MEMORANDO

PARA: SECRETARIA DE DESPACHO, SUBSECRETARIO GENERAL, DIRECTORES, SUBDIRECTORES, JEFES DE OFICINA y ASESORA DE DESPACHO

DE: NORMA LUCIA AVILA QUINTERO
Jefe Oficina de Control Interno

ASUNTO: Informe Final de Auditoría Interna con Base en Riesgos al Proceso de Gestión Tecnológica

En cumplimiento del Plan Anual de Auditoría 2023 aprobado para la Oficina de Control Interno, atentamente allegamos el Informe Final correspondiente a la Auditoría Interna con Base en Riesgos al Proceso del Proceso de Gestión Tecnológica.

OBJETIVO

Obtener evidencia de auditoría válida, suficiente y competente sobre la aplicación de los controles y actividades del proceso “Gestión Tecnológica”, relacionadas con el MSPI, PETI, Accesibilidad y Desempeño de Proceso

ALCANCE DE LA AUDITORIA

Plan Estratégico de Tecnologías de la Información – PETI: Verificación de la existencia, cumplimiento y nivel de avance del Plan Estratégico de tecnologías de la Información PETI, conforme Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015 (...) ARTÍCULO 2.2.3.5.3. (...) y riesgos asociados.

Modelo de Privacidad y Seguridad de la Información - MSPI: cumplimiento de la norma ISO 27001: 2013, el MSPI del MinTIC y riesgos asociados.

Accesibilidad Portal WEB de la Entidad: abarcando el anexo 1 de la Resolución No. 1519 de 2020 relacionado con el cumplimiento de los criterios de accesibilidad nivel “AA” en el portal web de la Entidad, los cuales son exigibles en los sujetos obligados a partir del 1 de enero del 2022. Dichos requerimientos se encuentran alineados con la Norma NTC 5854 del 15 de agosto de 2011 (Accesibilidad a páginas Web) y ésta a su vez con el estándar WCAG o “Web Content Accessibility Guidelines”, el cual establece los criterios de cumplimiento para los niveles de Accesibilidad “A”, “AA” o “AAA”.

Periodo de Alcance: agosto 2022 a agosto 2023.

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

RESUMEN EJECUTIVO DE LOS RESULTADOS

Fortalezas (aspectos positivos observados)

Fortaleza No.1: El Sistema de Gestión de Seguridad de la Información cuenta con las Políticas de Seguridad de la Información actualizadas, lo que permite proteger la información sensible, cumplir con los requisitos legales y normativos, prevenir brechas de seguridad, gestionar eficientemente los riesgos y mantener la confianza y reputación de la SDA.

Fortaleza No.2: Se observó la realización de análisis frente al Plan de Capacidades de los Servicios Tecnológicos, mediante el cual se diagnostican y determinan soluciones sobre el rendimiento y la capacidad de los servicios e infraestructura de Tecnologías de la Información y las Comunicaciones-TIC, y de esta manera mantener la operación de la entidad con una capacidad suficiente y correctamente dimensionada de los servicios e infraestructura TIC.

Fortaleza No.3: Con respecto al uso y apropiación de los componentes de TI frente a las necesidades manifestadas por los usuarios se generaron capacitaciones en temas como FOREST, correspondencia, Notificaciones, IAAP, IAAP jurídicos entre otros; lo que contribuye a mejorar la eficiencia operativa, fomentar la colaboración y la comunicación, habilidades en los servidores de la SDA para garantizar un uso efectivo y beneficio de estos componentes tecnológicos.

Fortaleza No.4: Al realizar la evaluación a través del ITA, el proceso de Gestión Tecnológica ha demostrado su compromiso con la transparencia y el acceso a la información. Esta evaluación le brinda la oportunidad de identificar fortalezas y debilidades en su gestión, y le permite implementar acciones de mejora para fortalecer su desempeño

Hallazgos de Auditoría (representan desviaciones respecto del resultado esperado y requieren la suscripción de un plan de mejoramiento interno).

A continuación, se señalan los aspectos que requieren de implementación de acciones de mejora, para continuar avanzando en el fortalecimiento del Proceso de Gestión Tecnológica.

1. Cumplimiento de los Planes de Seguridad y Planes de Tratamiento de Seguridad de la Información.
2. Riesgos de Seguridad de la Información en los Procesos de contratación de la SDA
3. Planificación, Implementación y Verificación de la Gestión de Continuidad de Negocio.
4. Aplicación Política de Mantenimiento Físico de las Operaciones.
5. Establecimiento de la Políticas de Seguridad de la Información de la SDA
6. Seguimiento, calidad y cumplimiento de los Entregables asociados al Proyecto de Inversión 7804.
7. Criterios de Accesibilidad del Portal Web de la SDA.

El Informe preliminar de la auditoría interna fue comunicado al responsable del proceso auditado mediante radicado Forest 2023IE245968 del 20 de octubre de 2023, sobre el cual se recibió respuesta por parte del proceso de Gestión Tecnológica con radicado Forest 2023IE250946 del 25 de octubre de 2023, considerando las observaciones y/o justificaciones entregadas, quedando agotados todos los mecanismos de subsanación de diferencias y culminadas las respectivas etapas del ciclo auditor.

En tal sentido, los responsables del proceso auditado deberán aplicar el procedimiento PC01-PR02 Plan de Mejoramiento por Procesos, que, en resumen, corresponde a:

- Realizar y documentar el análisis de causas correspondiente en el formato PC01- PR02 F2.
- Formular Plan de Mejoramiento en el formato PC01-PR02-F1 y remitirlo a la Oficina de Control Interno para su verificación y análisis correspondiente.
- Cargar las acciones una vez se cuente con los códigos de los hallazgos registrados en
- el aplicativo ISOLUCION.
- Iniciar la ejecución de las acciones y reportar los avances en el Sistema de Información ISOLUCION.
- Diligenciar la encuesta de percepción de auditoría que se anexa.

En documentos adjuntos encontrarán un ejemplar del Informe Final de Auditoría Interna con Base en Riesgos al Proceso de Gestión Tecnológica, con los resultados detallados de la actividad de aseguramiento.

Atentamente,

NORMA LUCIA AVILA QUINTERO

OFICINA DE CONTROL INTERNO

Anexos Informe Final al Proceso de Gestión Tecnológica
Anexo de Accesibilidad
Encuesta percepción de auditoría - PC01-PR04-M6 Versión 2

Elaboró:				
DIANA JAIDY PIÑEROS ESPEJO	CPS:	CONTRATO 20221643 DE 2022	FECHA EJECUCIÓN:	02/11/2023
Revisó:				
VIVIANA MARCELA MARIN OLMOS	CPS:	CONTRATO SDA-CPS-20220878 DE 2022	FECHA EJECUCIÓN:	02/11/2023
DIANA JAIDY PIÑEROS ESPEJO	CPS:	CONTRATO 20221643 DE 2022	FECHA EJECUCIÓN:	02/11/2023
VIVIANA MARCELA MARIN OLMOS	CPS:	CONTRATO 20230291 DE 2023	FECHA EJECUCIÓN:	02/11/2023
Aprobó: **Firmó:**				
NORMA LUCIA AVILA QUINTERO	CPS:	FUNCIONARIO	FECHA EJECUCIÓN:	03/11/2023



Informe Final de Auditoría al Proceso de Gestión Tecnológica

OFICINA DE CONTROL INTERNO

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE AMBIENTE

BOGOTÁ

1. OBJETIVO

Obtener evidencia de auditoría válida, suficiente y competente sobre la aplicación de los controles y actividades del proceso "Gestión Tecnológica", relacionadas con el MSPI, PETI, Accesibilidad y Desempeño de Proceso.

2. ALCANCE

1. Plan Estratégico de Tecnologías de la Información – PETI: Verificación de la existencia, cumplimiento y nivel de avance del Plan Estratégico de tecnologías de la Información PETI, conforme el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015 (...) ARTÍCULO 2.2.3.5.3. (...) y riesgos asociados.

2. Modelo de Privacidad y Seguridad de la Información - MSPI: cumplimiento de la norma ISO 27001: 2013, el MSPI del MinTIC y riesgos asociados.

3. Accesibilidad Portal WEB de la Entidad: abarcando el anexo 1 de la Resolución No. 1519 de 2020 relacionado con el cumplimiento de los criterios de accesibilidad nivel “AA” en el portal web de la Entidad, los cuales son exigibles en los sujetos obligados a partir del 1 de enero del 2022. Dichos requerimientos se encuentran alineados con la Norma NTC 5854 del 15 de agosto de 2011 (Accesibilidad a páginas Web) y ésta a su vez con el estándar WCAG o “Web Content Accessibility Guidelines”, el cual establece los criterios de cumplimiento para los niveles de Accesibilidad “A”, “AA” o “AAA”.

4. La gestión y operación del proceso especialmente lo relacionado con los procedimientos:

   • PA03-PR05 Gestión, restauración y verificación de las copias de respaldo
   • PA03-PR14 Gestión de Incidentes de TI • PA03-PR15 Gestión de la Capacidad de la Infraestructura de Tecnologías de la Información. • PE03-PR02 Administración de riesgos
   • PA03-PR05 Gestión, restauración y verificación de las copias de respaldo
   • PA06-PR02 Administración y control de los activos y registros de información
   • 126MSGSI- MANUAL DEL SUBSISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSPI)

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

3. DECLARACIÓN

La ejecución de esta auditoría fue aprobada por el Comité Institucional de Coordinación de Control Interno - CICCI de la Secretaría Distrital de Ambiente – SDA, y hace parte del Plan Anual de Auditoría 2023 de la Oficina de Control Interno.

4. EQUIPO AUDITOR

Líder de la Auditoría: Diana Jaidy Piñeros Espejo, Contratista

Emisor del Informe: Norma Lucia Ávila Quintero, Jefa Oficina de Control Interno

5. CRITERIOS

Para la realización de este trabajo se consideraron los siguientes criterios normativos:

Normatividad Externa

- Decreto 1078 de 2015 última fecha de actualización: 19 de agosto de 2021 - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- Ley 1581 de 2012 – Disposiciones generales para la protección de datos personales y decretos que la reglamenten.
- Modelo de Seguridad y Privacidad de la Información – MSPI conforme a lo establecido en el Decreto 1078 de 2015 última fecha de actualización: 19 de agosto de 2021 - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital.
- Norma ISO 27001 Sistema de Gestión de Seguridad de la Información
- Norma Técnica Colombiana (NTC) 5854 que establece los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA, Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1
- Resolución 1519 de 2020 del MinTIC incluir la descripción "por medio de la cual …"anexo 1 accesibilidad.
- Guía para la Administración de Riesgos y el diseño de controles en entidades públicas. Versión 4 y 5 del DAFP.
- Modelo Integrado de Planeación y Gestión - MIPG versión 4 de marzo del 2021
- Modelo de Gestión de Riesgos de Seguridad Digital, Anexo 4: Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).
- Demás normatividad interna aplicable.

Normatividad interna

- Declaración de aplicabilidad MSPI –SDA
- MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI Código: PA03-MA01
- POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE AMBIENTE Código: PA03-PO01
- Procedimiento: Gestión de Incidentes de TI Código: PA03-PR14

- Análisis de Impacto al Negocio (BIA)
- Plan de Recuperación de Desastres (DRP)
- Estrategias de Recuperación del BCP
- Procedimiento: Uso y apropiación de componentes de TI Código: PA03-PR07
- Procedimiento: Gestión de la Capacidad de la Infraestructura de Tecnologías de la Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN Código: PE01-PR05

6. RIESGOS ASOCIADOS AL PROCESO AUDITADO

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Incluidos en el Mapa de Riesgos de Gestión	
Posibilidad de afectación reputacional por la indisponibilidad de los servicios de tecnologías de la información y Comunicaciones, debido a la baja capacidad para aplicar los estándares y lineamientos en la gestión de los servicios de TI	Si
Posibilidad de afectación reputacional por la variación en los atributos de confidencialidad, disponibilidad, integridad y privacidad de la información, debido a la insuficiente	Si
Posibilidad de afectación económica por la desarticulación de los proyectos estratégicos de la entidad que tienen algún componente de tecnologías de la información y las comunicaciones debido a fallas en el seguimiento de las iniciativas y adquisiciones de TI.	Si
Posibilidad de afectación reputacional por la subutilización de las herramientas de TI en la Entidad debido al bajo uso y apropiación de servicios y capacidades tecnológicas de la entidad.	Si
Incluidos en el Mapa de Riesgos de Corrupción	
Alteración malintencionada o uso injustificado de la información gestionada en los sistemas de información, para un beneficio propio o privado.	Si
Identificados por la Oficina de Control Interno en su evaluación preliminar	
Posibilidad de hurto o pérdida de activos de la plataforma tecnológica (información, equipos de cómputo, comunicaciones, procesamiento, audiovisuales, etc.) debido a la insuficiencia de controles para su administración	Si
Posible pérdida, fuga de información confidencial almacenada en la plataforma tecnológica por utilización indebida o divulgación no autorizada.	Si
Identificados por la Oficina de Control Interno en su ejecución	
Posibilidad de afectación reputacional por la falta de oportunidad en la implementación y seguimiento a los instrumentos de gestión definidos por el proceso, afectando la gestión institucional y por consiguiente el análisis de resultados.	Si

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Posibilidad de hurto o perdida de información confidencial, como datos personales de clientes, información financiera o secretos comerciales, por acceso indebido a sistemas y datos sensibles de la entidad.	Si
Perdida de confidencialidad por exposición o acceso indebido de personas no autorizadas**.**	Si
Posibilidad de afectación reputacional por interrupción en la operación de la entidad debido a la inadecuada definición estrategias y medidas de continuidad en caso de situaciones de emergencia.	Si
Posibilidad de afectación económica por perdida de información por introducción de malware a través de medios extraíbles sin la debida verificación.	Si
Posibilidad de afectación reputacional por interrupción en la operación de la entidad debido a la inadecuada definición estrategias y medidas de continuidad en caso de situaciones de emergencia.	Si
Pérdida de confidencialidad de la información sensible debido a insuficientes mecanismos de verificación del cumplimiento efectivo de las Políticas de Seguridad de la Información de la SDA.	Si
Posibilidad de afectación reputacional y económica por incumplimiento de las metas definidas en el plan de acción a cargo del proceso	Si
Posibilidad afectación reputacional por falta de garantías en el acceso a la oferta institucional en la web a todos los usuarios, independientemente de sus capacidades físicas, mentales o motoras.	Si

Fuente: Elaboración Propia. **Tabla 1**. Riesgos asociados al proceso auditado

3 ÚLTIMO SEGUIMIENTO AL PLAN DE MEJORAMIENTO INTERNO

La Oficina de Control Interno realizo el Seguimiento al Plan de Mejoramiento por Procesos el cual fue comunicado mediante el Radicado 2023ER116570 del 25 mayo 2023.

De acuerdo con los resultados obtenidos en este seguimiento, se determina que el estado del Plan de Mejoramiento del proceso por procesos a 1º de abril de 2023, posterior a los cierres efectuados por la Oficina de Control Interno es el siguiente:

Proceso	Acciones Abiertas	Acciones Vencidas	Total
Gestión Tecnológica	1061, 1062, 1057,1058, 1059, 1060	-	6

Tabla 1 Estado de las Acciones de Planes de Mejoramiento de Auditorías Anteriores

De otra parte, la DPSIA solicito mediante radicado No. 2023IE215802 el cierre de acciones plan de mejoramiento proceso gestión tecnológica 1057, 1059, 1060, 1061 y 1062.; el cual será realizado y comunicado durante el mes de noviembre.

4 METODOLOGÍA

La Auditoría Interna al proceso de "Gestión Tecnológica" fue desarrollada mediante la aplicación de entrevistas, evaluación portal web, consulta de procedimientos, atendiendo a las etapas comunicadas en el Plan de Trabajo radicado mediante Forest 2023IE194140 del 24 de agosto de 2023:

PLANEACIÓN

- Se efectuaron mesas de trabajo e indagaciones con colaboradores del proceso, tanto para realizar las pruebas de recorrido a los controles identificados, como para obtener conocimiento del desarrollo de las actividades relevantes objeto de auditoría (temáticas de PETI, MSPI y ACCESIBILIDAD).

- Se realizó la inspección de los mapas de riesgos de corrupción y gestión del proceso, identificando los riesgos relevantes; así mismo, se analizaron otros posibles riesgos detectados por la Oficina de Control Interno. En ambos casos, se seleccionaron los controles pertinentes para evaluar su diseño, implementación y eficacia operativa.

EJECUCIÓN

- Se efectuaron requerimientos de información sobre el Plan Estratégico de Tecnologías de la Información – PETI 2020-2024, Modelo de Seguridad y Privacidad de la Información – MSPI, Desempeño del Proceso, y avances de accesibilidad.

- Se llevaron a cabo entrevistas con el objetivo de verificar el cumplimiento de los requisitos aplicables del MSPI dentro del periodo del 11 al 13 de septiembre.

- Se realizó una visita a las instalaciones de la SDA; en la que se revisaron los siguientes temas:

  - Políticas de Seguridad de la Información
  - Plan de Seguridad y Plan de Tratamiento del 2022 y 2023
  - Control de Software Operacional
  - Seguridad de la información en las relaciones con los proveedores
  - Gestión de incidentes de seguridad de la información
  - Planificación de la continuidad de la seguridad de la información
  - Implementación de la continuidad de la seguridad de la información.
  - Verificación, revisión y evaluación de la continuidad de la seguridad de la información
  - Controles: Gestión de medios removibles, Dispositivos móviles, Directrices de seguridad para el control de acceso físico, seguridad en zonas donde se lleve a cabo las actividades de tesorería, uso adecuado de internet y mantenimiento físico de las operaciones.

- Se efectuaron entrevistas durante los días 18,19, 25 y 26 de septiembre con el objetivo de verificar la ejecución del PETI 2020 – 2024 de acuerdo con lo establecido en las fichas de

los proyectos. Se selecciono el Proyecto 7804 como muestra, y se verificaron los entregables en relación con los alcances definidos para cada vigencia.

- Se realizó el análisis de accesibilidad al Portal WEB de la Secretaría Distrital de Ambiente con el objetivo de recopilar los datos necesarios para el análisis de las Url, con el fin de identificar el nivel de cumplimiento de los estándares de accesibilidad bajo la norma AA, establecido en la Resolución 1519 del 2020.

- Se verificó el desempeño del proceso a través de la revisión de los procedimientos Gestión de la Capacidad de la Infraestructura de Tecnologías de la Información - Código:PA03 - PR15, Procedimiento: Uso y apropiación de componentes de TI - Código:PA03 - PR07.

- Se informaron las situaciones preliminares identificadas a los delegados del Proceso de Gestión Tecnológica.

COMUNICACIÓN DE RESULTADOS

Este reporte corresponde a la comunicación final de resultados, donde se manifiestan los argumentos del equipo auditado, informados mediante Forest 2023IE250946 del 25 de octubre de 2023 con asunto Respuesta 2023IE245968 Informe Preliminar de Auditoría Interna con Base en Riesgos al Proceso de “Gestión Tecnológica”, y las conclusiones que sobre ellos tuvo la Oficina de Control Interno, todo lo cual fue abordado en la mesa de trabajo - reunión de cierre del 2 de noviembre de 2023, con los responsables del Proceso Auditado.

5 RESULTADOS DE LA AUDITORÍA

5.1 FORTALEZAS (ASPECTOS POSITIVOS OBSERVADOS)

En las pruebas de evaluación de controles (diseño, implementación y eficacia operativa) del proceso de Gestión Tecnológica, la Oficina de Control Interno identificó que las siguientes actividades se ejecutaron conforme a los lineamientos procedimentales o normativos establecidos:

Fortaleza No.1: El Sistema de Gestión de Seguridad de la Información cuenta con las Políticas de Seguridad de la Información actualizadas, lo que permite proteger la información sensible, cumplir con los requisitos legales y normativos, prevenir brechas de seguridad, gestionar eficientemente los riesgos y mantener la confianza y reputación de la SDA.

Fortaleza No.2: Se observó la realización de análisis frente al Plan de Capacidades de los Servicios Tecnológicos, mediante el cual se diagnostican y determinan soluciones sobre el rendimiento y la capacidad de los servicios e infraestructura de Tecnologías de la Información y las Comunicaciones-TIC, y de esta manera mantener la operación de la entidad con una capacidad suficiente y correctamente dimensionada de los servicios e infraestructura TIC.

Fortaleza No.3: Con respecto al uso y apropiación de los componentes de TI frente a las necesidades manifestadas por los usuarios se generaron capacitaciones en temas como FOREST, correspondencia, Notificaciones, IAAP, IAAP jurídicos entre otros; lo que contribuye a mejorar la eficiencia operativa, fomentar la colaboración y la comunicación, habilidades en los servidores de la SDA para garantizar un uso efectivo y beneficio de estos componentes tecnológicos.

Fortaleza No.4: Al realizar la evaluación a través del ITA, el proceso de Gestión Tecnológica ha demostrado su compromiso con la transparencia y el acceso a la información. Esta evaluación le brinda la oportunidad de identificar fortalezas y debilidades en su gestión, y le permite implementar acciones de mejora para fortalecer su desempeño.

5.2 HALLAZGOS DE AUDITORÍA (REPRESENTAN DESVIACIONES RESPECTO AL RESULTADO ESPERADO Y REQUIEREN LA SUSCRIPCIÓN DE UN PLAN DE MEJORAMIENTO INTERNO)

Para efectos de revelar los resultados asociados a las temáticas que fueron objeto de auditoría, a continuación, se discrimina cada una de ellas por separado, con el fin de ilustrar las respectivas situaciones identificadas. Sin perjuicio de esto, la numeración de los hallazgos se exhibe de manera consecutiva.

5.2.1 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACIÓN -MSPI

Hallazgo 1: Debilidad en el cumplimiento de los Planes de Seguridad y Planes de Tratamiento de Seguridad de la Información.

En la verificación realizada a los planes de Seguridad y Planes de Tratamiento de Seguridad de la información definidos para las vigencias 2022 y 2023 se evidenció lo siguiente:

- **Plan de Seguridad y Privacidad de la información 2022 y Plan de Tratamiento de Riesgos 2022**

  Los Planes se encuentra publicado en la sección de Transparencia del Portal Web de la Entidad con los nombres: 12. Plan de Seguridad y Privacidad de la Información 2022.pdf y 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información SDA_2022.pdf. a continuación, se detalla su ejecución:

No.	Actividad	Tiempo de Ejecución	Plan que pertenece la actividad		Soporte	Observación
			Plan de Seg. Y Priv.	Plan de Tratamiento		
1	Actualización de las políticas y lineamientos	Primer semestre del año.	X	X	Documento: políticas de seguridad y privacidad de la	No se ejecuta en la vigencia 2022, actividad ejecuta

No.	Actividad	Tiempo de Ejecución	Plan que pertenece la actividad		Soporte	Observación
			Plan de Seg. Y Priv.	Plan de Tratamiento		
	de gestión de riesgos				información de la Secretaría Distrital de Ambiente, Versión 3 aprobado en el Comité Institucional de Gestión y Desempeño Fecha: 04 de agosto de 2023 Radicado 2023IE174378 del 31 de julio de 2023	en agosto del 2023
2	Sensibilización en toda la entidad	Segundo y tercer trimestre del año.	X	X	Dentro de las evidecias se adjuntan soportes de socialización de Big Data y Protocolo de Anonimización	Se evidencia la socialización de algunos componentes de seguridad, sin embargo, no se abordó la socialización de las políticas de Seguridad de la Información de forma completa
3	Identificación y priorización de los activos de información	Segundo y tercer trimestre del año	X	X	Se inicio con algunos procesos el levantamiento de activos, se realizó a 8 de 18 procesos.	Actividad realizada parcialmente de los 18 procesos de la SDA se realizó el levantamiento de 8, se definió una metodología y herramienta para la identificación de activos.
4	Aceptación de riesgos identificados	Tercer trimestre del año.	X	X	El proceso informa que se trata de un riesgo general, que está identificado y tiene actividades de control.	Sin observación.

No.	Actividad	Tiempo de Ejecución	Plan que pertenece la actividad		Soporte	Observación
			Plan de Seg. Y Priv.	Plan de Tratamiento		
5	Socialización y publicación de riesgos de seguridad y privacidad de la información	Cuarto semestre del año.	X	X	Para la vigencia se comenzó con las actividades de análisis, para mejorar esta identificación y su respectivo tratamiento.	No se realizó esta actividad de socialización de los riesgos
6	Seguimiento a la fase de tratamiento	Segundo semestre del año.	X	X	El proceso identificó un riesgo de seguridad de la información de forma general que integra los componentes del MSPI, al cual le realizó seguimiento frente a los controles	Si bien se cuenta con un riesgo de Seguridad de la Información, este no es suficiente para asegurar la confidencialidad, disponibilidad e integridad de la información de acuerdo con el MSPI.
7	Evaluación de riesgos residuales	Segundo semestre del año	X	X	En Isolución se encuentra la evaluación con el consecutivo “GTEC 2019-21” en el módulo de “Riesgos DAFP V5”	Si bien se cuenta con un riesgo de Seguridad de la Información, este no es suficiente para asegurar la confidencialidad, disponibilidad e integridad de la información de acuerdo con el MSPI.
8	Monitoreo y revisión de la dirección SDA	Cuarto trimestre del año.	X	X	En el marco del Comité Institucional de Gestión y Desempeño, sesión # 7 del 15 de diciembre de 2022, en donde se presentaron los avances del SGSI	Si bien se realizó esta actividad, no se está cumpliendo con el MSPI al contar con un único riesgo que no permite identificar los posibles eventos, vulnerabilidades y amenazas sobre los activos de información

No.	Actividad	Tiempo de Ejecución	Plan que pertenece la actividad		Soporte	Observación
			Plan de Seg. Y Priv.	Plan de Tratamiento		
						situación que pone en riesgo la seguridad de la información de la SDA.
9	Mejoramiento	Segundo y cuarto trimestre del año.	X	X	Se midió con base en la herramienta de autodiagnóstico de MinTIC, así como la medición que se hace por medio del FURAG;	No se identificaron indicadores sobre incidentes de seguridad e implementación del modelo.

Tabla 2 Plan de Seguridad y Plan de Tratamiento vigencia 2022

De acuerdo con lo enunciado anteriormente, se concluye que de las nueve (9) actividades programadas, se ejecutó parcialmente una (1) actividad parcialmente del Plan de Seguridad y Plan de Tratamiento de la vigencia 2022

Plan de Seguridad y Privacidad de la información 2023 y Plan de Tratamiento de Riesgos 2023

Los Planes se encuentran publicados en la sección de Transparencia del Portal Web de la Entidad con los nombres: Plan de seguridad y privacidad de la información 2023.pdf y Plan de tratamiento de riesgos de Seguridad información 2023.pdf.

- **Plan de seguridad y privacidad de la información 2023**

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
1	Gestionar la aprobación de las políticas de seguridad de la Información.	Primer trimestre del año.	Documento: políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente, Versión 3 aprobado en el Comité Institucional de Gestión y Desempeño de fecha 04 de agosto de 2023 Radicado 2023IE174378 del 31 de julio de 2023.	Su aprobación se surtió el 4 de agosto del 2023, posterior al plazo establecido para su cumplimiento.

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
2	Adelantar la identificación y actualización de los riesgos de seguridad de la información	Anual	De acuerdo con lo manifestado por el equipo se tienen programados para el mes de noviembre del 2023 cumplir con esta actividad.	Sin observación.
3	Hacer seguimiento sobre la efectividad de los controles establecidos (mínimo de 3 meses) sobre los riesgos que de Seguridad de la Información	Cuarto trimestre del año.	El Proceso manifiesta que: "la efectividad se comenzará a medir, luego de iniciar con la identificación en la matriz de riesgos".	Dado que a la fecha de la auditoría (septiembre 30) no se había realizado la identificación de los riesgos y sus respectivos controles, existe un posible incumplimiento en realizar el seguimiento sobre la efectividad de los controles para esta vigencia.
4	Implementar lo establecido en la Estrategia de Sensibilización en temas de Seguridad de la Información de La Secretaría Distrital de AmbienteVigencia 2022-2023	Primer y segundo semestre del año.	Soportes de las sensibilizaciones: Invitación a contratistas y funcionarios 7/06/2023: Mesa de servicios y Lineamientos de Seguridad 28/06/2023: Sensibilización y Capacitación En Seguridad de la Información. 28/08/2023: Socialización de las Políticas de Seguridad de la Información El proceso manifiesta que: "*se adelantaron sensibilizaciones hacia todos los usuarios de la entidad, (…)* *Cumpliendo parcialmente con el objetivo de la actividad".*	Sobre el documento con nombre Estrategia de Sensibilización SGDI-SDA 2023 no se evidenciaron soportes de las siguientes actividades establecidas en el cronograma: 1. Campaña de sensibilización: **Periodicidad Quincenal.** 2. Inculcar en los colaboradores de la SDA la adopción de acciones preventivas para propender por la seguridad de la información y los equipos: **Periodicidad Trimestral.** 3.Determinar causas, posibles responsables y recomendaciones de mejora para los sistemas a través de la gestión de incidentes de seguridad.: **Periodicidad: Semestral** Por lo expuesto, se observó que esta actividad presenta cumplimiento parcial conforme a lo establecido en el cronograma del documento de la Estrategia de Sensibilización de Seguridad.

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
5	Realizar la gestión necesaria para contar con los ejercicios de Pen testing y análisis de vulnerabilidades necesarios	Anual	Se evidencia el acta de inicio del 11 de septiembre del 2023 del contrato de prestación de servicios No. SDA-20231689 cuyo objeto es: "realizar la renovación del servicio del centro de operaciones de seguridad (SOC), el cual incluye monitoreo, detección, protección y contención de amenazas en la Secretaría Distrital de Ambiente – SDA" Se aportan informes de monitoreo de la Plataforma.	Actividad cumplida de acuerdo con los informes de monitoreo presentados sobre el Servicio del Centro de Operaciones de Seguridad -SOC.
6	Hacer seguimiento sobre el monitoreo efectuado por el SOC	Primer y Segundo semestre del año.	Se evidenciaron los informes de monitoreo de la Plataforma	Sin observación.
7	Hacer seguimiento sobre las alertas generadas por el monitoreo de la infraestructura tecnológica de la Secretaría, relacionadas con la confidencialidad, integridad y disponibilidad de la información	Primer y Segundo semestre del año.	El proceso manifiesta: "*Al día de hoy no se han generado alertas que impacten a la entidad y se tenga que gestionar y generar informes de la situación para hacer seguimiento*"	Sin observación.
8	Atender hallazgos, incidentes y solicitudes, relacionadas con seguridad de la Información.	Anual	Se evidenciaron casos sin gestionar de manera oportuna clasificados en el proyecto de Seguridad de la Información en la herramienta de Aranda registrados con número de ticket: 10597, 10892, 193785, 194138.	Se evidencia casos registrados en la herramienta de Gestión como incidentes y requerimientos, los cuales dentro de la herramienta de Aranda no se encontraban registrado su gestión, por lo tanto, permanecían abiertos.
9	Aplicar y alimentar los indicadores de seguridad de la Información	Segundo semestre del año.	El proceso manifiesta: "*en la vigencia 2023 se establecen los nuevos indicadores del SGSI, los cuales se encuentran en el manual del sistema, actualmente ya fueron aprobados y de acuerdo con la periodicidad*	No se cuenta con la medición a la fecha de la auditoría de los Indicadores del SGSI en la vigencia 2022 y 2023 a la fecha.

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
			establecida, se comienza con alimentación de estos indicadores"	
10	Revisar y actualizar la documentación del SGSI, para garantizar su oportunidad de aplicación.	Primer semestre del año.	Se evidenció: Documento de la Política de Riesgos de la Entidad. Manual de Seguridad de la Información Política de Seguridad de la Información. Actualización de la Declaración de Aplicabilidad Evaluación del MSPI 2023	Avance
11	Cumplir con las actividades del plan de mejoramiento generado de la auditoría de Control Interno	Primer y segundo semestre del año.	En el seguimiento realizado por la oficina de control interno en el primer semestre del 2023, se cerraron acciones dando cumplimiento a lo establecido.	Se realizará el seguimiento al cierre de la vigencia.

Tabla 3 Plan de seguridad y privacidad de la información 2023

- **Plan de Tratamiento de Riesgos de Seguridad de la Información 2023**

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
1	Revisión y Actualización de las políticas y lineamientos de gestión de riesgos de seguridad de la información.	Primer trimestre.	Documento: Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente, Versión 3 aprobado Comité Institucional de Gestión y Desempeño Fecha: 04 de agosto de 2023 Radicado 2023IE174378 del 31 de julio de 2023	Actividad cumplida, posterior a la fecha programada.
2	Actualización e Identificación y priorización de los activos de información	Primer trimestre.	De acuerdo con lo manifestado por el proceso: "*logrando, a la fecha, contar con la identificación de los activos de información para los 18 procesos que tiene la entidad, cumpliendo al 100% con esta actividad."* En el marco de la ejecución de la auditoria estos se encontraban en construcción	No se cumplió de acuerdo con la fecha establecida en el Plan, situación que afecta la implementación de la metodología de gestión de Riesgos.

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
			y no pudieron ser verificados por la auditoria.	
3	Verificar el contexto de los diferentes procesos.	Segundo Trimestre	De acuerdo con lo manifestado por el proceso: "*ya se cumplió con esta actividad, dado que ya se tienen los activos de Información para los 18 procesos de la Entidad."* En el marco de la ejecución de la auditoria estos se encontraban en construcción y no pudieron ser verificados por la auditoria.	No se cumplió de acuerdo con la fecha establecida en el Plan, situación que afecta la implementación de la metodología de gestión de Riesgos.
4	Identificar los riesgos	Primer Semestre	De acuerdo con lo manifestado por el proceso: "*Identificar los riesgos: actualmente se encuentra la identificación de los riesgos de seguridad de la información actualizados y asociados con los activos de información de la entidad. Sin embargo, es preciso mencionar que, la entidad para el primer trimestre contaba con un riesgo general de seguridad de la información*"	No se cumplió de acuerdo con la fecha establecida en el Plan, situación que afecta la implementación de la metodología de gestión de Riesgos.
5	Analizar los riesgos, identificar y valorar controles	Segundo Semestre	De acuerdo con lo manifestado por el proceso: "*Analizar los riesgos, identificar y valorar controles: con el término del establecimiento de los activos de información al 100 %, se comenzó con la identificación de riesgos de seguridad de la Información, cumpliendo esta actividad en noviembre próximo."*	Programada para el mes de noviembre según respuesta del proceso.
6	Establecer las actividades de Tratamiento de los riesgos.	Segundo Semestre	Sin soporte a la fecha de la auditoría	Esto solo se puede realizar una vez se tengan los riesgos y su valoración, a la fecha de la auditoria no se había dado inicio.

No.	Actividad	Tiempo de Ejecución	Soporte	Observación
7	Iniciar los monitoreos	Primer y segundo semestre.	Sin soporte a la fecha de la auditoria	No se ha realizo la Comunicación a los procesos sobre el monitoreo de riesgos.

Tabla 4 Plan de Tratamiento de Riesgos de Seguridad de la Información 2023

De acuerdo con lo anterior, se evidencia debilidad en el cumplimiento de las actividades formuladas en los Planes de Seguridad y Tratamiento de Riesgos lo que pone en riesgo la integridad, confidencialidad y disponibilidad de la información, esto puede llevar a brechas de seguridad, pérdida de datos, acceso no autorizado a información sensible y daños reputacionales. Además, la falta de cumplimiento con los planes de tratamiento puede resultar en la falta de control y mitigación de los riesgos lo que aumenta la posibilidad de incidentes de seguridad.

Criterio

- ISO 27001:2013 Numeral 8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2.

La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado

- Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones

  ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título **deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio**. en la cual, **deberán hacer periódicamente una evaluación del riesgo de seguridad digital**. que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas. políticas. procedimientos. recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Modelo Integrado de Planeación y Gestión - MIPG
  Dimensión de Evaluación de Resultados
  Seguimiento y evaluación efectuados por los servidores que tienen a su cargo cada proyecto, plan, programa o estrategia, en sus diferentes etapas de desarrollo

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Debilidades frente al seguimiento y monitoreo de las actividades y planes programados a cargo del proceso. Debilidades en la planificación de los instrumentos de gestión del proceso alineados a la operación del proceso y por ende insuficientes recursos financieros y tecnológicos que permitan el cumplimiento efectivo de las acciones propuestas. Ausencia de esquema de líneas de defensa al interior del proceso que permita definir controles preventivos y la generación de alertas tempranas frente al nivel de cumplimiento de las actividades programadas a cargo del proceso.	Posibilidad de afectación reputacional por la falta de oportunidad en la implementación y seguimiento a los instrumentos de gestión definidos por el proceso, afectando la gestión institucional y por consiguiente el análisis de resultados.	Toma de decisiones que no se ajusten a las necesidades institucionales por el inadecuado seguimiento y oportuno análisis de resultados de las actividades y planes programados para la vigencia.

Tabla 5 Causas, Riesgos e Impactos del hallazgo 1

Recomendación(es):

Con el fin de dar cumplimiento a las actividades de los Planes de Seguridad de la Información se recomienda fortalecer el esquema de autocontrol del proceso, en donde se establezcan etapas de verificación y seguimiento al cumplimiento de las metas, se realice asignación efectiva de responsables para su ejecución y validación de resultados, de tal manera, que se generen alertas frente a las posibles desviaciones o retrasos que puedan presentarse para el cumplimiento de los planes y objetivos del proceso.

Respuesta del Auditado:

De acuerdo con el análisis anterior, se solicita comedidamente, se tengan en cuenta las diferentes actividades, esfuerzos y situaciones presentadas con cada plan, con el fin de establecer un escenario que permita evidenciar los avances que se han tenido con cada plan, y así, generar oportunidades de mejora acordes con el trabajo realizado.

Conclusión de la Oficina de Control Interno

Se resalta la gestión realizada por el proceso frente al avance de las diferentes actividades, se realiza ajuste al hallazgo conforme a lo manifestado por el proceso, sin embargo, se mantiene la identificación de aspectos con bajo nivel de avance en algunos componentes de la planificación del MSPI, por lo tanto, se debe de planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y objetivos de seguridad de la información, por lo anterior se ratifica este hallazgo.

Hallazgo No. 2 Ausencia de los riesgos de Seguridad de la Información en los Procesos de Contratación de la SDA.

Al realizar la evaluación del cumplimiento de la Política 6.9. Relaciones con los proveedores establecida en el Documento de Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3, la cual establece:

Desde la construcción de los estudios previos, el jefe de la dependencia interesado en la contratación debe identificar los riesgos de seguridad de la información los cuáles serán parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con ello, el análisis de riesgos de esta naturaleza debe incluir su identificación, clasificación, probabilidad de ocurrencia estimada, impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

En el marco de las pruebas de auditoria efectuadas, se seleccionó de manera aleatoria el contrato de prestación de servicios No. 20231689 cuyo objeto consistía en *"Realizar la renovación del servicio del centro de operaciones de seguridad (SOC), el cual incluye monitoreo, detección, protección y contención de amenazas en la Secretaría Distrital de ambiente – SDA".*

Una vez revisado su contenido, se observó que no cuenta con matriz de riesgos de seguridad de la información, en el que se determinen las medidas que debe tomar la entidad, en caso de presentarse situaciones como acceso no autorizado a la información, Violación de la privacidad de los datos, Interrupción del servicio, entre otras. Es fundamental identificar y abordar los riesgos de seguridad de la información en un contrato tecnológico para garantizar la protección de los datos, la continuidad del negocio y el cumplimiento de las regulaciones.

Lo anterior, denota debilidades en el cumplimiento de lo establecido en la Política .9. Relaciones con los proveedores establecida en el Documento de Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3.

Criterio

- Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3
  Numeral 6.9. Relaciones con los proveedores
  (…) Desde la construcción de los estudios previos, el jefe de la dependencia interesado en la contratación debe identificar los riesgos de seguridad de la información los cuáles serán parte de la estimación y cobertura de los riesgos del proceso de contratación (…)

- ISO 27001:2013 Anexo A - A.15 RELACIONES CON LOS PROVEEDORES
  Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Ausencia de requisitos de seguridad de la información establecidos de manera clara y específica en los documentos de contratación. Falta de orientación y directrices sobre inclusión de requisitos en los procesos de contratación.	Perdida de confidencialidad por exposición o acceso indebido de personas no autorizadas.	Posibles sanciones por incumplimiento de las regulaciones y normativas relacionadas con la protección de datos. Posibles sanciones legales y procesos disciplinarios por afectación en el uso de información sensible.

Tabla 6 Causas, Riesgos e Impactos del hallazgo 2

Recomendación(es):

Realizar una evaluación e identificación de posibles riesgos de seguridad de la información en los procesos de contratación. Así mismo, identificar posibles amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información durante las diferentes etapas de la gestión contractual de acuerdo con las Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente Código: PA03-PO01 definidas.

En términos de sensibilización y capacitación, se recomienda brindar capacitación regular y/o continua a los servidores involucrados en los procesos de contratación de la entidad, sobre las mejores prácticas de seguridad de la información, así como la identificación de posibles amenazas de seguridad durante el proceso de contratación que permita la definición de controles y la definición de los diferentes.

Respuesta del Auditado:

- *Por otro lado, en lo referente al contrato sobre el SOC (centro de operaciones de seguridad), no se entiende, la citación en el hallazgo, dado que es una fortaleza el contar con este tipo de contratos, ya que como lo menciona el hallazgo, "…que permite a la SDA, la detección amenazas y la protección de la seguridad de la información y de la infraestructura que pueden impactar la gestión institucional; cuente con una matriz de riesgos de seguridad de la información…"; pero no se concluye la idea, se solicita respetuosamente revisar el párrafo*.

- *Por otro lado, en los procesos de gestión contractual, la SDA cuenta con el formato de estudios previos Código: PA08-PR03-F1 versión 9, en donde en el numeral 6. SOPORTEQUE PERMITA LA TIPIFICACION, ESTIMACION Y ASIGNACION DE LOS RIESGOS PREVISIBLES QUE PUEDAN AFECTAR EL EQUILIBRIO ECONÓMICO DEL CONTRATO, se tiene establecido un cuadro que define la tipificación y estimación del riesgo para el proceso contractual teniendo en cuenta varios aspectos y una propuesta de clasificación de riesgos e indica que las actividades se realizarán de acuerdo con la metodología establecida por Colombia Compra Eficiente. En esta matriz se tiene en cuenta los riesgos de tipo tecnológico, como aquellos que "se refiere a eventuales fallos en las telecomunicaciones, suspensión de servicios públicos, advenimiento de nuevos desarrollos*

tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato, así como la obsolescencia tecnológica"

- *Finalmente, se desea aclarar que se actualizó la política de seguridad de la información, teniendo en cuenta la metodología a aplicar, con el fin de no generar confusiones en su interpretación y que esté alineada con lo aplicado en la SDA y en la metodología empleada por Colombia Compra Eficiente en los riesgos de los procesos contractuales.*

- *En consecuencia, respetuosamente, solicitamos se analice la conclusión de este hallazgo y analizar la pertinencia de establecer esta observación como un hallazgo, dado que no se han materializado situaciones que coloquen en riesgo la seguridad de la información; además que, ya se aplicaron acciones de mejora asociadas con la situación indicada. Siendo así más una recomendación para adelantar acciones preventivas.*

Conclusión de la Oficina de Control Interno

Con respecto a la primera respuesta, se retira el párrafo para no generar confusión respecto a la debilidad identificada en este.

Por otro lado, frente a la respuesta del proceso al informe preliminar de la auditoria (…) *En esta matriz se tiene en cuenta los riesgos de tipo tecnológico, (…)* se aclara que este riesgo identificado no corresponde a un riesgo de Seguridad de la Información no está relacionado con los activos de información, no identifica vulnerabilidades y amenazas a la disponibilidad, confidencialidad e integridad, de igual forma se debe identificar aspectos que puedan afectar la seguridad de la información de la SDA en desarrollo del objeto contractual de acuerdo con su naturaleza y definir sus respectivos controles que deba implementar el proveedor y la entidad para mitigar la masterización de los riesgos, conforme a sido definido en la política de seguridad de la información aprobada por la entidad en concordación con la ISO 27001.

Se ratifica el hallazgo, con el objetivo de que se fortalezcan los controles para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información -SGSI- de la SDA de manera oportuna y eficaz, específicamente con la Gestión de Proveedores, relacionado con los contratistas, personas naturales y jurídicas que por su actividad tengan acceso a los sistemas de información de la entidad.

Hallazgo No. 3 Debilidad en la Planificación, Implementación y Verificación de la Gestión de Continuidad de Negocio.

Frente a las evidencias aportadas sobre la Planificación, implementación, verificación y evaluación de la Continuidad de la Seguridad de la Información se observó lo siguiente:

- **Conformación del Comité de Crisis:**

En "la página 14 del documento SDA-20202469 ESTRATEGIAS BCP SDA.pdf se indica "que el *Comité de Crisis está conformado por los siguientes cargos y tendrán voz y voto: SG -*

Subsecretario General, DPSIA – Directora de Planeación y Sistemas de Información Ambiental, DPSIA – Asesor Técnico de TI, OAC – Líder de Comunicaciones y DGC – Líder de Gestión Humana".

Realizada la verificación por parte de la auditoria se encontró que las personas que tienen estos cargos nunca se les ha realizado una socialización y explicación de las funciones que ellos ejercen al hacer parte del Comité de Crisis, situación que genera un posible riesgo al generar confusión y dificulta en la toma de decisiones ante una crisis.

Es fundamental que todos los miembros del comité estén debidamente informados, capacitados y alineados en cuanto a los protocolos, procedimientos y roles que deben desempeñar durante una crisis.

- **Liderazgo del PCN o BCP (Plan de Continuidad del Negocio):**

El procedimiento Gestión de Incidentes de TI Código: PA03-PR14 tiene por objeto: "*Gestionar los incidentes que afecten la operación de los servicios de tecnologías de la información-servicios TI y la seguridad de los activos de información de la Secretaría Distrital de Ambiente - SDA*", sin embargo, en este no define claramente los roles y responsabilidades del BCP para garantizar una respuesta adecuada y eficiente en caso de interrupciones en las operaciones, algunos de los roles comunes en un BCP que deben de estar identificados son:

- Líder del PCN: Responsable de supervisar y coordinar la implementación del plan.
- Equipo de comunicaciones: Responsable de gestionar la comunicación interna y externa durante una crisis.
- Equipo de recuperación de TI: Encargado de restaurar los sistemas y la infraestructura tecnológica.
- Equipo de recursos humanos: Responsable de gestionar el personal y las necesidades de recursos humanos durante una crisis.
- Equipo de planificación y desarrollo del BCP: Este equipo se encarga de desarrollar y mantener el BCP o PCN. Ellos identifican las funciones críticas del negocio, establecen los procedimientos de respuesta y recuperación, y coordinan las actividades necesarias para implementar el plan.

Realizada la verificación por parte de la auditoria se encuentra que es necesario que la SDA, determine e identifique los roles y responsabilidades, que permitan, planificar, implementar y verificar la gestión, así como la toma de decisiones en caso de una situación de emergencia o desastre, que impacte el cumplimiento de los objetivos.

- **Árbol de Comunicación**[1]

En el numeral 3.4 del documento "ESTRATEGIAS BCP SDA" no se encuentra establecido el árbol de comunicación del BCP, dado que esta es una herramienta que se utiliza para establecer

[1] Mecanismo que implementa la cadena de llamadas y las responsabilidades de cada funcionario, incluye contactos de colaboradores, proveedores, firmas de outsourcing (si aplica), organismos de control y demás interesados en el Plan de Continuidad del Negocio.

y mantener una comunicación efectiva durante una situación de emergencia o contingencia que afecte a la SDA. El objetivo principal del árbol de comunicación es garantizar que la información crítica se transmita de manera rápida y precisa a las personas adecuadas de la entidad.

Al no contar con lo anteriormente mencionado se puede aumentar el riesgo de falta de coordinación, retraso en la comunicación, información incorrecta o incompleta, y falta de involucramiento de las partes interesadas durante una situación de emergencia o contingencia.

Es importante establecer y mantener un árbol de comunicación claro y efectivo para garantizar una respuesta adecuada y minimizar los impactos negativos en la SDA.

- **Aprobación de la Alta Gerencia la Estrategia de Migración.**

En el documento: SDA-20202469 ESTRATEGIAS BCP FINAL.pdf del 13 de agosto de 2021en el número 3.3. Escenarios y estrategias, se estable:

"*Se debe presentar a la alta gerencia para su aprobación una estrategia de migración parcial y/o total a un centro alterno de procesamiento de datos o a un proveedor de servicio de computación en la nube bajo las condiciones y niveles de servicios definidos en el BIA*".

Al respecto, no se aportaron evidencias, que permitieran confirmar que la estrategia fuese presentada ante la Alta Gerencia para su aprobación.

- **Análisis de Impacto al Negocio (BIA - Bussiness Impact Analisys)**

En el documento con el nombre: SDA-20202469 BIA SDA, en el numeral 8.8. se establece: "*Estimación inicial de los recursos para la implementación"*.

Al respecto no se observó, en ninguno de los documentos aportados, soporte que diera cuenta de la evaluación y estimación de los recursos necesarios para implementar las medidas de continuidad del negocio identificadas durante el análisis de impacto.

Lo enunciado, respecto a la no estimación de recursos para la implementación del BCP, podría comprometer la capacidad de respuesta y la efectividad de las medidas de reducción del riesgo y el manejo de desastres del proceso para asegurar la efectiva implementación del BCP.

- **Plan de Pruebas**

El documento del BCP, se contemplan las siguientes estrategias de recuperación:

Estrategias de Prevención: Diseñar, actualizar, mantener y probar procedimientos de instalación y desinstalación de sistemas de información crítica que involucren el cambio de servidor o máquina virtual e inclusive de sede.

Estrategias de Mitigación:

- Definir y mantener centros alternos de operación dentro del mismo edificio principal para el personal crítico y/o formalizar el Teletrabajo o Trabajo en casa como una alternativa probada en caso de imposibilidad de uso de los puestos de trabajo del edifico de chapinero.
- Implementar, mantener, actualizar y probar estrategias de tolerancia a fallos, balanceo de carga y alta disponibilidad para los sistemas de información críticos como (...)
- Mantener y actualizar proceso de instalación y desinstalación de cero de los sistemas de información listados en el punto anterior, así como un procesos unificado y ordenado de bajar y subir todos los sistemas de información de uno o varios servidores.

De acuerdo con lo anterior, el documento: Plan de Recuperación de Desastres (DRP) de agosto de 2021, establece frente a las pruebas lo siguiente:

> "El objetivo del plan de pruebas es garantizar que las estrategias de recuperación tecnológica ante desastres son válidas, realizables y se ejecuten de manera correcta y alineadas a las necesidades del negocio. Se hacen con el fin de verificar las funciones y procesos de los distintos recursos tecnológicos, así como también encontrar los posibles fallos o errores que se presenten durante el periodo de pruebas".
>
> *"Los diferentes tipos de prueba que se realizaran* ***se definirán de acuerdo con los escenarios definidos en el documento BCP*** *y en base a estos se elaborara* ***el documento Bitácora de Pruebas*** *de Operación en Contingencia.*
>
> ***Las pruebas del Plan de Continuidad de la SDA son definidas y aprobadas por el Comité de Contingencia y se deben realizar por lo menos una vez al año****, previo acuerdo con el responsable del BCP de la SDA, con los usuarios responsables de los procesos y los proveedores involucrados*
>
> ***Para cada prueba se requiere la elaboración del Set de Pruebas en donde se listan las actividades que se realizan en el transcurso de la prueba y al finalizar la prueba debe generar un acta de verificación de la ejecución de la prueba donde se describirán los inconvenientes presentados y se propondrán oportunidades de mejora por parte de los participantes en la prueba****".*
>
> De acuerdo con lo anterior frente al plan de pruebas el proceso aporto el documento con nombre: con nombre: 3.1 20220301 Registro DRP SIPSE, este documento no contine los criterios mínimos definidos por la SDA en el BCP (Plan de Continuidad del Negocio) y con la elaboración del Set de Pruebas en donde se deben listar las actividades que se realizan en el transcurso de la prueba y al finalizar la prueba debe generar un acta de verificación de la ejecución de la prueba donde se describirán los inconvenientes presentados y se propongan oportunidades de mejora por parte de los participantes en la prueba.

- **Identificación y Evaluación de Riesgos**

La Identificación de los Riesgos del BCP (Plan de Continuidad del Negocio) consiste en identificar y comprender los posibles eventos o situaciones que podrían afectar la continuidad de las operaciones de la SDA, esto implica analizar tanto los riesgos internos (como fallas en los sistemas, errores humanos etc.) como riesgos externos (ataques cibernéticos, etc.), a la

fecha, se observó que estos no han sido identificados por la SDA por lo tanto no han sido evaluados.

Esta situación, afecta la gestión de la entidad frente a la definición de las medidas necesarias para prevenir, mitigar o responder adecuadamente a los eventos adversos tales como: Interrupción de operaciones, pérdida de datos, ttiempo de inactividad prolongado, Incumplimiento de regulaciones y normativas.

Criterio

- ISO 27001:2013 Anexo A - A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO
  A.17.1.1 Planificación de la continuidad de la seguridad de la información
  A.17.1.2 Implementación de la continuidad de la seguridad de la información
  A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

- Documento SDA-20202469 ESTRATEGIAS BCP FINAL de agosto del 2021
  Numeral 3 Estrategias de recuperación

- Documento SDA-20202469 BIA SDA de junio del 2021
  Numeral 8.8. Estimación inicial de los recursos para la implementación

- Documento SDA-20202469 DRP SDA FINAL de agosto 2021
  Numeral 6 Plan de Pruebas

- Documento de Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3
  Numeral 6.11. Gestión de continuidad de negocio

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Omisión de las amenazas y no implementación de medidas de mitigación adecuadas. Falta de conocimiento sobre las vulnerabilidades que pueden surgir durante una interrupción del negocio.	Posibilidad de afectación reputacional por interrupción en la operación de la entidad debido a la inadecuada definición estrategias y medidas de continuidad en caso de situaciones de emergencia.	Posibles sanciones legales y procesos disciplinarios por afectación prestación del servicio y no satisfacer las necesidades de los diferentes grupos de interés de la SDA.

Tabla 7 Causas, Riesgos e Impactos del hallazgo 3

Recomendación(es):

Frente a las pruebas del BCP, se recomienda:

- **Definir los objetivos y alcance de las pruebas**: Antes de comenzar a diseñar el plan de pruebas, es fundamental tener claridad sobre los objetivos que se desean alcanzar y el alcance de las pruebas. Esto ayudará a enfocar los esfuerzos y recursos de manera efectiva.
- **Planificar y organizar las pruebas**: Es importante establecer un cronograma para las pruebas y asignar los recursos necesarios. Además, se debe definir la estrategia de pruebas, incluyendo los tipos de pruebas a realizar (funcionales, de rendimiento, de seguridad, etc.) y las técnicas y herramientas a utilizar.
- **Diseñar casos de prueba efectivos**: Los casos de prueba deben ser diseñados de manera efectiva, cubriendo todos los escenarios posibles y asegurando una cobertura adecuada. Se deben considerar diferentes combinaciones de datos de entrada, condiciones límite y casos de prueba negativos
- **Ejecutar las pruebas y registrar los resultados**: Una vez diseñados los casos de prueba, se deben ejecutar de manera sistemática y registrar los resultados obtenidos. Es importante documentar cualquier defecto encontrado durante las pruebas y realizar un seguimiento de su resolución.
- **Realizar pruebas de regresión**: Después de realizar modificaciones o mejoras en el sistema o software, es recomendable realizar pruebas de regresión para asegurarse de que los cambios no hayan introducido nuevos errores o afectado el funcionamiento existente.
- **Evaluar y mejorar el proceso de pruebas**: Al finalizar las pruebas, es importante realizar una evaluación del proceso de pruebas para identificar áreas de mejora. Se pueden realizar reuniones de retroalimentación con el equipo de pruebas y recopilar comentarios para futuros planes de pruebas.

Se recomienda realizar periódicamente a los integrantes, capacitaciones sobre sus responsabilidades, mostrar las estrategias, presentar los planes de la vigencia, involucrarlos en las pruebas para la continuidad.

Así mismo, se recomienda identificar y priorizar los riesgos del BCP y detectar activos críticos, de igual manera, evaluar el impacto que tendría la interrupción de cada uno de los activos críticos identificados, con el fin de establecer las medidas a tomar frente a las posibles afectaciones a nivel financiero, operativo, reputacional y legal que podría afectar gestión institucional.

Respuesta del Auditado:

- *En relación con los roles deferidos en el BCP, se aclara que el equipo de trabajo de infraestructura está conformado por dos personas, uno es el titular y el otro es el suplente de las actividades a realizar. En concordancia con lo anterior, el trabajo articulado entre estos roles permite dar una respuesta oportuna, ya que el canal de comunicaciones se establece desde el equipo de infraestructura tecnológica, la directora de la DPSIA y la alta dirección de la entidad.*

- *Para ejecutar una estrategia de migración, primero se debe priorizar una necesidad de recursos de hardware o software. Con la implementación de hiperconvergencia, se operativizan muchas necesidades de migración, es decir que ejecutamos las estrategias*

desde el recurso humano con el que se cuenta y también con equipos de vanguardia tecnológica.

- *El plan de pruebas para el DRP se ejecuta con las ventanas de mantenimiento y cambios en los sistemas de información, las pruebas no son recurrentes puesto que los administradores de las plataformas tienen control de los recursos y entregan los servicios por demanda.*

Conclusión de la Oficina de Control Interno

- Respeto a lo manifestado frente a los roles del BCP, se observó que estos no se encuentran formalmente establecidos, por lo tanto, no se definen de manera clara las responsabilidades que garanticen una respuesta adecuada y eficiente en caso de interrupciones en las operaciones., dado que, en primer lugar, al documentar las responsabilidades del BCP por escrito, se crea un registro claro y accesible de las tareas y funciones asignadas a cada persona o área dentro de la SDA.

  Lo anterior como lo establece la ISO 22301 en su numeral 8.4.2.4 para cada equipo debe haber: a) personal identificado y sus suplentes con las responsabilidades, autoridad y competencias necesarias para desempeñar la función designada; b) procedimientos documentados para guiar sus acciones (…) incluyendo aquellos para la activación, operación, coordinación y comunicación de la respuesta.

- Frente a la Estratégica de Migración esta fue expuesta en el documento del BCP de agosto del 2021, si bien, se consideró que con la implementación de hiperconvergencia se optimizaban muchas necesidades de migración, es pertinente tener en cuenta que esta se refiere a una arquitectura de infraestructura que combina todos los elementos de un centro de datos en una sola plataforma, mientras que un centro alterno de procesamiento de datos es un lugar de respaldo utilizado en caso de una interrupción en el centro de datos principal, con lo cual se concluye que la Hiperconvergenciapor sí sola no tiene el alcance definido en el BCP (Plan de Continuidad del Negocio) establecido por la SDA en el documento: SDA-20202469 ESTRATEGIAS BCP FINAL.pdf del 13 de agosto de 2021 en el numeral 3.3. Escenarios y estrategias:

  > "estrategia *de migración parcial y/o total a un centro alterno de procesamiento de datos o a un proveedor de servicio de computación en la nube bajo las condiciones y niveles de servicios definidos en el BIA"*

- Con respeto a las pruebas realizadas en las ventanas de mantenimiento y cambios en los sistemas de información para la vigencia 2022 y lo corrido de la vigencia 2023,estas no cumplen con lo establecido en el documento Plan de Recuperación de Desastres (DRP) de agosto de 2021: "*Los diferentes tipos de prueba que se realizaran se* ***definirán de acuerdo con los escenarios definidos en el documento BCP*** *y en base a estos se elaborara el documento* ***Bitácora de Pruebas de Operación en Contingencia****"*; las cuales son estrategias de Migración y Prevención.

Dado lo expuesto, se ratifica el hallazgo, con el objetivo que el BCP (Plan de Continuidad del Negocio) de la SDA sea una estrategia priorizada para garantizar la seguridad de la información de los procesos críticos de la Entidad, en caso de presentarse una contingencia, se garantice la continuidad de la operación, minimizar las pérdidas financieras, proteger la reputación y cumplir con los requisitos legales y regulatorios.

Hallazgo No. 4 Debilidad en la aplicación Política de Mantenimiento Físico de las Operaciones

Durante la prueba de recorrido se evidencio las siguientes situaciones a las cuales fueron aportados los siguientes contratos;

- Cuarto de las UPS no funciona el aire acondicionado, por lo tanto, las puertas mantienen abiertas y con la improvisación de ventiladores de aire (ver registro fotográfico), lo anterior generando un riesgo de sobrecalentamiento de los equipos, la reducción de la vida útil de los mismos y posibles interrupciones en el suministro de energía. Es fundamental mantener una adecuada refrigeración en estos espacios para garantizar el rendimiento y la protección de los equipos críticos.

- Contrato de extinción de incendios en desarrollo de la auditoria se solicitó al proceso el mecanismo implementado para garantizar el sistema de detección y extinción de incendios en el Centro de Computo, el proceso aporto el CONTRATO DE PRESTACION DE SERVICIOS No. SDA-20211457 cuya vigencia establecía que este no podrá exceder el 31 de diciembre de 2021, a la fecha la SDA no cuenta con contrato vigente de extinción de incendios, lo anterior generando el riesgo de que un incendio se salga de control y cause daños y pérdidas importantes para la SDA.
  Se reitero la solicitud mediante correo electrónico del 13 de octubre del 2023, conforme a lo manifestado en la sección de socialización de los resultados de la auditoria, sin embargo, no fue aportado.

- Contrato de UPS: en el formato General Servicio con nombre: FormatoGeneralServicio744847119.pdf del ***6/6/2023 informa***: El equipo queda en operación normal sin embargo **sin alarmas activas**, ***no es confiables ya que tienen las baterías la mayoría están dañadas*** son 40 unidades Emerson HF 12 650W; al no contar con la UPS funcionales con energía de respaldo en caso de interrupciones en el suministro eléctrico puede resultar en la pérdida de datos, tiempo de inactivación del sistema y posibles impactos negativos en la operación.



Tabla 8 Fotografías del cuarto de UPS de la SDA

Criterio

- Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3

Numeral 6.8.1 Mantenimiento físico de las operaciones, establece:

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Centro de Cómputo, como son el sistema de aire acondicionado y el **sistema de detección y extinción de incendios**, entre otros.

Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS, plantas eléctricas, y sistema de aire acondicionado, de acuerdo con el plan de mantenimiento de la infraestructura de la SDA que se establezca.

Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la Secretaría Distrital de Ambiente.

Los niveles de temperatura y humedad relativa en el centro de datos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

Numeral 6.3.2 Directrices de seguridad para el control de acceso físico

Las puertas de acceso al centro de cómputo, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, **deberán permanecer siempre cerradas y aseguradas**. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Insuficientes medidas de monitoreo del estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Centro de Cómputo, entre otros.	Posibilidad de afectación reputacional por interrupción en la operación de la entidad debido a la inadecuada definición estrategias y medidas de continuidad en caso de situaciones de emergencia.	Posibles sanciones legales y procesos disciplinarios por afectación prestación del servicio y no satisfacer las necesidades de los diferentes grupos de interés de la SDA.

Tabla 3: Causas, Riesgos e Impactos del hallazgo 5

Recomendación(es):

Establecer mecanismos de seguimiento y monitoreo, frente a la gestión contractual para la operación tecnológica, así como realizar revisiones periódicas para asegurar el cumpliendo de los términos y requisitos establecidos para el mantenimiento Físico de las Operaciones.

Respuesta del Auditado:

En el plan anual de adquisiciones vigencia 2023 de la SDA, la Dirección de Gestión Corporativa tiene contemplado adelantar el proceso de REALIZAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE AIRES ACONDICIONADOS EN LA SEDE PRINCIPAL DE LA SECRETARÍA DISTRITAL DE AMBIENTE con recursos de funcionamiento con el fin de cambiar los equipos que refrigeran el cuarto de UPS. Adicionalmente, se está adelantando el proceso de contratación REALIZAR EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS DE AIRE ACONDICIONADO Y CUARTOS FRÍOS DE LAS SEDES DE LA SECRETARÍA DISTRITAL DE AMBIENTE con el fin de brindar soporte a todos los equipos de aire acondicionado de la sede principal. Este proceso de contratación se encuentra en revisión por parte de la subdirección contractual para su posterior publicación en el Sistema Electrónico para la Contratación Pública (SECOP II).

Adicionalmente, en el plan anual de adquisiciones vigencia 2023 de la SDA la Dirección de Gestión Corporativa tiene contemplado adelantar el proceso de contratación del Servicio de mantenimiento de las bombas eléctricas, sistema hidráulico y los tanques de almacenamiento pertenecientes a la Secretaria Distrital de Ambiente, en donde viene implícito el mantenimiento del sistema de red contra incendios. Este proceso de contratación se encuentra en revisión por parte de la subdirección contractual para su posterior publicación en el Sistema Electrónico para la Contratación Pública (SECOP II). Es importante mencionar que el sistema de la red contraincendios se encuentra operativo, que la entidad ha dispuesto de un extintor de fuego CO2 especial para extinguir fuego en equipos electrónicos y que el personal de soporte lleva a cabo inspecciones periódicas para verificar el correcto funcionamiento de los equipos instalados en el datacenter.
Así mismo, en el plan anual de adquisiciones vigencia 2023 de la SDA, la Dirección de Gestión Corporativa tiene contemplado adelantar el proceso que tiene por objeto PRESTAR EL SERVICIO DE SOPORTE TÉCNICO PREVENTIVO Y CORRECTIVO CON BOLSA DE REPUESTOS Y REEMPLAZO DE BATERÍAS PARA LAS UPS DE LA SDA. Este proceso de contratación se encuentra publicado en el Sistema Electrónico para la Contratación Pública (SECOP II) y en los próximos días se estará adjudicando al contratista que nos brindará el mantenimiento correctivo de las UPS incluyendo el cambio de las baterías. Es importante mencionar que, si bien la UPS del informe presenta daños en unas de sus baterías, la entidad cuenta con dos UPS en operación de las cuales una de ellas cuenta con sus baterías en normal funcionamiento y con ello se brinda soporte a los servidores, almacenamiento y equipos activos que se encuentran en el Datacenter de la SDA en caso de falla del fluido eléctrico.

Conclusión de la Oficina de Control Interno

De acuerdo con lo mencionado por el proceso, esto no desvirtúa el riesgo en el que se encuentra la Entidad, la falta de contratos vigentes de los aires acondicionados, UPS y extinción de incendios en la entidad representa un riesgo significativo. Estos contratos son fundamentales para cumplir con la Política de Seguridad Mantenimiento físico de las operaciones y las Directrices de seguridad para el control de acceso físico. Por lo tanto, es necesario que la entidad tome medidas inmediatas para asegurar que estos contratos estén actualizados y vigentes. Esto garantizará el correcto funcionamiento de las operaciones tecnológicas de la SDA y reducirá el riesgo asociado a la falta de seguridad física. Frente a lo expuesto, se reafirma el hallazgo.

Hallazgo No. 5 Debilidad en el establecimiento de las Políticas de Seguridad de la Información de la SDA.

En el documento Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3, se establecen las siguientes políticas, frente a las cuales se detectaron desviaciones que afectan su cumplimiento:

- **6.3.2 Directrices de seguridad para el control de acceso físico; establece:**

  Contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, **la unidad de diagramación administración de infraestructura** y oficinas que almacén en información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la SDA considere pertinentes.

  Se observó que en la SDA no se cuenta con unidad de diagramación administración de infraestructura.

- **6.3.2.1 Seguridad en zonas donde se lleve a cabo las actividades de tesorería; establece:**

  Dado que las actividades de tesorería donde se realizan transacciones financieras se efectúan en la Subdirección financiera de la SDA, se fortalecerá los controles para los equipos de cómputo y se propenderá por implementar un acceso controlado y/o restringido al área física, por ejemplo a través de un registro y bitácora de visitantes debidamente autorizados y acompañados durante su estancia en la Subdirección, con el propósito de minimizar la probabilidad de fraude en la gestión de las operaciones transaccionales de valores, pagos por archivos planos y dispersiones desde los portales bancarios.

  De acuerdo con lo expuesto, y dada la falta de claridad sobre la definición de controles, se evidencio en el recorrido de la auditoria que no existe acceso controlado y/o restringido al

área física, por ejemplo, a través de un registro y bitácora de visitantes debidamente autorizados y acompañados durante su estancia en la Subdirección Financiera.

- **6.3.3 Uso adecuado de internet, establece:**

  "No se permite la descarga, uso, intercambio y/o instalación de juegos, aplicaciones web de uso personal, ***redes sociales,*** música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la entidad".

  Durante la prueba de recorrido se observaron equipos con YouTube activo; es necesario parametrizar su uso y disponibilidad, teniendo en cuenta, además, que la SDA hace uso de redes sociales para transmitir su gestión institucional, en streaming mediante la red social de Facebook.

  De acuerdo con lo anterior se recomienda revisar las Políticas de Seguridad de la Información establecidas definidas en el documento enunciado, con el fin de garantizar su articulación con la gestión institucional y garantizar su cumplimiento por parte de los diferentes usuarios de la SDA, esto con el fin de proteger los activos de información, cumplir las regulaciones y mitigar los riesgos que puedan impactar el logro de los objetivos propuestos.

  Criterio

- Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3
  Numeral 6.3.2 Directrices de seguridad para el control de acceso físico
  Numeral 6.3.2.1 Seguridad en zonas donde se lleve a cabo las actividades de tesorería
  Numeral 6.3.3 Uso adecuado de internet

- ISO 27001: 2013 Anexo A - A.5.1.2 Revisión de las políticas para la seguridad de la información.

  Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Insuficientes actividades de socialización que permitan la apropiación e implementación de las	Pérdida de confidencialidad de la información sensible debido a insuficientes mecanismos de verificación del cumplimiento	Posibles sanciones o procesos disciplinarios por pérdida de información confidencial que

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
políticas definidas en el documento de Políticas de Seguridad de la Información de la SDA.	efectivo de las Políticas de Seguridad de la Información de la SDA.	afecte a los diferentes grupos de valor de la SDA.

Tabla 9 Causas, Riesgos e Impactos del hallazgo 6

Recomendación(es):

Se recomienda, en términos de divulgación y comunicación efectiva, comunicar de manera clara y accesible las políticas definidas en el documento de Políticas de la SDA. Haciendo uso del lenguaje claro y simple evitando tecnicismos innecesarios.

Respuesta del Auditado:

Teniendo en cuenta la recomendación hecha en el marco de la auditoría, se actualizaron las políticas de seguridad y privacidad de la información, retirando la línea que mencionaba la unidad de diagramación de la infraestructura, dado que es esta unidad se traía de la versión antigua de las políticas, pero hoy en día ya no aplica, cabe mencionar que, esta situación no generó ningún riesgo que afectara la operación o la seguridad de la información de la entidad. De igual manera, de acuerdo con la recomendación hecha en la reunión de verificación de la auditoría, se ajustó el numeral de directrices de seguridad para el control de acceso físico, dando mayor claridad para su aplicación en la SDA.
Así mismo, se ajustó el numeral relacionado con la seguridad en zonas donde se lleven a cabo las actividades relacionadas con tesorería o transacciones financieras, con el fin de contar con mayor claridad en su redacción y aplicación en la SDA. Quedando de la siguiente manera:

“Seguridad en zonas donde se lleve a cabo actividades relacionadas con tesorería y transacciones financieras:
Las actividades en donde se realizan transacciones financieras, se efectúan por medio de la Subdirección financiera de la SDA, por lo tanto, en esta subdirección se debe propender por fortalecer los controles para los equipos de cómputo y contar con un acceso controlado al área física; por ejemplo a través de un registro y bitácora de visitantes debidamente autorizados y acompañados durante su estancia, con el propósito de minimizar la probabilidad de fraude en la gestión de las operaciones transaccionales de valores, pagos por archivos planos y dispersiones desde los portales bancarios”. (…)

Respecto al uso adecuado de internet, teniendo en cuenta la cultura organizacional y la operación de la SDA, se identifica la necesidad de utilizar estos medios para la divulgación interna de sus contenidos, en este sentido el uso de YouTube se encuentra autorizado, así como las redes sociales**. Por tal razón, ya se actualizó esta política y se retiró esta línea y se mejoró la redacción. (**Negrilla fuera del texto)

Conclusión de la Oficina de Control Interno

De acuerdo con lo manifestado por el proceso frente a la actualización de las políticas que estas ya fueron subsanadas, se realiza la verificación en el sistema Isolución al documento Políticas

de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente - Código: PA03-PO01 - Versión: 3, dado que no fue aportada la evidencia, sin embargo, no se encontró la evidencia de que las políticas se hayan actualizado de acuerdo con lo manifestado. Esto se puede observar en las imágenes tomadas del documento en Isolución, donde se muestra que la versión del documento auditado es la misma (versión 3)

6.3.2 Directrices de seguridad para el control de acceso físico

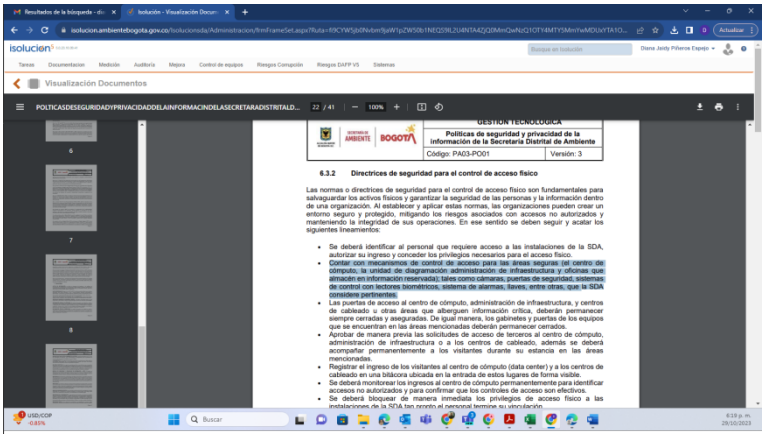


Ilustración 1 Pantallazo de Isolución de 6.3.2 Directrices de seguridad para el control de acceso físic

6.3.2.1 Seguridad en zonas donde se lleve a cabo las actividades de tesorería; establece

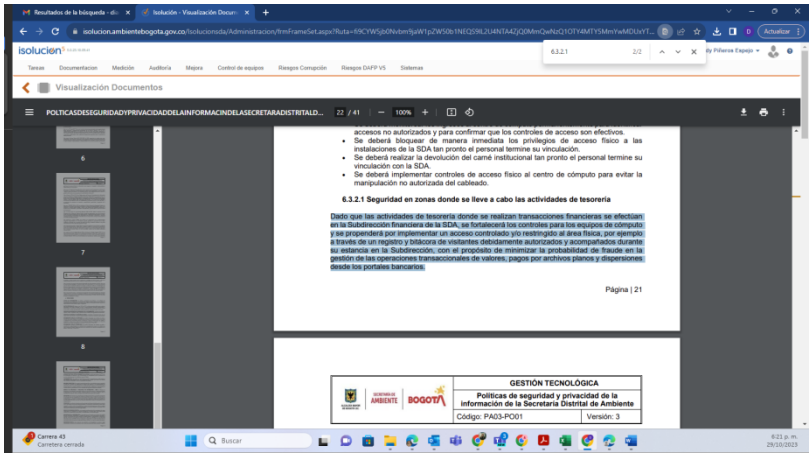


Ilustración 2 Pantallazo de Isolución 6.3.2.1 Seguridad en zonas donde se lleve a cabo las actividades de tesorería

6.3.3 Uso adecuado de internet

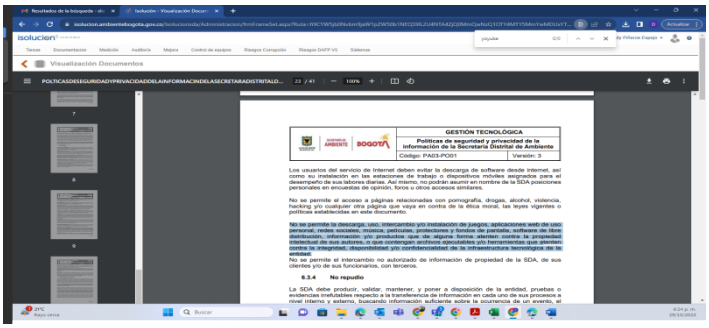


Ilustración 3 Pantallazo de Isolución 6.3.3Uso adecuado de internet

De acuerdo con lo anterior se recomienda revisar las Políticas de Seguridad de la Información establecidas definidas en el documento enunciado, con el fin de garantizar su articulación con la gestión institucional y garantizar su cumplimiento por parte de los diferentes usuarios de la SDA, esto con el fin de proteger los activos de información, cumplir las regulaciones y mitigar los riesgos que puedan impactar el logro de los objetivos propuestos, por lo anterior se ratifica el hallazgo

5.2.2 PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACIÓN – PETI 2021-2024 V4

Hallazgo No. 6 Debilidad en el seguimiento, calidad y cumplimiento de los Entregables asociados al Proyecto de Inversión 7804.

En el marco de la presente auditoría, se realizó la verificación del Documento PETI 2021-2024 v4, aprobado por Comité Institucional de Gestión y Desempeño de la SDA, en la Sesión #4 del 4 de agosto de 2023, respecto del cual se revisó el Proyecto 7804 en el cual se definieron cinco (5) metas, de las cuales se verificaron cuatro (4) para la vigencia 2023 y una (1) para la vigencia 2022, evidenciado lo siguiente:

Vigencia 2022:

- **PRY_7804_M1**: Actualización 24 servicios de información que permitan la implementación de un modelo para la gestión de sistemas de información.
  Valor Estimado: $1.580.170.500

Entregables vigencias 2022	Soportes / Entregables	Conclusión OCI
Derechos patrimoniales sobre los sistemas de información - LI.SIS.06 **Informe/Inventario Derechos patrimoniales de los S.I.**	Carpeta: LI.SIS.06 - Derechos patrimoniales sobre los sistemas de información - LI.SIS.06 contiene: 1. Anexo 1 Obligación de Cesión Patrimonial, sin código y aprobación. 2. Anexo 2 Formato Lista y descripción de los entregables: sin Código y aprobación. 3. Anexo 3 Acuerdo de Cesión Patrimonial: sin Código y aprobación. 4. Metodología de referencia para mantenimiento de sistemas de información_SDA_V.01: sin Código y aprobación 5. PROCEDIMIENTO_DERECHOS PATRIMONIALES: sin Código y aprobación.	Los entregables corresponden a documento y formatos que no se encuentran incluidos dentro del sistema integrado de Gestión para garantizar su uso y apropiación
LI.SIS.24 - Accesibilidad - LI.SIS.24	Carpeta: LI.SIS.24 - Accesibilidad - LI.SIS.24, contiene:	El entregable conforme a la ficha del Proyecto establece:

Entregables vigencias 2022	Soportes / Entregables	Conclusión OCI
Política de Accesibilidad	1. Accesibilidad SDA, se evidencia un diagnóstico del portal web de la SDA. Carpeta: ACCESIBILIDAD WEB: se evidencia una serie de documentos donde se evalúa el cumplimiento de accesibilidad del portal WEB	Política de Accesibilidad, esta no se evidencia en los entregables, de igual forma no es posible determinar el alcance de este documento.
LI.SIS.11 - Ambientes independientes en el ciclo de vida de los sistemas de información **Metodologías ambientes independientes en el ciclo de vida de los S.I.**	Carpeta: LI.SIS.11 - Ambientes independientes en el ciclo de vida de los sistemas de información - LI.SIS.11 contiene 1. Isolución - Visualización Documentos.pdf: no se puede abrir. 2. ARQUITECTURA VITAL 0.1 no se encuentra terminado y tiene las marcas en amarillo 3. ARQUITECTURA VITAL 0.2 no se encuentra terminado y tiene marcas en amarillo. 4. GUÍA AMBIENTES INDEPENDIENTES DESARROLLO DE SOFTWARE V.01: documento no se ubicó en el proceso de Gestión tecnológica, contiene en la tabla de control de versiones: 26/08/2020 Versión preliminar y en la tapa 12/05/2022 Versión 0.1, no genera claridad esta diferencia de fechas.	Se evidencian documentos que no son versiones finales, el entregable que es la *Metodologías ambientes* no se encuentra formalizado en Isolución.
LI.SIS.13 - Integración continua durante el ciclo de vida de los sistemas de información **Metodología Integración continua durante el ciclo de vida de los S.I.**	Carpeta: LI.SIS.13 - Integración continua durante el ciclo de vida de los sistemas de información - LI.SIS.13 contiene: 1. Integración continua durante el ciclo de vida de los sistemas de información - LI.SIS.13: sin aprobación no se evidencia dentro del proceso de Gestión Tecnológica	Documento sin aprobar, no se evidencia su formalización en Isolución El entregable conforme a la ficha del Proyecto establece: *Metodología Integración continua durante el ciclo de vida de los S.I.*
LI.SIS.14 - Plan de pruebas durante el ciclo de vida de los sistemas de información **Estrategia de mantenimiento de los S. I**	Carpeta: LI.SIS.14 - Plan de pruebas durante el ciclo de vida de los sistemas de información - LI.SIS.14 contiene: 1. Anexo_1_Formato Solicitud cambio, ajuste, creación y evaluación de software: (El archivo no se puede visualizar). 2. PLAN MAESTRO DE PRUEBAS 0.3: sin Código 3. GUIA-Plan de Pruebas-SDA; sin Código 4. Formato acta de pruebasv1.0_SDA: sin Código 5. Formato certificación de pruebas v1.0: sin Código, es mismo documento con nombre: Formato acta de pruebasv1.0_SDA 6. Formato-MatrizDeTrazabilidadPruebas-SDA: Sin Código	Documentos sin Código Anexo_1_Formato Solicitud cambio, ajuste, creación y evaluación de software: no se puede visualizar. Documento con contenido igual y diferente nombre. El entregable conforme a la ficha del Proyecto establece: Estrategia de mantenimiento de los S.I, lo cual no se evidenció en los soportes.
LI.SIS.17 - Actualización y requerimientos de cambio de los sistemas de información **Guía de actualización y requerimientos de cambios de los S.I.**	Carpeta: LI.SIS.17 - Actualización y requerimientos de cambio de los sistemas de información - LI.SIS.17 contiene: 1. Formato Solicitud cambio, ajuste, creación y evaluación de software Código: PA03-PR02-F1 versión X En Isolución se encuentra el documento Formato solicitud de cambio, ajuste y creación de nuevo software Código: PA03-PR02-F1 fecha de aprobación 4/04/2019	Sin aprobación a la fecha en Isolución El entregable conforme a la ficha del Proyecto establece: Guía de actualización y requerimientos de cambios de los S.I., lo cual no hace referencia frente a los soportes.
Plan de calidad de los sistemas de información - LI.SIS.20 **Plan de calidad de los S. I**	Carpeta: LI.SIS.20 - Plan de calidad de los sistemas de información - LI.SIS.20, contiene: 1. ANEXO PLAN DE CALIDAD DE LA INFORMACIÓN. 2. PLAN DE CALIDAD DE COMPONENTES DE INFORMACIÓN 18/07/2021 Versión 1.3: es un entregable de la vigencia 2021 y no haría parte como entregable del 2022. 3. Anexo_4 _Guía para la definición de arquitectura de solución de un S.I.: documento en blanco. 4. MODELO DE CALIDAD PARA HACER EL SEGUIMIENTO LA CONSTRUCCIÓN DE SOFTWARE Versión 1.0 20/12/2021, es un	Documentos presentados que corresponden a la vigencia 2021 Documentos en Blanco El entregable conforme a la ficha del Proyecto establece: Plan de calidad de los S.I., sin embargo, los soportes entregados corresponden a la vigencia 2021.

Entregables vigencias 2022	Soportes / Entregables	Conclusión OCI
	documento que pertenece a la vigencia 2021, es decir no hacia parte de este Proyecto de inversión.	

Tabla 10 Proyecto: PRY_7804_M1 vigencia 2022

De acuerdo con lo anterior, se evidenció debilidad frente a la verificación de los entregables para el Proyecto PRY_7804_M1 vigencia 2022, y teniendo en cuenta lo establecido en Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05. 7. RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto.

Vigencia 2023

A continuación, se relacionan las metas en las cuales se verificaron los entregables con corte a 31 de agosto de 2023:

PRY_7804_M1: Actualización 24 servicios de información que permitan la implementación de un modelo para la gestión de sistemas de información

Entregables vigencias 2023	Soportes / Entregables	Conclusión
Guía de estilo y usabilidad - LI.SIS.07	Carpeta: LI.SIS.07 Guía de estilo y usabilidad Vacía sin documentos	Entregables conforme a la Ficha de Proyecto: Guía de estilo única para los sistemas de información 20 de abril del 2024: Incumplido Lista de chequeo de la guía de estilo de los sistemas de información 31/08/2023: Incumplido
LI.SIS.08 Apertura de datos	Carpeta: LI.SIS.08 Apertura de datos Vacía sin documentos	Entregables conforme a la Ficha de Proyecto: Lista de chequeo apertura de datos 30/06/2023: Incumplido
Implementación de Componentes de información - LI.SIS.10	Carpeta: LI.SIS.10 Implementación de Componentes de información Vacía sin documentos	Entregables conforme a la Ficha de Proyecto: Entregable: Lista de chequeo de características de arquitectura de información 30/6/2023: Incumplido
Manual del usuario, técnico y de operación de los sistemas de información - LI.SIS.16	Carpeta: LI.SIS.16 Manual del usuario, técnico y de operación de los sistemas de información Vacía sin documentos	Entregables conforme a la Ficha de Proyecto: Entregable: Manual de Usuario 30/06/2023: incumplido
Estrategia de mantenimiento de los sistemas de información - LI.SIS.18	Carpeta: LI.SIS.18 Estrategia de mantenimiento de los sistemas de información. 1. Carpeta: Ventanas de Mantenimiento: 3 archivos de anuncio de ventanas de mantenimiento. 2. Carpeta: Planes de Mantenimiento: 3 archivos (1 del plan de manteamiento 2023 2 plan de mantenimiento 2022 y un word del 2023 PM). 3. Mantenimientos VISORGEO: contiene 4 archivos 4. Carpeta: Mantenimientos SIPSE: contiene 5 archivos 5. Carpeta: Mantenimientos SIAMOVIL: contiene 7 archivos	Los soportes y el lineamiento no se encontraron relacionados de forma clara con los entregables relacionados en la ficha del proyecto.

Entregables vigencias 2023	Soportes / Entregables	Conclusión
Servicios de mantenimiento de sistemas de información con terceras partes - LI.SIS.19	Carpeta: LI.SIS.19 Servicios de mantenimiento de sistemas de información con terceras partes 1. Carpeta: Planes de Mantenimiento:2 archivos 2. Mantenimientos STORM: 2023: 4 archivos 3. Mantenimientos MESA-ARANDA: 2 archivos 4. Mantenimientos FOREST:4 que pertenecen a la vigencia 2023	Los soportes y el lineamiento no se encontraron relacionados de forma clara con los entregables relacionados en la ficha del proyecto

Tabla 11 Proyecto: PRY_7804_M1 vigencia 2023

De acuerdo con lo anterior, se evidenció debilidad frente a los entregables para el Proyecto PRY_7804_M1 vigencia 2023 y su seguimiento, incumpliendo lo establecido en Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05 7. RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto.

- **PRY_7804_M2: Implementación de 15 servicios de información que permitan la implementación de un modelo para la gestión de información**
  Valor Estimado: $282.381.000

Entregables vigencias 2023	Soportes / Entregables	Conclusión
Gestión de documentos electrónicos - LI.INF.04	carpeta: LI.INF.04 - Gestión de documentos electrónicos - LI.INF.04 1. Documento: Evaluación SGDEA DC RTF - Ver 3.xlsx	Entregable: Política de manejo de documentos electrónicos 30/06/2023 El documento de soporte no hace referencia al entregable establecido que es la Política de Manejo de Documentos Electrónicos. Sin embargo, el proceso en respuesta al informe preliminar remite la URL donde se encuentra la Política de Manejo de documentos electrónicos.

Tabla 12 Proyecto: PRY_7804_M2 vigencia 2023

De acuerdo con lo anterior se evidenció, debilidad frente a los entregables para el Proyecto PRY_7804_M2 vigencia 2023, y el cumplimiento de lo establecido en Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05, RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto.

- **PRY_7804_M3: Construcción de 15 documentos de planeación para la implementación del gobierno de TI de la Entidad.**
  Valor Estimado: $166.980.000

Entregables vigencias 2023	Soportes / Entregables	Conclusión
Dominio de Gobierno (GO) de TI del MRAE: 1.Optimización de las compras de TI. 2. Criterios de adopción y de compra de TI.	Se observan una serie de documentos como estudios previos, fichas de los proyectos entre otros en la carpeta denominada: LI.GO.06 - Optimización de las compras de TI - LI.GO.06, sin embargo, en las carpetas denominadas: LI.GO.08 - Retorno de la inversión de TI - LI.GO.08 y LI.GO.07 - Criterios de adopción y de compra	Parte de los entregables relacionados en la ficha del proyecto que son periódicos o hasta agosto del 2023 son: Plan de acción PETI Plan de trabajo gobierno TI.

3. Retorno de la inversión de TI	de TI - LI.GO.07 no hay ningún soporte que dé cuenta del avance de estos dos documentos priorizados	Informe mensuales avance implementación gobierno TI. Reporte FURAG Informe avance PETI Revisión, ajuste y /o generación de procedimientos del proceso Gestión Tecnológica Revisión y ajuste y/o anexos de los procedimientos del proceso Gestión Tecnológica Reporte GAB Lo anteriormente relacionado no se encuentra en el drive, lo que dificulta establecer su cumplimiento y trazabilidad.

Tabla 13 Proyecto: PRY_7804_M3 vigencia 2023

De acuerdo con lo anterior se evidenció debilidad frente a los entregables para el Proyecto PRY_7804_M3 vigencia 2023, y lo estableció en Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05 7. RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto.

- **PRY_7804_M4: Mejoramiento del 38% de servicios tecnológicos en la SDA en el marco del Mintic**
  Valor Estimado: $3.855.320.500

Entregables vigencias 2023	Soportes / Entregables	Conclusión
	LI.ST.14 - Análisis de vulnerabilidades - LI.ST.14: se evidencia informes de reportes Security e informes de monitoreo de eventos Carpeta: Mantenimientos SEGURIDAD PERIMETRAL y Mantenimientos EQUIPOSCONECTIVIDAD	Parte de los entregables relacionados en la ficha del proyecto que son periódicos o hasta agosto del 2023 son: - Elaboración plan de mantenimiento 30/06/2023 - Sistemas de monitoreo de recursos tecnológicos con alertas configuradas. - Plan de pruebas de seguridad de la información 30/04/2023 - Matriz de riesgos de seguridad de la información 31/08/2023 No se evidencio el entregable de la Matriz de Riesgos de Seguridad de la Información, conforme a la fecha establecido para el 31 de agosto del 2023, dando incumplimiento a lo establecido en el proyecto.

Tabla 14 Proyecto: PRY_7804_M4 vigencia 2023

De acuerdo con lo anterior se evidencia debilidad frente a los entregables para el Proyecto PRY_7804_M4 vigencia 2023, y teniendo en cuenta lo establecido en Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05, 7. RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto

Según lo expuesto, se puede observar una debilidad en el documento PETI 2021-2024 v4, en cuanto a la falta de seguimiento y calidad de los entregables establecidos, al evidenciar situaciones tales como:

- Documentos en versión borrador
- Documentos no accesibles (no disponibles)
- Entregables que no se encuentran disponibles a la fecha de auditoría y que tenía ya fecha de cumplimiento.
- Entregables que no tienen relación con el producto esperado en la ficha del proyecto.
- Dificulta de la relación de los entregables con los lineamientos establecidos.

De acuerdo con las situaciones relacionadas anteriormente, se concluye, frente al proyecto 7804 de inversión, que no se realizó un seguimiento adecuado que frente a los entregables establecidos, así mismo, se observó que su ejecución se realizó fuera de los términos establecidos para la entrega de los resultados esperados, denotando retrasos en la ejecución del proyecto. Adicionalmente, se detectaron debilidades, frente a la calidad de los entregables tal como se describe en cada situación enunciada, afectando el análisis de resultados efectivo frente a la gestión de la SDA respecto a los compromisos en torno al PETI.

Criterio

- Procedimiento: Reprogramación, actualización y seguimiento plan de acción Componente de Inversión y Gestión en SEGPLAN - Código: PE01-PR05
-

  7. RESPONSABILIDAD Y AUTORIDAD: Gerente de Proyecto:

  - Responder por la calidad, veracidad y oportunidad de la información reportada en relación con la ejecución del proyecto de inversión a cargo.
  - Garantizar el archivo y custodia de la información soporte de los reportes realizados.

- Modelo Integrado de Planeación y Gestión - MIPG
  Dimensión de Evaluación de Resultados
  Seguimiento y evaluación efectuados por los servidores que tienen a su cargo cada proyecto, plan, programa o estrategia, en sus diferentes etapas de desarrollo

- NTC ISO 9001:2015
  Numeral 8.1 planificación y Control Operacional

  La organización debe de planificar, implementar y controlar los procesos necesarios para cumplir los requisitos para la provisión de productos y servicios y para implementar las acciones determinadas (..)
  b) La determinación de los recursos necesarios para lograr la conformidad con los requisitos de los productos y servicios
  c) La implementación de control de los procesos de acuerdo con los criterios.
  La determinación, el mantenimiento y la conservación de la información documentada en la extensión necesaria para:
  Tener confianza en que los procesos se han llevado a cabo según lo planificado.
  La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Falta de compromiso frente al cumplimiento de los lineamientos definidos para el seguimiento y verificación del plan de acción institucional. Insuficiente aplicación de medidas seguimiento y verificación de la calidad y oportunidad en los entregables acordes a las metas definidas	Posibilidad de afectación reputacional y económica por incumplimiento de las metas definidas en el plan de acción a cargo del proceso.	Retrasos en el logro de los objetivos establecidos. Perdida de recursos económicos que afecten la capacidad de la entidad para cumplir con las metas y el logro de los objetivos. Posibles sanciones o procesos disciplinarios por incumplimiento de los procedimientos establecidos.

Tabla 15 Causas, Riesgos e Impactos del hallazgo 8

Recomendación(es):

Se recomienda establecer controles efectivos de seguimiento sobre los proyectos del PETI con el fin de dar cumplimiento a las metas plan de la Entidad y su respectiva ejecución de recursos.

Asignar responsabilidades claras: Designar responsables específicos para cada entregable y establecer claramente sus roles y responsabilidades. Esto asegurará que haya una persona encargada de supervisar y garantizar la calidad de cada resultado.

Establecer estándares de calidad: Definir estándares claros de calidad para cada entregable y asegurarse de que se cumplan. Esto puede incluir la revisión de los resultados por parte de expertos.

Respuesta del Auditado y Conclusión de la Oficina de Control Interno

Respuesta del Auditado*:*

1. **(…)** Respecto a la Política de Accesibilidad, solicitamos dar alcance o claridad a la solicitud puesto que no se conoce de la existencia de dicha norma nacional o distrital relacionada con el tema o similar o lineamiento que exija la implementación de esta política con estas características.

Conclusión de la Oficina de Control Interno

Frente a los soportes entregados a esta auditoría, la ficha del proyecto con nombre: PRY_7804_M1, en la pestaña ENTREGABLES, como se ve en la siguiente imagen: Se observa en la columna C con título Entregable: Política de Accesibilidad.

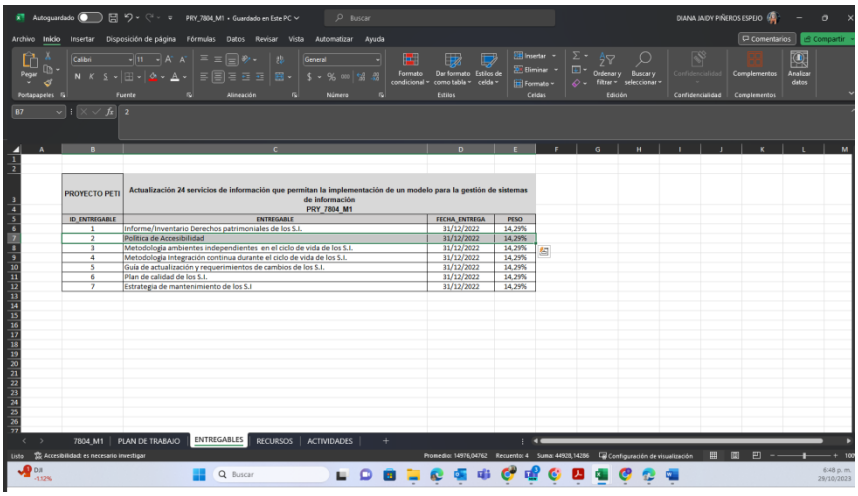


Ilustración 4 ficha del proyecto con nombre: PRY_7804_M1

Respuesta del Auditado*:*

El documento de política de manejo de documentos electrónicos es un documento que no pertenece al proceso de gestión tecnológica que lidera la DPSIA, sino que hace parte del proceso de gestión documental que lidera la Dirección de Gestión Corporativa. Por tal motivo, se puede consultar como un documento publicado en la URL https://www.ambientebogota.gov.co/documents/893475/3512455/4+Anexo+-Politica+de+Gesti%C3%B3n+Documental.pdf/3d29b0ef-8ed4-4306-83ef-be2fbfc351f8 Este documento permite la articulación de todos los actores involucrados en la gestión documental, pero la aplicabilidad depende de las tablas de retención documental

Conclusión de la Oficina de Control Interno

Frente a los soportes entregados a esta auditoría, la ficha del proyecto con nombre: PRY_7804_M2, en la pestaña 7804_M2 como se observa en la imagen la gerente del Proyecto es la DPSIA, sin embargo, no se garantizó que el entregable correspondiente estuviese disponible para su consulta.

Respuesta del Auditado*:*

Tal y como quedó programado en el plan de acción del proyecto de inversión 7804 en la meta 3, y en la hoja de ruta del PETI proyecto PRY_7804_M3 para la vigencia 2023, las actividades definidas para la adopción de los lineamientos de Gobierno de TI en la vigencia 2023 son las dos siguientes actividades: 1. Gestionar y consolidar (03) tres documentos priorizados para la vigencia, que reflejen la implementación de los lineamientos relacionados con gobierno TI. 2. Actualizar los (10) diez documentos generados en las vigencias anteriores. (…) a continuación se precisan las actividades ejecutadas a la fecha correspondientes a los lineamientos que pertenecen a cada actividad: Actividad 1: Gestionar y consolidar (03) documentos priorizados para la vigencia, que reflejen la implementación de los lineamientos relacionados con gobierno TI: (…) A continuación, se detallan los tres lineamientos priorizados para esta actividad:

1. Optimización de las compras de TI (LI.GO.06), 2. Criterios de adopción y de compra de TI (LI.GO.07) 3. Retorno de la inversión de TI (LI.GO.08). (…)

Conclusión de la Oficina de Control Interno

Con respecto a lo manifestado por el proceso sobre el proyecto PRY_7804_M3 para la vigencia 2023, el cual establecen que las actividades que se ejecutan para dar cumplimiento a la Actividad 1: Gestionar y consolidar (03) documentos priorizados para la vigencia, que reflejen la implementación de los lineamientos relacionados con gobierno TI se detallan en tres lineamientos priorizados para esta actividad: 1. **Optimización de las compras de TI** (LI.GO.06), 2. **Criterios de adopción y de compra de TI** (LI.GO.07) 3. **Retorno de la inversión de TI** (LI.GO.08); a lo cual anexan una URL donde se observan una serie de documentos como estudios previos, fichas de los proyectos entre otros en la carpeta denominada: LI.GO.06 - Optimización de las compras de TI - LI.GO.06, sin embargo, en las carpetas denominadas: LI.GO.08 - Retorno de la inversión de TI - LI.GO.08 y LI.GO.07 - Criterios de adopción y de compra de TI - LI.GO.07 no hay ningún soporte que dé cuenta del avance de estos dos documentos priorizados como se observa en las imágenes:

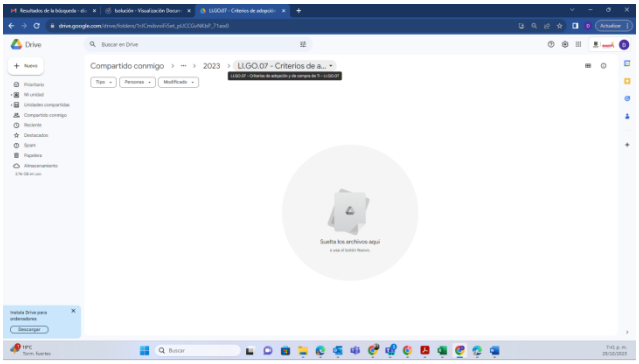


Ilustración 5 Carpeta del drive con nombre: LI.GO.07 - Criterios de adopción y de compra de TI - LI.GO.07

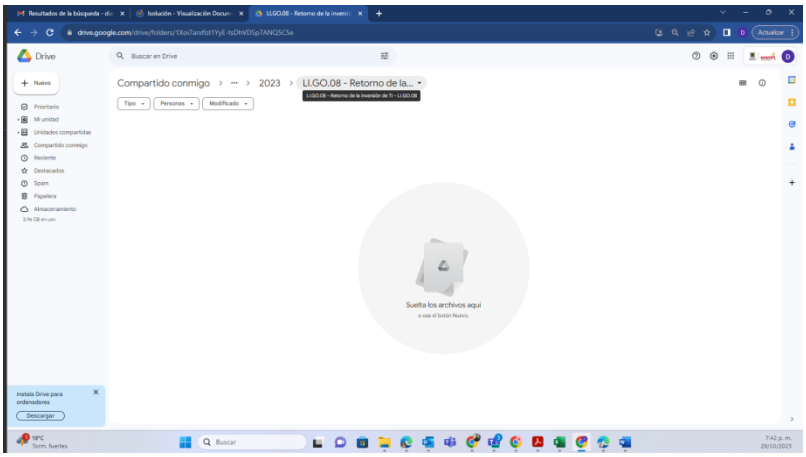


Ilustración 6 Carpeta del drive con nombre: LI.GO.08 - Retorno de la inversión de TI - LI.GO.08

Tomando en consideración frente a lo expuesto y de acuerdo con lo manifestado por el proceso que busca evidenciar el progreso en la implementación de estos tres lineamientos, se observa que la información de la URL proporcionada no resulta eficaz para llevar a cabo esta auditoría. Esto se debe a que las carpetas correspondientes a los otros dos lineamientos se encuentran vacías, lo cual genera incertidumbre respecto a lo esperado para estas actividades.

Respuesta del Proceso

Actividad 2: Actualizar los (10) documentos generados en las vigencias anteriores: durante lo transcurrido de la vigencia 2023, se vienen llevando a cabo actividades que conlleven a la actualización de los documentos elaborados en las vigencias anteriores. ***Dentro de estas actividades se encuentran la formulación de los planes de trabajo, seguimiento a indicadores, actualización de procedimientos, mesas de trabajo realizadas con procesos, planes de acción y mejoramiento, entre otros, los cuales responden a los 10 lineamientos priorizados de gobierno, así****:* Alineación del gobierno de TI - LI.GO.01, Liderazgo de proyectos de TI - LI.GO.09, Mejoramiento de los procesos - LI.GO.13, Macroproceso de gestión de TI- LI.GO.04, Capacidades y recursos de TI - LI.GO.05, Gestión de proyectos de TI – LI.GO.10, Evaluación del desempeño de la gestión de TI - LI.GO.12, Apoyo de TI a los procesos - LI.GO.02, Conformidad - LI.GO.03, Indicadores de gestión de los proyectos de TI - LI.GO.11.
(Negrilla fuera de texto)

Conclusión de la Oficina de Control Interno

Conforme a lo manifestado por el proceso: "*Dentro de estas actividades se encuentran la formulación de los planes de trabajo, seguimiento a indicadores, actualización de procedimientos, mesas de trabajo realizadas con procesos, planes de acción y mejoramiento, entre otros, **los cuales responden a los 10 lineamientos priorizados de gobierno**, así*:
No se observo soportes en la ruta entregada: https://drive.google.com/drive/folders/1vbyayOTQ3imGZ-M5yPgyyq0CAVIeruZo, que den cuenta al cumplimiento de los lineamientos: Capacidades y recursos de TI - LI.GO.05 y Evaluación del desempeño de la gestión de TI - LI.GO.12. que hacen parte de esta actividad como se observa en las imágenes:

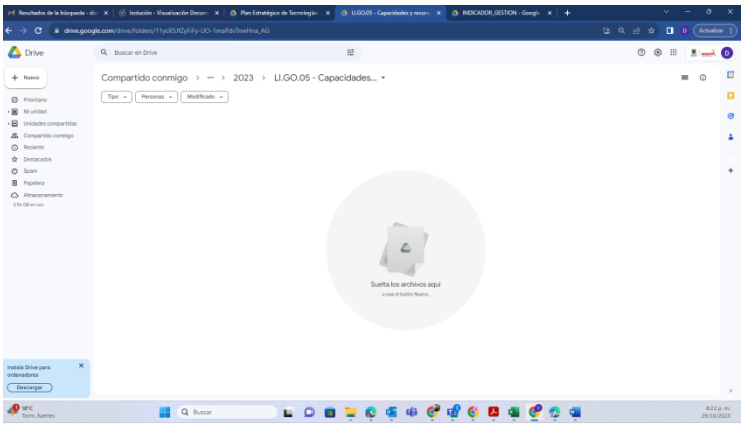


Ilustración 7 Carpeta del drive: LI.GO.05 y Evaluación del desempeño de la gestión de TI

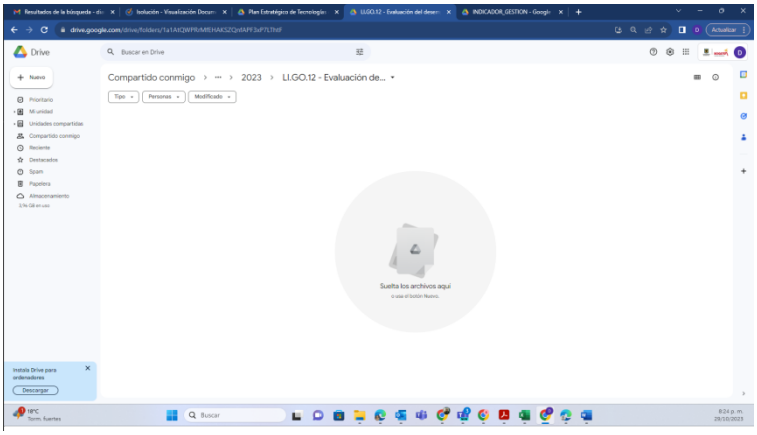


Ilustración 8 Carpeta del drive Evaluación del desempeño de la gestión de TI - LI.GO.12

Se concluye que, si bien se observa soportes que dan cuenta de la gestión en relación a los lineamientos mencionados en el informe preliminar (*Plan de acción PETI, Plan de trabajo gobierno TI, Informe mensuales avance implementación gobierno TI, Reporte FURAG Informe avance PETI, Revisión, ajuste y /o generación de procedimientos del proceso Gestión Tecnológica, Revisión y ajuste y/o anexos de los procedimientos del proceso Gestión Tecnológica, Reporte GAB*), no se evidencia soportes específicos para los dos lineamientos: Evaluación del desempeño de la gestión de TI - LI.GO.12 y LI.GO.05 y Evaluación del desempeño de la gestión de TI.

De igual forma, se invita a generar una trazabilidad más precisa en la Hoja del Proyecto en relación con los entregables (pestaña denominada ENTREGABLES), ya que no se encuentra relacionada con cada uno de los lineamientos mencionados anteriormente, lo que dificulta el seguimiento.

Con respecto a lo manifestado sobre el proyecto Vigencia 2023 PRY_7804_M4: Mejoramiento del 38% de servicios tecnológicos en la SDA en el marco del Mintic, es importante la gestión realizada a la fecha, sin embargo, esto no desvirtúa lo establecido en el proyecto conforme se mencionó en el informe preliminar:

Parte de los entregables relacionados en la ficha del proyecto que son periódicos o hasta agosto del 2023 son:

- Elaboración plan de mantenimiento 30/06/2023
- Sistemas de monitoreo de recursos tecnológicos con alertas configuradas.
- Plan de pruebas de seguridad de la información 30/04/2023
- Matriz de riesgos de seguridad de la información 31/08/2023

Aunque se destaca la gestión realizada, es importante mencionar que persisten diferentes situaciones identificadas durante esta auditoría en relación con la calidad, veracidad y oportunidad de la información reportada sobre la ejecución del proyecto de inversión a cargo. Por lo tanto, se confirma este hallazgo.

5.2.3 ACCESIBILIDAD

Hallazgo No. 7 Debilidad en los Criterios de Accesibilidad del Portal Web de la SDA

Esta auditoría especializada se efectuó a partir del documento titulado Evaluación de Accesibilidad.pdf, entregado por la entidad como parte de los insumos documentales allegados para la realización del presente proceso.

A continuación, se relacionan las situaciones evidenciadas por los criterios de accesibilidad, las evidencias se encuentran en el documento: Evaluación de Accesibilidad SDA

1. Elementos que no son texto

Recurso	Observaciones	Urls
Imágenes que van a secciones de oferta de actividades ambientales, visor geográfico y otras (4 imágenes)	El texto alternativo si bien describe el link a donde va o el texto de la imagen, en al menos un caso no corresponde con la acción del enlace.	01-
Botón Familiando por los derechos	El texto alternativo o Alt no describe la imagen que se está mostrando. Dice "familiando", en este caso no se indica que la imagen incluye texto y éste está incompleto.	01-
Botón Informe de rendición de cuentas a la ciudadanía	La imagen no tiene Alt.	02-

Recurso	Observaciones	Urls
Banner Voluntariado Ambiental	El Alt describe la imagen de la foto correctamente, sin embargo, al ser un banner con un link o llamado a la acción de "Inscríbete aquí" debería incluir también la información en texto. Ej. "Banner con la foto de una mujer sembrando una planta y el texto: Voluntariado Ambiental, sí lideras una organización que fomente esta labor, inscríbete".	02-
Botón Encuesta de calidad del aire	La imagen no tiene Alt.	03-
Banner Conoce nuestras actividades ambientales!	El Alt describe la intención del contenido de la página, pero no la imagen como tal y tampoco aclara que es un banner.	04-
Iconos trámites	El Alt de los íconos es igual y no diferencia un trámite del otro. Todos se llaman "icono tramite". En este caso sería descriptivo algo como "Icono de un computador portátil", para el primero de los iconos.	05-
Imagen Cuadro Conceptual PGA	El Alt dice "Cuadro conceptual PGA" pero esto es una muy pequeña parte de lo que la imagen incluye. Más allá de que viola el criterio de 1.4.5, si la imagen tuviera que ser descrita por un párrafo en el texto, por ejemplo, podría vincularse a éste mediante la propiedad aria-labelled-by.	06-
Banner principal landing Convención Internacional Emergencia Climática	EL Alt dice "Banner principal" pero no describe de que se trata o que al menos es el banner del evento y la información que incluye.	07-
Imagen informativa del evento	El Alt dice "Lugar del evento" pero la imagen no indica el nombre del lugar, la fecha y otra información adicional que se incluye dentro de la imagen.	07-
Botón Descargar Cronograma	El Alt dice "cronograma" pero no indica que es un botón para descargar el cronograma. Ej "Botón con el texto: descargar cronograma".	07-
Texto en imagen ¡Vincúlate ahora!	El Alt dice "contacto" sin embargo el texto incluido en la imagen no se aporta en la descripción.	07-
Imagen logo Secretaria Distrital de Ambiente footer	El Alt dice "Imagen SDA" pero existen personas que no saben que significa SDA, se debe indicar el nombre completo de la entidad o sigla utilizada.	01-02-03-04-05-06-07-08-
Logotipo header AmbienTic	La imagen no tiene Alt.	09-
Imágenes links varios "Gestión del riesgo" y otras secciones (5 imágenes)	3 de las imágenes no tienen Alt establecido.	09-
Imágenes en el rotador de indicadores ambientales.	Algunas imágenes no tienen Alt. Tanto en los botones, como en las tarjetas de acceso a la información.	10-
Banner principal.	La imagen no tiene Alt.	11-12-

Tabla 16 Elementos que no son texto

2. Audio y Video

Recurso	Observaciones	Urls

Video Mujeres que reverdecen	Presenta un video de Youtube embebido "Mujeres que reverdecen Arelis Salgado", el cual tiene subtitulos, pero no es una descripción en texto completa, además carece de audiodescripción.	01-
Video Ambientick	Presenta un video embebido con textos y efectos de audio, sin embargo, no tiene link a audiodescripción, ni a una descripción en texto de los contenidos.	09-
Video ambiental	Presenta un video embebido con textos y efectos de audio, sin embargo, no tiene link a audiodescripción, ni a una descripción en texto de los contenidos.	09-

Tabla 17 Audio y Video

3. Características Sensoriales

Recurso	Observaciones	Urls
Calendario de ambiente	En el calendario de ambiente hay unas fechas verdes destacadas, pero no existe un recurso en el código que indique lo mismo, por lo que una persona que no puede ver los colores no se daría cuenta que esta es una fecha especial.	01-
Infografía Instrumento de planeación ambiental	Se incluye una diferenciación por colores entre los elementos que corresponden a instrumentos operativos de planeación ambiental y a otros instrumentos, pero como no se explica esta diferencia en el texto y tampoco existe un recurso en el código que explique cuales corresponden a uno y al otro, no podría ser detectada por una persona que no pueda ver los colores.	06-
Convenciones del mapa	Las convenciones del mapa tienen una diferenciación en colores, pero no existe un recurso en el código que indique a qué corresponde cada uno, ni tampoco que permita a la persona acceder a los sectores del mapa a los cuales pertenece a cada convención.	11-

Tabla 18 Características Sensoriales

4. Texto en Imágenes

Recurso	Observaciones	Urls
Múltiples imágenes: Carrusel de banners (5 imágenes), algunas imágenes de soporte en las noticias y banner animado.	Todos los banners tienen exceso de texto en imagen y aunque se intenta incluir éste a través del ALT, resulta difícil crear una descripción que incluya la información.	01-
Imágenes para ir a secciones de Oferta de Actividades Ambientales, Visor Geográfico,	Todos los botones o imágenes presentan texto.	01-

Recurso	Observaciones	Urls
Red de Monitoreo de Calidad del Aire y Observatorio Ambiental (5 imágenes)		
Botones de servicios de ambiente (5 imágenes)	Todas las imágenes de servicios de ambiente contienen una pregunta larga incluida en la imagen.	01-
Imágenes sección "Menú Participa"	Varias imágenes, desde el banner hasta los botones a subsecciones tienen texto incluido.	02-
Imágenes con texto que se podría evitar.	Las imágenes presentan texto que se hubiera podido incluir fácilmente de otra forma que evite esta práctica desaconsejada.	03-09-11-12-
Imágenes con exceso de texto. Banners, gráficos, infografías y otras piezas con múltiples palabras, frases e incluso párrafos completos embebidos.	Las imágenes presentan texto que incluso si se trata de incluir a través de la propiedad ALT resulta difícil de garantizar que no existan pérdidas de información.	04-06-07-09-
Banner principal y carrusel "1 Minuto con el Observatorio Ambiental de Bogotá".	La mayoría de los Banners tienen gran cantidad de texto sobre la imagen.	10-

Tabla 19 Texto en Imágenes

5. Título Vs Contenido

Recurso	Observaciones	Urls
Titulo página de inicio Secretaría de Ambiente	Se repite el nombre de la entidad, no aclara en qué sección se encuentra.	01-
Título landing "Convención Emergencia Climática"	El título es "inicio", sin embargo, debería ser el nombre de la convención pues confunde con la verdadera página de inicio de la entidad.	07-
Título página de Mapas interactivos	La página no tiene etiqueta "Title".	11-

Tabla 20 Título Vs Contenido

6. Encabezados Enlaces y Etiquetas

Recurso	Observaciones	Urls
Se usan encabezados como recurso para usos diferentes.	El encabezado no tiene propósito semántico, solo se usa para destacar estructuras como enlaces o textos generales. En consecuencia, aunque se pudiera argumentar que el texto particular en cada caso tiene sentido, éste no se usa para encabezar.	01-02-09-10-11-

Tabla 21 Encabezados Enlaces y Etiquetas

7. Lenguaje en otro idioma

Recurso	Observaciones	Urls
La página en sí misma.	No se cuenta con la propiedad LANG en la etiqueta HTML.	11-

Tabla 22 Lenguaje en otro idioma

8. Orientación del Contenido

Recurso	Observaciones	Urls
Bloques de Imagen con texto	Al navegar desde dispositivos móviles el texto sobre la imagen en formato vertical se reduce y queda ilegible.	07-
Mapa humedales	Al navegar desde dispositivos móviles el texto sobre la imagen en formato vertical se reduce y queda ilegible.	09-
Formulario Actos Administrativos	La página no es responsive, por lo que al navegar en dispositivos móviles el formulario y su texto quedan muy pequeños en formato vertical.	12-

Tabla 23 Orientación del Contenido

9. Ampliación sin pérdida de funcionalidad

Recurso	Observaciones	Urls
Links inferiores de términos y condiciones, políticas y mapa del sitio.	El texto de color verde queda montado sobre el fondo del mismo color dificultando su visibilidad y contraste. Adicionalmente, se presentan cortes y se generan barras de desplazamiento lateral cuando se visualiza en pantallas más estrechas, especialmente ante la presencia de determinadas imágenes.	01-02-03-04-05-06-07-08-
El sitio no es responsive y poco ampliable.	Al no estar configurado el responsive del sitio se genera barra de desplazamiento horizontal al hacer una ampliación perdiéndose parte del texto descriptivo y los menús de registro, historia y sugerencias.	12-

Tabla 24 Ampliación sin pérdida de funcionalidad

10. Convulsiones

Recurso	Observaciones	Urls
Banner animado en GIF	El único elemento que podría generar cierto parpadeo es la animación de las cifras de corte junio 2023, ya que es muy rápida y al ser infinita pareciera que esta zona de la pantalla parpadea. Como es algo leve no se marca como incumplimiento, pero se deja la observación y la evidencia.	Ninguna de las URLs inspeccionadas reporta elementos evaluables para este criterio. Recomendaciones no causales de incumplimiento

Tabla 25 Convulsiones

11. Capacidad de Operar con Teclado

Recurso	Observaciones	Urls
Widget de twitter	Al hacer tabulación con el teclado y llegar al widget de Twitter, el control se queda navegando en los tweets un gran tiempo saliéndose del tema principal y dificultando el retorno a la página de inicio.	01-
Calendario de eventos de ambiente	En ningún momento se llega al calendario de ambiente a través del teclado constituyendo a este elemento como una trampa para este dispositivo.	01-
Agenda de la Convención Internacional Emergencia Climática	Al tabular con el teclado y llegar al bloque Agenda solamente se puede ingresar al programa del día septiembre 19 y en consecuencia la información de la otra fecha queda inaccesible.	07-
Menús y Submenús	No se puede ingresar a los submenús del Portal de Niños a través del teclado.	09-
Focos no visibles	No se resaltan todos los elementos al ser enfocados a través del teclado, por ejemplo, cuando se recorren con la tecla de tabulación.	09-10-12-
Menús y Submenús	No se puede ingresar a los submenús del Observatorio a través del teclado, constituyéndose en una trampa para éste.	10-
Buscador	No se puede acceder al buscador superior a través del teclado.	10-
Focos no visibles	No se resalta suficientemente todos los elementos al ser enfocados a través del teclado, por ejemplo, cuando se recorren con la tecla de tabulación.	10-12-

Tabla 26 Capacidad de Operar con Teclado

12. Eventos de hover

Recurso	Observaciones	Urls
El menú principal en sus pestañas de primer nivel.	El contenido de las pestañas como "Participa" indica que es "hoverable", sin embargo, este nuevo contenido no es accesible a través del ratón, tan solo por el teclado. Lo que va en contravía del principio de ser visible bajo las condiciones correctas (hoverable). También se dificulta la salida del "hover" cuando se da por teclado, teniendo que ser necesario descubrir que esto es posible gracias a un clic por fuera del elemento.	01-02-03-04-05-06-07-08-

Tabla 27 Eventos de hover

13. Estructuras y el tiempo

Recurso	Observaciones	Urls
El "elemento animado" de panelistas.	El elemento muestra información rotativa, es decir que depende de tiempo y no se puede detener o pausar.	07-

Tabla 28 Estructuras y el tiempo

14. Formularios

Recurso	Observaciones	Urls
El campo de entrada del formulario de búsqueda.	El campo de búsqueda carece de un "label" asociado o una propiedad ARIA equivalente. El propósito del campo no se puede establecer fácilmente por *software*, dado que la única indicación de su funcionalidad es el "*placeholder*" y el atributo "*title*", que, aun estando presentes, no son los elementos más adecuados para cubrir esta necesidad.	01-02-03-04-05-06-07-08-
Botón de "submit" del formulario de búsqueda.	El botón no tiene un valor que permita indicar su propósito y dado que el elemento fundamental que lo compone es una imagen, no hay indicaciones claras acerca de éste. Nótese también como el ALT incluido es un tanto ambiguo con relación al propósito del botón, pues el texto "buscador" no es explícito de una acción, sino más bien de un elemento.	01-02-03-04-05-06-07-08-
Campos de entrada en el buscador.	El campo referencia un label que incluye un texto que no corresponde con el nombre del campo. Este fenómeno se presenta en los dos campos de esta estructura.	10-
Buscador.	El elemento no dispara una búsqueda sin que se introduzca un valor en cualquiera de los campos, aunque esto está bien, esta característica no se le informa al usuario y la estructura simplemente parece no funcionar por falta de instrucciones claras o de sugerencias ante un error.	10-
Intercambiador de opciones en el mapa.	El objeto de tipo select, carece de etiquetas asociadas y/o propiedades que permitan establecer su propósito por software.	11-
Formularios de consulta.	No existen instrucciones u otras ayudas que permitan evitar los errores.	12-

Tabla 29 Formularios

15. Los mismos elementos con identificaciones diferentes

Recurso	Observaciones	Urls
Botones de inicio del menú principal y del área de migas de pan.	Primero es extraño que el ítem de "migas de pan" se ubique en la página de inicio, porque en teoría no es muy necesario en esa ubicación en donde aún no se desarrolla la navegación. Pero más allá de ello -que no es una falta a la accesibilidad-, lo que resulta contrario al presente principio es ofrecer dos enlaces tan cerca entre sí para el mismo fin, a los cuales se suma el enlace dispuesto en el logo principal de la página. Ahora bien, son repetitivos y además carecen de una identificación común, lo que a las luces de la norma convendría agrupar en una única estructura que permitiera lo indicado.	01-
Indicadores ambientales y temas vs actualidad ambiental.	Se utilizan dos estructuras de carrusel completamente diferentes en la misma URL, una primera a través de Swiper y la segunda Slick Slider. Esto sin contar el hecho de que para los carruseles	10-

Recurso	Observaciones	Urls
	de banners se utiliza una tercera denominada "Camera".	

Tabla 30 Los mismos elementos con identificaciones diferentes

16. Elementos especiales

Recurso	Observaciones	Urls
Tabulador de redes sociales.	No se establece un rol adecuado a la estructura LI que representa las pestañas seleccionables.	01-08-
Elemento de búsqueda.	No hay una indicación por software posible acerca del estado del buscador y/o sus eventuales errores.	10-
Calendario de ambiente.	Es un elemento especial creado a través de un script, que no permite establecer su estado y operación utilizando exclusivamente el software.	01-
Tabulados de agenda.	Es un elemento especial creado a través de un script, que no permite establecer su estado y operación utilizando exclusivamente el software.	07-
Componente mixto: indicadores ambientales y temas ambientales.	Es un elemento especial creado a través de un script, que no permite establecer su estado y operación utilizando exclusivamente el software.	10-

Tabla 31 Elementos especiales

17. Estructuras y Relaciones

Recurso	Observaciones	Urls
Formulario principal.	Los componentes de tipo select del formulario se utilizan ocultos, pero se operan a través de un *script* que se activa por el uso de una lista vinculada. Esto hace que en determinadas condiciones no se comprenda la información que se pretende en los formularios y que en consecuencia se genere una dependencia al *script*.	12-
Carruseles de novedades.	Los ítems en el carrusel entregan información a través de imágenes usadas como fondos, esto hace que no se pueda determinar su contenido por software y en consecuencia se dependa de la estructura visual para acceder al contenido. Dado que la imagen es un fondo, no tiene la ayuda de un texto alternativo o método similar.	10-
Pie de página.	El footer de la página es una única imagen con texto muy extenso que más allá de que sea difícil de incluir a través de alt, en este caso es imposible pues la imagen no se incluye a través de un objeto IMG, sino mediante el uso de un fondo, lo que la hace indeterminable por software.	11-

Tabla 32 Estructuras y Relaciones

18. Contraste

Recurso	Observaciones	Urls
Imágenes usadas como títulos y botones con texto incluido ante el efecto "hover".	Los radios de contraste en estos elementos ante el efecto de "hover", son menores a los requeridos.	01-02-
Imágenes usadas como títulos y botones con texto incluido.	El radio de contraste en estos elementos es menor al requerido.	01-02-09-
Pestaña no activa del intercambiador de widgets de las redes sociales.	El radio de contraste en este elemento es menor al requerido.	01-08-
Texto de enlace en la miga de pan.	El radio de contraste en este elemento es menor al requerido.	01-02-03-04-05-06-07-08-
Flechas que sirven para cambiar de slide en el carrusel, especialmente cuando están ante un evento de "hover".	El radio de contraste en este elemento es menor al requerido.	01-
Elementos gráficos con texto.	El radio de contraste en este elemento es menor al requerido.	02-
Elementos gráficos con texto.	El radio de contraste en este elemento es menor al requerido.	03-
Elementos gráficos con texto.	El radio de contraste en estos elementos es menor al requerido.	07-
Los elementos del menú.	El radio de contraste en este elemento es menor al requerido.	09-
Subtítulos en naranja y verde claro.	El radio de contraste en estos elementos es menor al requerido.	09-
Diversos elementos en texto.	El radio de contraste en estos elementos es menor al requerido.	10-
Botones de selección.	El radio de contraste en este elemento es menor al requerido.	11-
Aviso sobre el mapa.	El radio de contraste en este elemento es menor al requerido.	11-
Texto al pie del formulario.	El radio de contraste en este elemento es menor al requerido.	12-
Texto de algunos selectores.	El radio de contraste en este elemento es menor al requerido.	12-

Tabla 33 Contraste

19. Procesamiento

Recurso	Observaciones	Urls
Código de salida de la página.	El código se somete a una validación sintáctica utilizando el instrumento estándar de la W3C, en donde se aprecia un volumen relevante de problemas conocidos (entre 21 y 245).	01-02-03-04-05-06-07-08-09-10-11-12-

Tabla 34 Procesamiento

De acuerdo con lo anterior se recomienda:

1. Crear un plan de remediación para la plantilla general que privilegie la sencillez y el avance, antes que la resolución retroactiva. Para ello se puede utilizar la información aquí incluida (anexo evaluación de accesibilidad) para crear un Pareto de puntos de alto impacto y priorizarlos en su resolución para maximizar el impacto y ganar confianza en su mitigación.

2. Crear para piezas flexibles como "landing pages", un sistema de diseño accesible y reciclaje que permita aplicar estructuras válidas preconstruidas de acuerdo con las necesidades de las áreas con una mayor flexibilidad.

3. Adoptar prácticas de accesibilidad en la producción audiovisual y extender los estándares de accesibilidad a los equipos de desarrollo y/o proveedores que estén ejecutando nuevos productos digitales para la entidad.

4. Utilizar el presente instrumento (anexo evaluación de accesibilidad) y sus resultados para construir un plan de mitigación y registrar su avance.

5. El indicador se concluye en lo siguiente frente a la muestra evaluada (anexo evaluación de accesibilidad):

- Ninguna de las urls analizadas pasa el 100% de los criterios.
- El 27.3% de las directrices se cumplen a nivel prácticamente global, o su incidencia es mínima.
- En La página principal este indicador sube a 45.4%
- Los errores más desafiantes son: procesamiento, contraste, (issues variados sobre el menú principal), textos alternativos y texto en imágenes.

6. Con respecto a lo manifestado en la sección de socialización de resultados realizado el 13 de octubre del 2023, en referencia a los videos, se recomienda evaluar la accesibilidad de los videos que actualmente se encuentran publicado en la web; esto implica asegurarse de que los videos cuenten con subtítulos, descripciones de audio y opciones de contraste adecuadas. Además, se sugiere proporcionar alternativas, como transcripciones del contenido del video, para aquellos que no puedan acceder al video en sí. Al tomar estas medidas, se promoverá la inclusión y se asegurará que el contenido de los videos sea accesible para todos los usuarios.

   Este proceso debe ser gradual y requiere realizar una valoración de los videos disponibles en la web para priorizar su intervención, analizando el costo, beneficio de su mejora, lo que impactará positivamente en el indicador de accesibilidad.

El detalle de la evaluación de los criterios se encuentra en el documento anexo denominado: Evaluación de Accesibilidad SDA.xlsx

Criterio

NTC 5854 que establece los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA, así como de la

Resolución 1519 de 2020 en su Anexo No. 1 accesibilidad, Artículo 3. DIRECTRICES DE ACCESIBILIDAD WEB, que manifiesta*:*

A partir del 1 de enero del 2022, los sujetos obligados deberán dar cumplimiento a los estándares AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C), conforme con el Anexo 1 de la presente resolución aplicable en todos los procesos de actualización, estructuración, reestructuración, diseño, rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en esas

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Limitaciones técnicas para el cumplimiento de los criterios de accesibilidad por falta de falta de recursos o conocimientos técnicos insuficientes para implementar soluciones accesibles.	Posibilidad afectación reputacional por falta de garantías en el acceso a la oferta institucional en la web a todos los usuarios, independientemente de sus capacidades físicas, mentales o motoras.	Posibles sanciones o procesos disciplinarios por incumplimiento de los criterios de accesibilidad conforme a la normatividad vigente.

Tabla 35 Causas, Riesgos e Impactos del hallazgo 9

Recomendación(es):

Capacitación y sensibilización: Es importante brindar capacitación y crear conciencia sobre los requisitos de accesibilidad y cómo cumplir con ellos. Esto incluye capacitar a los desarrolladores, diseñadores y otros profesionales involucrados en la creación de contenido accesible, así como a los responsables de la toma de decisiones en la entidad

Establecer controles y políticas de operación que permita dar cumplimiento a los criterios de accesibilidad para todos los responsables de la publicación de la información en el portal de la SDA, los generadores de contenidos y demás usuarios que intervengan en el cumplimiento.

Realizar un plan de mejoramiento a partir de los resultados obtenidos en el presente documento, con el fin de determinar acciones, recursos y tiempos y así garantizar el cumplimiento de los requisitos establecidos en la Resolución 1519 de 2020.

Respuesta del Auditado

Teniendo en cuenta que la entidad ya cuenta con la acción No. 1062 en el plan de mejoramiento del proceso y en ejecución, acción suscrita para subsanar una a una las observaciones encontradas en la auditoría anterior en relación con los criterios de accesibilidad, mediante la implementación progresiva de los criterios de cumplimiento o directrices de accesibilidad incluidas en el Anexo No. 1 de la Resolución 1519 de 2020, referenciados en el “Informe Técnico Auditoría en accesibilidad Web”, se solicita respetuosamente, se analice la pertinencia de establecer este hallazgo relacionado con la “debilidad en los criterios de accesibilidad del portal

web", cuando la entidad ya ha generado un plan de trabajo interno y se han realizado esfuerzos para que el 100% de la sede electrónica cumpla con lo que indica la norma. Sin embargo, este es un proceso que lleva tiempo para que sea finalmente visible para un usuario en su totalidad y para ello nos encontramos en etapas de intervención, mejora o en proceso de ajuste

(…)

Por lo anterior, se solicita respetuosamente, se analice la pertinencia de clasificar esta observación como una recomendación que se maneja de forma integral como una oportunidad de mejora, en la que podamos ir adecuando los componentes del portal Web de la SDA con los criterios de accesibilidad como ya lo venimos realizando con el esfuerzo de la Oficina Asesora de Comunicaciones y la Dirección de Planeación y Sistemas de Información Ambiental de la SDA y utilizando las herramientas o mecanismos recomendados por la auditora que facilite el seguimiento o monitoreo a la implementación de los criterios.

Conclusión de la Oficina de Control Interno

La Oficina de Control Interno no desconoce las mejoras que ha venido implementando el proceso frente a los criterios de accesibilidad, lo que ha permitido mejorar algunos aspectos de la página web, adicional a los ejercicios de verificación y autoevaluación periódica que realiza.

Frente a los soportes entregados en la verificación realizada por el proceso de los diferentes criterios donde se puede evidenciar el cumplimiento de condiciones de accesibilidad, es necesario ampliar la revisión de la totalidad de los contenido publicados, evaluar el costo beneficio e implementar acciones que permitan mejorar los estándares y resultados de las mediciones para lo cual la verificación realizada por esta auditoría se constituyen en un referente que debe ser evaluado por el proceso dentro de sus acciones de mejoramiento continuo.

Con respecto a lo manifestado: "Así mismo, se quiere aclarar que un porcentaje de las observaciones encontradas corresponden a publicaciones realizadas antes de que entrara en vigor la mencionada Resolución 1519 de 2020, por lo que consideramos que las observaciones realizadas en la auditoría que comprende el periodo entre agosto de 2022 a agosto de 2023 no deberían ser retroactivas, debido a que en este portal web se encuentran contenidos migrados desde el año 2006. Cabe recalcar que los resultados del Índice de Transparencia y Acceso a la Información (ITA) el cual es evaluado por la Procuraduría General de la Nación en el marco de la medición anual que se realiza a los sujetos obligados de la Ley 1712 de 2014*."*

Esta Oficina de Control Interno se permite informar que, de acuerdo con lo establecido en la Resolución 1519 del 2020: "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos" (…)

"Artículo 3°. Directrices de accesibilidad web. A partir del 1° de enero del 2022, los sujetos obligados deberán dar cumplimiento a los estándares AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C), conforme con el Anexo 1 de la presente resolución aplicable

en todos los procesos de actualización, estructuración, reestructuración, diseño, rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en esas"; así mismo *el*

"Artículo 8°. Vigencia y derogatorias. (…), los sujetos obligados deberán implementar las disposiciones aquí referidas en las siguientes fechas: el artículo 3 se deberá implementar a más tardar el 31 de diciembre del 2021, conforme con los términos referidos en el anexo 1 de esta misma Resolución. Los lineamientos y directrices determinados en los artículos 4, 5, 6 y 7 se deberán implementar a más tardar el 31 de marzo del 2021."

No es pertinente atender la solicitud de evaluar la accesibilidad de las publicaciones a partir de agosto del 2022, dado que normatividad no realiza una exclusión en este sentido, sino se debe de realizar de forma integral, por lo que se recomienda al proceso complementar la acción correctiva No. 1062 incluyendo los nuevos aspectos identificados en esta auditoría y definir acciones que contribuyan al cumplimiento de los requisitos normativos expuestos.

7. OTROS ASUNTOS PARA LA MEJORA

Lineamientos para controlar la instalación de software en los sistemas operativos de la SDA.

Teniendo en cuenta que el proceso cuenta con el documento de Políticas de Seguridad y Privacidad de la Información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3 en el que se contempla la Política de Control de Software Operacional donde establezca como el Proceso de Gestión Tecnológica controlará la ***restricción de la instalación de software no permitido***, si bien, establece en el numeral 6.3.3 Uso adecuado de internet "*La Dirección de Planeación y Sistemas de Información Ambiental debe establecer procedimientos y junto con la Dirección de Gestión Corporativa implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos y de alta peligrosidad."* ;

Se recomienda incluir y hacer referencia a la instalación de software permitido por la SDA.

Lo anterior con el fin de evitar que se presenten riesgos de instalación de software malicioso o no autorizado en los sistemas de la SDA y de esta manera contribuir al cumplimiento de lo definido en los siguientes criterios:

- ISO 27001:2013 Anexo A - A.12.5 Control de software operacional
  A.12.5.1 Instalación de software en sistemas operativos
  Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

- Modelo Integrado de Planeación y Gestión - MIPG
  Dimensión 3. Gestión con valores por Resultado
  3.4.2 Política de Seguridad Digital
  Actividades de Control

Recomendación(es):

Establecer una política de software operacional que describa las reglas y directrices para la adquisición, instalación, uso y actualización del software en la SDA, que sea clara y comprensible a los diferentes grupos de valor, con el fin de facilitar la administración, gestión y control de licencias, actualizaciones y parches, y se garantice que el software utilizado en la entidad cumpla con las condiciones de legalidad, actualización y seguridad requeridas.

Respuesta del Auditado:

La Política de Seguridad y Privacidad de la Información de la SDA se actualizó el 4 de agosto de 2023 en la sesión No. 4 del Comité Institucional de Gestión y Desempeño (…)

Conclusión de la Oficina de Control Interno

De acuerdo con lo manifestado por el proceso frente a la actualización de las políticas que estas ya fueron subsanadas, se realiza la verificación en el sistema Isolución al documento Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente - Código: PA03-PO01 - Versión: 3, dado que no fue aportada la evidencia, sin embargo, no se encontró la evidencia de que las políticas se hayan actualizado de acuerdo con lo mencionado en esta mejora.

8. BENEFICIO DE AUDITORIA

Dentro del ejercicio de la auditoria se evidencio debilidad en la implementación de la Política de Gestión de Medios Removibles.

El documento de Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3 numeral 6.3.3 Gestión de medios removibles, establece:

"*Los puertos USB deben estar inhabilitados. Sólo se habilitará previa autorización de la Dirección de Planeación y Sistemas de Información Ambiental*."

Al realizar la prueba en sitio los puertos USB de todos los equipos de cómputo de la SDA se encontraban habilitados, por lo anterior, no se da cumplimiento a la política de Gestión de Medios Removibles.

Criterio

- Políticas de seguridad y privacidad de la información de la Secretaría Distrital de Ambiente Código: PA03-PO01 versión 3 numeral 6.3.3 Gestión de medios removibles.

- ISO 27001: 2013 Numeral 8.3.1 Gestión de medios removibles

Posibles Causa(s), Riesgo(s) e Impacto(s)

CAUSA(S)	RIESGO(S) ASOCIADO(S)	IMPACTO(S)
Falta de controles para garantizar el cumplimiento de la política de gestión de medios removibles. Insuficientes mecanismos de monitoreo y seguimiento para asegurar del cumplimiento de las directrices establecidas.	Posibilidad de afectación económica por perdida de información por introducción de malware a través de medios extraíbles sin la debida verificación.	Posibles sanciones o procesos disciplinarios por pérdida de información confidencial que afecte a los diferentes grupos de valor de la SDA.

Tabla 36 Causas, Riesgos e Impactos del hallazgo 4

Respuesta del Auditado:

(…) De acuerdo con lo recomendado en el ejercicio de auditoría, se agilizó la aplicación de esta política y se tomaron medidas de inmediato, de tal manera que, el pasado 21 de septiembre de 2023 se remitió un comunicado mediante correo electrónico institucional con el asunto "Implementación de medidas de seguridad de la información adicionales: Bloqueo de puertos USB y Unidades de CD/DVD" para todos los usuarios de la Entidad (funcionariosycontratistas@ambientebogota.gov.co).

Así mismo, mediante radicado 2023IE224474 del 26 de septiembre de 2023 se emitió comunicación a los administradores de los sistemas de información indicando las medidas que se deben tener, informando que, a partir del 22 de septiembre de 2023, se actualizaron los parámetros de seguridad, incluido el manejo de los puertos USB, CD y DVD. Por tal razón, desde ese día ya fueron bloqueados estos puertos, y se indicó que, en caso de necesitar este acceso, se debería solicitar por el jefe de la dependencia, con la justificación respectiva y por medio de la mesa de servicio.
Por lo anterior, se solicita respetuosamente, considerar la pertinencia del hallazgo, dado que ya se implementó la mejora respectiva mediante una corrección en el mismo momento en que la auditora indicó sobre el control

Conclusión de la Oficina de Control Interno

Teniendo en cuenta que el proceso tomó acciones inmediatas para abordar la debilidad identificada durante la ejecución de la auditoría, y considerando la muestra presentada y las declaraciones realizadas, donde se menciona "*que se bloquearon los puertos y se estableció un procedimiento para solicitar acceso a través del jefe de la dependencia y la mesa de servicio*", se espera que la política se cumpla al 100% en los equipos de la entidad.

Con base en lo anterior, se concluye que el hallazgo se retira y se insta al proceso a llevar a cabo un monitoreo continuo para garantizar el cumplimiento de la Política de Gestión de medios removibles.

9. RESUMEN DE HALLAZGOS

N°	Título del Hallazgo	Repetitivo
1	Debilidad en el cumplimiento de los Planes de Seguridad y Planes de Tratamiento de Seguridad de la Información.	NO
2	Ausencia de los riesgos de Seguridad de la Información en los Procesos de Contratación de la SDA	NO
3	Debilidad en la Planificación, Implementación y Verificación de la Gestión de Continuidad de Negocio.	NO
4	Debilidad en la aplicación Política de Mantenimiento Físico de las Operaciones.	NO
5	Debilidad en el establecimiento de la Políticas de Seguridad de la Información de la SDA	NO
6	Debilidad en el seguimiento, calidad y cumplimiento de los Entregables asociados al Proyecto de Inversión 7804.	SI
7	Debilidad en los Criterios de Accesibilidad del Portal Web de la SDA.	SI

Tabla 37 Resumen de Hallazgos

10. NOTAS:

1. La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo, recursos y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

2. Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionados por los auditores a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

3. La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por el personal y/o colaboradores pertenecientes al proceso o actividad auditada, a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.

Bogotá D.C., 2 de noviembre de 2023

NORMA LUCÍA AVILA QUINTERO
Jefe Oficina de Control Interno

Elaboró: Diana Jaidy Piñeros E. - Contratista-Rol Auditor Líder
Revisó: Viviana Marcela Marín Olmos – Contratista- Rol revisión

Aprobó: Norma Lucía Ávila Quintero- jefe Oficina de Control Interno

Anexo: Documento Excel descripción Evaluación de Accesibilidad SDA.xlsx