de activos de información en los 15 procesos de la SDP durante la vigencia 2023, la Dirección de TIC llevó a cabo esta importante tarea y publicó el inventario actualizado en la página web institucional: https://www.sdp.gov.co/transparencia/datos-abiertos/instrumentos-gestion-info/registro-de-activos-de-Informacion.

El archivo "registroactivosinformacion_2023" que se encuentra disponible en el enlace mencionado, constituye una evidencia tangible de que se ha cumplido con el requerimiento de actualizar el inventario. Este archivo forma parte de los soportes proporcionados para sustentar la situación crítica 3 y puede ser consultado para verificar la información contenida (Se adjunta archivo en Excel "registroactivosinformacion_2023"),

En cuanto al control "Gestión de la vulnerabilidad técnica", aclaráramos que la ejecución de este control fue del 100%. A pesar de que en el informe preliminar se indicó un avance del 50%, la evidencia presentada al equipo auditor demuestra claramente que se llevaron a cabo todas las actividades programadas para este control (Se anexa archivo PlanDeAccion_GestionVulnerabilidades presentado en desarrollo del seguimiento).

En consecuencia con los argumentos anteriores, aunque no se hayan definido actividades específicas para estos controles en el plan de acción 2023, la Dirección de TIC ha implementado medidas para garantizar el cumplimiento de los requisitos establecidos.

Solicitamos reconsiderar la calificación de "situación crítica" asignada a esta observación, ya que consideramos que la metodología utilizada para la priorización y programación de los controles es sólida y transparente.

Creemos que es importante destacar que, a pesar de las inconsistencias identificadas en la presentación de los datos, el compromiso de la Dirección de TIC con la implementación del Modelo de Seguridad y Privacidad de la Información es firme y continuo en pro de mejorar nuestros procesos y garantizar la transparencia en la comunicación de nuestros avances.

NOTA: Se adjuntan evidencias"

Análisis de la respuesta por parte de la OCI:

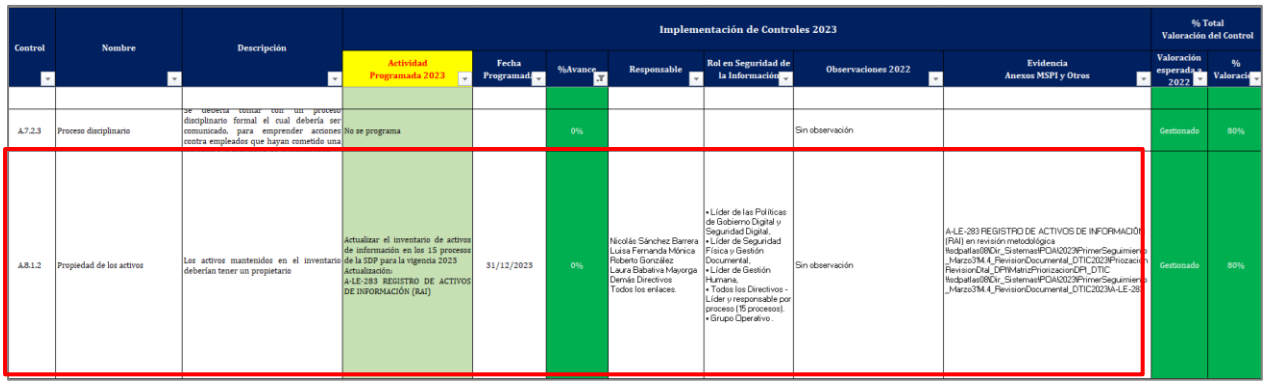
La Oficina de Control Interno reconoce los esfuerzos de la Dirección de TIC para implementar el Modelo de Seguridad y Privacidad de la Información en la entidad, así como el suministro de Información desde el diagnóstico, los planes de trabajo y los seguimientos, que demuestran el compromiso de las personas que hacen parte de la Dirección de TIC por establecer, implementar, mantener y mejorar continuamente el MPSI.

No obstante, el hallazgo identificado se refiere a las inconsistencias en la información consignada en el instrumento denominado "PlanAccionControles" suministrado como Evidencia No 8 por parte de la Dirección de TIC, el cual no refleja todo el esfuerzo realizado, así como parte de los resultados en cero contradicen la información y demás evidencias suministradas por la Dirección TIC durante el desarrollo de esta auditoría.

En el documento suministrado, no hay coherencia entre las actividades programadas y las actividades ejecutadas, entre las fechas de realización y los valores de la columna porcentaje de avance vs las evidencias, aspectos mínimos en la formulación y seguimiento de un plan de trabajo.

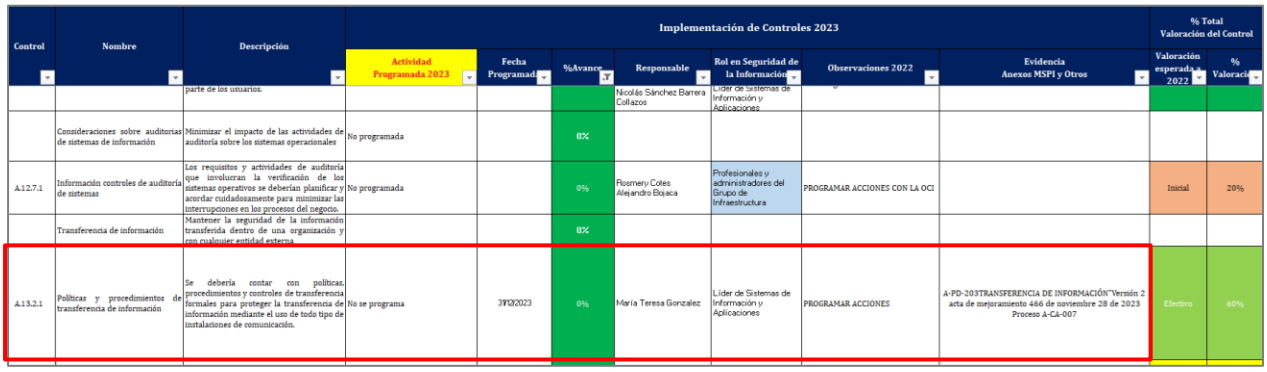
Como se mencionó algunos controles tienen en la columna de avance una calificación de 0%. Por ejemplo: *"Actualizar el inventario de activos de información en los 15 procesos de la SDP para la vigencia 2023",* lo cual es impreciso dado todo el esfuerzo y las actividades lideradas por la Dirección de TIC y adelantadas por la entidad para la actualización de los activos de información de la SDP en la vigencia 2023.

En otros casos se observó, por ejemplo, que algunas de las acciones tienen como fecha de cumplimiento el 31 de diciembre de 2023, y la Dirección de TIC relaciona la evidencia de la ejecución en la columna correspondiente, sin embargo tienen ejecución de cero %:



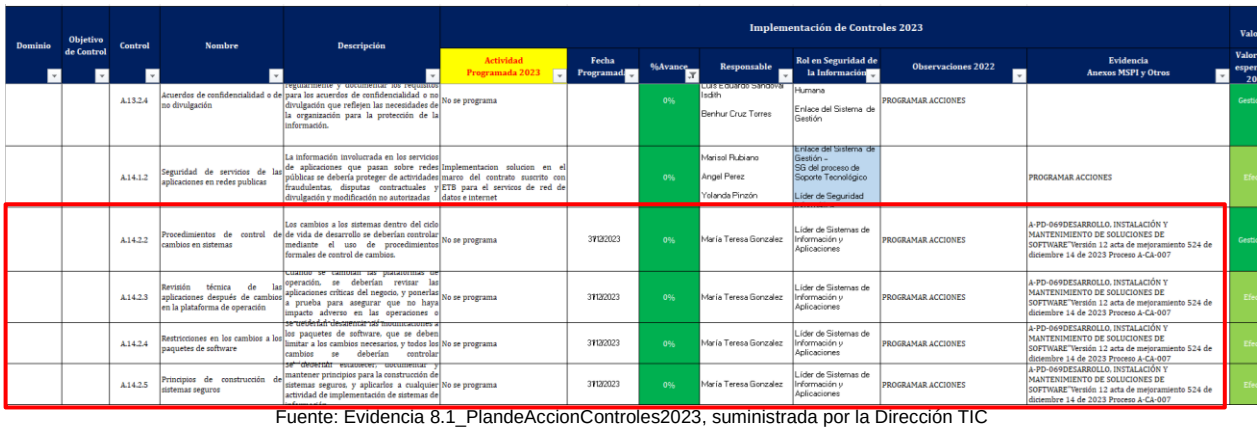
Control	Nombre	Descripción	Implementación de Controles 2023						% Total Valoración del Control	
			Actividad Programada 2023	Fecha Programada	%Avance	Responsable	Rol en Seguridad de la Información	Observaciones 2022	Evidencia Anexos MSPI y Otros	Valoración esperada 2022	% Valoración
A.7.2.3	Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una	No se programa		0%			Sin observación		Gestionado	80%
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario	Actualizar el inventario de activos de información en los 15 procesos de la SDP para la vigencia 2023 Actualización: A-LE-283 REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI)	31/12/2023	0%	Nicolás Sánchez Barrera Luisa Fernanda Mónica Roberto González Laura Babativa Mayorga Demás Directivos Todos los enlaces.	• Líder de las Políticas de Gobierno Digital y Seguridad Digital, • Líder de Seguridad Física y Gestión Documental, • Líder de Gestión Humana, • Todos los Directivos - Líder y responsable por proceso (15 procesos). • Grupo Operativo .	Sin observación	A-LE-283 REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI) en revisión metodológica \\sdpatlas08\Dir_Sistemas\PCIA\2023\PrimerSeguimiento_Marzo31\4.4_RevisionDocumental_DTIC2023\Priorización RevisionDtal_DPI\MatrizPriorizacionDPI_DTIC \\sdpatlas08\Dir_Sistemas\PCIA\2023\PrimerSeguimiento_Marzo31\4.4_RevisionDocumental_DTIC2023\A-LE-28	Gestionado	80%

Fuente: Evidencia 8.1_PlandeAccionControles2023, suministrada por la Dirección TIC



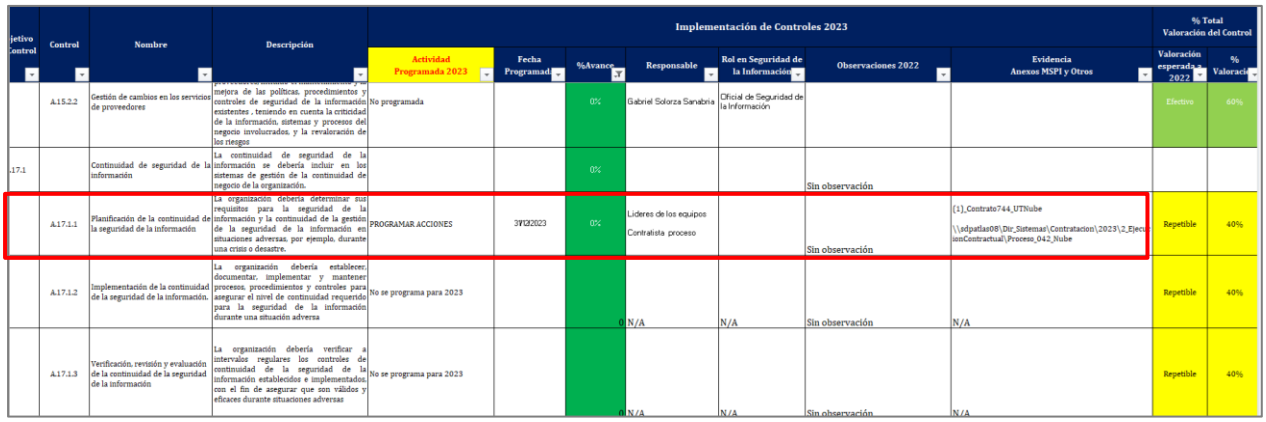
Control	Nombre	Descripción	Implementación de Controles 2023						% Total Valoración del Control	
			Actividad Programada 2023	Fecha Programada	%Avance	Responsable	Rol en Seguridad de la Información	Observaciones 2022	Evidencia Anexos MSPI y Otros	Valoración esperada 2022	% Valoración
		parte de los usuarios.				Nicolás Sánchez Barrera Collazos	Líder de Sistemas de Información y Aplicaciones				
	Consideraciones sobre auditorias de sistemas de información	Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales	No programada		0%						
A.12.7.1	Información controles de auditoría de sistemas	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No programada		0%	Rosmery Cotes Alejandro Bojaca	Profesionales y administradores del Grupo de Infraestructura	PROGRAMAR ACCIONES CON LA OCI		Inicial	20%
	Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa			0%						
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	No se programa	31/12/2023	0%	María Teresa Gonzalez	Líder de Sistemas de Información y Aplicaciones	PROGRAMAR ACCIONES	A-PD-203TRANSFERENCIA DE INFORMACIÓN"Versión 2 acta de mejoramiento 466 de noviembre 28 de 2023 Proceso A-CA-007	Efectivo	60%

Fuente: Evidencia 8.1_PlandeAccionControles2023, suministrada por la Dirección TIC



Dominio	Objetivo de Control	Control	Nombre	Descripción	Implementación de Controles 2023							Valo
					Actividad Programada 2023	Fecha Programada	%Avance	Responsable	Rol en Seguridad de la Información	Observaciones 2022	Evidencia Anexos MSPI y Otros	Valor esper 20
		A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Requerimiento y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	No se programa		0%	Luis Escalon Sanchez Isdith Benhur Cruz Torres	Humana Enlace del Sistema de Gestión	PROGRAMAR ACCIONES		Gesti
		A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	Implementacion solucion en el marco del contrato suscrito con ETB para el servicos de red de datos e internet		0%	Marisol Rubiano Angel Perez Yolanda Pinzón	Enlace del Sistema de Gestión - SSI del proceso de Soporte Tecnológico Lider de Seguridad		PROGRAMAR ACCIONES	Efe
		A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar, mediante el uso de procedimientos formales de control de cambios.	No se programa	31/12/2023	0%	María Teresa Gonzalez	Líder de Sistemas de Información y Aplicaciones	PROGRAMAR ACCIONES	A-PD-069DESARROLLO. INSTALACIÓN Y MANTENIMIENTO DE SOLUCIONES DE SOFTWARE"Versión 12 acta de mejoramiento 524 de diciembre 14 de 2023 Proceso A-CA-007	Gesti
		A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No se programa	31/12/2023	0%	María Teresa Gonzalez	Líder de Sistemas de Información y Aplicaciones	PROGRAMAR ACCIONES	A-PD-069DESARROLLO. INSTALACIÓN Y MANTENIMIENTO DE SOLUCIONES DE SOFTWARE"Versión 12 acta de mejoramiento 524 de diciembre 14 de 2023 Proceso A-CA-007	Efe
		A.14.2.4	Restricciones en los cambios a los paquetes de software	No se debería desarrollar documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de	No se programa	31/12/2023	0%	María Teresa Gonzalez	Líder de Sistemas de Información y Aplicaciones	PROGRAMAR ACCIONES	A-PD-069DESARROLLO. INSTALACIÓN Y MANTENIMIENTO DE SOLUCIONES DE SOFTWARE"Versión 12 acta de mejoramiento 524 de diciembre 14 de 2023 Proceso A-CA-007	Efe
		A.14.2.5	Principios de construcción de sistemas seguros	Los cambios a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	No se programa	31/12/2023	0%	María Teresa Gonzalez	Líder de Sistemas de Información y Aplicaciones	PROGRAMAR ACCIONES	A-PD-069DESARROLLO. INSTALACIÓN Y MANTENIMIENTO DE SOLUCIONES DE SOFTWARE"Versión 12 acta de mejoramiento 524 de diciembre 14 de 2023 Proceso A-CA-007	Efe

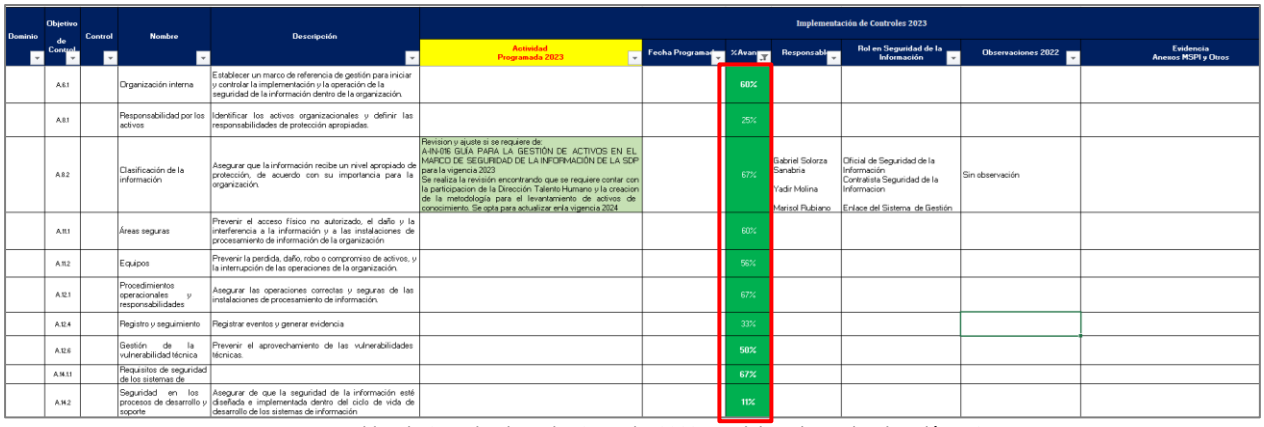
Fuente: Evidencia 8.1_PlandeAccionControles2023, suministrada por la Dirección TIC



jetivo ontrol	Control	Nombre	Descripción	Implementación de Controles 2023							% Total Valoración del Control	
				Actividad Programada 2023	Fecha Programad	%Avance	Responsable	Rol en Seguridad de la Información	Observaciones 2022	Evidencia Anexos MSPI y Otros	Valoración esperada a 2022	% Valoraci
	A.15.2.2	Gestión de cambios en los servicios de proveedores	mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos	No programada		0%	Gabriel Solorza Sanabria	Oficial de Seguridad de la Información			Efectivo	60%
.17.1		Continuidad de seguridad de la información	La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.			0%			Sin observación			
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	PROGRAMAR ACCIONES	31/12/2023	0%	Líderes de los equipos Contratista proceso		Sin observación	(1)_Contrato744_UTNube \\sdpatlas08\Dir_Sistemas\Contratacion\2023\2_Ejecu ionContractual\Proceso_042_Nube	Repetible	40%
	A.17.1.2	Implementación de la continuidad de la seguridad de la información.	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	No se programa para 2023		0	N/A	N/A	Sin observación	N/A	Repetible	40%
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas	No se programa para 2023		0	N/A	N/A	Sin observación	N/A	Repetible	40%

Fuente: Evidencia 8.1_PlandeAccionControles2023, suministrada por la Dirección TIC

En otras actividades, la Dirección de TIC presenta avances porcentuales, pero la actividad “no estaba programada”, como tampoco se relacionan las evidencias que permitan aclarar el porcentaje de avance consignado, como sucede en los siguientes controles:



Dominio	Objetivo de Control	Control	Nombre	Descripción	Implementación de Controles 2023						
					Actividad Programada 2023	Fecha Programad	%Avance	Responsable	Rol en Seguridad de la Información	Observaciones 2022	Evidencia Anexos MSPI y Otros
	A.6.1		Organización interna	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			60%				
	A.8.1		Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			25%				
	A.8.2		Clasificación de la información	Asegurar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la organización.	Revision y ajuste si se requiere de: A-IN-016 GUIA PARA LA GESTIÓN DE ACTIVOS EN EL MARCO DE SEGURIDAD DE LA INFORMACIÓN DE LA SDP para la vigencia 2023 Se realiza la revisión encontrando que se requiere contar con la participacion de la Dirección Talento Humano y la creacion de la metodología para el levantamiento de activos de conocimiento. Se opta para actualizar esta vigencia 2024		67%	Gabriel Solorza Sanabria Yadir Molina Marisol Rubiano	Oficial de Seguridad de la Información Contratista Seguridad de la Información Enlace del Sistema de Gestión	Sin observación	
	A.11.1		Áreas seguras	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización			60%				
	A.11.2		Equipos	Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			56%				
	A.12.1		Procedimientos operacionales y responsabilidades	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			67%				
	A.12.4		Registro y seguimiento	Registrar eventos y generar evidencia			33%				
	A.12.6		Gestión de la vulnerabilidad técnica	Prevenir el aprovechamiento de las vulnerabilidades técnicas.			50%				
	A.14.1.1		Requisitos de seguridad de los sistemas de				67%				
	A.14.2		Seguridad en los procesos de desarrollo y soporte	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información			11%				

Fuente: Evidencia 8.1_PlandeAccionControles2023, suministrada por la Dirección TIC

Lo anterior, no permite demostrar con precisión y objetividad el avance del Plan de implementación de controles del Modelo de Seguridad y Privacidad de la Información-MPSI de la Secretaría Distrital de Planeación.

La formulación y seguimiento de un plan propuesto, en este caso del Plan de implementación de controles del MSPI en el fondo lo que busca es formular las acciones que den cuenta de cómo se van a implementar cada uno de los controles que hacen parte del Modelo y hacer monitoreo y seguimiento en varios momentos de la fase de implementación para realizar los ajustes y corregir el rumbo cuando sea necesario.

Por lo expuesto, anteriormente, se ratifican las debilidades encontradas dado que los argumentos de la respuesta no desvirtúan las inconsistencias señaladas por la auditoría, razón por la que se mantiene la situación crítica.

4.4.3.2 ACCIONES ADELANTADAS POR LA DIRECCIÓN DE TIC FRENTE A LOS TEMAS DE MAS BAJO PUNTAJE DE LOS AUTODIAGNÓSTICOS MPSI REALIZADOS

Al indagar sobre cuáles fueron las acciones adelantadas frente a los temas que obtuvieron puntajes más bajos en los Autodiagnósticos, la Dirección TIC informó cuales fueron las acciones en el marco del plan de acción 2023 del Modelo de Seguridad y Privacidad de la Información:

Control A.10.1 Controles criptográficos

Para cumplir con el control A10 Controles criptográficos de la norma ISO 27001, la Secretaría Distrital de Planeación (SDP) realizó las siguientes acciones:

a) Suscripción de los siguientes contratos:
   Contrato 764-2023 con objeto "Adquisición de certificados de firma digital para los servidores públicos de la SDP."
   Contrato 759-2023 con objeto "Renovar el servicio de certificados de servidor seguro."

   Es así como La Secretaría Distrital de Planeación cuenta con los métodos de autenticación DomainKeys Identified Mail -DKIM y Sender Policy Framework – SPF, para el correo electrónico institucional.

   "SPF significa "marco de políticas del remitente". Este protocolo permite identificar o listar los servidores de correo electrónico autorizados por la organización para enviar mensajes desde su dominio, tanto internos como externos. Esto significa que evita que terceros suplanten su dominio de correo electrónico.
   DKIM: sus siglas significan claves de identificación de dominio digitales. Se trata de una técnica que utiliza criptografía asimétrica para agregar una firma digital, única a e intransferible, a la cabecera de los correos electrónicos. Gracias a esto, el receptor puede verificar la autenticidad y la integridad del mensaje, y garantizar que no ha sido manipulado entre los servidores de correo"[4]

b) Actualización, presentación y aprobación de la Política De Criptografía enfocada a los Certificados de Firma Digital, A-LE-477, según Acta de Mejoramiento 432 del 09/11/2023, dentro de la cual fueron definidos los objetivos de uso de la criptografía, como la protección de la confidencialidad, integridad y autenticidad de la información, la determinación de los roles y responsabilidades para la gestión de las claves criptográficas.

[4] CSIRT. MANUAL Implementación SPF, DKIM y DMARC en servicios públicos. Csirt.Chile. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://csirt.gob.cl/documents/4563/Manual_SPF_DKIM_y_DMARC.pdf

De acuerdo con lo anterior en la utilización de firmas digitales para garantizar la autenticidad e integridad de los documentos electrónicos se tuvieron en cuenta entre otras, las siguientes especificaciones:

Características técnicas:

- ✓ Algoritmo de firma de certificado con hash SHA256
- ✓ Dispositivo criptográfico de almacenamiento compatible con el puerto USB

Las Plataformas tecnológicas sobre las cuales se utilizarán los certificados de Firma Digital son:

- ✓ Secretaría Distrital de Hacienda – BOGDATA.
- ✓ Contraloría de Bogotá – SIVICOF.
- ✓ Ministerio del Trabajo – Certificados Pensionales.
- ✓ Firma de cualquier tipo de documentos
- ✓ Vigencia del Certificado: 12 meses
- ✓ Certificados a utilizar en la Plataforma “BOGDATA” de la Secretaría Distrital de Hacienda.
- ✓ El certificado de firma digital debe cumplir con el estándar ITU X.509 V3 y las disposiciones de campos mínimos requeridos definidas por la ley 527 de 1999 y la circular Única No. 10 de la Superintendencia de Industria y Comercio.
- ✓ De acuerdo con la reglamentación de la ONAC, los certificados digitales deben ser entregados en dispositivos criptogramas (Token Físico).
- ✓ Certificación: Certificado de Acreditación aprobado vigente por ONAC y Certificado de operador homologado por parte de la Administración de SIIF Nación del Ministerio de Hacienda y Crédito Público.
- ✓ Reposición: para proveer el servicio de reposición del token, sin que genere costos adicionales a la SDP. Se aclara que la reposición aplica para la misma modalidad de token, es decir token físico y debe contemplar reposición ante eventos tales como a)daño físico, por deterioro, ruptura, daño lógico no imputable a usuario.
- ✓ Retiro definitivo de la Entidad del responsable del token, con el fin de habilitarlo a la persona que lo reemplazará en el cargo.
- ✓ Integración con la Infraestructura de la SDP : Los tokens físicos se integran a la infraestructura de la SDP, deben operar sobre computadores que operen tanto con sistema operativo Windows (mínimo versión 10) como Mac OS X 10, facilitando su uso en escenarios operando en sitio (Oficinas de la SDP) como de manera remota por medio de trabajo en casa.
- ✓ Realizar revisiones: se revisará la política de criptografía y los controles criptográficos de forma regular para adaptarlos a los cambios en el entorno de amenazas.

Control A.17.1 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio

El Control A17.1.1 Planificación de la continuidad de la seguridad de la información de la norma ISO 27001 base del Modelo de Seguridad y Privacidad de la Información,

adoptado mediante la Resolución 500 de 2021, "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" menciona que:

(…)*ARTÍCULO 17. Etapas generales de la gestión de incidentes de seguridad digital*
1. Prevención

1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.

"La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización." (…)

De otra parte, la Directiva Presidencial 002 de 2022 menciona en el artículo 12:

"12. Contar con planes de continuidad del negocio, orientados a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información. Igualmente, se deben realizar ejercicios que permitan probar la efectividad del plan de continuidad del negocio frente al escenario de materialización de riesgos de seguridad de la información."

Situación Crítica identificada

No se cuenta con un plan de continuidad de la seguridad de la información, en el marco de un plan de continuidad del negocio.

De acuerdo con las respuestas recibidas de la Dirección mencionan que **la Secretaría Distrital de Planeación no cuenta con un plan de continuidad de la seguridad de la información**, en el marco de un plan de continuidad del negocio.

La Dirección de TIC reconoce la ausencia de un Plan de continuidad de seguridad de la información PCSI completo y actualizado, lo que representa una brecha en la seguridad de la información de la entidad. Sin embargo, menciona el siguiente contexto para comprender las razones que han impedido su implementación hasta el momento:

"La entidad ha enfocado su mirada en la implementación de otras iniciativas críticas para la SDP, como la migración a la nube, la modernización de la infraestructura tecnológica, el desarrollo y modernización del software y aplicaciones entre otras. Estas iniciativas han demandado una gran cantidad de recursos humanos, financieros y técnicos, lo que ha dificultado la dedicación de los recursos necesarios para desarrollar e implementar un plan de continuidad de la seguridad de la información completo.

La elaboración de un plan de continuidad de la seguridad de la información requiere de un análisis profundo de los procesos, sistemas y activos de información de la entidad. Con el rediseño institucional, el proyecto no procede hasta que no se hagan los ajustes necesarios y se formalicen los procesos y su caracterización.

A pesar de las dificultades mencionadas, la entidad cuenta con el A-LE-016 PLAN DE CONTINGENCIA INFORMÁTICO, el cual propende por la continuidad de la operación de los elementos considerados críticos que componen y soportan los servicios informáticos de la Secretaría Distrital de Planeación, mediante la descripción documentada de los pasos que se deben seguir frente a escenarios de falla donde se requiera la activación, restauración y/o recuperación de los servicios críticos bajo la gestión de la Dirección de TIC y contemplados en la estrategia de continuidad relacionada con el Plan de Contingencia Informático, de acuerdo con los lineamientos de MINTIC."

Frente a la Situación Crítica No 5 identificada en la Auditoria, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Se solicita de manera respetuosa reconsiderar y retirar la situación crítica reportada, dada la siguiente argumentación:

Alineado con los requisitos establecidos en la Resolución 500 de 2021 y el Decreto 767 de 2022, la Dirección de TIC ha llevado a cabo proyectos específicos y contractuales enfocados en garantizar la resiliencia tecnológica y la continuidad del negocio, como lo evidencia la implementación progresiva del DRP. A continuación se relacionan algunas de las contrataciones que apalancan la consecución del DRP y contribuye a la continuidad de negocio de la SDP:

Desde la Dirección de TI se reconoce la importancia de estos planes DRP y BCP para asegurar la resiliencia operativa y la protección de la información, por ello en el Plan Estratégico de Tecnologías de la Información se han planteado iniciativas y proyectos en los cuales se involucran y priorizan los servicios tecnológicos críticos de la entidad. Dentro de estas actividades se ha contemplado la adquisición de servicios profesionales altamente especializados y servicios de nube; así mismo, se han adquirido e implementado servicios de escritorios virtuales, los cuales permite asegurar que los colaboradores de la SDP en procesos esenciales de la misionalidad cuenten con herrimientas necesarias para la prestación del servicio.

De acuerdo con la hoja de ruta en los proyectos de TI, mediante el contrato 369 de 2021 cuyo objeto consistió en "REALIZAR EL ESTUDIO DE LA SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA SDP Y PLANTEAR LAS ACCIONES NECESARIAS Y LA ESTIMACIÓN DE COSTOS DE LA MIGRACIÓN DE LOS SERVICIOS DE LA SDP A LA NUBE Y DE LA IMPLEMENTACION DE UN DRP DE ACUERDO A LOS LINEAMIENTOS DE MINTIC." en el cual se realizó un diagnóstico, análisis de la situación actual de la SDP y el establecimiento de la línea base y la hoja de ruta para la consolidación, implementación y puesta en funcionamiento del DRP.

Revisada y ajustada la hoja de ruta propuesta en el PETI, durante la vigencia 2022 mediante el contrato 810 del mismo año, cuyo objeto consistió en "REALIZAR LAS ACTIVIDADES DE LA FASE I, PARA LA MIGRACIÓN DE SERVICIOS TECNOLOGICOS DE LA SDP A LA NUBE Y DE LA OPERACIONALIZACION DEL PLAN DE RECUPERACION DE DESASTRES - DRP", mediante el cual se realizó la migración de los primeros sistemas de información y aplicaciones a la nube de servicios TI de producción y la implementación de un DRP, que incluyerá infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y recurso humano para implementación.

Durante la vigencia 2023, mediante el contrato 773 de 2023 cuyo objeto consistió en "REALIZAR LAS ACTIVIDADES DE MIGRACIÓN DE SERVICIOS DE LA SDP A LA NUBE Y DE LA

OPERACIONALIZACION DEL PLAN DE RECUPERACION DE DESASTRES - DRP" se continuó con actividades de estabilización y migración de servicios tecnológicos priorizados para mejorar la disponibilidad, flexibilidad y escalabilidad de los servicios, los cuales dentro del alcance inicial de pruebas se han realizado actividades de restauración rápida de bases de datos cruciales para la operación de la SDP, para asegurar la recuperación efectiva y minimizar el impacto de posibles incidentes en la continuidad del negocio.

Durante la vigencia 2024, la DTIC publicó el proceso 1194 de 2024 a fin de renovar los servicios de nube, el cual incluye los servicios de soporte especilizados y garantizar la continuidad de los servicios de operación misional, además de los servicios DRP en nube. Las acciones realizadas por la Dirección de TIC y sustentadas en diferentes comités de contratación demuestra el compromiso con la resiliencia tecnológica y el fortalecimiento de la seguridad y disponibilidad de los servicios esenciales para la continuidad operacional de la SDP.

Teniendo en cuenta los anteriores avances desde la Dirección de TIC que contribuyen a la continuidad de la seguridad de la información; sin embargo, es indispensable un trabajo conjunto entre los Subsecretarios de la SDP, Dirección de Planeación Institucional, Dirección Administrativa, Dirección de Talento Humano y Dirección de TIC."

Análisis de la respuesta por parte de la OCI:

El control A.17.1 Continuidad de seguridad de la información del Modelo de Seguridad y Privacidad de la Información, menciona que la continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.

- 17.1.1 Planificación de la continuidad de la seguridad de la información: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
- 17.1.2 Implementación de la continuidad de seguridad de la información
- 17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información

La información y los procesos críticos de la entidad deben ser protegidos de manera apropiada, con el fin de asegurar la continuidad de la operación de la Secretaría Distrital de Planeación, durante una crisis o un desastre.

El objetivo del plan debe orientarse a establecer estrategias con medidas concretas para restablecer la disponibilidad de la información, cómo se va a mantener la seguridad de la información en un nivel mínimo planificado, cómo se van a proteger los activos de información para mantener su confiabilidad, integridad y disponibilidad ante amenazas internas o externas, deliberadas o accidentales. Cómo la entidad podrá recuperar sus funciones críticas dentro de un tiempo determinado.

Se trata de identificar los activos de información que requieran ser dotados de redundancia atendiendo a la exigencia de los procesos en los que están involucrados, no solo es un tema de atención de una contingencia, ya que va mas allá, hacia la continuidad de la operación.

Es importante reconocer los esfuerzos que he venido realizando la Dirección de TIC relacionados con migración de servicios tecnológicos de la SDP a la nube y de la Operacionalización del Plan De Recuperación de Desastres – DRP.

Sin embargo, el Plan de Recuperación de Desastres DRP, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan que tiene un enfoque más reactivo, más de contingencia ante una posible crisis o una catástrofe. Por lo anterior, es imperativo realizar pruebas del Plan de continuidad de la información, involucrando a los diferentes niveles y procesos de la entidad.

Frente a la observación de la Dirección de TIC "*Con el rediseño institucional, el proyecto no procede hasta que no se hagan los ajustes necesarios y se formalicen los procesos y su caracterización",* se debe aclarar que la entidad cuenta con una estructura y funciones actualizadas aprobadas mediante el Decreto 432 de 2022. Así mismo, en la vigencia 2023, fueron actualizados los activos de información bajo su liderazgo, por lo que el argumento no desvirtúa la situación crítica identificada.

Finalmente, el control A.17.1 Continuidad de seguridad de la Información es un DEBE dentro del Modelo de Seguridad y Privacidad de la Información, convirtiéndose en un requisito legal definido por la Resolución 500 de 2021, *"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".*

Por los argumentos expuestos y teniendo en cuenta el impacto que tiene el control A.17.1 Continuidad de seguridad de la Información en el marco del Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la SDP de una manera adecuada y oportuna, se mantiene la situación crítica.

<u>Situación Crítica identificada</u>

Así mismo, se identificó por parte del Equipo Auditor que la entidad **no cuenta con un plan de continuidad de negocio** que permita a la alta dirección y a los procesos misionales dentro de la entidad el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

Frente a la Situación Crítica No 6 identificada en la Auditoria, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Se solicita de manera respetuosa reconsiderar y retirar la situación crítica reportada en cuanto a la falta de un Plan de Continuidad de Negocio (BCP) específico para las comunicaciones de voz, datos, TI, personal esencial y ubicaciones alternas, teniendo en cuenta las siguientes acciones implementadas y en ejecución por la Secretaría Distrital de Planeación (SDP) para asegurar la resiliencia operativa.

La Dirección de TIC, en concordancia con las normativas de la Resolución 500 de 2021, el Decreto 767 de 2022 y la Directiva Presidencial 002 de 2022, ha avanzado en la implementación de medidas de continuidad orientadas a asegurar la disponibilidad de las comunicaciones críticas y la infraestructura tecnológica de la entidad. Estas acciones incluyen la adopción de estrategias de contingencia que garantizan la recuperación y reanudación de servicios prioritarios en eventos disruptivos, tales como la migración de servicios clave a la nube, la habilitación de escritorios virtuales para personal esencial y la implementación de infraestructuras redundantes de comunicaciones. Estas medidas han sido diseñadas para mitigar el impacto en la operación ante la materialización de incidentes que puedan comprometer la disponibilidad y continuidad de los servicios críticos."

Análisis de la respuesta por parte de la OCI:

En primer lugar, es importante mencionar que cuando se trate de hallazgos que involucren varias dependencias, se debe realizar el análisis de manera conjunta con los responsables de esas áreas.

Ahora bien, es importante recordar nuevamente el lineamiento establecido en la Directiva Presidencial 002 de 2022. "Reiteración de la Política Pública en Materia de Seguridad Digital" Artículo 12:

> *"12. Contar con **planes de continuidad del negocio**, orientados a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información. Igualmente, se deben realizar ejercicios que permitan probar la efectividad del plan de continuidad del negocio frente al escenario de materialización de riesgos de seguridad de la información"*

El control A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio es un DEBE dentro del Modelo de Seguridad y Privacidad de la Información, convirtiéndose en un requisito legal definido por la Resolución 500 de 2021, *"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".*

A la fecha no fueron aportadas evidencias de la realización de ejercicios que permitan probar la existencia y efectividad de un plan de continuidad del negocio frente a un escenario de materialización de riesgos de seguridad de la información.

De otra parte, en el Anexo 1 del Modelo de Privacidad y seguridad de la Información, Resolución 500 de 2021 se describe en el numeral 11.2.9 Control Interno, el papel del responsable de seguridad y privacidad de la información de la entidad:

"Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
- Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información"

Se requiere la implementación de una Plan de Continuidad de Negocio en la SDP que permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los servidores públicos, afectar el debido desarrollo de las actividades propias de la entidad, impedir la prestación y continuidad del servicio a los grupos de valor o el cumplimiento de los compromisos establecidos en el Plan de Desarrollo.

Por los argumentos expuestos y teniendo en cuenta el impacto que tiene para la continuidad de las operaciones de la SDP en el marco del Modelo de Seguridad y Privacidad de la Información, se mantiene la situación crítica identificada.

3. Control A. 16 Gestión de Incidentes de Seguridad de la Información

a) Actualización, presentación y aprobación del procedimiento de Gestión de Incidentes de Seguridad y Privacidad en la SDP A-PD-187, según Acta de Mejoramiento 357 del 29/09/2023.
b) Durante las jornadas de inducción/reinducción la Entidad realizar presentación de las generalidades en temas de Seguridad y Privacidad de la Información donde se da a conocer el procedimiento A-PD-187 y se reitera la importancia de reportar los incidentes de seguridad a través de la herramienta de Mesa de Ayuda de la SDP.
c) Estrategias de Sensibilización y Capacitación del Política de Sensibilización y Capacitación de Seguridad y Privacidad de la Información, A-LE-375, donde a través de boletines se refuerza sobre los tipos de incidentes y el procedimiento para reportar los incidentes de seguridad de la información.

Gestión de Riesgos de seguridad y privacidad de la información

La Dirección de TIC realizó un ejercicio de acompañamiento a los diferentes procesos de la entidad para la identificación y valoración de riesgos de la seguridad y privacidad de la información, que permita identificar los riesgos que puedan ocasionar la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información.

En cumplimiento de las normas y estándares de seguridad de la información ISO 27001 y Modelo de Ciberseguridad NIST y en respuesta a la materialización de riesgos de seguridad en la Secretaría Distrital de Planeación (SDP) durante el 2023, la Dirección de TIC manifestó que no se presentó materialización de riesgos identificados y documentados en el Modelo de Seguridad y Privacidad de la Información (MSPI).

Desde la Dirección de TIC fueron implementadas las siguientes acciones encaminadas a mitigar los riesgos identificados:

* Identificación y documentación de riesgos potenciales de seguridad y privacidad de la información que podrían afectar a la SDP.
* Implementación de controles para mitigar cada uno de los riesgos identificados. Estos controles incluyen medidas técnicas, organizativas y físicas.

* Monitoreo y seguimiento: Se estableció un proceso continuo de monitoreo y seguimiento de la efectividad de los controles implementados, para identificar y abordar cualquier problema potencial de manera oportuna.
* Capacitación y sensibilización: Se brindó capacitación y sensibilización a todos los miembros de la SDP sobre los riesgos de seguridad y privacidad de la información, y sobre las medidas que deben tomar para proteger la información de la SDP.

Al revisar los soportes se evidenció que la Secretaría Distrital de Planeación (SDP), ha realizado un gran esfuerzo para incorporar la seguridad de la información en los procesos, trámites, servicios, sistemas de información e infraestructura de la siguiente manera:

Procesos:

- Fueron realizados los análisis de riesgos de seguridad de la información para todos los procesos de la SDP.
- Se han implementado controles de seguridad para mitigar los riesgos identificados.
- Se documentaron Políticas de seguridad de la información en los procedimientos de la entidad

Trámites y servicios:

- Se han implementado medidas de seguridad para proteger los datos personales de los ciudadanos durante la prestación de trámites y servicios.
- Se han establecido mecanismos de control para asegurar la autenticidad, integridad y no repudio de los trámites y servicios electrónicos, aseguramiento del servicio de correo mediante configuraciones que permiten validar la autenticidad del dominio y la legitimidad de las cuentas de correo.
- Se han realizado socializaciones a los servidores públicos de la SDP en materia de seguridad de la información y protección de datos personales.
- La entidad cuenta con una política de tratamiento de datos personales, y tiene establecidos lineamientos para la protección y conservación de datos personales.
- La entidad divulga su política de tratamiento de datos personales mediante aviso de privacidad, en su página web y personalmente al titular en el momento de la recolección de los datos.
- La entidad cuenta con la autorización del ciudadano para la recolección de los datos personales.
- La entidad permite al titular de la información, conocer en cualquier momento la información que exista sobre él en sus bases de datos.
- La entidad conserva la información bajo condiciones de seguridad para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

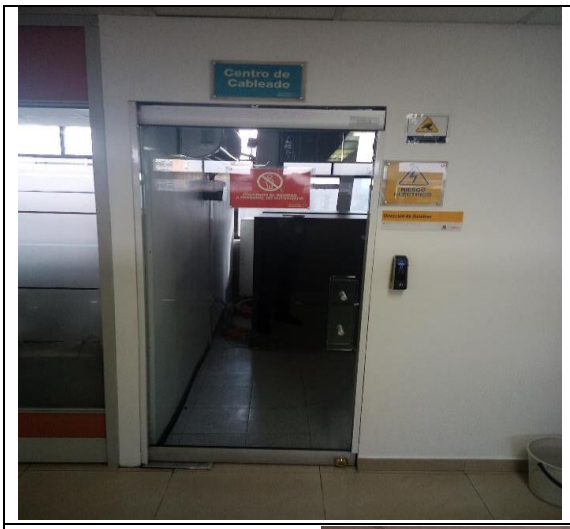
Sistemas de información:

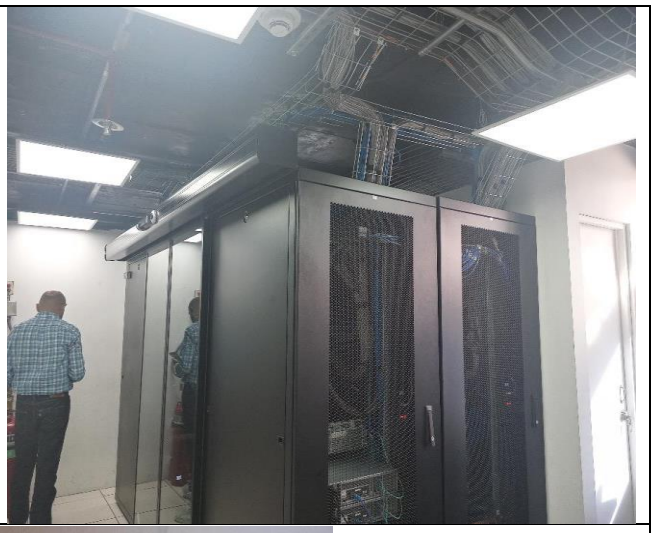
- Se han implementado controles de seguridad para proteger los sistemas de información de la SDP contra ataques cibernéticos.

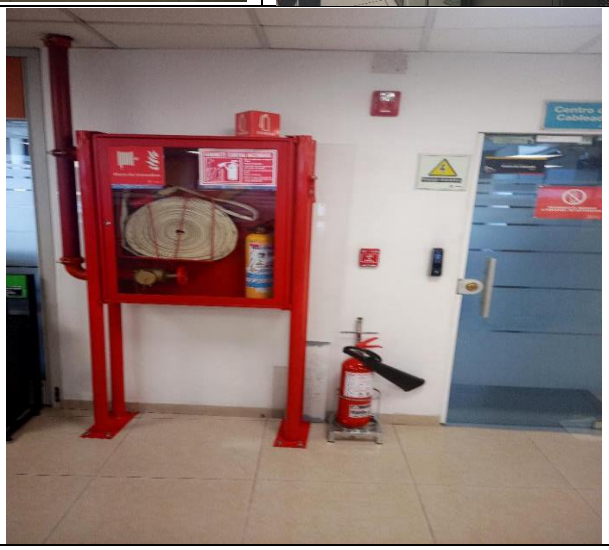
- Se realiza la gestión de vulnerabilidades para identificar y corregir las vulnerabilidades de los sistemas de información de manera oportuna.
- La gestión de vulnerabilidades se realiza mediante el plan formulado cada año; para la vigencia 2023, se realizó el escaneo de vulnerabilidades mediante la herramienta TENABLE el cual fue cumplido en el 100%.

Infraestructura:

- Se han implementado medidas de seguridad física para proteger la infraestructura de la SDP.
- Se cuenta con un sistema de control de acceso físico, con tarjetas de identificación y biometría, para restringir el acceso a las áreas sensibles mediante al cual se restringe el acceso físico a las áreas donde se encuentran los equipos y sistemas informáticos solo al personal autorizado.
- Se cuenta con doble puerta para el acceso a los equipos instados en el centro de cómputo.
- Se cuenta con elementos necesarios para el control y extinción de incendios.







Fuente: Dirección de Tecnologías de la Información y las Comunicaciones

- Se han establecido controles de acceso para restringir el acceso a la infraestructura de la SDP a las personas autorizadas.

  Cada año se remite a la Dirección Administrativa el listado de personal autorizado para ingresar a las áreas restringidas.

- Se han implementado medidas de seguridad para proteger la red de la SDP contra ataques cibernéticos.

  La entidad cuenta con Firewall perimetral, Firewall de aplicaciones WAF, IPS y SIEM para protección de acceso de usuarios a la red, así mismo cuenta con un antivirus licenciado e instalado en todos los equipos de la entidad

Evidencias:

- **Análisis de riesgos de seguridad de la información:** Informes primera, segunda y tercera línea de defensa.
- **Controles de seguridad implementados:**
  Controles de acceso físico como autorización de permisos, controles físicos de acceso
  Controles de seguridad de la red como lo son Firewall perimetral, Firewall de aplicaciones WAF, IPS para el control de usuarios para el acceso a la red.
  Controles de seguridad de la información con el objetivo de proteger la información contra malware, ramsomware y otras amenazas tale como antivirus, antiramsomware y copias de seguridad
  Evidencias de contratos de soporte y mantenimiento de Firewall perimetral, Firewall de aplicaciones WAF, IPS y balanceadores
- **Procedimientos y manuales con la seguridad de la información incorporada:**
  Desarrollo, instalación y mantenimiento de soluciones de software. A-PD-069
  Soporte y atención de la mesa de ayuda. A-PD-089
  Copias de seguridad y recuperación de información. A-PD-092
  Gestión cuentas de usuario. A-PD-104
  Instalación y configuración de servidores de la SDP. A-PD-107
  Administración de reglas y políticas en el firewall. A-PD-110
  Valoración de aplicaciones de software y/o sistemas de información. A-PD-166
  Gestión de incidentes de seguridad y privacidad en la SDP. A-PD-187
  Monitoreo de la infraestructura tecnológica de la SDP. A-PD-192
  Instalación y administración de software. A-PD-198
  Transferencia de información. A-PD-203
  Gestión del cambio informático. A-PD-204
  Guía para la gestión de activos de información de la SDP. A-IN-016
  Guía usuario final definición del plan de acción y seguimiento a las actividades de la PPGDLGBT. A-IN-391
  Guía usuario final procedimiento seguimiento denuncias LGBTI. A-IN-397
  Manual para el manejo del módulo de planes de mejoramiento del sistema de información de procesos automáticos – SIPA. A-IN-412

Manual de usuario final proceso control de documentos. A-IN-413
Guía estándar para la creación de usuarios en la SDP. A-IN-422

Servicios Ciudadanos digitales - Interoperabilidad

Respecto a cómo se ha acompañado desde la Dirección de TIC a las dependencias de la entidad para avanzar en la interoperabilidad respecto de los servicios ciudadanos digitales, la Dirección de TIC aclaró lo siguiente:

- En el marco de la Política de Gobierno Digital realizó la suscripción de la adición y prórroga del Contrato 865 de 2022 cuyo objeto consistió en "Adquirir los servicios de comunicación de salida hacia los ciudadanos a través de medios virtuales, texto y voz para aumentar las interacciones de la SDP con la ciudadanía.
- Suscripción del Contrato 869 de 2022 cuyo objeto fue "Contratar los servicios del centro de contacto Línea 195 para prestar la atención de información especializada de la Secretaria Distrital de Planeación a los usuarios que acceden a través del canal telefónico respectivamente", disponibles para consulta pública en https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/103216.
- Se dio continuidad al mantenimiento y soporte del web service de intercambio para la generación de trámites al servicio de la ciudadanía, y se realiza intercambio de datos con otras entidades a través de Webservice, permitiendo fortalecer la generación de trámites al servicio de la ciudadanía:

  a) Webservice Estratificación:
  http://aplicaciones.sdp.gov.co:7777/consultaestrato/EstratoWSSoapHttpPort
  -->Dirección de Estratificación (Dec. 016-2013) - Servicio: Ventanilla Única de la Construcción con Secretaría de Hábitat
  b) Webservice Plusvalía:
  http://aplicaciones.sdp.gov.co:7777/consultaplusvalia/WSPlusvaliaSoapHttpPort
  -->Dirección de Estratificación (Dec. 016-2013) - Servicio: Ventanilla Única de la Construcción con Secretaría de Hábitat para solicitudes de licencia según Decreto 190/2004
  c) Webservice Cámara de comercio:
  http://aplicaciones.dapd.gov.co:7777/WebServiceccb/WebServiceSDPSoapHttpPort
  -->Dirección de Cartografía, Información y Estadística (Dec. 016-2013) - Funciones que ahora se encuentran a cargo Dirección de Información y Estadística - Servicio: Desarrollo Componente Económico (Matrícula Mercantil de Establecimiento de Comercio, Estadística de Bogotá).
  d) -->Interoperabilidad entre Bogotá TE ESCUCHA y SIPA
  Dirección de Servicio a la Ciudadanía. Servicio: Interoperabilidad en doble vía entre Bogotá TE ESCUCHA - SDP y Viceversa

Sin embargo, se recomienda tener en cuenta las observaciones de la Evaluación FURAG enunciadas anteriormente, para cambiar el puntaje de cero, teniendo en cuenta lo definido en la nueva Política de Gobierno Digital:

Servicios Ciudadanos Digitales: Este habilitador busca desarrollar, mediante soluciones tecnológicas, las capacidades de los sujetos obligados a la Política de Gobierno Digital para mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública. [5]

4.4.3.3 GESTIÓN DE VULNERABILIDADES

A.12.6. Gestión de la vulnerabilidad técnica. Prevenir el aprovechamiento de las vulnerabilidades técnicas.

El equipo auditor solicitó a la Dirección TIC describir cuáles fueron las estrategias desarrolladas durante 2023 para afrontar las vulnerabilidades de TI en la SDP y los casos de Indisponibilidad no programada de servicios de TI.

Sobre el particular la Dirección TIC respondió que en cumplimiento de la norma ISO 27001 de 2013, en la cual se establece entre otros, un conjunto de requisitos para la gestión de vulnerabilidades como un proceso continuo que tiene como objetivo identificar, evaluar y remediar las vulnerabilidades de seguridad en los sistemas de información de la entidad para proteger la confidencialidad, integridad y disponibilidad de la información, y 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, la SDP desarrolló e implementó las siguientes actividades:

1. Suscripción del Contrato 071 de 2023 cuyo objeto consistió en “Prestar servicios profesionales de apoyo a la Dirección de Tecnologías de la Información y las Comunicaciones para la operación de las herramientas de administración de seguridad informática y actividades de aseguramiento de la conectividad de la SDP.”

2. Establecimiento de un plan de trabajo para la gestión de vulnerabilidades definiendo el alcance del, los roles y responsabilidades en el proceso de identificación, evaluación y remediación de vulnerabilidades, y los criterios para la aceptación del riesgo. El plan de trabajo contempló 14 actividades las cuales se relacionan a continuación:

a) Inventario general de infraestructura, servidores y servicios

[5] Decreto 767 de 2022, “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

b) Clasificación de los activos más importantes (Joyas de la corona), determinar el impacto si fueran comprometidos
c) Identificación de Servidores para intervenir
   - Generar un informe de diagnóstico de lo realizado en la vigencia anterior diagramando los resultados de mitigación aplicada
d) Generar un escaneo con la herramienta Tenable para definir el estado actual y establecer una línea base de vulnerabilidades a mitigar
e) Socializar los servidores definidos a intervenir y determinar los responsables administradores de cada servidor o aplicación
f) Generación de un Plan de Acción para mitigar vulnerabilidades basado en Top "25-10" 25(servidores)-10(vulnerabilidades más comunes). De servidores analizados
g) Presentación del plan y estrategia de mitigación, con responsables y tiempo límite de aplicación de remediaciones
h) Validación de los tiempos por parte de los participantes en las acciones de Mitigación y generar el plan de acción de remediación
i) Ejecución Plan de Acción de remediación de vulnerabilidades top 25-10 Definitivo y retroalimentación de posibles inconvenientes, y realizar seguimiento
j) Con base al resultado de remediaciones evaluar el % de correcciones aplicadas y con esto se emitirá un informe de la primera etapa de Gestión de vulnerabilidades
k) Segundo escaneo de vulnerabilidades con herramienta Tenable acotando los servidores definidos en el plan de acción
l) Socialización y retroalimentación de los resultados obtenidos en el segundo escaneo, realizando la comparación de la línea base con respecto al resultado del segundo escaneo
m) Generación de un plan con un nuevo grupo de mitigación de vulnerabilidades basado en el segundo escaneo, el cual debe incluir nuevas vulnerabilidades y ampliación del espectro de acción en servidores
n) Presentación del plan de Acción del Segundo Grupo de Servidores - Definitivo

3. Identificación de las vulnerabilidades de seguridad mediante el uso de la herramienta Tenable adquirida en la vigencia 2021 para el escaneo de vulnerabilidades, pruebas de penetración y otras técnicas de análisis de seguridad.

4. Evaluación de las vulnerabilidades identificadas para determinar su gravedad y el riesgo que representaban para la entidad. La gravedad de una vulnerabilidad se basa en el impacto potencial que podría tener en la SDP si se explota. El riesgo se basa en la probabilidad de que la vulnerabilidad sea explotada y la gravedad del impacto potencial.

5. Remediación de las vulnerabilidades identificadas en un plazo de tiempo razonable. Esta actividad implica la posibilidad de aplicación de parches de seguridad, la actualización del software, la configuración de los sistemas de información o la implementación de controles de seguridad adicionales.

6. Monitoreo de las vulnerabilidades conocidas para asegurarse de que se han remediado y que no han surgido nuevas vulnerabilidades.

7. Revisión y actualización en la gestión de vulnerabilidades de forma periódica para asegurarse de que sigue siendo efectiva y se adapta a las necesidades cambiantes de la entidad.

Además de las actividades mencionadas anteriormente, la SDP también realizó en la vigencia 2023 sesiones de trabajo lideradas al interior de la Dirección de TIC para comunicar y tomar decisiones sobre la gestión de vulnerabilidades y documentó las acciones realizadas en el proceso.

La Dirección de TIC mencionó que para el mes de diciembre el plan para la gestión de vulnerabilidades se encuentra ejecutado en un 100%.

Situación crítica:

De acuerdo con las respuestas recibidas a los cuestionarios 1 y 2 por parte de la Dirección TIC, y a las entrevistas realizadas, las reuniones efectuadas y los soportes revisados, se identificó por parte del equipo auditor que se presenta una criticidad importante a nivel del software y de infraestructura obsoleta, aspecto que afecta las acciones y esfuerzos que se realizan en la SDP relacionada con la gestión de vulnerabilidades. A nivel de software que soporta las aplicaciones de la SDP algunos ya cumplieron su ciclo e incluso se tiene software obsoleto y sin soporte.

Esto a pesar de que la Dirección de TIC adquirió una solución de hiperconvergencia en el 2021, que en la vigencia 2022 trabajaron en la migración de los servicios alojados en servidores obsoletos hacia los servidores hiperconvergentes adquiridos y en el 2023 fue adquirida una solución KVM (máquina virtual basada en el kernel KVM, por sus siglas en inglés) y continuaron con migración de servicios existentes en la infraestructura de la SDP soportados por servidores físicos Blade generaciones 1, 5, 7, 8, 9 a la solución de hiperconvergencia y a la nueva solución KVM.[6]

De acuerdo a lo encontrado en los análisis realizados por la Dirección de TIC:

- La SDP cuenta con la herramienta de monitoreo Tenable para detectar las vulnerabilidades. Las detecciones que se realizan con esta herramienta permiten tipificar por nivel de criticidad cada vulnerabilidad y emite las recomendaciones para su mitigación.
- Se pasó de 327 vulnerabilidades criticas identificadas en la vigencia 2022 a 171 vulnerabilidades críticas en abril de 2023.
- La Dirección TIC generó un Plan de Acción para mitigar vulnerabilidades basado en Top "25-10" 25(servidores)-10(vulnerabilidades más comunes).
- Posterior a la identificación de vulnerabilidades y aplicación de las medidas de remediación tomadas de manera inmediata, se identificó que no todas las remediaciones pudieron ser solucionadas con acciones directas sobre la infraestructura tecnológica.

[6] Dirección de TIC. Respuesta a cuestionario -Evidencia 9. Informe insumo Revisión por la Dirección diciembre de 2023

- En un gran porcentaje, a partir de los reportes de la herramienta, se identifica a que las vulnerabilidades apuntan a **versionamiento obsoleto, utilizado para servidores web (Nginex, apache,)**
- **Se debe mantener un porcentaje importante de infraestructura obsoleta** que no ha podido ser dada de baja porque soporta servicios y SI legacy que **no tienen soporte** y consecuentemente son **de difícil migración** o servicios y sistemas de información que son soportados por versiones obsoletas de software base que no permiten actualización o migración a nuevas tecnologías o a sistemas operativos con versiones más actualizadas. La Dirección de TIC **aclara que no depende de licenciamiento si no de cambio de versión** ej: motor php, Web server IIS, hipervisores e incluso herramienta de backup.
- Revisando el análisis de infraestructura se observa que la entidad tiene la necesidad de asegurar actualizaciones en switches y firewall.
- El EOL (End of Life) aplica tanto para software como para hardware. El cual se refiere a la caducidad de un producto de software. Es decir, es el momento en el cual un software deja de tener mantenimiento y soporte oficial por parte de su desarrollador.

Para la SDP es un tema critico a nivel del software aquellos que soportan las aplicaciones de la SDP, ya que algunos ya cumplieron su ciclo e incluso se tiene una gran cantidad de software y hardware obsoleto y sin soporte.

Este tema ya había sido identificado por parte de la Oficina de Control Interno en vigencias anteriores:

***"4.3.4.1 Plan para la Gestión de Vulnerabilidades**.*[7]

*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.*

[7] Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información. Segundo semestre de 2021 al 30 de septiembre de 2022.

*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."

La Oficina de Control Interno identificó e incluyó en el referido informe:

(…)"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**. (…)*

Frente a la Situación Crítica No 2 identificada en la Auditoria, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"** Se solicita de manera respetuosa reconsiderar y retirar la situación crítica reportada, dada la siguiente argumentación:*

Si bien es cierto que en la SDP existe infraestructura tecnológica catalogada como obsoleta, la Dirección de TIC ha venido trabajando arduamente en la migración de servicios hacia infraestructura hiperconvergente y nube, a tal punto que a la fecha se migraron los sistemas de información que se ejecutaban en servidores blade generación 1 a la 7, como se puede evidenciar en los controles de cambio ejecutados en años 2023 y 2024. A la fecha, se apagaron 16 servidores blabe previa migración.

Adicionalmente, la infraestructura que se encuentra catalogada obsoleta está cubierta con un contrato de mantenimiento y soporte No. 698-2023 (cada año la Dirección de TIC realiza el proceso de contratación respectivo).
La Dirección de TIC con el fin de mitigar posibles brechas de seguridad, ha implementado soluciones de seguridad como es un Firewall de Aplicaciones - WAF, el cual complementa con solución de seguridad perimetral y la solución de antivirus, otras estrategias como es el doble factor de autenticación e inclusión de capchats en los sistemas de información vía web, así como también la implementación de certificado seguro a las diferentes aplicaciones y acceso remoto de forma segura (VPN).

A continuación se relaciona los contratos de soporte y mantenimiento para las soluciones de seguridad:
Firewall Aplicaciones - Cto 760-2023
Firewall Perimetral - Cto 603-2023
Solución Antivirus, DLP Antiramsomware - Cto 843-2022
Certificado Seguro - Cto 759-2023

En lo relacionado con los contratos de migración a nube se tiene:
** Nube pública Oracle - Cto 744-2023*
** Se migró SICAPITAL a nube Oracle*
** Se configuró DRP a nivel de base de datos para algunas aplicaciones*
** Se configuró OracleAnalytics para registro social*

Igualmente se relacionan los diferentes contratos que la Dirección de TIC ha realizado para mantener actualizada la infraestructura:

Adquisición de la solución de escritorios virtuales - Cto 704-2023
Adquisición de infraestructura de procesamiento implementación KVM Migración Servicios - Cto 737-2022
Ampliación de dos nodos a la solución de hiperconvergencia - Cto 711-2023 y Cto 723-2023
Renovación solución de almacenamiento NAS SAN - Cto 542-2023
Ampliación de almacenamiento - Cto 722-2023
Actualización solución de copias de respaldo - Cto 762-2022

En lo referente a los PC de escritorio, durante la vigencia 2023, mediante plan de mejoramiento 2150 se instalaron y entregaron 132 equipo de escritorio, realizando actualización de la infraestructura de puestos de trabajo.

Es preciso indicar que la Dirección de TIC año tras año realiza la renovación de los contratos teniendo en cuenta la vigencia de las garantías de cada proceso.

En atención a la nota sobre reincidencia en temas de obsolescencia, se aclara que la Dirección de TIC en las vigencias 2022, 2023, 2024 ha venido realizando migraciones hacia la nube y hacia la solución del sistema hiperconvergente; sin embargo, la dinámica cambiante del mercado año tras año hace que la tecnología adquirida en la entidad se quede rezagada por los nuevos desarrollos tecnológicos.

Análisis de la respuesta por parte de la OCI:

- Se debe aclarar que la Oficina de Control Interno viene haciendo seguimiento a la gestión de vulnerabilidades de la SDP, las cuales no han sido remediadas incluso desde la vigencia 2019, 2020, 2021, 2022, a pesar de haberse formulado acciones correctivas, algunas inactivadas.

- La Dirección de TIC mencionó que para el mes de diciembre se encontraba ejecutado en un 100% el Plan de Acción de Gestión de Vulnerabilidades vigencia 2023 enviado como soporte de la evidencia 18 para este Seguimiento, pero se pudo verificar por parte del equipo auditor que algunas actividades no fueron ejecutadas en su totalidad, por ejemplo:

  (…) "Actividad 4.Generar un escaneo con la herramienta Tenable para definir el estado actual y establecer una línea base de vulnerabilidades a mitigar/

  Observación: "Se redefine la actividad de acuerdo a lo acordado en el primer seguimiento"

  Actividad 5. socializar los servidores definidos a intervenir y determinar los responsables administradores de cada servidor o aplicación.

  Observación: "Se reprograma esta actividad y las siguientes dado que hay una dependencia del resultado del escaneo objeto de la actividad anterior."

  Actividad 6. Generación Plan de Acción para mitigar vulnerabilidades basado en Top "25-10" 25(servidores)-10(vulnerabilidades mas comunes). De servidores analizados.

  Observación: "Con base a las reuniones realizadas se inicio con mitigar en los servidores que presentaban vulnerabilidade de SSl desactualizado y el cual reportaba critico , para con ello quitar ese vector, se avanzo en un 2% ya que actividades distintas quitaron tiempo para culminar esta actividad" Subrayado nuestro

  Actividad 14. presentar el plan de Acción de el Segundo Grupo de Servidores – Definitivo

  Observación: "realizar plan para proxima vigencia"

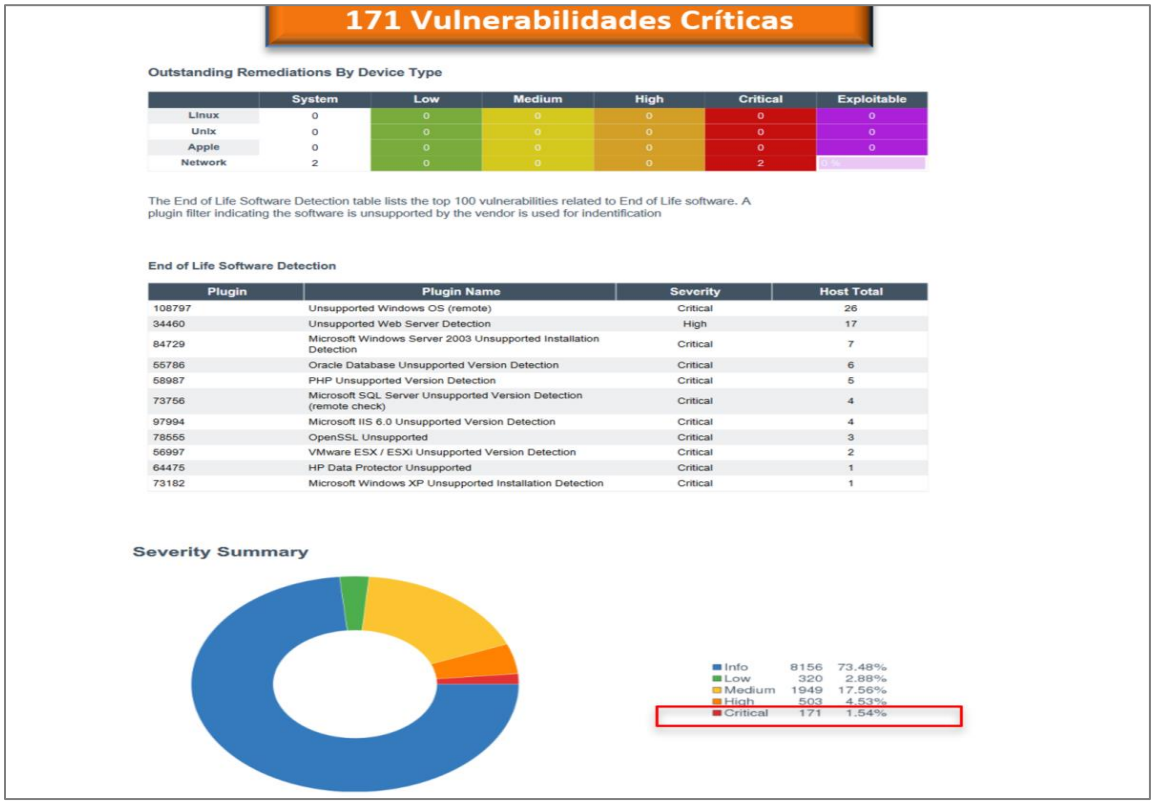
Plan de Trabajo						Seguimiento
Actividad	Ejecutor - Responsable	Fecha Inicio	Fecha Final	Peso Porcentual Programado	Peso Porcentual	Observaciones
1.Inventario general de infraestructura, servidores y servicios	Ing. Angel Maria Perez Ing. Alejandro Chala Ing. Jhon Rativa Ing. Henry Cepeda	1/03/2023	6/03/2023	8%	8%	se realizo el inventario, de equipos fisicos y maquinas virtuales asi como de un % de servicios a tener en cuenta.//se complementa archivo para incluir informacion a tener en cuenta al oento de escaneo
2.Clasificacion de los activos mas importantes (Joyas de la corona), determinar el impacto si fueran comprometidos	Equipo Infraestructura	8/03/2023	8/03/2023	7%	7%	con base al trabajo diario y de manera experimental se estan incluyendo los servicios criticos //se realiza primer clasificacion de de servidores mas relevantes para la operación de la entidad
3. Indentificación de Servidores a intervenir	Equipo Infraestructura	9/03/2023	14/03/2023	5%	5%	Se han identificado ya algunos servidores con brechas de seguridad, pero por no tener completa la priorización no se pueden clasificar // se clasifican lo servidores a intervenir con base a la identificacion de servicios criticos y su importancia para la SDP
3.1 Generar un informe de diagnostico de lo realizado en la vigencia anterior diagramando los resultados de mitigacion aplicada	Equipo Infraestructura	10/03/2023	15/04/2023	2%	2,0%	Con base a las vulnerabilidades que vienen de tiempo atrás, y evidenciando que aún se tienen // se realiza un analisis de las vulnerabilidades con las que cuentan los 10 servidores mas importantes para la entidad y se argumenta por que no han sido comprometidos y por que la importancia de mitigar las vulnerabilidaes que presentan.
4.Generar un escaneo con la herramienta Tenable para definir el estado actual y establecer una línea base de vulnerabilidades a mitigar	Ing. Angel Maria Perez Ing. Henry Cepeda	15/04/2023	15/05/2023	5%	5,0%	Se redefine la actividad de acuerdo a lo acordado en el primer seguimiento
5. socializar los servidores definidos a intervenir y determinar los responsables administradores de cada servidor o aplicación	Equipo Infraestructura	16/05/2023	16/05/2023	3%	3%	Se reprograma esta actividad y las siguientes dado que hay una dependencia del resultado del escaneo objeto de la actividad anterior.
6. Generación Plan de Acción para mitigar vulnerabilidades basado en Top "25-10" 25(servidores)-10(vulnerabilidades mas comunes). De servidores analizados	Ing. Henry Cepeda	5/07/2023	7/07/2023	6%	6%	Con base a las reuniones realizadas se inicio con mitigar en los servidores que presentaban vulnerabilidade de SSl desactualizado y el cual reportaba critico , para con ello quitar ese vector , se avanzo en un 2% ya que actividades distintas quitaron tiempo para culminar esta actividad
7.Presentación del plan y estrategia de mitigación , con responsables y tiempo limite de aplicación de remediaciones	Ing. Henry Cepeda presentado al equipo de Infraestructura	7/07/2023	7/07/2023	5%	5%	Elplan propuesto según las reuniones fue , que con el Ing de SO (Fredy Salinas) se realizara un 75% de correcciones en los SO
8. Validación de los tiempos por parte de los participantes en las acciones de Mitigación y generar el plan de accion de remediacion	Equipo Infraestructura	10/07/2023	14/07/2023	5%	5%	Las validaciones de tiempos se dieron y con Fredy se concluyo que tenemos lo que ,mas afecta los tiempos de correccion es que algunos sistemas pueden requerir reinicio lo que apuntaria a una ventana para la aplicación de los cambios
9. Ejecución Plan de Acción de remediación de vulnerabilidades top 25-10 Definitivo y retroalimentación de posibles inconvenientes , y realizar seguimiento	Equipo Infraestructura	17/07/2023	17/10/2023	10%	10%	Con base a las reuniones la evidencia de los tipos de correccion que se debe aplicar e incluyendo los servidores que se dan de baja o se migran , este item inició su avance // se realizan remediaciones en Waf referentyes a perfiles de seguridad
10.Con base al resultado de remediaciones evaluar el % de correcciones aplicadas y con esto se **emitirá un informe de la primera etapa de Gestión de vulnerabilidades**	Ing. Henry Cepeda Ing. Angel Perez	18/10/2023	25/10/2023	10%	10%	se hacen dos lanzamientos de escaneos , a las dos infraestructuras fisica y virtual , se obtienen datos que muestran correcciones en algunos servidores pero descublimiento de nuevas vulnerabilidades.
11. Segundo **escaneo de vulnerabilidades con herramienta Tenable** acotando los servidores definidos en el plan de acción	Ing. Henry Cepeda Ing. Angel Perez	16/08/2023	23/08/2023	10%	10%	scaneo realizado al target de WAF se inicia a parametrizar en la herramienta de escaneo el analisis que se realizara en agosto
12.**Socializacion y retroalimentación de los resultados obtenidos en el segundo escaneo**, realizando la comparación de la línea base con respecto al resultado del segundo escaneo	Equipo Infraestructura	26/10/2023	27/10/2023	6%	6%	realizar esta reunion para mostrar y aportar el avsnce corespondiente , mostrar las evidencias de el escaneo , y hasta donde se pudo llegar con base a la mitigacion // reunion programada para diciembre 18 para exponer lo realizado y dar las recoendaciones
13.**Generar un plan con un nuevo grupo de mitigación de vulnerabilidades** basado en el segundo escaneo, el cual debe incluir nuevas vulnerabilidades y ampliación del espectro de acción en servidores	Ing. Henry Cepeda	30/10/2023	3/11/2023	8%	8%	el nuevo plan se basara en hacer que TODOS los servicios que se exponen asi sea para conexiones VPN pasen por WAF y de esta manera mitigar vulnerabilidades Se realizará un plan de acción propuesto para la vigencia 2024// el nuevo plan debe incluir en su gran mayoria al area de desarrollo ya que por la evidencia de esta vigencia se denoto la falencia en desarrollo seguro
14. **presentar el plan de Acción de el Segundo Grupo** de Servidores - Definitivo	Equipo Infraestructura	6/11/2023	6/11/2023	10%	10%	realizar plan para proxima vigencia
		TOTALES		**100%**	**100%**	

Fuente: Evidencia 18. PlanDeAccion_GestionVulnerabilidades enviado por la Dirección TIC como respuesta al cuestionario de la OCI

- Se siguen presentando dificultades para la remediación de vulnerabilidades, tal y como fue identificado en el Informe de Auditoría vigencia 2022, es decir, se repiten las situaciones identificadas:

  (…) *"No fueron 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."*

- Menciona la Dirección de TIC acciones y contratos relacionados con Firewall Aplicaciones, Firewall Perimetral, Solución Antivirus, las cuales contribuyen a mitigar riesgos, no obstante, se observa que se siguen repitiendo las situaciones observadas en vigencias anteriores respecto a la remediación de las vulnerabilidades.



171 Vulnerabilidades Críticas

Outstanding Remediations By Device Type

	System	Low	Medium	High	Critical	Exploitable
Linux	0	0	0	0	0	0
Unix	0	0	0	0	0	0
Apple	0	0	0	0	0	0
Network	2	0	0	0	2	0 %

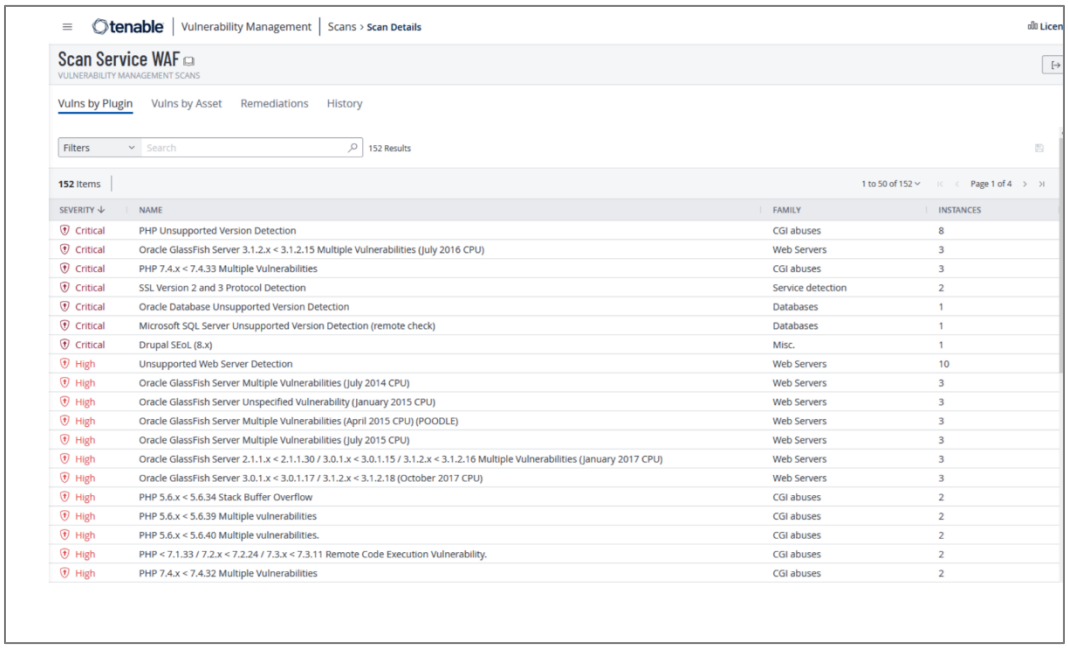
The End of Life Software Detection table lists the top 100 vulnerabilities related to End of Life software. A plugin filter indicating the software is unsupported by the vendor is used for indentification

End of Life Software Detection

Plugin	Plugin Name	Severity	Host Total
108797	Unsupported Windows OS (remote)	Critical	26
34460	Unsupported Web Server Detection	High	17
84729	Microsoft Windows Server 2003 Unsupported Installation Detection	Critical	7
55786	Oracle Database Unsupported Version Detection	Critical	6
58987	PHP Unsupported Version Detection	Critical	5
73756	Microsoft SQL Server Unsupported Version Detection (remote check)	Critical	4
97994	Microsoft IIS 6.0 Unsupported Version Detection	Critical	4
78555	OpenSSL Unsupported	Critical	3
56997	VMware ESX / ESXi Unsupported Version Detection	Critical	2
64475	HP Data Protector Unsupported	Critical	1
73182	Microsoft Windows XP Unsupported Installation Detection	Critical	1

Severity Summary

Fuente: Evidencia 18- Respuesta recibida de la Dirección TIC



SEVERITY	NAME	FAMILY	INSTANCES
Critical	PHP Unsupported Version Detection	CGI abuses	8
Critical	Oracle GlassFish Server 3.1.2.x < 3.1.2.15 Multiple Vulnerabilities (July 2016 CPU)	Web Servers	3
Critical	PHP 7.4.x < 7.4.33 Multiple Vulnerabilities	CGI abuses	3
Critical	SSL Version 2 and 3 Protocol Detection	Service detection	2
Critical	Oracle Database Unsupported Version Detection	Databases	1
Critical	Microsoft SQL Server Unsupported Version Detection (remote check)	Databases	1
Critical	Drupal SEoL (8.x)	Misc.	1
High	Unsupported Web Server Detection	Web Servers	10
High	Oracle GlassFish Server Multiple Vulnerabilities (July 2014 CPU)	Web Servers	3
High	Oracle GlassFish Server Unspecified Vulnerability (January 2015 CPU)	Web Servers	3
High	Oracle GlassFish Server Multiple Vulnerabilities (April 2015 CPU) (POODLE)	Web Servers	3
High	Oracle GlassFish Server Multiple Vulnerabilities (July 2015 CPU)	Web Servers	3
High	Oracle GlassFish Server 2.1.1.x < 2.1.1.30 / 3.0.1.x < 3.0.1.15 / 3.1.2.x < 3.1.2.16 Multiple Vulnerabilities (January 2017 CPU)	Web Servers	3
High	Oracle GlassFish Server 3.0.1.x < 3.0.1.17 / 3.1.2.x < 3.1.2.18 (October 2017 CPU)	Web Servers	3
High	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	CGI abuses	2
High	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	CGI abuses	2
High	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.	CGI abuses	2
High	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	CGI abuses	2
High	PHP 7.4.x < 7.4.32 Multiple Vulnerabilities	CGI abuses	2

Fuente: Evidencia 18- Respuesta recibida de la Dirección TIC

Como se mencionó anteriormente existe una criticidad importante a nivel del software y de infraestructura, aspecto que afecta las acciones y esfuerzos que se realizan en la SDP relacionada con la gestión de vulnerabilidades; a nivel de software que soporta las aplicaciones de la SDP, algunos ya cumplieron su ciclo e incluso se tiene software obsoleto y sin soporte.

Se recomienda efectuar un análisis de causas a profundidad que permita identificar un plan de trabajo con acciones orientadas a la efectividad en la gestión de vulnerabilidades, con apoyo de la alta Dirección dado el impacto que puede generar en los procesos y servicios de la entidad.

Por los argumentos expuestos y el impacto que tiene el tema de gestión de vulnerabilidades para la ciberseguridad y la protección de la información de la entidad, se mantiene la situación crítica.

4.4.3.4 INDISPONIBILIDAD NO PROGRAMADA DE SERVICIOS DE TI

La indisponibilidad no programada de servicios de TI puede generar graves consecuencias para la Secretaría Distrital de Planeación (SDP), como la pérdida de productividad, la interrupción de operaciones críticas y el daño a la reputación. Para afrontar estos casos de manera efectiva y minimizar su impacto, la SDP a través de la Dirección de Tecnologías de la Información y las comunicaciones realizó las siguientes actividades en la vigencia 2023:

1. Recorrido diario de los centros de cómputo y centros de cableado para la detección de incidentes
2. Implementación del sistema de monitoreo host monitor para detectar anomalías de operación de los equipos de TI.
3. Uso de la herramienta GLPI para que los usuarios reporten incidentes de forma oportuna.
4. Contratación de personal experto para la gestión del incidente y la restauración del servicio.
5. Priorización de la restauración de los servicios críticos para la organización
6. Informar de forma oportuna a los usuarios y partes interesadas a través de mensajes información mediante correo electrónico.
7. Análisis de las causas del incidente para identificar las áreas de mejora.
8. Mantenimientos preventivos regulares de los sistemas de TI.
9. Implementación de actualizaciones de seguridad de manera oportuna.
10. Contratación de servicios especializados de TI confiables para brindar soporte en caso de incidentes.

4.4.3.5 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
Control A.16

La Dirección de TIC registró 14 incidentes de seguridad, desde la herramienta de mesa de ayuda GLPI todos de impacto medio, los cuales estuvieron relacionados con: actualización firewall- emergencia, correo electrónico sospechoso, correos no deseados, error correos electrónicos, falta de conectividad a las carpetas compartidas instaladas en mi PC, posible detección de virus en correspondencia externa, productos financieros, sin conexión a ARC GIS, Solicitud BackUp, solicitud de listas negras y solicitud listado usuarios, clasificados en urgencia mediana, alta y muy alta, con tiempos de espera enmarcados en alguno de los siguientes:

0 Segundo(s)
1 Hora(s) 13 Minuto(s)
15 Minuto(s)
5 Dí-a(s) 22 Hora(s) 56 Minuto(s)
6 Dí-a(s) 21 Minuto(s)
7 Hora(s) 54 Minuto(s)
8 Dí-a(s) 22 Hora(s) 13 Minuto(s)

El más demorado se dio con ocasión de una falsa alarma sobre un posible virus en correspondencia.

Los tiempos de atención fueron de

1 Hora(s)
10 Minuto(s)
11 Minuto(s)
13 Minuto(s)
16 Hora(s) 1 Minuto(s)
16 Minuto(s)
2 Hora(s) 45 Minuto(s)
3 Minuto(s)
31 Minuto(s)
34 Minuto(s)
39 Minuto(s)
8 Minuto(s)

El mayor de ellos se dio con ocasión de una solicitud de listado usuarios, para lo cual no es claro que para la solución/cierre se invirtieran 197 Dí-a(s) 22 Hora(s) 5 Minuto(s), si el tiempo de espera fue de 0 Segundo(s) y el tiempo para atender el servicio fue de 16 Hora(s) 1 Minuto(s).

De acuerdo con los estándares establecidos en la norma ISO 27001, específicamente en el Dominio A16: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y, en particular, en el Control A16.1.6: Aprendizaje obtenido de los incidentes de seguridad de la información, El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

La Dirección de TIC mencionó que, en el desarrollo de la gestión de los incidentes reportados en la herramienta de mesa de ayuda, no se identificaron aprendizajes nuevos ni lecciones aprendidas diferentes a la ya conocidas y socializadas al interior de la Dirección de Tecnologías de la Información y las Comunicaciones.

4.4.3.6 PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

Control A.18.1.4

Medidas de seguridad para proteger los datos personales:

La Dirección TIC realizó acciones dentro de las medidas encaminadas a proteger los datos personales en la entidad dentro de las cuales se implementaron:

- Capacitaciones directas y otras en colaboración con la Consejería Distrital de TIC se realizó socialización sobre la protección de datos personales. Capacitación en materia de protección de datos personales: https://drive.google.com/file/d/1zwrd9zENFXGrbGIk4NvMnY4h1c3oGZnA/view

- Se cuenta con un sistema automatizado para la gestión de usuarios y contraseñas mediante el cual se tiene establecida la política para solicitar a todos los usuarios el cambio de contraseñas cada mes.

- La SDP cuenta con una herramienta para el control de instalaciones de software, mediante este mecanismo se controla que solo personal autorizado por la Dirección de TIC realice instalaciones y desinstalaciones de software.

- La SDP realiza un análisis de vulnerabilidad y aplicabilidad del software antes de su instalación.

- Publicación de la política de datos personales en la sede electrónica.

- Mecanismos de control para la autenticidad, integridad y no repudio: firmas digitales

- Capacitación en seguridad de la información y protección de datos personales: Capacitación a través de la escuela del pensamiento https://drive.google.com/file/d/1zwrd9zENFXGrbGIk4NvMnY4h1c3oGZnA/view

- Controles de seguridad para proteger los sistemas de información:

  Controles técnicos
  Controles de acceso: Se cuenta con mecanismos de autenticación y autorización para restringir el acceso a los sistemas de información solo a usuarios autorizados. Esto incluye el uso de contraseñas seguras y tokens de autenticación de dos factores.

  Evidencia: Contrato CtoFirmasDigitale_764-2023

  Gestión de vulnerabilidades: Se realiza un proceso continuo para identificar, evaluar y remediar las vulnerabilidades de seguridad en los sistemas de información. Esto incluye la instalación de actualizaciones de software y parches de seguridad de manera oportuna.

  Evidencia: **Proyecto01_GestionVulnerabilidades**

  Protección de redes: Implementar firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para proteger las redes de la SDP contra ataques cibernéticos.

  Evidencia: CtoMttoFirewall 603-2023 (2) (1) el IDS e IPS son funcionalidad del Firewall

  Cifrado de datos: Cifrar los datos confidenciales en reposo y en tránsito para protegerlos contra el acceso no autorizado.

  La solución de VPN maneja cifrado de datos. Evidencia: No se encontró la evidencia

  Copias de seguridad y recuperación de desastres: cuenta con un plan de copias de seguridad y se adelanta un contrato para la implementación del DRP para garantizar que la información de la SDP pueda ser restaurada en caso de un incidente de seguridad.

  Controles organizativos:

Se cuenta con una política de seguridad de la información mediante la cual se definen los requisitos de seguridad para los sistemas de información de la SDP.
La entidad cuenta con procedimientos de seguridad que describan cómo se deben implementar los controles de seguridad.

La SDP brinda capacitación periódica a los servidores públicos, contratistas y pasantes activos en la entidad sobre seguridad de la información y cómo proteger los sistemas de información.

Se realizan estrategias para fomentar una cultura de conciencia de seguridad dentro de la SDP para que los servidores públicos, contratistas y pasantes activos en la entidad estén atentos a las amenazas y sepan cómo informar incidentes de seguridad.

Controles físicos

Las medidas de seguridad física para proteger los activos físicos de la SDP, como los servidores y los dispositivos de almacenamiento incluye el control de acceso físico a las instalaciones, el uso de cámaras de seguridad y la implementación de medidas de seguridad contra incendios e inundaciones.

Se cuenta con un proceso de borrado seguro de información en los equipos de la SDP cuando ya no sea necesaria o por baja de bienes, a través de la mesa de ayuda de la Dirección de TIC.

Preservación de la confidencialidad, integridad, disponibilidad y privacidad de los datos en la SDP

La Dirección de TIC informó que se implementaron entre otras las siguientes medidas:

Confidencialidad:

- Se ha restringido el acceso a áreas seguras a las personas autorizadas.
- Se han implementado medidas de seguridad para proteger los datos contra el acceso no autorizado.
- Se ha capacitado a los funcionarios de la SDP en materia de confidencialidad de la información.

Integridad:

- Se han implementado medidas de seguridad para proteger los datos contra la alteración no autorizada como por ejemplo autorización de permisos y roles en los sistemas de información.
- Se han establecido mecanismos para controlar y registrar los cambios realizados en los datos. Uno de ellos es la recolección de logs de bases de datos y registro del usuario que realiza los cambios.
- Se han realizado copias de seguridad de los datos de forma periódica.

Disponibilidad:

- Se han implementado medidas de seguridad para proteger los datos contra la pérdida o destrucción accidental o intencional.
- Se han establecido Acuerdos de Nivel de Servicios – ANS en el contrato con proveedores de infraestructura y sistemas de información.
- Se ha realizado un mantenimiento preventivo de los sistemas de información que almacenan los datos.

Privacidad:

- Se ha obtenido el consentimiento de los ciudadanos para la recolección y tratamiento de sus datos personales, a través de la Dirección de Servicio a la Ciudadanía.
- Se ha capacitado a los funcionarios de la SDP en materia de protección de datos personales. https://drive.google.com/file/d/1zwrd9zENFXGrbGIk4NvMnY4h1c3oGZnA/view

Evidencias:

- **Políticas y procedimientos para la confidencialidad, integridad, disponibilidad y privacidad de los datos:**

Modelo de seguridad y privacidad de la información de la SDP . A-LE-373
Plan de mantenimiento de infraestructura tecnológica de la SDP . A-LE-389
Políticas de protección de datos personales. A-LE-289
Política para la gestión de copias de respaldo y recuperación de la información institucional. A-LE-297
Política de control de acceso. A-LE-315
Política de escritorio y pantalla limpios. A-LE-317
Política de uso de medios removibles. A-LE-320
Política para el uso de dispositivos móviles en la SDP. A-LE-321
Política de uso de software. A-LE-362
Política de capacitación y sensibilización en seguridad de la información en la SDP. A-LE-375
Políticas de seguridad y privacidad de la información. A-LE-429
Política para la gestión de carpetas compartidas. A-LE-414

- **Medidas de seguridad para proteger la confidencialidad de los datos:**

Política de control de acceso. A-LE-315
Controles biométricos en las entradas a todas las áreas.

Capacitaciones en inducción y reinducción, adicionalmente se realizan jornadas de socialización en materia de confidencialidad de la información.

- **Mecanismos para controlar y registrar los cambios realizados en los datos:** Se recolectan y almacenan Logs de las transacciones en las soluciones de software definidas.

- **Copias de seguridad de los datos:** Bitácora de copias de seguridad

- **Planes de recuperación de desastres:** Contrato 744 – 2023 del DRP

- **Mantenimiento preventivo de los sistemas de información:** Contratos de mantenimiento.
- **Consentimiento de los ciudadanos para la recolección y tratamiento de sus datos personales:**

  Solicitud para consulta o reclamos de datos personales. M-FO-130
  Atención de solicitudes de información, consultas y reclamos - datos personales. M-PD-163
  Autorización de tratamiento de datos personales. A-FO-530
  Políticas de protección de datos personales. A-LE-289

Protección de datos almacenados en la nube

La Secretaría Distrital de Planeación suscribió el Contrato 810-2022 con UT SOAIN THINK IT y renovó el servicio mediante Contrato 744-2023 con Unión Temporal Nube Pública It.

Con el objeto de preservar y proteger los datos almacenados y en tránsito en la nube, la SDP realizó las siguientes actividades:

• Arquitectura de Referencia Nube Oracle.
• Selección del proveedor de servicios en la nube confiable a través de la plataforma Colombia Compra Eficiente con el fin de garantizar que tanto el contrato como los acuerdos de nivel de servicio (SLAs) cumplen con los requisitos de protección de datos y que tenga las certificaciones de seguridad y privacidad adecuadas.
• Implementación de controles de acceso para restringir el acceso a los datos en la nube solo a las personas autorizadas y para limitar el acceso a los datos.
• Monitoreo y registro de la actividad en la nube para detectar actividades sospechosas mediante la consola de administración del proveedor.

Situación Critica

Sobre este particular es importante mencionar que el control A.18.1.4 Privacidad y protección de datos personales menciona que “Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes”.

Dentro de los contenidos de la Política de Protección de Datos Personales (A-LE-289), se hace alusión a que "la Secretaría Distrital de Planeación adoptará las medidas técnicas, humanas y administrativas para garantizar la seguridad de la información registrada en las bases de datos, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

A pesar de las acciones y los esfuerzos realizados por la Dirección de TIC se encontró por parte del equipo auditor que, al hacer la consulta aleatoria de 16 radicados de la vigencia 2023 y sus soportes en el Sistema de Información de Procesos Automáticos-SIPA, **se puede acceder abiertamente a información sensible de los funcionarios** relacionada con temas tales como: teletrabajo, calamidad, permisos, cuenta bancaria, diagnóstico médico incapacidades, historias clínicas asociadas a incapacidades, acoso, entre otros.

La situación identificada contraviene el Literal g) del artículo 4 de la Ley 1581 de 2012, "la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, **consulta, uso o acceso no autorizado** o fraudulento" y el control A.18.1.4 Privacidad y protección de datos personales del MSPI

Es importante recordar el Principio de Responsabilidad Demostrada. Artículo 26, del Decreto 1377 de 2013. En materia de Tratamiento de Datos personales impera la necesidad de implementar medidas de responsabilidad demostrada o "accountability', que exige a los Responsables **la capacidad de demostrar**, a petición de la Superintendencia de Industria y Comercio, que se han implementado medidas **apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto**.

Mediante correo electrónico del 31 de octubre de 2024, la Dirección de TIC manifestó lo siguiente:

"El Sistema de Procesos Automáticos SIPA de la SDP cuenta con la funcionalidad de colocar candado de seguridad a los procesos creados en el módulo de correspondencia, esto sin excepción aplica para que todos los usuarios que hacen uso del sistema y quienes bajo criterio propio consideren que la comunicación a tramitar contiene datos sensibles, es así como se ofrece un mecanismo de seguridad de la información para los usuarios internos, quienes deben marcar la opción respectiva en el momento de crear y tramitar sus procesos."

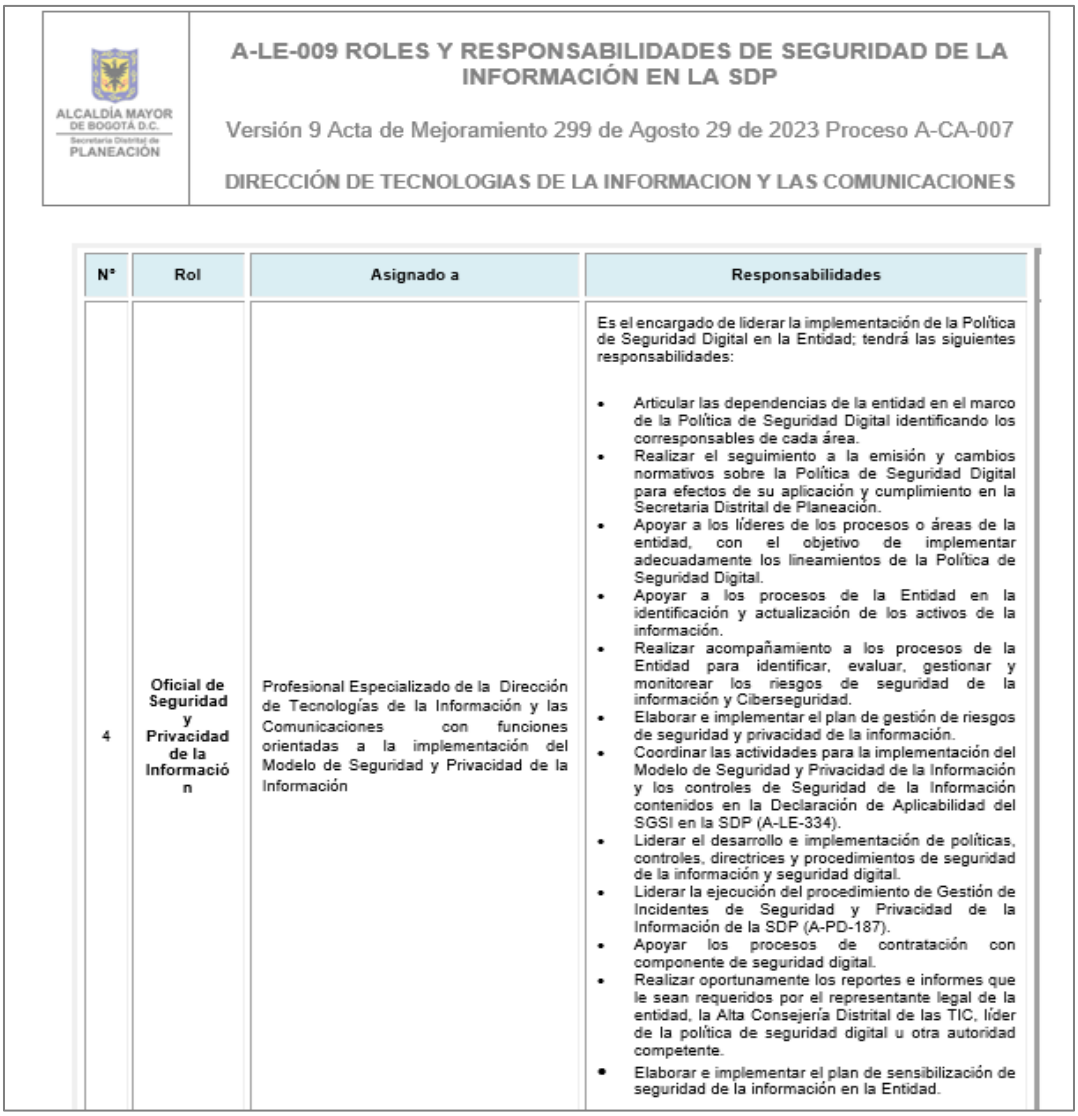
Análisis de la respuesta por parte de la OCI:

La Oficina de Control Interno revisó cada una de las acciones adelantadas y encaminadas a la protección de datos personales descritas por la Dirección de TIC, no obstante, al hacer la prueba en el Sistema de Información de Procesos Automáticos-SIPA, se evidenció la materialización del riesgo. Es importante mencionar que la aplicación de la Política de protección de datos personales no es a discreción de "*quienes bajo criterio*

propio consideren que la comunicación a tramitar contiene datos sensibles", de acuerdo a la respuesta de la Dirección de TIC.

Se evidenció que no fue suficiente ni efectiva la funcionalidad de colocar candado de seguridad a los procesos creados en el módulo de correspondencia para garantizar la seguridad y privacidad de información personal, ya que de acuerdo a la prueba realizada por el equipo auditor de la OCI, se evidenció que no se trató de un caso aislado, sino que como se mencionó anteriormente, se detectaron 16 casos tomados de forma aleatoria.

De otra parte y de acuerdo al documento "Roles y Responsabilidades de Seguridad de la Información en la SDP", Versión 9 Acta de Mejoramiento 299 de Agosto 29 de 2023, revisado durante el desarrollo de la auditoría, documento en el cual se presentan los roles y responsabilidades definidos para la gestión de la seguridad de la información en la SDP, en concordancia con las Políticas de Gobierno y Seguridad Digital se observan las responsabilidades asignadas al Oficial de Seguridad y Privacidad de la Información, dentro de los cuales se encuentra "*Liderar el desarrollo e implementación de políticas, controles, directrices y procedimientos de seguridad de la información y seguridad digital"* y además:



ALCALDÍA MAYOR DE BOGOTÁ D.C.
Secretaría Distrital de PLANEACIÓN

A-LE-009 ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP

Versión 9 Acta de Mejoramiento 299 de Agosto 29 de 2023 Proceso A-CA-007

DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES

N°	Rol	Asignado a	Responsabilidades
4	**Oficial de Seguridad y Privacidad de la Información**	Profesional Especializado de la Dirección de Tecnologías de la Información y las Comunicaciones con funciones orientadas a la implementación del Modelo de Seguridad y Privacidad de la Información	Es el encargado de liderar la implementación de la Política de Seguridad Digital en la Entidad; tendrá las siguientes responsabilidades: • Articular las dependencias de la entidad en el marco de la Política de Seguridad Digital identificando los corresponsables de cada área. • Realizar el seguimiento a la emisión y cambios normativos sobre la Política de Seguridad Digital para efectos de su aplicación y cumplimiento en la Secretaria Distrital de Planeación. • Apoyar a los líderes de los procesos o áreas de la entidad, con el objetivo de implementar adecuadamente los lineamientos de la Política de Seguridad Digital. • Apoyar a los procesos de la Entidad en la identificación y actualización de los activos de la información. • Realizar acompañamiento a los procesos de la Entidad para identificar, evaluar, gestionar y monitorear los riesgos de seguridad de la información y Ciberseguridad. • Elaborar e implementar el plan de gestión de riesgos de seguridad y privacidad de la información. • Coordinar las actividades para la implementación del Modelo de Seguridad y Privacidad de la Información y los controles de Seguridad de la Información contenidos en la Declaración de Aplicabilidad del SGSI en la SDP (A-LE-334). • Liderar el desarrollo e implementación de políticas, controles, directrices y procedimientos de seguridad de la información y seguridad digital. • Liderar la ejecución del procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información de la SDP (A-PD-187). • Apoyar los procesos de contratación con componente de seguridad digital. • Realizar oportunamente los reportes e informes que le sean requeridos por el representante legal de la entidad, la Alta Consejería Distrital de las TIC, líder de la política de seguridad digital u otra autoridad competente. • Elaborar e implementar el plan de sensibilización de seguridad de la información en la Entidad.

Igualmente, se retoman algunos principios contemplados en el Acuerdo 822 de 2021, “Por medio del cual se dictan los lineamientos para la promoción del ciclo virtuoso de la seguridad, el uso y aprovechamiento de los datos en Bogotá” Artículo 3. Principios que deben regir en el uso de los datos:

d. Principio de responsabilidad demostrada. Compromiso de las autoridades distritales por incrementar sus estándares de protección para garantizar a las personas sus derechos como titulares y mantenerlos actualizados.

e. Principio de anonimización de los datos. Se velará por la privacidad de los datos personales y se anonimizarán cuando estos sean de uso abierto.

g. Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas,

humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Finalmente, es importante mencionar que frente a los hallazgos que se relacionan en los informes, deben participar todas las direcciones involucradas en los mismos.

Por lo anterior, la Oficina de Control Interno mantiene la situación crítica, con el fin de que se identifiquen las causas y se formulen las acciones correctivas que eviten que se vuelva a materializar la situación encontrada.

4.4.3. 7 COPIAS DE RESPALDO

Control A.12.3. Este control menciona que se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

El equipo auditor realizó visita al Datacenter, el cual se tiene en convenio con la Secretaría Distrital de Hacienda para verificar cómo se conservaban las copias de respaldo de la información. Así mismo solicitó la realización de prueba de restauración de información de un backup.

Se puedo verificar que la Entidad guarda las copias de respaldo en tres sitios diferentes:

1) Datacenter Secretaría Distrital de Hacienda Segundo Piso CADE,

2) Datacenter Principal de la SDP y fuera.

3)Fuera de la SDP bajo la custodia del GRUPO TIEDOT SAS.

El Contrato suscrito en el 2023 con la empresa de Guardacustodia corresponde al No. 713-2023 con el objeto: "Prestar el servicio de guarda custodia y transporte de medios magnéticos y documentos de la SDP.”

Como evidencia se cuenta con instrumentos de gestión como: La “Política para la gestión de copias de respaldo y recuperación de la información institucional” y el Procedimiento de “Copias de seguridad y recuperación de información”. Adicionalmente, se tiene la programación de copias de respaldo en las soluciones (A-FO-295 por demanda), imagen del registro de eventos de DataProtector y Veeam y de las restauraciones del 2023.

PRUEBA DE RESTURACIÓN DE BACKUP

Se solicitó y efectuó Prueba de Restauración de Backup el 21 de junio de 2024, la cual se pudo realizar de manera satisfactoria:

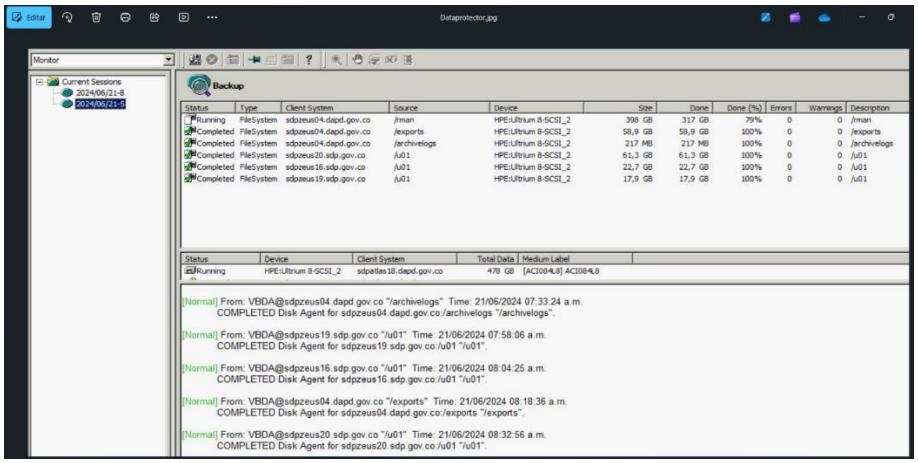
A-FO-296 BITÁCORA CINTOTECA
Versión 5 Acta de Mejoramiento 366 de Octubre 05 de 2023 Proceso A-CA-007
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

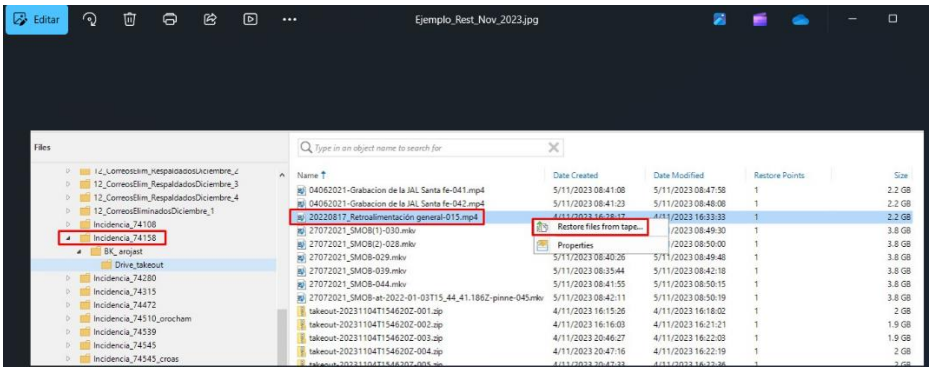
Etiqueta de la cinta	Ubicación de la cinta	Estado	Solución de backup utilizada	Fecha de Protección (DD/MM/AAAA)	Fecha Retiro Libreria (DD/MM/AAAA)	Políticas / Jobs	Año de Expiración (AAAA)	Responsable Movimiento	Observaciones
ACI080L8	Libreria	Good	DataProtector			Free_Pool_DP		Alejandro Chala	
ACI081L8	Empresa Guarda Custodia	Good	DataProtector	01/02/2028 07:27 p.m.	01/03/2023	PoolLTO_Anual_Linux	02/2028	Alejandro Chala	
ACI082L8	Cintoteca de Hacienda	Good	DataProtector	01/01/2025 11:59 a.m.	23/05/2024	PoolLTO_Anual_Windows	01/2025	Alejandro Chala	
ACI083L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	12/03/2021	PoolLTO_Semanal_Linux	manente	Alejandro Chala	
ACI084L8	Libreria	Good	DataProtector			Free_Pool_DP		Alejandro Chala	
ACI085L8	Empresa Guarda Custodia	Good	DataProtector	01/01/2025 06:20 p.m.	22/04/2023	PoolLTO_Anual_Linux	01/2025	Alejandro Chala	
ACI086L8	Libreria	Good	DataProtector			Free_Pool_DP		Alejandro Chala	
ACI087L8	Empresa Guarda Custodia	Blank	DataProtector	Permanente	05/03/2021	Pool001_Varios_LTO	manente	Alejandro Chala	
ACI088L8	Cintoteca de Hacienda	Good	DataProtector	08/01/2024 10:46:02 p.m.	05/03/2021	PoolLTO_Anual_Linux	01/2024	Alejandro Chala	
ACI089L8	Cintoteca de Hacienda	Good	DataProtector	15/07/2023 01:57 p.m.	22/04/2023	PoolLTO_Semanal_Linux	07/2023	Alejandro Chala	
ACI090L8	Empresa Guarda Custodia	Good	DataProtector	09/09/2024 10:49 p.m.	22/04/2023	PoolLTO_Mensual_Linux	09/2024	Alejandro Chala	
ACI091L8	Libreria	Good	DataProtector	Permanente		Pool01_Varios_LTO	manente	Alejandro Chala	
ACI092L8	Empresa Guarda Custodia	Good	DataProtector	19/06/2024 09:03 p.m.	26/12/2022	PoolLTO_Mensual_Windows	06/2024	Alejandro Chala	
ACI093L8	Empresa Guarda Custodia	Good	DataProtector	31/01/2028 11:26 p.m.	01/03/2023	PoolLTO_Anual_Linux	01/2028	Alejandro Chala	
ACI094L8	Empresa Guarda Custodia	Good	DataProtector	22/01/2028 07:26 p.m.	01/03/2023	PoolLTO_Anual_Linux	01/2028	Alejandro Chala	
ACI095L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	01/03/2023	Pool001_Varios_LTO	manente	Alejandro Chala	
ACI096L8	Empresa Guarda Custodia	Good	DataProtector	19/09/2024 05:42 a.m.	18/04/2023	PoolLTO_Mensual_Windows	09/2024	Alejandro Chala	
ACI097L8	Empresa Guarda Custodia	Good	DataProtector	09/09/2024 10:49 p.m.	22/04/2023	PoolLTO_Mensual_Linux	09/2024	Alejandro Chala	
ACI098L8	Cintoteca de Hacienda	Good	DataProtector	28/08/2023 09:19 a.m.	15/03/2022	PoolLTO_Network_Windows	08/2023	Alejandro Chala	
ACI099L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	08/10/2010	internaldatabase	manente	Alejandro Chala	
ACI100L8	Cintoteca de Hacienda	Good	DataProtector	08/01/2024 11:24 p.m.	20/12/2023	PoolLTO_Diario_Produccion	01/2024	Alejandro Chala	
ACI101L8	Cintoteca de Hacienda	Good	DataProtector	21/02/2024 08:28 a.m.	04/01/2024	PoolLTO_Mensual_Linux	02/2024	Alejandro Chala	
ACI102L8	Empresa Guarda Custodia	Good	DataProtector	12/03/2025 10:52 a.m.	05/10/2023	PoolLTO_Mensual_Linux	03/2025	Alejandro Chala	
ACI103L8	Cintoteca de Hacienda	Good	DataProtector	13/10/2023 03:25 a.m.	05/10/2023	PoolLTO_Diario_Produccion	10/2023	Alejandro Chala	
ACI104L8	Cintoteca de Hacienda	Good	DataProtector	18/04/2024 01:46 a.m.	19/11/2022	PoolLTO_Mensual_Windows	04/2024	Alejandro Chala	
ACI105L8	Cintoteca de Hacienda	Good	DataProtector	03/11/2023 01:18 a.m.	05/10/2023	PoolLTO_Diario_Produccion	11/2023	Alejandro Chala	
ACI106L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	18/06/2012	internaldatabase	manente	Alejandro Chala	
ACI107L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	26/10/2021	PoolLTO_Mensual_Linux	manente	Alejandro Chala	
ACI108L8	Cintoteca de Hacienda	Good	DataProtector	22/09/2023 03:06 p.m.	04/07/2023	PoolLTO_Semanal_Linux	09/2023	Alejandro Chala	
ACI109L8	Cintoteca de Hacienda	Good	Veeam	08/09/2024 02:29 A.M.	17/06/2024	SEMANAL #9	09/2024	Alejandro Chala	
ACI110L8	Empresa Guarda Custodia	Good	DataProtector	Permanente	09/08/2012	internaldatabase	manente	Alejandro Chala	
ACI111L8	Cintoteca de Hacienda	Off Line	DataProtector			Free_Pool		Alejandro Chala	
ACI112L8	Cintoteca de Hacienda	Good	Veeam	11/06/2024 04:27 a.m.	01/04/2024	GFS SEMANAL #21	06/2024	Alejandro Chala	
ACI113L8	Empresa Guarda Custodia	Good	DataProtector	22/05/2025 07:00 a.m.	20/12/2023	PoolLTO_Mensual_Linux	05/2025	Alejandro Chala	
ACI114L8	Libreria	Good	Veeam	11/09/2035 15:00 P.M.		MENSUAL #22	09/2035	Alejandro Chala	

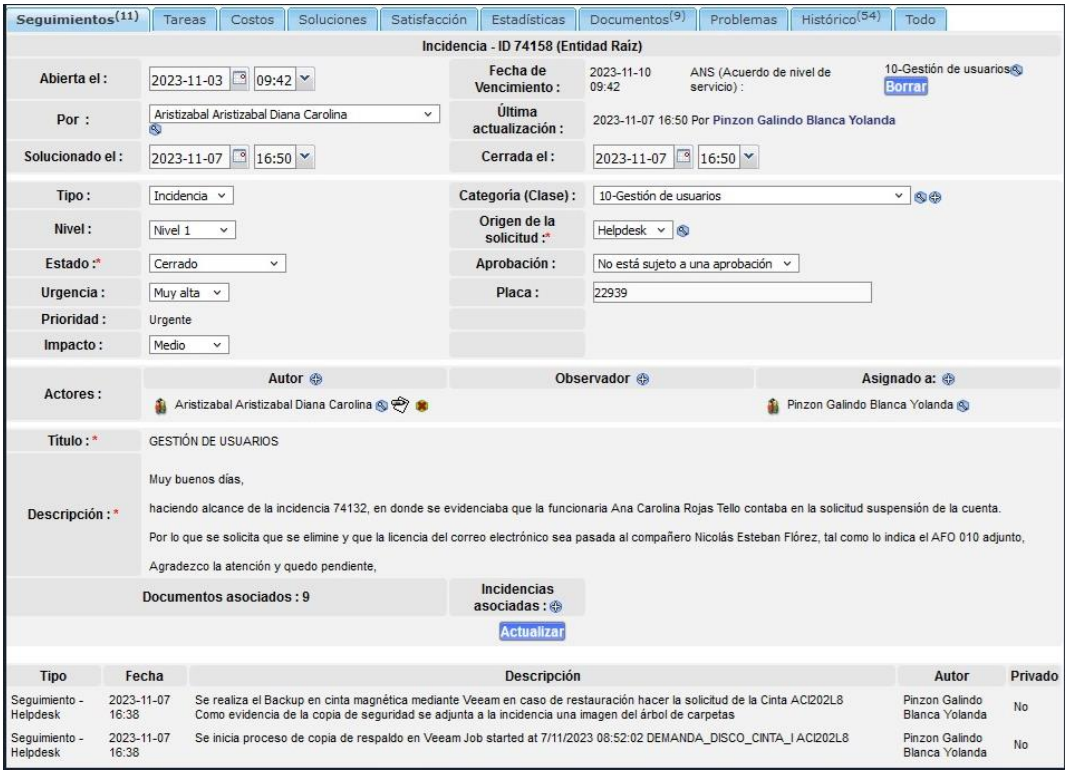
A-FO-295 BITÁCORA DE COPIAS DE RESPALDO SOBRE EQUIPOS DE CÓMPUTO o SERVIDORES
Versión 2 acta de mejoramiento 271 de abril 7 de 2016 Proceso A-CA-007
DIRECCION DE SISTEMAS

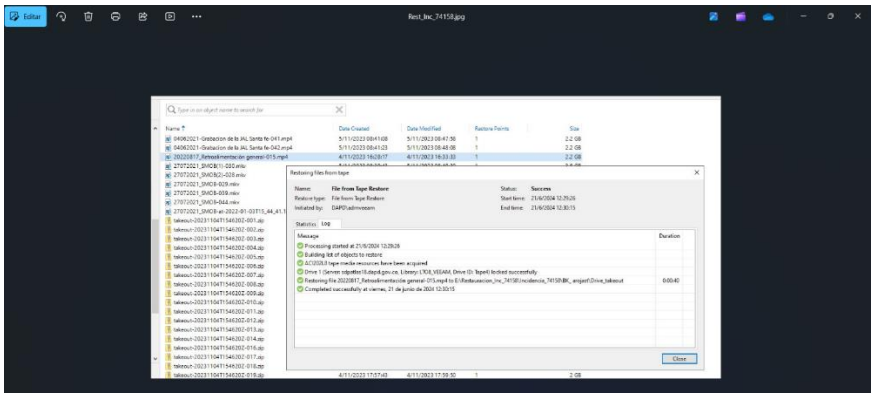
Fecha <día/mes/año ..>	No. Ticket	Nombre Solicitante	Nombre Carpeta Principal	Número de Sesión	Código de la cinta	Nombre Equipo con Agente	Observaciones
1/11/2023	74001	Laiton Sergio Andres	Disco COLABORACION2:\Incidencia_74001	VEEAM	ACI202L8	1065SDP22	Se realiza copia de respaldo satisfactoriamente
1/11/2023	74026	Ceballos Garcia Samaris Magnolia	ID_eromeroj_74026	VEEAM	ACI202L8	1065SDP22	Se realiza copia de respaldo satisfactoriamente
2/11/2023	74009	Chala Granados Alejandro	/OVS/Repositories/0004fb000030000e0ff0dc81561ef1e	2023/11/02-10	ACI151L8	SDPTHOR06	Se realiza restauración satisfactoriamente
2/11/2023	74108	Pinzon Bermudez Jose Antonio	G:\Incidencia_74108\BK_ jforero	VEEAM	ACI202L8	1065SDP22	Se realiza copia de respaldo satisfactoriamente
7/11/2023	74158	Diana Carolina Aristizabal Aristizabal	G:\Incidencia_74158\BK_ arojast	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente
8/11/2023	74213	Rativa Martin John Edgar	\\1065sdp21\GS\02_Eliminados_Febrero_II\	VEEAM	ACI202L8	1065SDP21	Se realiza copia de respaldo satisfactoriamente
8/11/2023	74216	Rativa Martin John Edgar	\\1065sdp21\GS\03_Eliminados_Marzo_II	VEEAM	ACI202L8	1065SDP21	Se realiza copia de respaldo satisfactoriamente
8/11/2023	74230	Rativa Martin John Edgar	\\1065sdp21\GS\04_Eliminados_Abril	VEEAM	ACI202L8	1065SDP21	Se realiza copia de respaldo satisfactoriamente
8/11/2023	74231	Rativa Martin John Edgar	\\1065sdp21\GS\05_Eliminados_Mayo	VEEAM	ACI202L8	1065SDP21	Se realiza copia de respaldo satisfactoriamente
9/11/2023	74238	Rativa Martin John Edgar	\\1065sdp21\GS\08_Eliminados_Agosto	VEEAM	ACI202L8	1065SDP21	Se realiza copia de respaldo satisfactoriamente
15/11/2023	74280	Andres Leonardo Acosta Hernandez	G:\Incidencia_74280\BK_lquintero	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente
22/11/2023	74315	Juan David Vinasco Idarraga	G:\Incidencia_74315\BK_gmosquera	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente
22/11/2023	74407	Bejarano Rubiano Nohora Isabel	/exports/bk_permanentes/incidencia_74407	2023/11/22-7	ACI091L8	SDPZEUS04	Se realiza copia de respaldo satisfactoriamente
22/11/2023	74425	Bejarano Rubiano Nohora Isabel	/exports/bk_permanentes/incidencia_despues cierre_74425	2023/11/22-7	ACI091L8	SDPZEUS04	Se realiza copia de respaldo satisfactoriamente
23/11/2023	74472	Nelson Humberto Gamboa Baracaldo	G:\Incidencia_74472\BK_nlozanop	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente
23/11/2023	74491	Cotes Solano Rosmery	sdpapolo16	2023/11/23-9	ACI151L8 ACI137L8	SDPAPOLO16	Se realiza restauración satisfactoriamente
23/11/2023	74545	Diana Carolina Aristizabal Aristizabal	G:\Incidencia_74545_econteras	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente Bizon de econteras@sdp.gov.co contratista de Gestion Contractual
27/11/2023	74539	Carolina Herrera Ramirez	G:\Incidencia_74539\BK_smarin	VEEAM	ACI202L8	1065SDP88	Se realiza copia de respaldo satisfactoriamente Bizon de smarin@sdp.gov.co contratista de Gestion Contractual

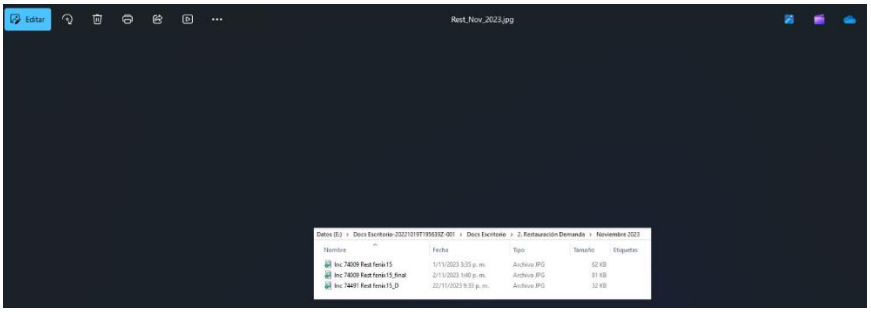
Nombre	Fecha	Tipo	Tamaño
Inc 74001 ggonzaleza	1/11/2023 10:30 a. m.	Archivo JPG	47 KB
Inc 74001 ggonzaleza_final	1/11/2023 11:46 a. m.	Archivo JPG	75 KB
Inc 74001 ggonzaleza_peso	1/11/2023 10:31 a. m.	Archivo JPG	57 KB
Inc 74026 eromeroj	1/11/2023 11:48 a. m.	Archivo JPG	33 KB
Inc 74026 eromeroj_final	1/11/2023 12:30 p. m.	Archivo JPG	75 KB
Inc 74026 eromeroj_peso	1/11/2023 11:49 a. m.	Archivo JPG	56 KB
Inc 74108 jforero	2/11/2023 1:47 p. m.	Archivo JPG	48 KB
Inc 74108 jforero_final	2/11/2023 2:35 p. m.	Archivo JPG	68 KB
Inc 74108 jforero_peso	2/11/2023 1:48 p. m.	Archivo JPG	57 KB
Inc 74213 02_Eliminados_Febrero_II	8/11/2023 11:11 a. m.	Archivo JPG	45 KB
Inc 74213 02_Eliminados_Febrero_II_Final	8/11/2023 5:08 p. m.	Archivo JPG	73 KB
Inc 74213 02_Eliminados_Febrero_II_Peso	8/11/2023 11:11 a. m.	Archivo JPG	59 KB
Inc 74216 03_Eliminados_Marzo_II	8/11/2023 5:14 p. m.	Archivo JPG	50 KB
Inc 74216 03_Eliminados_Marzo_II_Peso	8/11/2023 5:16 p. m.	Archivo JPG	57 KB
Inc 74216-74230-74231 Final	9/11/2023 8:05 a. m.	Archivo JPG	73 KB
Inc 74216-74230-74231 Peso	8/11/2023 5:20 p. m.	Archivo JPG	63 KB
Inc 74230 04_Eliminados_Abril	8/11/2023 5:15 p. m.	Archivo JPG	52 KB
Inc 74230 04_Eliminados_Abril_Peso	8/11/2023 5:17 p. m.	Archivo JPG	57 KB
Inc 74231 05_Eliminados_Mayo	8/11/2023 5:16 p. m.	Archivo JPG	46 KB
Inc 74231 05_Eliminados_Mayo_Peso	8/11/2023 5:18 p. m.	Archivo JPG	56 KB
Inc 74238 08_Eliminados_Agosto	9/11/2023 8:11 a. m.	Archivo JPG	45 KB
Inc 74238 08_Eliminados_Agosto_Final	9/11/2023 9:35 a. m.	Archivo JPG	69 KB
Inc 74238 08_Eliminados_Agosto_Peso	9/11/2023 8:11 a. m.	Archivo JPG	60 KB
Inc 74407 Bk_Antes 74425 Bk_Dps Nomina	22/11/2023 1:47 p. m.	Archivo JPG	38 KB
Inc 74407 Bk_Antes 74425 Bk_Dps Nomina_final	22/11/2023 2:52 p. m.	Archivo JPG	108 KB


Dataprotector.jpg
Backup
[Normal] From: VBDA@sdpzeus04.dapd.gov.co "/archivelogs" Time: 21/06/2024 07:33:24 a.m.
COMPLETED Disk Agent for sdpzeus04.dapd.gov.co:/archivelogs "/archivelogs".
[Normal] From: VBDA@sdpzeus19.sdp.gov.co "/u01" Time: 21/06/2024 07:58:06 a.m.
COMPLETED Disk Agent for sdpzeus19.sdp.gov.co:/u01 "/u01".
[Normal] From: VBDA@sdpzeus16.sdp.gov.co "/u01" Time: 21/06/2024 08:04:25 a.m.
COMPLETED Disk Agent for sdpzeus16.sdp.gov.co:/u01 "/u01".
[Normal] From: VBDA@sdpzeus04.dapd.gov.co "/exports" Time: 21/06/2024 08:18:36 a.m.
COMPLETED Disk Agent for sdpzeus04.dapd.gov.co:/exports "/exports".
[Normal] From: VBDA@sdpzeus20.sdp.gov.co "/u01" Time: 21/06/2024 08:32:56 a.m.
COMPLETED Disk Agent for sdpzeus20.sdp.gov.co:/u01 "/u01".


Editar
Ejemplo_Rest_Nov_2023.jpg
Files
Incidencia_74158
20220817_Retroalimentación general-015.mp4
Restore files from tape...
Properties


Seguimientos(11)
Tareas
Costos
Soluciones
Satisfacción
Estadísticas
Documentos(9)
Problemas
Histórico(54)
Todo
Incidencia - ID 74158 (Entidad Raíz)
Abierta el : 2023-11-03 09:42
Fecha de Vencimiento : 2023-11-10 09:42
ANS (Acuerdo de nivel de servicio) :
10-Gestión de usuarios
Borrar
Por : Aristizabal Aristizabal Diana Carolina
Última actualización : 2023-11-07 16:50 Por Pinzon Galindo Blanca Yolanda
Solucionado el : 2023-11-07 16:50
Cerrada el : 2023-11-07 16:50
Tipo : Incidencia
Categoría (Clase) : 10-Gestión de usuarios
Nivel : Nivel 1
Origen de la solicitud :* Helpdesk
Estado :* Cerrado
Aprobación : No está sujeto a una aprobación
Urgencia : Muy alta
Placa : 22939
Prioridad : Urgente
Impacto : Medio
Actores :
Autor
Observador
Asignado a:
Aristizabal Aristizabal Diana Carolina
Pinzon Galindo Blanca Yolanda
Título : * GESTIÓN DE USUARIOS
Descripción : *
Muy buenos días,
haciendo alcance de la incidencia 74132, en donde se evidenciaba que la funcionaria Ana Carolina Rojas Tello contaba en la solicitud suspensión de la cuenta.
Por lo que se solicita que se elimine y que la licencia del correo electrónico sea pasada al compañero Nicolás Esteban Flórez, tal como lo indica el AFO 010 adjunto,
Agradezco la atención y quedo pendiente,
Documentos asociados : 9
Incidencias asociadas :
Actualizar
Tipo
Fecha
Descripción
Autor
Privado
Seguimiento - Helpdesk
2023-11-07 16:38
Se realiza el Backup en cinta magnética mediante Veeam en caso de restauración hacer la solicitud de la Cinta ACI202L8
Como evidencia de la copia de seguridad se adjunta a la incidencia una imagen del árbol de carpetas
Pinzon Galindo Blanca Yolanda
No
Seguimiento - Helpdesk
2023-11-07 16:38
Se inicia proceso de copia de respaldo en Veeam Job started at 7/11/2023 08:52:02 DEMANDA_DISCO_CINTA_I ACI202L8
Pinzon Galindo Blanca Yolanda
No





4.4.3.8 MANTENIMIENTO DE EQUIPOS.

Control A.11.2.4 Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas

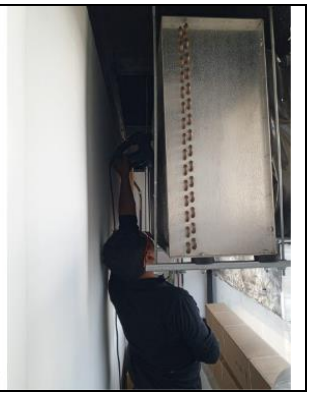
Se solicitó por parte del equipo auditor evidencia del Mantenimiento Preventivo del Aire Acondicionado de Precisión del Datacenter principal de la SDP, el cual es de suma importancia para proteger la integridad de los servidores, controlando los niveles de humedad y temperatura en el centro de datos. Es así como se obtuvo la ficha técnica que arrojó el estado del Aire Acondicionado de Precisión.

Es importante mencionar que se verificaron entre otros los siguientes aspectos:

Verificación del área de trabajo -	
Revisión de condiciones iniciales: Revise las condiciones iniciales de operación en temperatura ambiente, temperatura de suministro y humedad relativa. Recuerde verificar también los valores en el panel, revise la temperatura y humedad por cada sensor. -	

Estado de motores: Revise la operación de los motores, verifique que no existan ruidos fuera de lo normal, fisuras o partes sueltas. -	
Revisión de compresor:Verifique la ausencia de sonidos anormales y vibraciones. Revise que no existan manchas de aceite en el compresor o en paredes, suelo y tubería del equipo. -	

Revisión de acumulador de succión y modulo Inverter:Revise que el acumulador de succión no tenga fugas de gas refrigerante líquido. Por otro lado revise el estado general de limpieza del módulo inverter. Revise las válvulas de servicio, que no existan manchas de aceite en los gusanillos y no se evidencien fugas. -	
Revisión de circuitos de control y fuerza: Retire la tapa del sistema eléctrico del equipo, verifique que no exista ningún componente con evidencia de quemadura o sulfatado. Revise que la tarjeta no se encuentre alarmada. Revise las borneras del breaker totalizador del equipo, verifique ajuste de bornes y ausencia de desgaste o evidencia de recalentamiento. -	

Estado de la Tarjeta AT: Revise que el led que esté alumbrado sea el verde, verifique que los cables de comunicación no estén rotos o sueltos (revise su conexión especialmente la tierra). -		Estado de la Tarjeta AT: Revise que el led que esté alumbrado sea el verde, verifique que los cables de comunicación no estén rotos o sueltos (revise su conexión especialmente la tierra). -	
Revise que la tarjeta IOC se encuentre con una buena conexión -		Limpieza general interna del equipo -	
Limpieza externa de condensadora -		Limpieza externa de condensadora -	

Como observaciones generales se observa que el proveedor realizó el mantenimiento preventivo y que el equipo queda funcionando en óptimas condiciones.

De otra parte, la firma que efectuó el mantenimiento recomendó el cambio de cilindro humidificador, **por tener pasadas las horas de uso del fabricante.**

Situación crítica

Se observó en el reporte del mantenimiento no programado del Aire Acondicionado de Precisión del Datacenter principal de la SDP, que el cilindro humidificador debía ser cambiado por "tener pasadas las horas de uso del fabricante."

Frente a la Situación Crítica No 9 identificada en la Auditoría, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Se solicita de manera respetuosa reconsiderar y retirar la situación crítica reportada, dada la siguiente argumentación:

El equipo de aire acondicionado en mención (Piso 5) cuenta con garantía activa y vigente hasta marzo de 2025 de conformidad con las condiciones del contrato 626 de 2021. Desde la Dirección de TIC se siguió el procedimiento según el respectivo protocolo, una vez se alarmó el equipo de aire se solicitó la revisión, el proveedor programó visita y dio solución."

Análisis de la respuesta por parte de la OCI:

Se solicitó aclaración a la Dirección de TIC, dado que, si el equipo de aire acondicionado tiene garantía hasta marzo de 2025, no es comprensible la observación consignada en el reporte realizado por el proveedor al efectuar el mantenimiento de junio de 2024, en el cual recomendó el "*cambio de cilindro humidificador, **por tener pasadas las horas de uso del fabricante."***

El proveedor aclaró al ingeniero de la Dirección de TIC que *"reemplazará el cilindro humidificador, el cual fue solicitado para importación y estará llegando a finales de noviembre o primera semana de diciembre. Que actualmente tiene 6428 horas. Y que, a pesar de funcionar las 24 horas, hay días en los que se requiere mas humidificación y hay días en los cuales no se usa el humidificador, ya que depende de las condiciones del ambiente. Que no hay fecha exacta para el cambio, ya que se va verificando con los mantenimientos."*

La Oficina de Control interno solicitó el plan de mantenimiento, el cual fue enviado via correo electrónico:

Datos Generales	Contrato	x	Convenio		No.	626	2021
	Tipo	CONTRATO DE PRESTACION DE SERVICIOS				
Contratista	REDNEET					
Identificación (CC – Nit)	9.004.344.627					
Representante Legal	John Velasco Rodriguez REPRESENTANTE LEGAL					
Objeto	Adquirir los elementos necesarios para la instalación y puesta en funcionamiento de los centros de cableado de la SDP.					

Elemento de Infraestructura Objeto de Mantenimiento	SERIAL	Fecha Inicial Programada	Fecha Final Programada	Fecha Inicio Ejecucion	Fecha Fin Ejecucion	Verificación Supervisión	Nro servicio Tecnico	Recomendaciones Mantenimiento Preventivo
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	29/12/2022	29/12/2022	29/12/2022	29/12/2022	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	15/03/2023	15/03/2023	15/03/2023	15/03/2023	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	27/06/2023	27/06/2023	27/06/2023	27/06/2023	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	12/09/2023	12/09/2023	12/09/2023	12/09/2023	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	12/12/2023	12/12/2023	12/12/2023	12/12/2023	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	12/03/2024	12/03/2024	13/03/2024	13/03/2024	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	12/06/2024	12/06/2024	20/06/2024	20/06/2024	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	10/09/2024	10/09/2024	14/10/2024	14/10/2024	ok		
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	10/12/2024	10/12/2024					
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	11/03/2025	11/03/2025					
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	10/06/2025	10/06/2025					
Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 (AQ-EQ-RDNT-	15023461	10/09/2025	10/09/2025					

MantenimientosPreventivos

Fuente Dirección de TIC

Así mismo, la Dirección de TIC por solicitud de la Oficina de Control Interno, remitió las siguientes órdenes de trabajo de mantenimiento realizadas al Aire Acondicionado Stulz 5 TR CCD 151 A 15023461 { AQ-EQ-RDNT-001 }

Fecha	No Orden	Código de Barras	Prioridad	Descripción	Fecha y Hora de Inicio	Fecha y Hora de Finalización	Observaciones
13/03/24 10:03 a.m.	OTT-S8851	Tarea No Planificada	Alta	Mantenimiento Preventivo de Aire Acondicionado de Precisión	13/03/24 12:50 pm	13/03/24 12:50 pm	Fue realizada la limpieza del cilindro humidificador y de los demás componentes. Estado del humidificador: Aprobado
26/06/2024 9:08 a.m.	OTT-S9529	Tarea No Planificada	Alta	Mantenimiento Preventivo de Aire Acondicionado de Precisión	20/06/24 15:55 p.m.	20/06/24 15:55 p.m.	Se realiza mantenimiento preventivo y el equipo queda funcionando sin alarmas. Se recomienda cambio de cilndro humidificador, por tener pasadas las horas de uso recomendadas por el fabricante.
14/10/24 22:37	OTT-S10443	Tarea No Planificada	Alta	Mantenimiento Preventivo de Aire Acondicionado de Precisión	15/10/24 11:27 a.m.	15/10/24 11:27 a.m.	Se encuentra el equipo en funcionamiento alarmado por falla en el humidificador, el código de error se presenta por falta de agua al momento del llenado. Se limpia el sistema de humidificación, se desalarma la tarjeta. Se hacen pruebas de funcionamiento. Se realiza mantenimiento preventivo y el equipo queda en funcionamiento sin alarmas. Se cambia el set point de temperatura de 21.5 a 20.5

Fuente: Elaboración propia con base en las órdenes de mantenimiento enviadas por la Dirección de TIC

En conclusión, se observó que los mantenimientos al Aire Acondicionado del Datacenter principal de la SDP se realizan cuatro veces en el año. Sin embargo, no es clara la clasificación en las órdenes de trabajo en el sentido de que se trata de una “Tarea no Planificada” y al revisar las observaciones se puede ver que se generaron alarmas en el funcionamiento del aire acondicionado, es decir, que pasa de lo preventivo a lo correctivo.

Así mismo, aún no quedó claro porqué el proveedor menciona que el cilindro humidificador tenía pasadas las horas de uso recomendadas por el fabricante, cuando de acuerdo con lo informado por la Dirección de TIC la garantía se vence en marzo de 2025. De igual manera, al revisar el detalle de las órdenes de trabajo, se observa que no es consistente la hora de inicio y de finalización de dichos trabajos. Por último, se recomienda diligenciar en su totalidad el cuadro excel suministrado, para que sea un verdadero instrumento de seguimiento y control del Equipo de aire acondicionado para la Dirección de TIC, ya que se observó que no está diligenciado en su totalidad, por lo que no agrega valor.

Se cambia de “Situación Crítica” a “Situaciones susceptibles de mejora / oportunidades (observaciones)”

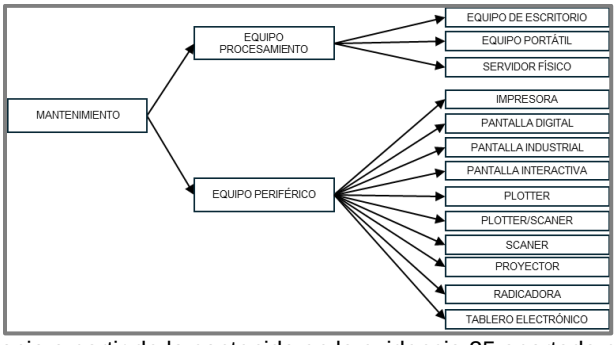
4.4.3.9 MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS

La Secretaría Distrital de Planeación en la vigencia 2023 atendió el mantenimiento preventivo y correctivo de equipos mediante los contratos:

Contrato No. 529 de 2022 suscrito con System Digital Computer SAS cuyo objeto consistió en “Prestar el servicio de mantenimiento preventivo y correctivo de los equipos de cómputo propiedad de la SDP con reposición de elementos”. El cual inició el 23/05/2022 y vencimiento 22/05/2023.

Contrato No. 589 de 2023 suscrito con la Firma System Digital Computer SAS con objeto “ Prestar el servicio de mantenimiento preventivo y correctivo de los equipos de cómputo propiedad de la SDP, con reposición de elementos el cual inició el 23/05/2023 y finalizó el 22 de febrero de 2024.

El mantenimiento preventivo se adelantó en dos frentes: equipos de procesamiento y equipos periféricos



Fuente: Análisis propio a partir de lo contenido en la evidencia 25 aportada por la Dirección TIC

La evidencia corresponde a la formulación y ejecución del plan de mantenimiento preventivo de la vigencia.

4.4.3.10 LICENCIAS DE SOFTWARE DE LOS EQUIPOS SDP - VIGENCIA 2023

En cumplimiento de la Ley 23 de 1982 y la Ley 1712 de 2014, la SDP formuló la política de uso de software A-LE-362 en la cual se establecen los lineamientos mínimos necesarios, aplicables al interior de la Secretaría Distrital de Planeación para 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).

En este documento se definen directrices claras para el uso del software dando lineamientos frente al cumplimiento del procedimiento de uso de software, el respeto a los Derechos de Autor, condiciones del licenciamiento, derecho de uso de software o

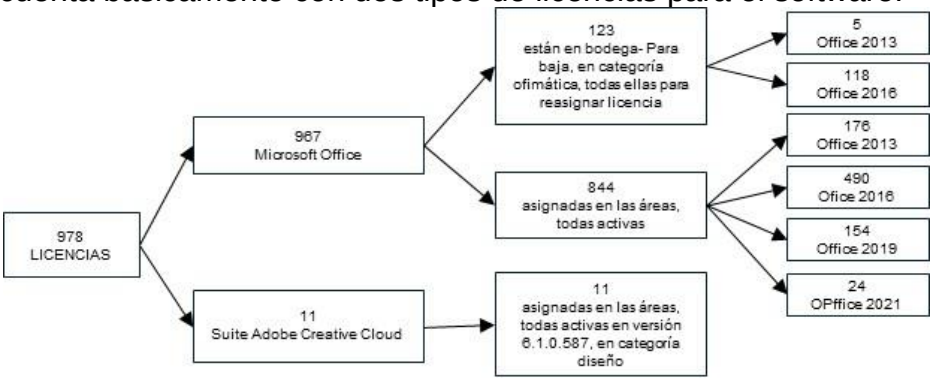
condiciones por trasferencia de terceros, la administración y control del Software como activo institucional, la revisión del software instalado de la SDP, el uso de software legal en el desarrollo de productos y servicios y la solicitud de instalación de software.

Así mismo, define las responsabilidades que le competen a la Dirección TIC, como son la instalación software, llevar el control del licenciamiento adquirido y autorizado, dar concepto para el uso de software específico (propietario, freeware y software libre). En cuanto a los usuarios, la citada política define que les corresponde entre otras responsabilidades las de utilizar únicamente software licenciado o autorizado en la SDP, observar la normatividad en el desarrollo de productos o servicios. Para el caso del grupo directivo de la SDP, establece directrices sobre las solicitudes de software y para asegurar que los productos que demanden la utilización de cualquier tipo de software sean elaborados con software legal y aprobado por la Dirección TIC.

Adicionalmente, esta política articulada con el modelo de seguridad y privacidad de la información es complementada con las siguientes políticas:

- Políticas de Seguridad y Privacidad de la Información. A-LE-429
- Política de Control de Acceso A-LE-315
- Política de Desarrollo Seguro A-LE-359

La entidad cuenta básicamente con dos tipos de licencias para el software:



Fuente: Análisis propio a partir de lo contenido en la evidencia 23

Se indagó a la Dirección de TIC sobre cuál fue el destino final que se le dio al software dado de baja en la SDP en la vigencia 2023, frente a la cual se recibió la siguiente respuesta:

El destino final del software en la Secretaría Distrital de Planeación, se da acorde con lo definido en la Resolución 001 de 2019 Secretaría Distrital de Hacienda - Contaduría General de Bogotá D.C. y el anexo 1 Manual de Procedimientos Administrativos y Contables para el manejo y control de los bienes en las Entidades de Gobierno Distritales, y el procedimiento A-PD-045 Administración De Bienes De La SDP, Versión 23 aprobada mediante Acta de Mejoramiento 248 de octubre 03 de 2022, instrumentos en los cuales se establecieron los lineamientos para el tratamiento de los bienes intangibles y la disposición final.

En aplicación de estas directrices, a la Dirección de Tecnologías de la Información y las Comunicaciones, le corresponde realizar periódicamente la revisión del software y emitir concepto técnico acerca del estado de obsolescencia siguiendo lo establecido en el procedimiento mencionado, informando a la Dirección Administrativa para la gestión del proceso de disposición final conforme lo establece el manual.

La evidencia corresponde a los procedimientos A-PD-166, A-PD-045 y A-PD-028, los cuales pueden ser consultados en SIPA Módulo Control de Documentos. https://sipa.sdp.gov.co/sipa/

4.4.3.11 EQUIPOS

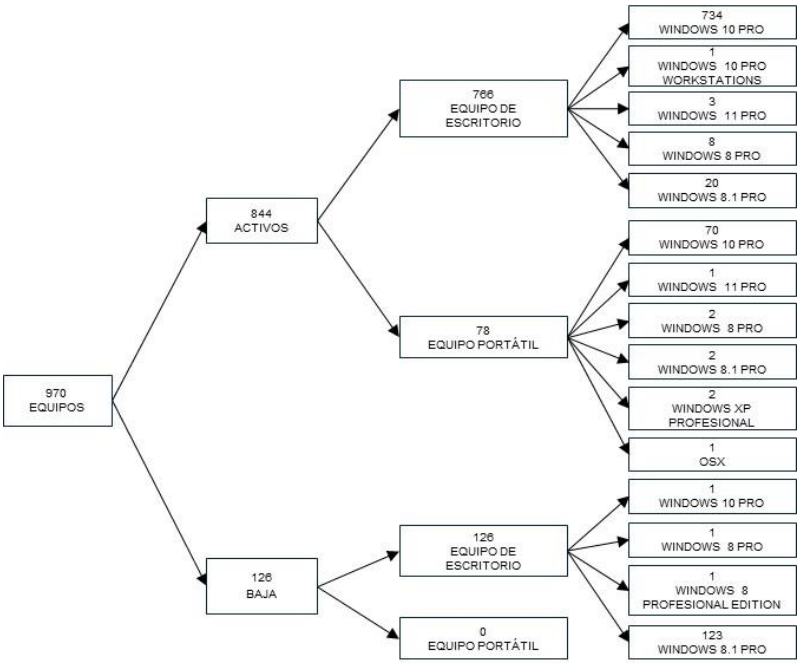
Respecto al destino final de los equipos de cómputo que fueron renovados o cambiados en la vigencia 2023 se tiene que:

El destino final de los equipos de cómputo en la Secretaría Distrital de Planeación, se da acorde con lo definido en la Resolución 001 de 2019 Secretaría Distrital de Hacienda - Contaduría General de Bogotá D.C. y el anexo 1 Manual de Procedimientos Administrativos y Contables para el manejo y control de los bienes en las Entidades de Gobierno Distritales, y el procedimiento Administración de bienes de la SDP, A-PD-045 Versión 23 aprobada mediante Acta de Mejoramiento 248 de octubre 03 de 2022, instrumentos en los cuales se establecieron los lineamientos para el tratamiento de los bienes intangibles y la disposición final.

En aplicación de estas directrices, a la Dirección de Tecnologías de la Información y las Comunicaciones, le corresponde realizar periódicamente la revisión del hardware y emitir concepto técnico acerca del estado de obsolescencia siguiendo lo establecido en el procedimiento mencionado, informando a la Dirección Administrativa para la gestión del proceso de disposición final conforme lo establece el manual.

La evidencia corresponde al listado de la renovación de 132 equipos durante el 2023 en el marco del Contrato 644-2022 e inventario de la totalidad de 844 equipos de cómputo y portátiles.

Por su parte, en la matriz de Equipos Entregados, Instalados Y Configurados - Marco Del Contrato 644-2022, entregada por la Dirección de TIC, teniendo en consideración que dicho reporte es a 30 de diciembre de 2023, se encontró desactualización en la información toda vez que hay personas que aparecen como usuarios a cargo de los equipos a diciembre 30 de 2023 pero se retiraron de la entidad antes de dicha fecha, por ejemplo el director de Registros Sociales (1064SBO06, 2043SDP03 y 2043SDP04) que se retiró de la entidad en junio 12 de 2023, y la Subsecretaria Jurídica que se retiró en junio 23 del mismo año (205SDP02).



Fuente: Análisis propio a partir de lo contenido en la evidencia 25 equipos de cómputo SDP - vigencia 2023

Situación Crítica:

En la matriz Equipos Entregados, Instalados y Configurados entregada por la Dirección de TIC, se encontró desactualización en la información toda vez que hay personas que aparecen como usuarios a cargo de los equipos a diciembre 30 de 2023 pero se retiraron de la entidad antes de dicha fecha, por ejemplo el director de Registros Sociales (1064SBO06, 2043SDP03 y 2043SDP04) que se retiró de la entidad en junio 12 de 2023, y la Subsecretaria Jurídica que se retiró en junio 23 del mismo año (205SDP02).

Frente a la Situación Crítica No 9 (antes 10) identificada en la Auditoría, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Se solicita de manera respetuosa reconsiderar y retirar la situación critica reportada, dada la siguiente argumentación:

Según el procedimiento GTI-PD-002 Soporte y Atención de la Mesa de Ayuda se establece que el Jefe de Área debe crear 3 incidencias cuando se presenta el retiro de un empleado, una de ellas es la entrega de los equipos a cargo a la nueva persona que queda responsable de los bienes. Con base en esa incidencia la Dirección de TIC realiza la respectiva actualización en el aplicativo GLPI, quedando así el registro del nuevo responsable. Si la incidencia no es creada en la mesa de ayuda de la Dirección de TIC (caso del exfuncionario Helmut Menjura), dichos bienes seguirán registrados al funcionario retirado, razón se considera necesario que desde la Dirección Administrativa se informen dichas novedades al momento de firmar el paz y salvo y de esa manera mediante la incidencia que ellos creen poder realizar los cambios desde la Dirección de TIC."

Análisis de la respuesta por parte de la OCI:

La entidad tiene establecido que con el formato “Entrega de Bienes y Documentos” AFO 128, todos los servidores públicos solicitan el paz y salvo para su retiro, previo la recolección de firmas, entre ellas de la Dirección de TIC para la deshabilitación de la cuenta de usuario, del correo institucional y sistemas de información, así como solicitud de copias de respaldo de información del equipo que tenía a cargo o asignado, y se hace la solicitud de entrega del equipo. De igual manera se entrega el carnet de la Entidad y la tarjeta de acceso. P

Ahora respecto a la observación de la Dirección de TIC relacionada con *: “Si la incidencia no es creada en la mesa de ayuda de la Dirección de TIC (caso del exfuncionario Helmut Menjura), dichos bienes seguirán registrados al funcionario retirado”* , no es aceptable para esta auditoria, ya que finalmente el control de los bienes informáticos también está en cabeza de la Dirección de TIC, así como lo enunciado anteriormente, la deshabilitación de la cuenta de usuario y del correo institucional, entre otros aspectos.

Por lo que se identificó una debilidad en los controles que ejecuta la Dirección de TIC ya que al deshabilitar el usuario o el correo se debió tener un soporte para realizar dicha acción y es de conocimiento institucional el retiro del Director Helmut Menjura como Dirección de la entonces Dirección de Sisbén.

Finalmente, la Dirección de TIC en el análisis de la situación crítica deberá hacer los análisis correspondientes para identificar las acciones correctivas a que haya lugar, y que eviten que se vuelva a materializar la situación encontrada,

Por lo expuesto, se ratifican las debilidades encontradas dado que los argumentos de la respuesta no desvirtúan las inconsistencias señaladas por la auditoría, razón por la que se mantiene la situación crítica

DISPOSITIVOS MÓVILES.

Respecto a la política para el Uso de Dispositivos Móviles en la SDP (A-LE-321), se preguntó a la Dirección de TIC acerca de cuáles son los dispositivos móviles (Smartphones, Tabletas, Relojes inteligentes, Laptops y Chromebooks, Dispositivos de realidad virtual - VR) que están activos y cómo están asignados en la entidad.

Sobre el particular se recibió la respuesta de la Dirección de TIC así:

- La entidad cuenta con 78 portátiles, que se utilizan para las labores administrativas y operativas de las diferentes dependencias.
- En el año 2023 se adquirió una tableta como equipo de trabajo del despacho de la Secretaría, la cual se encuentra asignada al Secretario Distrital de Planeación.

- La entidad cuenta con equipos móviles a cargo de la Dirección de Registros Sociales y de la Dirección Administrativa, de lo cual adjuntan archivo en Excel con el nombre "Inventario_Completo".
- No se cuentan con dispositivos de realidad virtual, Chromebooks, relojes inteligentes u otros tipos de dispositivos móviles en la SDP.

4.4.4 FASE 3: EVALUACIÓN DE DESEMPEÑO

Indicadores de Gestión Seguridad de la Información 2023
Situación crítica:

Respecto a los Indicadores de Gestión Seguridad de la Información, se encontraron diferencias en la información remitida por la Dirección de TIC en la programación como en el seguimiento:

1)Evidencia 14: El "Plan de Modelo de Seguridad y Privacidad de la Información de la SDP", A-LE -373, Versión 5 Acta de Mejoramiento 257 de Julio 27 de 2023.
2)Evidencia 9: Documento "Avances y Logros_MSPI_Dic_2023_12032024" como entrada para la Revisión por la Dirección.
3)Evidencia 8 .Plan de acción de controles MSPI 2023.

Comparativo información -Indicadores de Gestión Seguridad de la Información 2023							
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**META PERIODO EVIDENCIA 14**	**META PERIODO EVIDENCIA 9**	**EJECUCION REPORTADA EVIDENCIA 9**	**Observaciones OCI**
ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Nivel de Compromiso de la Alta Dirección	Hacer seguimiento, al compromiso sobre el sistema seguridad de la información, por parte de la alta dirección	# de revisiones realizadas por la alta dirección al año / # revisiones programadas para el año	100%	100%	100%	Sin observaciones
CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la SDP revisados y actualizados	Revisar y actualizar los activos de información de la SDP por proceso	# de procesos con activos de información (RAI) revisados y actualizados en la vigencia/# de procesos de la SDP	95%	95%	11%	En el indicador la Dirección de TIC mencionó que se actualizaron los activos de información de 15 procesos programados. Por lo que no es claro el porcentaje de avance
PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN	Nivel de Ejecución del Plan de Capacitación y Sensibilización en Seguridad de la Información de la SDP	Hacer seguimiento a la ejecución del Plan Capacitación y Sensibilización en Seguridad de la Información de la SDP	# de estrategias desarrolladas al año que cumplen con la meta de ejecución >=90% / # de estrategias programadas para desarrollar al año siguiendo lo establecido en el plan de capacitación y sensibilización	90%	80%	100%	Está diferente la programación , aunque se destacan las acciones adelantadas en este indicador
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP	Porcentaje de políticas de Seguridad de la Información actualizadas o definidas en la vigencia	Mide el porcentaje de actualización o creación de políticas de seguridad de la información definidas en la vigencia	# de políticas de Seguridad de la Información actualizadas o creadas en la vigencia / # de políticas de seguridad de la información planeadas para actualización o creación en la vigencia	90%	100%	100%	Está diferente la programación
EJECUCIÓN DEL MSPI EN LA SDP	Nivel de Madurez de las fases del MSPI	Controlar el avance de las Fases del MSPI en términos de Madurez	# de actividades desarrolladas durante la vigencia en el Plan de Acción del MSPI / # de actividades definidas para desarrollar en la vigencia en el Plan de Acción del MSPI	90%	90%	100%	No es coherente este reporte de ejecución con el documento de la evidencia 8 , denominado 8.1_PlandeAccionControles2023 que da cuenta de la ejecución de los controles del MSPI, teniendo en cuenta que existe dificultad para conocer con precisión el nivel de implementación de controles del MPSI para la vigencia 2023, capítulo 4.4.3.1 de este informe
GESTIÓN DE INCIDENCIAS DE SEGURIDAD	Porcentaje de atención a las incidencias de seguridad realizadas por los usuarios de la SDP	Medir el porcentaje de incidencias de Seguridad de la Información atendidas en la vigencia	(# de incidencias de seguridad atendidas en la vigencia /# de incidencias de seguridad recibidas en la vigencia) *100	92%	100%	100%	Está diferente la programación

Fuente: Elaboración propia, con base en los documentos de las evidencias 8, 9 y 14

Evidencia 14. Indicadores de Gestión Seguridad de la Información						
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**TIPO**	**UNIDAD DE MEDIDA**	**META PERIODO**
ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Nivel de Compromiso de la Alta Dirección	Hacer seguimiento, al compromiso sobre el sistema seguridad de la información, por parte de la alta dirección	# de revisiones realizadas por la alta dirección al año / # revisiones programadas para el año	Eficacia	Porcentaje	100%
CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la SDP revisados y actualizados	Revisar y actualizar los activos de información de la SDP por proceso	# de procesos con activos de información (RAI) revisados y actualizados en la vigencia/# de procesos de la SDP	Eficacia	Porcentaje	95%
PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN	Nivel de Ejecución del Plan de Capacitación y Sensibilización en Seguridad de la Información de la SDP	Hacer seguimiento a la ejecución del Plan Capacitación y Sensibilización en Seguridad de la Información de la SDP	# de estrategias desarrolladas al año que cumplen con la meta de ejecución >=90% / # de estrategias programadas para desarrollar al año siguiendo lo establecido	Eficacia	Porcentaje	90%

Evidencia 14. Indicadores de Gestión Seguridad de la Información						
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**TIPO**	**UNIDAD DE MEDIDA**	**META PERIODO**
			en el plan de capacitación y sensibilización			
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP	Porcentaje de políticas de Seguridad de la Información actualizadas o definidas en la vigencia	Mide el porcentaje de actualización o creación de políticas de seguridad de la información definidas en la vigencia	# de políticas de Seguridad de la Información actualizadas o creadas en la vigencia / # de políticas de seguridad de la información planeadas para actualización o creación en la vigencia	Eficacia	Porcentaje	90%
EJECUCIÓN DEL MSPI EN LA SDP	Nivel de Madurez de las fases del MSPI	Controlar el avance de las Fases del MSPI en términos de Madurez	# de actividades desarrolladas durante la vigencia en el Plan de Acción del MSPI / # de actividades definidas para desarrollar en la vigencia en el Plan de Acción del MSPI	Eficacia	Porcentaje	90%
GESTIÓN DE INCIDENCIAS DE SEGURIDAD	Porcentaje de atención a las incidencias de seguridad realizadas por los usuarios de la SDP	Medir el porcentaje de incidencias de Seguridad de la Información atendidas en la vigencia	(# de incidencias de seguridad atendidas en la vigencia /# de incidencias de seguridad recibidas en la vigencia) *100	Eficacia	Porcentaje	92%

Fuente: Dirección de TIC. Plan de Modelo de Seguridad y Privacidad de la Información de la SDP", Versión 5 Acta de Mejoramiento 257 de Julio 27 de 2023

Evidencia 9: Indicadores de Gestión Seguridad de la Información. Evidencia No. 9							
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**TIPO**	**META PERIODO**	**Resultado Indicador**	**Fuente**
1. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN	Nivel de Compromiso de la Alta Dirección	Hacer seguimiento, al compromiso sobre el sistema seguridad de la información, por parte de la alta dirección	# de revisiones realizadas por la alta dirección al año =1 # revisiones programadas para el año = 1	Eficacia	100%	100%	**Archivo:** Actas N.02 el 27 de abril y Acta N.03 del 03 de mayo de 2023 de las Sesiones Ordinarias del Comité Institucional de Gestión y Desempeño, donde se llevó a cabo la Revisión por la Dirección, numeral 9.3 de la ISO 9001:2015. Ind1. Salida7.1.1_ Revisión por la Dirección Sesión 2- 27 de abril. Ind1. Salida7.1.1_ Revisión por la Dirección Sesión 3- 3 de mayo **Ruta:** https://drive.google.com/drive/folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553
2. CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la SDP revisados y actualizados	Revisar y actualizar los activos de información de la SDP por proceso	# de procesos con activos de información (RAI) revisados en la vigencia: **15** # de procesos de la SDP: **15**	Eficacia	95%	11%	**Archivo:** Ind2. Actualización Activos de Información **Ruta:** https://drive.google.com/drive/folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553
3. PLAN DE SENSIBILIZACIÓN Y COMUNICACIÓN	Nivel de Ejecución del Plan de Sensibilización y Comunicación en Seguridad de	Hacer seguimiento a la ejecución del Plan de Sensibilización y	# de estrategias desarrolladas al año que cumplen con la meta de ejecución	Eficacia	80%	100%	**Archivo:** Ind3. Salida7.4.2_PlanSensibilizacion2023 **Ruta:** https://drive.google.com/drive/

Evidencia 9: Indicadores de Gestión Seguridad de la Información. Evidencia No. 9							
PRODUCTO	**NOMBRE DEL INDICADOR**	**OBJETIVO DEL INDICADOR**	**FÓRMULA**	**TIPO**	**META PERIODO**	**Resultado Indicador**	**Fuente**
	la Información de la SDP	Comunicación en Seguridad de la Información de la SDP	>=80%:**6** # de estrategias programadas para desarrollar al año siguiendo lo establecido en el plan de sensibilización :**6**				folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553
4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA SDP	Porcentaje de políticas de Seguridad de la Información actualizadas o definidas en la vigencia	Mide el porcentaje de actualización o creación de políticas de seguridad de la información definidas en la vigencia	# de políticas TI actualizadas o creadas en la vigencia: 14 # de políticas planeadas para actualización o creación en la vigencia: **15**	Eficacia	100%	100%	En la vigencia se programó el seguimiento a todas las políticas y se realizó a cada una de ellas. Los documentos, incluidas las Políticas se publicaron en el aplicativo SIPA. **Archivo:** Ind4. RevisionDocumental_ DTIC2023 **Ruta:** https://drive.google.com/drive/ folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553
5. EJECUCIÓN DEL MSPI EN LA SDP	Nivel de Madurez de las fases del MSPI	Controlar el avance de las Fases del MSPI en términos de Madurez	# de actividades desarrolladas durante la vigencia en el Plan de Acción del MSPI: (Diagnostico=3 Fase 1= 41 Fase 2= 4 Fase 3= 1 Fase 4= 1) = 50 # de actividades definidas para desarrollar en la vigencia en el Plan de Acción del MSPI: (Diagnostico=3 Fase 1= 41 Fase 2= 4 Fase 3= 1 Fase 4= 1) = 50	Eficacia	90%	100%	**Archivo:** Ind5_8.1_PlanImplentacion MSPI Ind5_8.1_PlandeAccion Controles2023 **Ruta:** \\sdpatlas08\Dir_Sistemas\ SIG\Informes\ https://drive.google.com/drive/ folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553
6. GESTION DE INCIDENCIAS DE SEGURIDAD	Porcentaje de atención a las incidencias de seguridad realizadas por los usuarios de la SDP	Medir el porcentaje de incidencias de Seguridad de la Información atendidas en la vigencia	# de incidencias de seguridad atendidas en la vigencia 14 # de incidencias de seguridad recibidas en la vigencia 14	Eficacia	100%	100%	Revisado el sistema de gestión de incidencias - GLPI, se reportaron 14 casos catalogados como seguridad y privacidad de la información los cuales fueron gestionados y cerrados. **Archivo:** Ind6_8.1_Gestión_ Incidencias_Seguridad_2023 https://drive.google.com/drive/ folders/1Gj2FgtZ-gq6p7cId8fSLFvQ4T4XLG553

Fuente: Dirección de TIC. Evidencia No 9. Avances y Logros_MSPI_Dic_2023_12032024" como entrada para la Revisión por la Dirección.

Frente a la Situación Crítica No 7 identificada en la Auditoría, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Reconocemos la importancia de la coherencia y precisión en la información presentada en los diferentes documentos relacionados con el seguimiento del Modelo de Seguridad y Privacidad de la Información (MSPI). Las discrepancias identificadas en el cuadro comparativo se deben principalmente a los siguientes factores:

- *Las evidencias 14 (Plan de Modelo de Seguridad y Privacidad de la Información) y 9 (Avances y Logros) corresponden a diferentes momentos en el tiempo y capturan distintos aspectos del avance del MSPI. Algunas metas se ajustaron en el informe de avances y logros alcanzados durante el periodo de seguimiento.*
- *En algunos casos, la interpretación de los indicadores puede variar ligeramente, lo que llega a generar diferencias en los valores reportados.*
- *El MSPI es un proceso en constante evolución, y es posible que se hayan realizado actualizaciones en los documentos durante el periodo de seguimiento, lo que podría explicar algunas de las discrepancias.*

No obstante lo anterior, se presenta algunas justificaciones específicas a continuación:

- *La diferencia en el porcentaje de avance del Indicador "Cubrimiento del SGSI en Activos de Información" se debe a que la evidencia 9 refleja un cálculo más detallado que considera los avances realizados durante el periodo de seguimiento, mientras que la evidencia 14 presenta una estimación inicial.*
- *Las diferencias en los indicadores del "Plan de Capacitación y Sensibilización", "Políticas de Seguridad de la Información" y "Ejecución del MSPI" corresponden a ajustes en la programación de las actividades, a la incorporación de nuevas iniciativas o a una mejor comprensión de los requisitos.*
- *La diferencia en este indicador "Gestión de Incidencias de Seguridad" se debe a la inclusión de una actualización en la metodología de cálculo.*

Para mejorar la coherencia y la precisión de la información, la Dirección de TIC implementará acciones para revisar y validar los datos utilizados en los informes de seguimiento, garantizando así la coherencia entre las diferentes fuentes de información.

Agradecemos sean tenidas en cuenta las aclaraciones anteriores y a la vez solicitamos sea reevaluada la calificación de situación crítica asignada a esta observación, ya que consideramos que las diferencias observadas no reflejan necesariamente un incumplimiento de los requisitos, sino más bien matices en la forma de reportar la información y pueden ser abordadas de manera proactiva. Proponemos establecer un plan de acción que incluya la armonización de los indicadores, la mejora de los procesos de documentación y la capacitación del personal involucrado en el seguimiento del MSPI."

Análisis de la respuesta por parte de la OCI:

Se identificó por parte del equipo auditor que existen debilidades en el control, revisión y seguimiento a la trazabilidad de los registros que dan cuenta del avance Modelo de Seguridad y Privacidad de la información MPSI, aspecto que puede afectar la toma de decisiones de la Entidad al no contar con información precisa de la gestión adelantada y de los resultados obtenidos y en consecuencia en el logro de objetivos, metas y recursos asignados.

Por ejemplo, frente en el indicador relacionado con el número de procesos con activos de información (RAI) revisados en la vigencia 15 sobre el número de procesos de la SDP 15, no es claro porque arrojan un resultado de 11%.

Esto lleva a otras preguntas, por ejemplo, ¿no se cumplió con la meta de actualización de activos de información en los 15 procesos de la entidad para la vigencia 2023?

Evidencia 9: Indicadores de Gestión Seguridad de la Información. Evidencia No. 9

PRODUCTO	NOMBRE DEL INDICADOR	OBJETIVO DEL INDICADOR	FÓRMULA	TIPO	META PERIODO	Resultado Indicador	Fuente
2. CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN	Activos de Información de la SDP revisados y actualizados	Revisar y actualizar los activos de información de la SDP por proceso	# de procesos con activos de información (RAI) revisados en la vigencia: **15** # de procesos de la SDP: **15**	Eficacia	95%	11%	**Archivo:** Ind2. Actualización Activos de Información **Ruta:** https://drive.google.com/drive/folders/1Gj2FgtZ-gq6p7cld8fSLFvQ4T4XLG553

Ahora bien, si las programaciones de los indicadores fueron ajustadas, ¿por qué no fue actualizado el documento “Plan de Modelo de Seguridad y Privacidad de la Información de la SDP A-LE -373 en la vigencia 2023?

De otra parte, el Documento “Avances y Logros_MSPI_Dic_2023_12032024” fue presentado con esta información ante el Comité Directivo como entrada para la Revisión por la Dirección.

Y finalmente se confirma lo expresado por esta auditoría frente a las inconsistencias de información encontradas en el documento “Plan de acción de controles MSPI 2023”, (descritas en la situación crítica No 3 de este Informe), y su concordancia **con las acciones que con gran esfuerzo fueron ejecutadas por la Dirección de TIC** en la vigencia 2023 y que reposan en diferentes seguimientos, planes y documentos de la misma Dirección. Ya que independiente de si se habla de un avance de Plan de gestión de vulnerabilidades, o de los indicadores del MSPI o del documento de Avances y Logros del MSPI, o de los Avances del Plan de Controles 2023, la información debe ser coherente, completa y clara, de tal manera que permita conocer con precisión y confiabilidad los avances del Modelo de Seguridad y Privacidad de la Información.

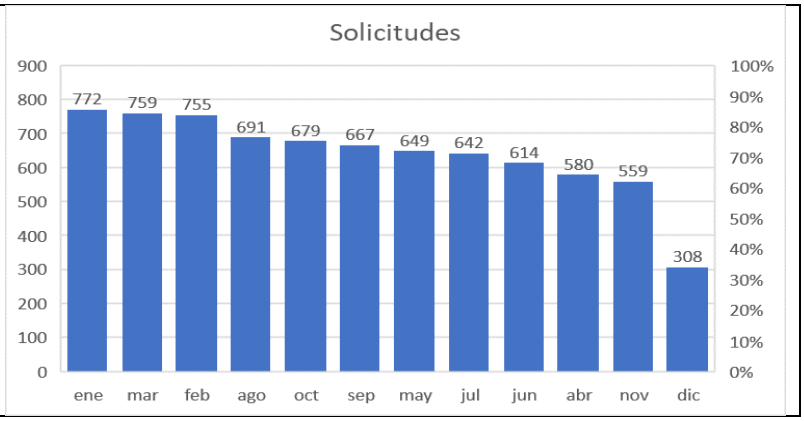
4.4.5 FASE 4: MEJORAMIENTO CONTINUO

MESA DE AYUDA

Se observó que durante la vigencia 2023, se recibieron 7675 solicitudes en la mesa de ayuda de TIC, con una tendencia decreciente a medida que avanzaban los meses.

MES	Servicios
ene	772
feb	755
mar	759
abr	580
may	649
jun	614
jul	642

ago	**691**
sep	**667**
oct	**679**
nov	**559**
dic	**308**
Total	**7675**



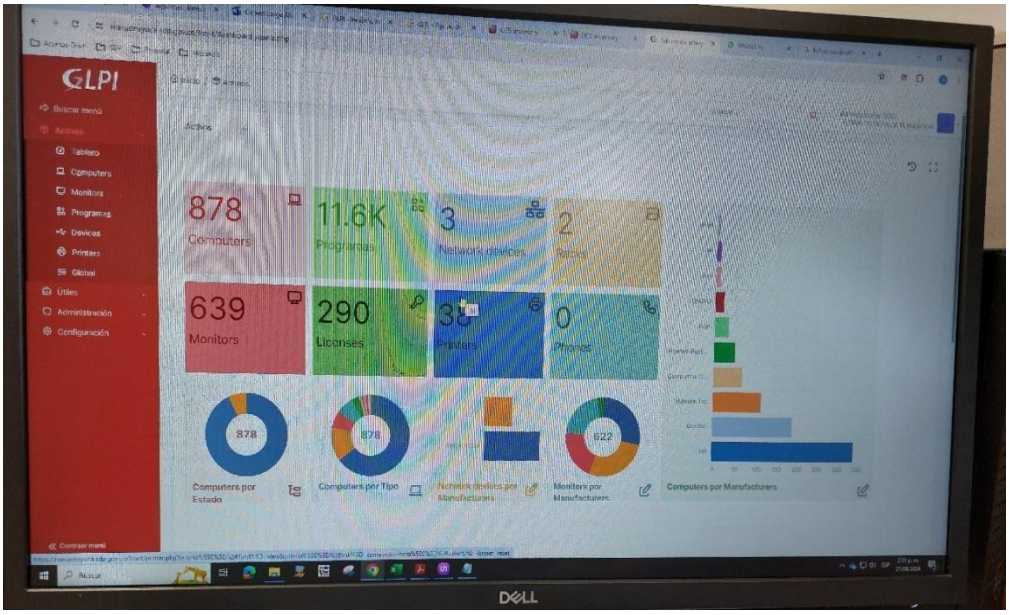
Fuente: Dirección TIC Evidencia 26

También se observó que la mesa de ayuda dedicó la tercera parte de sus esfuerzos a asuntos relacionados con la gestión de usuarios, como se muestra a continuación:

Categoría	Servicios
01-Revisión Equipo de cómputo/parte/periférico	722
02-Asignación Equipo de cómputo/parte/periférico	268
03-Traslado de equipo de cómputo/parte/periférico	97
04-Retiro de equipo de cómputo/parte/periférico	20
05-PrÃ©stamo equipos/videobeam	271
07-Gestión de mantenimientos (hardware)	9
08-Instalación/desinstalación de software	102
09-Soluciones de Software administradas por DTIC.	1961
10-Gestión de usuarios	2773
11-Generación copias de seguridad y recuperación	340
12-Gestión de conectividad	158
13-Seguridad y Privacidad de la información	13
14-Acceso VPN	558
15-Gestión de Impresión	118
16-Gestión de Cambio Informático	22
17-SIPA Módulo correspondencia	2
18-Soporte telefonía IP	38
Alistamiento de Infraestructura para despliegue de soluciones de software	6
Alistamiento de servidores	193
Configuración firewall	1
Sin Asignar	3
(en blanco)	0
Total, general	**7675**

Fuente: Dirección TIC. Evidencia 26

Se informó al equipo auditor por parte del ingeniero que coordina la Mesa de Ayuda, que se implementará una herramienta que facilitará el monitoreo de las solicitudes vs incidencias, y proporcionará información estadística para toma de decisiones.



Fuente: Dirección de TIC

SATISFACCIÓN USUARIOS

En cuanto a la satisfacción, los usuarios calificaron la atención de sus incidencias de la siguiente manera:

Calificación	**servicios**
Bueno	7264
Malo	31
Regular	66
Sin calificar	314
Total, general	**7675**

Fuente: Dirección de TIC Evidencia 26

Las 31 calificadas por los usuarios en el nivel más bajo, todas ellas tienen una nota de la mesa de ayuda de TIC como “incidencia solucionada”. Las mismas se relacionan con:

Situación	Incidencias con esa situación
La falla reincide	67 682, 68 707, 69 309, 69 404, 69 492, 70 347, 70 393, 71 835, 73 352, 73 957, 74 068
Sin oportunidad en la atención	70 154, 70 567, 70 869, 74 617
Deficiente orientación	69 008, 70 147
No se atendió la situación	67 513, 71 076, 71 809, 72 356, 72 843, 71 623, 73 229, 73 964
Cierre con argumento no real	73 037
Cierre sin que usuario valide el ajuste	72 873
Sin comentario sobre la calificación	68 186, 68 603, 72 810, 74 523

Fuente: Dirección de TIC. Evidencia 26

Aunque se trata de pocos casos frente a las 7675 incidencias registradas, vale la pena señalar que hay casos que reinciden o que no fueron atendidos.

Por otro lado, las 66 calificadas por los usuarios en el nivel regular, todas ellas tienen una nota de la mesa de ayuda de TIC como "incidencia solucionada". Las mismas se relacionan con:

Situación	Incidencias con esa situación
La falla reincide	68 521, 70 755, 73 022, 73 278, 73 937
Demora en la atención	68 450, 68 453, 68 457, 68 458, 68 813, 68 816, 68 917, 69 125, 69 616, 69 619, 69 621, 70 352, 70 933, 71 187, 71 189, 70 435, 72 033, 72 232, 72 442, 72 443, 72 445, 72 447, 72 450, 72 455, 72 456, 72 457, 72 902, 72 910, 72 911, 72 912, 71 248, 72 913, 73 096, 73 108, 73 532, 73 959, 74 239, 74 240, 74 241, 74 243, 74 244, 74 245, 72 423, 74 402
Deficiente orientación	74 317, 74 478
No se resolvió la situación	68 633, 70 433, 70 743, 73 052, 73 859, 74 487
Cierre con argumento no real	69 932
Para revisar	74 863
Sin comentario sobre la calificación	67 332, 68 438, 70 108, 70 156, 73 005
Ni oportunidad, ni solución	68 459, 71 833

Fuente: Dirección de TIC. Evidencia 26

Dentro de las que fueron calificadas como "bueno", llama la atención los comentarios de los usuarios en las incidencias **72 764 y** 74 196, toda vez que, aunque evalúan bien, ponen un "pero" en el servicio recibido.

Se presentan los resultados de las encuestas de satisfacción de la mesa de ayuda.

Tabla 1. Calificación por categorías segundo semestre 2023

Categoría	Bueno	Malo	Regular	Total general
01-Revisión Equipo de cómputo/parte/periférico	62		1	63
02-Asignación Equipo de cómputo/parte/periférico	15		1	16
03-Traslado de equipo de cómputo/parte/periférico	5			5
04-Retiro de equipo de cómputo/parte/periférico	1			1
05-Préstamo equipos/videobeam	47			47
08-Instalación/desinstalación de software	5		1	6
09-Soluciones de Software administradas por DTIC.	208	12	10	230
10-Gestión de usuarios	113	2	23	138
11-Generación copias de seguridad y recuperación	4			4
12-Gestión de conectividad	13			13
13-Seguridad y Privacidad de la información	1			1
14-Acceso VPN	49	1	2	52
15-Gestión de Impresión	17			17
17-SIPA Modulo correspondencia	1			1
18-Soporte telefonia IP	5			5
Total general	**546**	**15**	**38**	**599**

Fuente: Dirección de TIC. Reporte herramienta mesa de ayuda

Evaluaciones calificadas como "**BUENO":** En el ítem calificado como bueno las partes interesadas de la mesa de ayuda se pronunciaron como se muestra en el archivo Partes Interesadas:

CalificaSolicitudesMesaAyudaPI_Julio_Dic2023 Hoja "NotaCalificacionBueno" donde se observa que, de las 599 calificaciones, se obtuvieron 368 diferentes tipos de observaciones o comentarios.

Evaluaciones calificadas como **"REGULAR":** En el ítem calificado como regular, de las 38 calificaciones, se obtuvieron de las partes interesadas de la mesa de ayuda 20 diferentes observaciones o comentarios.

Evaluaciones calificadas como "**MALO":** En el ítem calificado como malo, se obtuvieron de las partes interesadas de la mesa de ayuda 15 diferentes observaciones o comentarios por el mismo número de calificaciones.

Tabla 2. Calificación Regular Segundo Semestre 2023
Fuente: Dirección TIC -Reporte herramienta mesa de ayuda 2023

Comentarios	Cuenta de Comentarios a la encuesta
Sin comentarios	1
A mi solucionaron pero el problema persiste en el formato	1
Buena tardeSiempre he recibido una atención oportuna, en este caso coloque la incidencia desde el viernes 15 a	1
El tabulador dejó de funcionar. Voy a solicitar el arreglo en otra incidencia.	1
El tabulador no quedó funcionando	1
El tiempo de espera para la solución del problema fue extenso y generó retrasos en las labores.	1
En realidad me parece que el no haber tenido la opción de poder ingresar de una vez al usuario con la clave que	1
Fue muy demorada la repuesta a la incidencia Gracias	7
La atención a la incidencia no fue de la forma mÃ¡s eficiente y oportuna.Cordialmente	1
La incidencia la solicitÃ© temprano en la mañana, solo hasta las 3pm fue atendida, Lamentablemente arreglaro	1
La Respuesta a la incidencia se demoroGracias	1
Me hubiera gustado que desde mesa de Ayuda (Hangouts) me hubieran orientado mejor, en cuanto a que el tema	1
Muy demorada la respuesta a la incidencia Gracias	8
Muy demorada la respuesta a la incidenciaGracias	1
Muy demorada la respuesta de la incidencia Gracias	6
No es regular por el funcionario que nos ayuda sino porque es un tema recurrente que se bloquea solo pero cada	1
No quedo solucionado el tema, escalaran el tema para que se pueda solucionar a futuro	1
No se tenía que hacer nada. Se debería actualizar el formato de paz y salvo a la estrategia Camaleón.	1
para mi no es claro si se soluciono el tema o esta aun en revision. Menciona que otra incidencia reporto pero pr	1
Pese a tener reserva, no se pudo usar en la tarde del dia viernes 20 de octubre la herramienta ArcGis y la soluci	1
Total general	**38**

Tabla 3. Calificación Malo Segundo Semestre 2023

Comentarios	Cuenta de Comentarios a la encuesta
cierran la incidencia sin solucionar de fondo parece que se trata de sacar al peticionario del camino. Gracias	1
Es un tema que se presenta a diario, siempre es lo mismo. No entiendo porque estan modificando permanentemente los enlaces, eso impide laborar. esto sucede hace 5 meses. Agradezco solucionar de una vez por todas, pues dificulta el trabajo. Por favor actualizar el departamos con los enlaces correctos.	1
He presentado tres casos por la misma falla, cierran los casos con la misma plantilla. Por favor revisar la plantilla, es posible que en el proceso de elaboración del borrador o se hayan borrado marcas propias de la plantilla o se hayan insertado caracte	1
La atención del requerimiento fue atendido en el momento que ya no se necesitaba	1
Los desprendibles siguen sin el logo	1
No me enviaron al correo la clave para el desbloqueo como lo indica el cierre de la incidencia.	1
No se acercó ningun tecnico, se requeria con prioridad para iniciar las labores asignadas que se requieren, un contratista interno que no estab en la entidad tuvo que asistir remotamente el equipo	1
No se da respuesta, solo se cerró la incidencia.	1
No se recibió retroalimentación de la supuesta resolución del caso; esto es, no hubo resolución del caso	1
Paso todo el mes y nunca me dieron respuestas el descargue de SIPA estuvo intermitente todo el tiempo hasta el 2 octubre tengo que volver a ingresar y en ese momento podre mirar si esta funcionando, el mes pasado no descargaba los memorandos en pdf y me toco solucionarlo descargando el archivo por por otro lado la demora perjudico el proceso de distribución de cuentas para pago, mil gracias y mil disculpas pero realmente no me ofrecieron ningún apoyo en el tema	1
Realmente la persona de mesa de ayuda, NUNCA me ayudo, estaba muy confundido, me contacto por chat de google pero no fue claro y se demoraba mucho en contestar de un dia a otro. realmente muy mal servicio, finalmente una persona de la dirección de TO (fernando cifuentes) fue el que me ayudo.	1
Se cerró muy rápido la incidencia y no se espero para verificar si se podía acceder o no	1
Sin comentario	2
¿Cómo es posible que cierren una incidencia con una solución temporal (drive como allí mismo indican)?	1
Total general	**15**

Fuente: Dirección TIC -Reporte herramienta mesa de ayuda 2023

Satisfacción Servicios de TI 2023

Dentro de los servicios que tuvieron baja calificación en los niveles de satisfacción, se encuentran:

Internet Dispositivos Móviles (WiFi) :67%
Servicio de Telefonía: 72%

Satisfacción Servicios de TI 2023

Opción	2023			
	Uso por servicio	Altamente Satisfactorio (5) + (4)	Satisfactorio (3)	No Satisfactorio (2)+(1)
Internet Puestos de Trabajo	306	90%	8%	1%
Internet Dispositivos Móviles (WiFi)	305	67%	17%	16%
Correo Electrónico	311	97%	2%	0%
Administración Servicios de Impresión	301	86%	9%	4%
Servicio de Telefonía	301	72%	19%	9%
Gestión de usuarios	315	89%	9%	3%
Mesa de Ayuda	317	94%	4%	2%
Gestión de copias de respaldo	303	86%	13%	2%
Mantenimiento de Equipos	307	89%	8%	3%
Instalación y desinstalación de software	307	86%	10%	3%
Requerimientos de Software	305	87%	10%	4%
Sistemas de Información y/o Aplicaciones	307	89%	7%	4%
Conexión a servicios de forma segura	306	92%	7%	1%

Fuente: FichaTecnicaEncuesta_DTIC2023

Situación Crítica

No se identificó un documento que dé cuenta de las acciones adelantadas o un plan de mejoramiento con acciones correctivas, relacionadas con aquellas situaciones que presentaron reiteración o recurrencia y que obtuvieron puntajes bajos en las encuestas de satisfacción relacionadas con mesa de ayuda y servicios de TI y cuya trazabilidad se observe dentro de la matriz Todo de la entidad. Es así como se identificó entre otros:

Dentro de los incidentes de seguridad recibidos por mesa de ayuda GLPI, se identificó uno con un tiempo alto relacionado con una solicitud de listado usuarios, para lo cual no es claro que para la solución/cierre se invirtieran 197 Dí-a(s) 22 Hora(s) 5 Minuto(s), si el tiempo de espera fue de 0 Segundo(s) y el tiempo para atender el servicio fue de 16 Hora(s) 1 Minuto(s).

De las encuestas de satisfacción de mesa de ayuda se identificaron 31 calificadas por los usuarios en el nivel más bajo, de las cuales se observó que hay casos que reinciden o que no fueron atendidos, y además tienen una nota de la mesa de ayuda de TIC como “incidencia solucionada”. De las 66 calificadas por los usuarios en el nivel regular, todas ellas tienen una nota de la mesa de ayuda de TIC como “incidencia solucionada”, de las cuales se identifica que 88 se refieren a “Demora en la atención”.

Respecto a los servicios de TIC se observaron calificaciones de satisfacción de Internet Dispositivos Móviles (Wifi): 67% y Servicio de Telefonía: 72%.

Frente a la Situación Crítica No 8 identificada en la Auditoría, mediante correo electrónico del 31 de octubre de 2024 la Dirección de TIC manifestó lo siguiente:

"Se solicita de manera respetuosa reconsiderar y retirar la situación critica reportada, dada la siguiente argumentación:

La incidencia 69007 (requerimiento de soporte) reportada el 8 de marzo de 2023 fue relacionada con la solicitud de un listado de usuarios activos e inactivos en sistemas de información, VPN, bases de datos y directorio activo de la SDP, gestionada inicialmente en la herramienta de gestión de incidentes GLPI, solicitud que fue atendida el 9 de marzo de 2023, cumpliendo con los tiempos establecidos de respuesta dentro del horario habitual de la entidad (7:00 a.m. - 4:30 p.m.). El 17 de marzo de 2023 se realizó una primera solución parcial. Sin embargo, debido a la necesidad de información adicional y la complejidad del proceso, el nivel 2 actualizó el caso el 11 de mayo de 2023 con información adicional requerida para la elaboración del informe final. A partir de la información entregada el 11 de mayo, se llevó a cabo una revisión detallada para asegurar que la información estuviera actualizada y libre de errores. Este proceso incluyó la conciliación de datos con otras fuentes y la aplicación de filtros adicionales para refinar los resultados. Así mismo, se desarrollaron dos informes personalizados; el primero con relación a los usuarios del directorio activo y el segundo, referente a los usuarios de bases de datos que incluyeron información relevante sobre cada usuario, como roles, permisos y fechas de creación. Adicionalmente, en el marco de la mejora continua se realizaron ajustes y actualizaciones en el directorio activo. Estas tareas adicionales, aunque necesarias para garantizar la calidad de la información entregada, demandaron un tiempo considerable y contribuyeron al tiempo total de resolución del incidente. (Anexa informes en la carpeta: "TiempoRtaIncidencia 69007" ubicada en la carpeta Soportes/Situación Crítica 8). Finalmente, el caso fue cerrado por el oficial de seguridad el 22 de septiembre de 2023, una vez verificada la completitud de la información y la satisfacción del requerimiento inicial.

Aunque la herramienta muestra un tiempo total acumulado de 197 días, 22 horas y 5 minutos, es importante resaltar que esto se debe a la naturaleza del requerimiento, que precisó intervenciones adicionales de otros niveles (profesional de aplicaciones, bases de datos, infraestructura y oficial de seguridad), por lo cual, la solicitud inicial fue atendida en el marco de los tiempos acordados, pero la dependencia de información adicional para completar el informe extendió el tiempo total. Estos tiempos acumulados reflejan la duración total del proceso hasta su resolución definitiva, más no la atención continua en horas hábiles por parte del equipo de soporte y mesa de ayuda. La gestión expuesta, demuestra la sinergia y el compromiso del equipo de la DTIC para atender las incidencias y contar con la información necesaria y suficiente en pro de la mejora continua y la resolución de las causas que originaron para este caso en particular la necesidad de un tiempo de holgura en el cierre del caso, lo cual se evidencia en la calidad y completitud de los informes de gestión aportados por la DTIC.

Respecto a la observación de las encuestas de satisfacción, es preciso aclarar lo siguiente:

Existen solicitudes creadas en la mesa de ayuda (Ej:67682), las cuales fueron atendidas dentro de los acuerdos de nivel de servicio (ANS) y donde se evidencia el seguimiento realizado por los Ing. de mesa de ayuda y/o de nivel 2. Se identifica igualmente que después de atendida la incidencia, esta se cierra y al siguiente día el funcionario autor de la incidencia, califica "Malo" o "Regular", por que en el nuevo día se presenta nuevamente la falla. Es algo fortuito o inesperado que hace que el funcionario generalice y responda de manera negativa a la encuesta.

En la incidencia 72873 el Ing. de nivel 2 atiende inmediatamente el caso y cierra la incidencia, teniendo en cuenta que el inconveniente presentado estaba bien identificado; es decir, que la solución dada era la correcta (Enrutamiento de servidor de licenciamiento), gestión conocida como "atención en primera llamada".

En la incidencia 70435 el usuario informa que no podía ingresar a un aplicativo, esto sucedió porque a dicho usuario se le traslado de dependencia, por lo cual los permisos de ingreso estuvieron retirados de manera temporal, el procedimiento que debía seguir el funcionario es que la nueva jefatura le informara al usuario funcional de la Dirección de Contratación para que desde allí se creara una incidencia solicitando los nuevos permisos al aplicativo que se menciona. Esta información fue registrada por parte del coordinador de la mesa de ayuda y cabe aclarar que fue atendida dentro de los ANS.

La incidencia 74863 fue creada para dar cumplimiento al procedimiento del paz y salvo, teniendo en cuenta el traslado de dependencia del funcionario, en la cual se aclara que dicho funcionario no tenía equipo de cómputo a cargo. El comentario a la encuesta de satisfacción se refiere a realizar algún tipo de ajuste en el formato de paz y salvo para estos casos en que los equipos de cómputo son de tipo flotante, según la estrategia camaleón. Es un tema de común acuerdo entre la Dir. de Talento Humano y la Dir. TIC.

Respecto a las incidencias que se refieren a "demora en la atención", es preciso indicar que estas corresponden a la situación que se venía presentando dentro proceso interno anterior, en el cual se realizaba un paso adicional para aprobación de roles concentrado en el un rol de equipo de la Dirección de TIC, lo cual fue reportado inicialmente por la Oficina de Control Interno en el Radicado: 3-2023-26408 Informe de seguimiento a la mesa de ayuda, atendida con la formulación del plan de mejoramiento 2164, Acción 2993 en la que se realizó la "Actualización la matriz de escalamiento de atención y gestión de los servicios de la mesa de ayuda de la Dirección de TIC" lo que permitió que desde el equipo de operaciones un responsable de la aplicación haga la asignación y aprobación de los roles. Estas acciones han permitido agilizar la gestión de usuarios en las aplicaciones de cara al usuario final.

NOTA: Se adjuntan evidencias”

Análisis de la respuesta por parte de la OCI:

El equipo auditor durante el desarrollo de la auditoria de seguimiento, revisó cada uno de los registros relacionados con las Encuestas de Satisfacción adelantadas por la Dirección de TIC para los diferentes servicios.

MEDICIÓN DE LA PERCEPCIÓN DE LOS SERVICIOS TI y SEGURIDAD DE LA INFORMACIÓN EN LA SDP
Administración Servicios de Impresión
Conexión a servicios de forma segura
Correo Electrónico
Gestión de copias de respaldo
Gestión de usuarios
Instalación y desinstalación de software
Internet Dispositivos Móviles (WIFI)
Internet Puestos de Trabajo
Mantenimiento de Equipos
Mesa de Ayuda
Requerimientos de Software
Servicio de Telefonía IP
Sistemas de Información y/o Aplicaciones

MEDICIÓN CONOCIMIENTO TEMAS ESPECIFICOS SEGURIDAD DE LA INFORMACIÓN EN LA SDP
Políticas de Seguridad de la Información
Control de acceso a recursos tecnológicos
Gestión y uso de contraseñas
Activos de Información
Buenas prácticas de seguridad de la información en el trabajo y en el hogar
Experiencias seguras en internet y redes sociales
Identifica riesgos asociados a seguridad digital

Es así como se encontraron entre otras las siguientes observaciones, algunas reiterativas:

- *Revisar la conectividad de internet de la entidad, se presenta mucha intermitencia.*
- *Muchos formatos, se solicita que sean más fáciles de diligenciar, especialmente en Gestión de usuarios*
- *Mejorar tiempos de respuesta de Mesa de Ayuda*
- *Mejorar tiempos en requerimientos, ejemplo actualización de información para publicar en SINUPOT.*
- *Solicitud de acompañamiento para interoperabilidad entre SIPA y Bogotá Te Escucha.*
- *Distribuir algunas actividades de sensibilización durante todo el año y no solo al finalizar.*
- *Se solicita que la capacitación a la Red Cade se pueda hacer en tiempos que no sean los de atención a usuarios en módulo.*
- *En el archivo central falta más apoyo en el proceso de mantenimiento de los equipos de cómputo, el internet muchas veces es lento, no se cuenta con equipos óptimos el Wifi muchas veces no funciona y **nunca han podido instalar la impresora** a los equipos en planoteca y biblioteca (subrayado y resaltado nuestro)*
- *En general son muy buenos, sin embargo el tema de desarrollo es un poco lento, entiendo que existen muchas situaciones que no permiten celeridad, pero estas demoras afectan las acciones de la Dirección de Talento Humano, porque tenemos el aplicativo PERNO pero solo sirve para liquidar la nómina y eso es mucho decir porque **todos los meses presenta problemas lo que obliga a tener un profesional de "soporte" casi que 7X24 dedicado a apagar incendios** ya que la nómina si o si se debe pagar oportunamente, dejando de lado las otras funcionalidades como seguridad y salud en el trabajo, Capacitación y Bienestar, entre otros, sin hablar de los reportes de planta; entonces, es momento de hacer un alto en el camino y reflexionar si ese desgaste administrativo todo el tiempo sirve para garantizar la misionalidad del área, pues como se puede colegir nos toca trabajar con archivos de excel para informes y reportes de los demás temas incluidos los reportes de la planta ya que la información histórica de PERNO no es confiable. (subrayado y resaltado nuestro)*

Respecto a los servicios de TIC se observaron calificaciones de satisfacción de Internet **Dispositivos Móviles (Wifi): 67% y Servicio de Telefonía: 72%.**

Se reconoce la gestión adelantada por la Dirección de TIC para hacer evaluación de su gestión y de sus productos a través de las encuestas de satisfacción, es una de las Direcciones que más información y cobertura tiene frente a la realización de este tipo de evaluación. Las encuestas reflejan necesidades y expectativas que deben ser evaluadas y/o atendidas.

No obstante, al revisar los análisis de las encuestas no se observa un capítulo o un documento que dé cuenta de las acciones adelantadas sobre las mismas, o un plan de trabajo o una acción documentada como acción correctiva, preventiva o de mejora cuya trazabilidad se observe dentro de la matriz Todo de la entidad.

Es importante recordar que el Modelo de Seguridad y Privacidad de la Información adoptado mediante Resolución 500 de 2021 establece en el

Numeral 10.1 Mejora: Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.

Por lo anteriormente expuesto, se ratifica la situación crítica No 8, dado que los argumentos de la respuesta no desvirtúan las debilidades señaladas por la auditoría.

Riesgos

1. Teniendo en cuenta que durante la visita del equipo Auditor se informó por parte de la Dirección de TIC que la **Secretaría Distrital de Hacienda no continuará con el Convenio que se tiene relacionado con el Datacenter ubicado en el Edificio del CAD,** y en el cual la Secretaría Distrital de Planeación tiene servidores con información de la entidad, existe el riesgo de afectar la disponibilidad, confiabilidad e integridad de la información de la SDP, al no contar con un espacio como el que se tiene actualmente, así como riesgo de afectación económica y reputacional e incluso afectar la continuidad de la operación de la SDP. Adicionalmente, con los costos que generaría este tipo de cambios para la entidad.

2. La Dirección de TIC realiza gestión de vulnerabilidades mediante un plan formulado cada año. Para la vigencia 2023, se realizó el escaneo de vulnerabilidades (mediante la herramienta TENABLE adquirida para tal fin en el 2022). La Dirección de TIC informó que había cumplido este plan al 100%, sin embargo, **se identificó que no todas las vulnerabilidades identificadas pudieron ser remediadas, debido al nivel de obsolescencia en la infraestructura tecnológica de la entidad** (hardware, software, aplicaciones bases de datos, conectividad, servidores, entre otros).

   Sobre el particular la Dirección de TIC tiene identificado en el documento Mapa de Riesgos Institucional, el riesgo:

   "Posibilidad de afectación reputacional por falta de oferta de servicios de soporte y garantías para componentes de TI, debido a obsolescencia tecnológica."

   Este riesgo fue evaluado por la Dirección de TIC **como riesgo residual bajo y sin plan de acción,** después de aplicar los siguientes controles:

   (…) "*1. El (la) líder técnico con base en el informe de laboratorio, valida las razones para tomar la decisión de reparar los elementos tecnológicos o dar concepto para baja en el inventario. Emite concepto técnico en el documento correspondiente e informa a las dependencias pertinentes para adelantar las acciones a que haya lugar.*
   2. El (la) líder técnico realiza estudio de mercado de las partes/repuestos con fines de aprobar la adquisición de las mismas y la reparación y del equipo por parte del contratista de la mesa de ayuda. Emite concepto técnico en el documento correspondiente e informa a las dependencias pertinentes para adelantar las acciones a que haya lugar.
   3. El (la) líder técnico verifica cada vez que se requiera que el inventario priorizado de obsolescencia tecnológica esté actualizado para escalar a través del Director de Tecnologías de la Información y las Comunicaciones y el Gerente del Proyecto, con el fin de establecer las proyecciones para el Plan Anual de Adquisiciones - PAA, según requerimientos actuales del proceso y la situación del mercado. Si encuentra novedades, realiza los ajustes correspondientes en el inventario priorizado."

Teniendo en cuenta que muchas de las actividades del plan de gestión de vulnerabilidades **son reprogramadas** en cada vigencia, ya que no se pueden remediar

la totalidad de vulnerabilidades identificadas debido al nivel de obsolescencia que tiene la entidad, se ha identificado por parte del equipo auditor que no fue suficiente la adquisición de la herramienta de Escaneo Tenable, ni los controles establecidos en el mapa de riesgos de la entidad. Se requiere un plan de acción que atienda de manera eficiente, eficaz y efectiva la actualización de la infraestructura tecnológica de la entidad, con el fin de evitar la afectación de la disponibilidad, la confiabilidad y la integridad de la información de la Secretaría Distrital de Planeación, con ocasión de las vulnerabilidades que no pueden ser remediadas.

5. Fortalezas

- ✓ De acuerdo a las actividades realizadas en la SDP, en el marco del MSPI se observó un aumento en la evaluación general pasando de 78% al 79% en la vigencia 2023, lo cual lo clasifica el Modelo en nivel Gestionado.

- ✓ El Modelo de Seguridad y Privacidad de la Información- MSPI de la Secretaría Distrital de Planeación está alineado con la Metodología y Políticas establecidas por el Ministerio de las TIC y los lineamientos distritales a través de la Alta Consejería Distrital de TIC.

- ✓ Información disponible del Modelo de Privacidad y Seguridad de la Información, desde el diagnóstico, los planes de trabajo y los seguimientos, 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 reconoce la transparencia y disponibilidad en la entrega de la información y disposición del Director como de todo el equipo de trabajo de la Dirección de TIC.

- ✓ Se destacan las actividades de sensibilización y capacitación desarrolladas a través de 6 estrategias lideradas 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 reconoce la gestión adelantada por la Dirección de TIC para hacer evaluación de su gestión y de sus productos a través de las mediciones de satisfacción, es una de las Direcciones que más información y cobertura tiene frente a la realización de este tipo de evaluación.

- ✓ La permanente revisión y actualización de los documentos del MSPI.

6. Situaciones susceptibles de mejora / oportunidades (observaciones)

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
1.	Se recomienda a la Dirección TIC identificar las acciones necesarias que permitan a la entidad avanzar hacia la transformación digital[8] y mejorar los resultados obtenidos en el FURAG 2023, especialmente en lo que se refiere a: a)Seguridad y Privacidad de la información (puntaje de 69,6). b)Servicios Ciudadanos Digitales (puntaje 0): Este habilitador busca desarrollar, mediante soluciones tecnológicas, las capacidades de los sujetos obligados a la Política de Gobierno Digital para mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública. c)Servicios y Procesos Inteligentes (puntaje 42.9): Esta línea de acción busca que los sujetos obligados desarrollen servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad, a partir del entendimiento de las necesidades del usuario y su experiencia, implementando esquemas de atención proactiva y el uso de tecnologías emergentes.	4.2.2. Resultados FURAG 2023	Dirección de TIC

[8] DNP. ESTRATEGIA NACIONAL DIGITAL DE COLOMBIA. 2023-2026. *"La transformación digital es un proceso de cambio fundamental sobre lo que sucede en la sociedad con la irrupción de las tecnologías digitales. Este proceso parte de un fin que es aprovechar los datos y las tecnologías digitales para alcanzar los objetivos y hacer frente a los retos que tienen los diferentes agentes de la sociedad. Para que esto ocurra es esencial promover un conjunto de habilitadores, entre ellos, conectividad digital, infraestructura de datos, confianza y seguridad digital, y habilidades y talento digital."*

N°	Descripción de situación susceptible de mejora / oportunidades (observación)	Numeral del informe Capítulo 4	Responsable
2.	Se identificó que las órdenes de trabajo de los mantenimientos al Aire Acondicionado del Datacenter principal de la SDP tienen como descripción “Tarea no Planificada” y al revisar las observaciones se menciona que se generaron alarmas en el funcionamiento del aire acondicionado, es decir, que pasa de lo preventivo a lo correctivo. Así mismo, aún no es claro porqué el proveedor menciona que el cilindro humidificador tenía pasadas las horas de uso recomendadas por el fabricante, ya que de acuerdo con lo informado por la Dirección de TIC la garantía se vence en marzo de 2025. De igual manera, al revisar el detalle de las órdenes de trabajo, se observa que no es consistente la hora de inicio y de finalización de dichos trabajos. Por último, se recomienda diligenciar en su totalidad el cuadro excel suministrado del contrato, para que sea un verdadero instrumento de seguimiento y control del Equipo de aire acondicionado para la Dirección de TIC, ya que se observó que no está diligenciado en su totalidad, por lo que no agrega valor. Control A.11.2.4 Mantenimiento de equipos. “Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas”	4.4.3.8 Mantenimiento de equipos	Dirección de TIC
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	Al hacer la consulta aleatoria de 16 radicados de la vigencia 2023 y sus soportes en el Sistema de Información de Procesos Automáticos-SIPA, se encontró que información sensible de los funcionarios puede ser consultada abiertamente con ocasión de temas tales como: teletrabajo, calamidad, permisos, cuenta bancaria, diagnóstico médico incapacidades, historias clínicas asociadas a incapacidades, acoso, dirección, entre otros.		

Criterio Incumplido (Estándar/norma/reglamento)	Literal g) del artículo 4 de la Ley 1581 de 2012, "la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Principio de Responsabilidad Demostrada. Artículo 26, del Decreto 1377 de 2013. Resolución 500 de 2021, "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", control A.18.1.4 Privacidad y protección de datos personales del MSPI.
Numeral del informe (capítulo 4)	4.4.3.6 Privacidad y protección de datos personales Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente
Responsable	Dirección de Talento Humano Dirección de TIC Dirección Administrativa
Posible efecto	Investigaciones. Demandas. Sanciones a la entidad por no conservar la información bajo condiciones de seguridad necesarias para impedir su consulta o acceso no autorizado
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Privacidad y protección de datos personales

N°	2	**Reincidente (si/no)**	SI
Descripción de la situación crítica	Se presenta una alta vulnerabilidad técnica en la SDP por criticidad y obsolescencia tecnológica (hardware y software), que no permite realizar la remediación de la totalidad de las vulnerabilidades identificadas en la SDP.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021, "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"-MSPI A.12.6 Gestión de la vulnerabilidad técnica. Decreto Nacional 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario		

	del Sector de Tecnologías de la Información y las Comunicaciones": Artículo 2.2.9.1.1.3. Principios. La Política de Gobierno Digital. 12.Resiliencia Tecnológica. Y Sección 2 Elementos de la Política de Gobierno Digital. Artículo 2.2.9.1.2.1 Estructura. 3.2. Seguridad y Privacidad de la Información
Numeral del informe (capítulo 4)	4.4.3.3 Gestión de vulnerabilidades A.12.6. Gestión de la vulnerabilidad técnica. Prevenir el aprovechamiento de las vulnerabilidades técnicas. 3. Habilitadores Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente
Responsable	Dirección de TIC
Posible efecto	Pérdida en la confiabilidad, disponibilidad e integridad, de la información, pérdida de activos de información, afectación económica y reputacional e incluso afectar la continuidad de la operación de la SDP
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Vulnerabilidad técnica Criticidad y obsolescencia tecnológica

N°	3	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Se identificó información inconsistente en el seguimiento del Plan de Acción de controles 2023 del Modelo de Seguridad y Privacidad de la Información, proporcionado por la Dirección de TIC, el cual es el corazón del modelo. En el documento suministrado, no hay coherencia entre las actividades programadas y las actividades ejecutadas, entre las fechas de realización y los valores de la columna porcentaje de avance vs las evidencias; aspectos mínimos en la formulación y seguimiento de un plan de trabajo, dificultando conocer con exactitud el nivel de implementación de los controles del MPSI en la SDP para la vigencia 2023. Es así como entre otros aspectos se encontró: -Cincuenta y cuatro (54) controles tienen en la columna de avance una calificación de 0%. Por ejemplo: "Actualizar el inventario de activos de información en los 15 procesos de la SDP para la vigencia 2023", lo cual es impreciso dado todo el esfuerzo y las actividades lideradas por la Dirección de TIC y adelantadas por la entidad para la actualización de los activos de información de la SDP en la vigencia 2023		

	-53 controles de 114 tienen la observación “no se programa para la vigencia 2023. -En otras actividades, la Dirección de TIC presenta avances porcentuales, pero la actividad “no estaba programada”, como tampoco se relacionan las evidencias que permitan aclarar el porcentaje de avance consignado. -En otros casos se observó, por ejemplo, que algunas de las acciones tienen como fecha de cumplimiento el 31 de diciembre de 2023, y la Dirección de TIC relaciona la evidencia de la ejecución en la columna correspondiente, sin embargo, tienen ejecución de cero %. -El control “Gestión de la vulnerabilidad técnica” tiene ejecución del 50%. Pero en otro documento, informa la Dirección TIC que se ejecutó al 100%. -En otros casos las acciones están previstas para la vigencia 2024 pero con ejecución del 100% en el 2023.
Criterio Incumplido (Estándar/norma/reglamento)	Principios básicos de la información dispuestos en los literales b, c, d, e y g del artículo 2 de la Ley 87 de 1993. Principio de Calidad de la información artículo 3 de la Ley 1712 de 2014. Resolución 500 de 2021, “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”-MSPI del Ministerio de las TIC.
Numeral del informe (capítulo 4)	4.4.3.1 Plan de acción implementación de controles del MSPI 2023 Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente
Responsable	Dirección TIC
Posible efecto	La debilidad en el control, revisión y seguimiento a la trazabilidad de los registros que dan cuenta del avance del Plan de seguimiento a los controles obligatorios del MPSI, puede afectar la toma de decisiones de la Entidad al no contar con información confiable y veraz de la gestión adelantada y resultados obtenidos y en consecuencia en la proyección de objetivos, metas y recursos
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Calidad de la Información- Plan Seguimiento de controles del MSPI

N°	4	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Se identificó por parte del equipo auditor, que ante el cambio de la plataforma Gmail a Outlook, el equipo humano de la Dirección TIC no contó con la capacitación previa necesaria para atender una adecuada gestión del cambio en el tema y los requerimientos propios de las dependencias y funcionarios. Dichas capacitaciones fueron solicitadas para el cumplimiento de la gestión (temas de seguridad de la información, en seguridad informática, ciberseguridad, programación, en ofimática, innovación pública y en tecnologías emergentes y de la Cuarta Revolución Industrial, entre otras temáticas y en concordancia con la actualización de la Política de Gobierno Digital Decreto Nacional 767 de 2022)		
Criterio Incumplido (Estándar/norma/reglamento)	-Resolución 500 de 2021, "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" Artículo 5. La estrategia de seguridad digital. Numeral 4: *"Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces"* Resolución 500 de 2021. Artículo 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Numeral 5: *"Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas."* -MSPI Control A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información Control A.12.1.3 Gestión de capacidad -Política de Gobierno Digital Decreto Nacional 767 de 2022.		
Numeral del informe (capítulo 4)	4.4.2.4 Soporte/Recursos necesarios 4.4.2.4 .2 Talento Humano		
Responsable	Dirección de Talento Humano		
Posible efecto	Demoras a requerimientos relacionados con el Modelo de Seguridad y Privacidad de la Información al no tener el		

	conocimiento y/o las competencias para responder oportunamente. Riesgos de seguridad de la información
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Capacitación Formación

N°5	5	**Reincidente (si/no)**	NO
Descripción de la situación crítica	No se cuenta con un plan de continuidad de la seguridad de la información, en el marco de un plan de continuidad del negocio.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021, “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”. Control A17.1.1 de la norma ISO 27001. Numeral 7.3.2 Valoración de los riesgos de seguridad de la información del Modelo de Seguridad y Privacidad de la Información Numeral 3.6 de la ISO 27000, Factores Críticos de Éxito de una Sistema de Gestión de Seguridad de la Información literal g. Decreto Nacional 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”. Artículo 2.2.9.1.1.3. Principios. Numeral 12. Resiliencia Tecnológica. -Directiva Presidencial 002 de 2022. “Reiteración De La Política Pública en Materia de Seguridad Digital” Artículo 12: *“12.Contar con planes de continuidad del negocio, orientados a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información. Igualmente, se deben realizar ejercicios que permitan probar la efectividad del plan de continuidad del negocio frente al escenario de materialización de riesgos de seguridad de la información”*		
Numeral del informe (capítulo 4)	4.4.4 Acciones adelantadas por la Dirección de TIC frente a los temas de más bajo puntaje de los autodiagnósticos MPSI realizados		

	Control A.17.1 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente
Responsable	Dirección de TIC
Posible efecto	Afectación reputacional y económica de la entidad Afectación de la continuidad en la operación de la entidad Posibilidad de pérdida de disponibilidad, integridad y confidencialidad de la información. Posibilidad de pérdida de la propiedad intelectual de la entidad y de la información importante de la SDP. Interrupción en la prestación de servicios a los grupos de valor y de interés.
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Plan de continuidad de seguridad de la información

N°	6	**Reincidente (si/no)**	NO
Descripción de la situación crítica	La Secretaría Distrital de Planeación no cuenta con un plan de Continuidad de negocio para cubrir las necesidades para las comunicaciones de voz, datos y TI, así como para el personal esencial y las ubicaciones alternas.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021, “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” Artículo 17. Etapas generales de la gestión de incidentes de seguridad digital. -Decreto 767 de 2022. Artículo 2.2.9.1.1.3. Principios. Numeral 12. Resiliencia Tecnológica -Directiva Presidencial 002 de 2022. “Reiteración De La Política Pública en Materia de Seguridad Digital” Artículo 12 *“12. Contar con planes de continuidad del negocio, orientados a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información. Igualmente, se deben realizar ejercicios que permitan probar la efectividad del plan de continuidad del negocio frente al escenario de materialización de riesgos de seguridad de la información”*		
Numeral del informe (capítulo 4)	4.4.3.2 Acciones adelantadas por la Dirección de TIC frente a los temas de más bajo puntaje de los autodiagnósticos MPSI realizados Control A.17.1 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio		

	Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente
Responsable	Subsecretarios de la SDP Dirección de Planeación Institucional Dirección Administrativa Dirección de Talento Humano Dirección de TIC
Posible efecto	Afectación reputacional y económica de la entidad Afectación de la continuidad en la operación de la entidad. Demoras en la recuperación de incidentes. Posibilidad de pérdida de disponibilidad, integridad y confidencialidad de la información. Interrupción en la prestación de servicios a los grupos de valor y de interés.
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Plan de continuidad de negocio

N°	7	**Reincidente (si/no)**	NO
Descripción de la situación crítica	Respecto a los Indicadores de Gestión Seguridad de la Información, se encontraron diferencias en la información remitida por la Dirección de TIC en: 1)Evidencia 14: El "Plan de Modelo de Seguridad y Privacidad de la Información de la SDP", A-LE -373, Versión 5 Acta de Mejoramiento 257 de Julio 27 de 2023. 2)Evidencia 9: Documento "Avances y Logros_MSPI_Dic_2023_12032024" como entrada para la Revisión por la Dirección. 3)Evidencia 8 .Plan de acción de controles MSPI 2023.		
Criterio Incumplido (Estándar/norma/reglamento)	-Principios básicos de la información dispuestos en los literales b, c, d, e y g del artículo 2 de la Ley 87 de 1993. -Principio de Calidad de la información artículo 3 de la Ley 1712 de 2014. -Resolución 500 de 2021, "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 Ministerio de las TIC		
Numeral del informe (capítulo 4)	4.4.4 FASE 3: Evaluación de desempeño Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente		
Responsable	Dirección de TIC		
Posible efecto	La debilidad en el control, revisión y seguimiento a la trazabilidad de los registros que dan cuenta del avance del Plan, sus indicadores y los controles obligatorios del MPSI, puede afectar la toma de decisiones de la Entidad y en consecuencia en la proyección de objetivos, metas y recursos		

Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Indicadores MSPI Calidad de la información

N°	8	**Reincidente (si/no)**	NO
Descripción de la situación crítica	No se identificó un documento que dé cuenta de las acciones adelantadas o un plan de mejoramiento con acciones correctivas, relacionadas con aquellas situaciones que presentaron reiteración o recurrencia y que obtuvieron puntajes bajos en las encuestas de satisfacción relacionadas con mesa de ayuda y servicios de TI y cuya trazabilidad se observe dentro de la matriz Todo de la entidad. Es así como se identificó entre otros: Dentro de los incidentes de seguridad recibidos por mesa de ayuda GLPI, se identificó uno con un **tiempo alto** relacionado con una solicitud de listado usuarios, para lo cual no es claro que para la solución/cierre se invirtieran 197 Dí-a(s) 22 Hora(s) 5 Minuto(s), si el tiempo de espera fue de 0 Segundo(s) y el tiempo para atender el servicio fue de 16 Hora(s) 1 Minuto(s). De las encuestas de satisfacción de mesa de ayuda se identificaron 31 calificadas por los usuarios en el nivel más bajo, de las cuales se observó que hay casos que reinciden o que no fueron atendidos, y además tienen una nota de la mesa de ayuda de TIC como “incidencia solucionada”. De las 66 calificadas por los usuarios en el nivel regular, todas ellas tienen una nota de la mesa de ayuda de TIC como “incidencia solucionada”, de las cuales se identifica que 88 se refieren a “Demora en la atención”. Respecto a los servicios de TIC se observaron calificaciones de satisfacción de Internet Dispositivos Móviles (Wifi): 67% y Servicio de Telefonía: 72%.		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021- “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” Anexo 1 del MSPI. Fase 4: Mejoramiento continuo 10.1 Mejora		
Numeral del informe (capítulo 4)	4.4.3.5 Gestión de incidentes de seguridad de la información. Control A.16 4.4.5 FASE 4: Mejoramiento continuo. Mesa de ayuda Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente		
Responsable	Dirección de TIC		
Posible efecto	Riesgo de pérdida de calidad en los datos y en la información obtenida para la mejora.		

	Riesgo de pérdida en la eficacia, la eficiencia y economía en las operaciones de la Dirección de TIC Riesgo reputacional; pérdida de credibilidad en los servicios que se prestan.
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Mesa de ayuda Incidentes de seguridad Encuestas de Satisfacción Mejoramiento continuo

N°	09	**Reincidente (si/no)**	NO
Descripción de la situación crítica	En la matriz Equipos Entregados, Instalados y Configurados entregada por la Dirección de TIC, se encontró desactualización en la información toda vez que hay personas que aparecen como usuarios a cargo de los equipos a diciembre 30 de 2023 pero se retiraron de la entidad antes de dicha fecha, por ejemplo el director de Registros Sociales (1064SBO06, 2043SDP03 y 2043SDP04) que se retiró de la entidad en junio 12 de 2023, y la Subsecretaria Jurídica que se retiró en junio 23 del mismo año (205SDP02).		
Criterio Incumplido (Estándar/norma/reglamento)	Resolución 500 de 2021 de MINTIC. Resolución 500 de 2021, “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” Anexo 1. Control A.8 Gestión de activos Control A.9.2.1Registro y cancelación del registro de usuarios. Control Control A.9.2.6 Retiro o ajuste de los derechos de acceso		
Numeral del informe (capítulo 4)	4.4.3.11 Equipos Análisis de la respuesta de la Dirección TIC en el capítulo correspondiente		
Responsable	Dirección de TIC		
Posible efecto	Pérdida de confiabilidad en la información relacionada Equipos Entregados, Instalados y Configurados Pérdida de trazabilidad en la administración de los equipos de cómputo.		
Palabra(s)clave(s) para identificar en SIPA (Máximo 5)	Gestión de activos		

- 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

- De acuerdo con la respuesta de la Dirección de TIC, en el desarrollo de la gestión de los incidentes reportados en la herramienta de mesa de ayuda, se recibió respuesta en el sentido de que “no se identificaron aprendizajes nuevos ni lecciones aprendidas”, contrario a lo manifestado por la misma Dirección TIC cuando menciona que a través de boletines se refuerza sobre los tipos de incidentes. Por lo que se recomienda aprovechar los casos y documentarlos como parte de la gestión de conocimiento para la misma Dirección TIC y las dependencias y para las jornadas de capacitación y sensibilización que se realicen en la entidad.

- Si bien es cierto se destaca la permanente revisión y actualización de los documentos del MSPI, se sugiere analizar la posibilidad de a) reducir los documentos b) Unir los documentos de políticas para hacer uno solo de políticas TIC, en donde cada una constituya un capítulo y c) Racionalizar o simplificar los formatos en que se hacen compromisos, para que en uno solo la persona se comprometa con lo que haya a lugar en materia TIC.

- Se recomienda al responsable de seguridad y privacidad de la información de la entidad atender lo descrito en el Anexo 1 del Modelo de Privacidad y seguridad de la Información, Resolución 500 de 2021, numeral 11.2.9 Control Interno, respecto a su papel o rol en cuanto a:

  “Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres ***y los planes de continuidad del negocio.***
  - Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información”.

Nombres / Equipo Auditor	
Auditor líder	Lucy Divanelly Muñoz Rodríguez
Auditor(es)	Eulalia Porras Salek

Denis Parra Suárez
Jefe Oficina de Control Interno