INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Informe de Evaluación Independiente Final	Fecha de Expedición	11	12	2020

Proceso (s) y/o proyecto auditado:	Proceso de Gestión Tecnológica / Gobierno Digital – Habilitador Transversal Seguridad de la Información
Responsable proceso y/o proyecto auditado:	Subsecretaria de Gestión Corporativa y Control Interno Disciplinario
Objetivo de la Auditoría:	Evaluar el nivel de implementación de la Política de Gobierno Digital en el Habilitador Transversal Seguridad de la Información, al proceso de Gestión Tecnológica de la Secretaría Distrital del Hábitat - SDHT conforme a los requisitos legales vigentes.
Alcance de la Auditoría:	El alcance se definió para el proceso de gestión tecnológica como responsable de la implementación del Modelo de Seguridad de la Información (MSPI) en la SDHT, sin discriminación del área, dependencia funcional, Subdirección y/o subsecretaria que tenga relación directa con este y demás procedimiento e insumos del proceso auditado. Se realizará el seguimiento al normograma del proceso auditado en cumplimiento del Plan Anual de Auditoria 2020.
Criterios de la Auditoría:	• Caracterización de Proceso PS05-CP01, Proceso de Gestión Tecnológica. • Decreto 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". • Guía Modelo de Seguridad de la Información MSPI MinTIC Versión 3.0.2 del 29/07/2016 y guías relacionadas. • Decreto 1499 de 2017. "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015". • Implementación de la Estrategia del MSPI de las Entidades Distritales - Alta Consejería Distrital de TIC de agosto 3 de 2017. • Circular No.033 de 10/11/2017 sobre Lineamiento de Avance implementación MSPI. • Decreto 1008 de 2018 "Política de Gobierno Digital" (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del Sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de Planeación y Gestión (MIPG). • Manual de la Política de Gobierno Digital Versión 7 de abril de 2019. • Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos. • Guía para la administración del riesgo y el diseño de control en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital Versión 4 del Departamento Administrativo de la Función Pública (DAFP) octubre de 2018. • Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones y Departamento Administrativo de la Función Pública (DAFP) 2018.
Metodología	Técnicas de auditoría basados en los métodos de observación, confrontación, revisión y comparación. De acuerdo con las normas internacionales de auditoria, la presente es una auditoria de cumplimiento legal, es decir se verificará el cumplimiento del Modelo de Seguridad de la Información establecido por el MinTIC.

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	05	**Mes**	10	**Año**	2020	**Desde**	06/10/2020 D / M / A	**Hasta**	30/11/2020 D / M / A	Día	01	Mes	12	Año	2020

Representante Alta Dirección	Asesor de Control Interno	Auditor (es)
Nelson Javier Vásquez Torres	Viviana Rocío Bejarano Camargo	Julián Andrés Ruiz Méndez

I. FICHA TECNICA

Mediante memorando No. 3-2020-03467 del 5 de octubre de 2020 se cita a los responsables a la reunión de apertura de la Auditoria Política de Gobierno Digital Habilitador Transversal Seguridad de la Información.

Para el desarrollo de la auditoria se realizó una reunión de apertura el día 05 de octubre de 2020 de forma virtual por la plataforma Microsoft Teams.

Posteriormente se realizó una reunión virtual de conocimiento del área con los integrantes del Proceso de Gestión Tecnológica el día 8 de octubre de 2020 por la plataforma Microsoft Teams.

Mediante el memorando No.3-2020-03586 del 14 de octubre de 2020 se hizo la solicitud de información para la auditoria.

Se realizó una segunda reunión virtual de conocimiento del área el 15 de octubre de 2020 por la plataforma Microsoft Teams.

Con los memorandos No.3-2020-03851 del 23 de octubre de 2020 y No.3-32020-03976 del 29 de octubre de 2020 se recibió respuesta a la solicitud de información.

Universo:

- ✓ **Modelo de Seguridad de la Información (MinTIC)**

  El universo corresponde a la implementación del Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC en la Secretaría Distrital del Hábitat por parte del proceso de Gestión Tecnológica el cual se compone de 5 fases que son:

  - **Diagnóstico**: En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad de la Información (MSPI).
  - **Planificación**: Con los resultados de la fase anterior se elabora el plan de seguridad de la información de la entidad y se diseñan las acciones a implementar.
  - **Implementación**: Se lleva a cabo la implementación definida en la fase anterior.
  - **Evaluación de Desempeño**: Se realiza el seguimiento y monitoreo a la implementación del Modelo de Seguridad de la Información (MSPI).
  - **Mejora Continua**: Se consolidan los resultados obtenidos para diseñar el plan de mejoramiento continuo en Seguridad de la Información

Población objeto:

- ✓ **Modelo de Seguridad de la Información (MinTIC)**

La población objeto corresponde a las 5 fases para la implementación del Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC que son:

- **Diagnóstico**: En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad de la Información (MSPI). Para esta fase se solicitó 1 entregable.
- **Planificación**: Con los resultados de la fase anterior se elabora el plan de seguridad de la información de la entidad y se diseñan las acciones a implementar. Para esta fase se solicitaron 36 entregables.
- **Implementación**: Se lleva a cabo la implementación definida en la fase anterior. Para esta fase se solicitaron 12 entregables.
- **Evaluación de Desempeño**: Se realiza el seguimiento y monitoreo a la implementación del Modelo de Seguridad de la Información (MSPI). Para esta fase se solicitaron 4 entregables.
- **Mejora Continua**: Se consolidan los resultados obtenidos para diseñar el plan de mejoramiento continuo en Seguridad de la Información. Para esta fase se solicitaron 3 entregables.

Muestra de Auditoria:

- ✓ **Modelo de Seguridad de la Información (MinTIC)**

A criterio del auditor la muestra de auditoría correspondió a 57 entregables correspondientes a las 5 fases para la implementación del Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC en la SDHT que son:

- **Diagnóstico**: En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad de la Información (MSPI).
- **Planificación**: Con los resultados de la fase anterior se elabora el plan de seguridad de la información de la entidad y se diseñan las acciones a implementar.
- **Implementación**: Se lleva a cabo la implementación definida en la fase anterior.
- **Evaluación de Desempeño**: Se realiza el seguimiento y monitoreo a la implementación del Modelo de Seguridad de la Información (MSPI).
- **Mejora Continua**: Se consolidan los resultados obtenidos para diseñar el plan de mejoramiento continuo en Seguridad de la Información.

Herramientas Utilizadas:

Se utilizaron las siguientes herramientas documentales dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones:

- Manual de Gobierno Digital Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 7 de abril de 2019.
- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 26 de Julio de 2016.
- Guía No. 4 Roles y Responsabilidades Versión 1 del 25 de abril de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Guía No.6 de Referencia sobre Gestión Documental Versión 1 del 11 de marzo de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

- Guía No. 14 Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información Versión 1 del 17 de marzo de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Guía No.16 de Evaluación del Desempeño Versión 1 del 16 de febrero de 2017 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Guía para la administración del riesgo y el diseño de control en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital Versión 4 del Departamento Administrativo de la Función Pública (DAFP) octubre de 2018.
- Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones y Departamento Administrativo de la Función Pública (DAFP) 2018.
- Plan de Mejoramiento Institucional SDHT.

II. FORTALEZAS

- ✓ Se evidenció la disposición, colaboración y atención a las preguntas realizadas por parte de los funcionarios y contratistas responsables del Proceso de Gestión Tecnológica durante el desarrollo de la auditoria, así como la atención, importancia y respeto hacia los auditores.
- ✓ La SDHT cuenta con una Política General de Seguridad de la Información y con las Políticas Específicas para uso de dispositivos móviles, teletrabajo, control de acceso a la información, controles criptográficos, escritorio limpio y pantalla limpia, respaldo de la información (backup), transferencia o intercambio de información, desarrollo de software, relaciones con proveedores, autorización de nuevos recursos de procesamiento, clasificación de activos de información, seguridad física, antivirus, correo electrónico corporativo, uso de contraseñas, uso de servicios de red, uso de internet, red privada virtual (VPN), control de cambios, propiedad intelectual y tratamiento de la información, las cuales fueron debidamente aprobadas mediante Acta No.02 del Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones del 18 de Septiembre de 2018 y se encuentran formalizadas bajo el sistema integrado de gestión como Manual de Políticas del Subsistema de Gestión de Seguridad de la Información PS05-MM13 del 26 de Septiembre de 2018.
- ✓ La SDHT cuenta con un inventario con la identificación, valoración y clasificación de los activos de información en el formato PS05-FO232 Matriz de inventario de activos de información. Este inventario fue realizado bajo el procedimiento PS05-PR05 de Clasificación y Etiquetado de la Información Clasificación Versión 4 del 21 de octubre de 2019. Este inventario fue aprobado mediante resolución No. 788 del 17 de diciembre 2019 y se encuentra publicado en la sección de Transparencia y Acceso a la información pública de la SDHT.
- ✓ La SDHT cuenta con el Procedimiento PG03-PR06 de Administración de Riesgos de Gestión, Corrupción y Seguridad Digital del 30 de abril de 2020, con el instructivo PG03-IN55 Versión 1 del 9 de agosto de 2019 para el diligenciamiento del Formato PG03-F0401 Mapa de riesgos Versión 6 para la identificación de riesgos de seguridad digital de los procesos de la entidad.

III. RESULTADOS DE LA AUDITORÍA

Observación N°1. Ausencia de un Diagnóstico completo y actualizado de Seguridad de la Información en la SDHT

Se evidenció que el Proceso de Gestión Tecnológica no cuenta con un diagnóstico actualizado y completo respecto a los requerimientos del Modelo de seguridad de la información (MSPI), el documento presentado se encuentra desactualizado, incompleto y no corresponde con la última versión entregada por el Ministerio de Tecnologías de la Información y las Comunicaciones la cual se encuentra en:
https://gobiernodigital.mintic.gov.co/692/articles-150507_Instrumento_Evaluacion_MSPI.xlsx

Se recomienda que este diagnóstico sea realizado por lo menos una vez cada vigencia con el fin de evaluar el avance permanente de la implementación del Modelo de Seguridad de la Información (MSPI). En resumen, se observó lo siguiente referente a la fase de diagnóstico:

Fase	Criterio	Entregable	Estado
Fase de Diagnóstico	Herramienta de Diagnóstico MSPI	Herramienta de Diagnóstico MSPI completamente diligenciada con identificación de: • Estado actual de la gestión de seguridad de la información al interior de la entidad • Nivel de madurez de los controles de seguridad implementados • Avance de la implementación del ciclo de operación al interior de la entidad • Hallazgos encontrados en las pruebas de vulnerabilidad • Nivel de cumplimiento de la legislación vigente relacionada con seguridad de la información	**No cumple.** El diagnóstico presentado no corresponde a la última versión del instrumento dado por MinTIC y no se encuentra diligenciado completamente por lo que se desconoce el estado actual de la entidad en la implementación del Modelo de Seguridad.

Análisis de los controles frente a los riesgos

Al no contar con un diagnóstico completo de seguridad de la información en la entidad, se puede generar el riesgo de una inadecuada implementación del Modelo de Seguridad de la Información.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado estos riesgos y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.1 Fase de Diagnóstico.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.

Observación N°2. Inoperancia del Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones establecidos en la Resolución 874 de 2018 Artículos 17 y Artículos 18 en la Vigencia 2019 y 2020

La entidad cuenta con la Resolución 874 de 2018 por la cual: "*se unifican las disposiciones de las instancias de coordinación interna de la Secretaría Distrital del Hábitat, se crea el Comité Institucional de Gestión y Desempeño, y se deroga la Resolución 137 de 2017*". En el artículo 17 de dicha resolución, se crea el Comité de Seguridad de la información y de Tecnologías de la Información y las Comunicaciones como la instancia donde se coordina, articula los diferentes actores, programas y proyectos relacionados con sistemas de información, infraestructura tecnológica y seguridad de la información. En el artículo 18 de dicha resolución, se definen las funciones del comité donde algunas de ellas son:

- Definir las estrategias y acciones que, en materia de seguridad, tecnologías de información y conectividad debe implementar la entidad.
- Validar las políticas de seguridad de la información y velar por su cumplimiento.
- Emitir directrices y recomendaciones para la implementación de las políticas de seguridad de la información.
- Promover el cumplimiento de la política de seguridad de la información.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Evaluar y validar el componente de gestión y seguridad de la información de los programas y proyectos desarrollados por la entidad.
- Conocer y socializar lo relacionado con la implementación del Modelo de Seguridad y los cambios que se generen del mismo.

No obstante, el Proceso de Gestión Tecnológica en el marco de la auditoria no aportó las actas que permitieran validar y evidenciar la operación periódica del comité en las vigencias 2019 y 2020 y el cumplimiento de las funciones planteadas en el artículo 18. Por tal razón se concluye que el Comité es inoperante y no aporta a la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de las Información y las Comunicaciones – MinTIC.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Planificación	Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifican las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.	**Cumple** con la entrega de la Resolución 874 de 2018
		Copias de las actas de las sesiones del Comité de Seguridad de la Información y de Tecnologías de La Información y las Comunicaciones del cual hace referencia la Resolución 874 de 2018. Estas actas deben corresponder al periodo comprendido entre el 1 de enero de 2019 a 31 de julio de 2020.	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos

El no funcionamiento del Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones, puede generar el riesgo de una inadecuada implementación del Modelo de Seguridad de la Información y de una desarticulación de la Política de Gobierno Digital con el Modelo Integrado de Planeación y Gestión – MIPG del Departamento Administrativo de la Función Pública a través del Comité Institucional de Gestión y Desempeño.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado estos riesgos y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía No. 4 Roles y Responsabilidades Versión 1 del 25 de abril de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Observación N°3. Ausencia de un Plan de Comunicación, Sensibilización y Capacitación en Seguridad de la Información para la SDHT

Se evidenció que el Proceso de Gestión Tecnológica viene adelantando sensibilizaciones sobre las políticas específicas de seguridad de la información por medio de correos masivos enviados a través del correo electrónico institucional, no obstante, la entidad no cuenta con un Plan de Comunicación, Sensibilización y Capacitación específico, formalizado y estructurado en Seguridad de la Información como lo exige la Guía No.14 del Modelo de Seguridad de la Información (MSPI), el cual debe contemplar las fases de diseño, desarrollo, implementación y mejoramiento.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Planificación	Plan de Comunicación, Sensibilización y Capacitación en Seguridad de la información para la SDHT	Plan de comunicación, sensibilización y capacitación para la entidad en Seguridad de la Información de la SDHT Vigencia 2019 y 2020.	**No Cumple**: El proceso entregó el Plan Estratégico de Comunicaciones Vigencia 2019 de la Oficina Asesora de Comunicaciones el cual no contempla ningún elemento relacionado con el MSPI.
		Copia del acta de aprobación por parte de la alta dirección del Plan de comunicación, sensibilización y capacitación para la entidad en Seguridad de la Información de la SDHT Vigencia 2019 y 2020.	**No Cumple** No presentó avance
		Evidencias de la implementación del Plan de comunicación, sensibilización y capacitación para la entidad en Seguridad de la Información de la SDHT Vigencia 2019 y 2020.	**No Cumple:** El proceso entregó pantallazos de las sensibilizaciones realizadas vía correo electrónico, no obstante, estas sensibilizaciones no se encuentran alineadas a un Plan de Comunicación, Sensibilización y Capacitación en Seguridad de la Información en la SDHT.

Análisis de los controles frente a los riesgos
La falta de comunicación, capacitación y sensibilización a los funcionarios en cuanto a las Políticas Específicas de Seguridad de la Información en la entidad puede conllevar a incumplimientos de estas, lo que puede generar potenciales brechas o materialización de los riesgos de seguridad de la información.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado estos riesgos y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía No. 14 Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información Versión 1 del 17 de marzo de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Observación N°4. Falta de Integración del Modelo de Seguridad de la Información (MSPI) con el sistema de Gestión Documental de la SDHT

La entidad debe alinear el Modelo de Seguridad de la Información (MSPI) con el Sistema de Gestión Documental de la entidad de acuerdo con los criterios establecidos en la Guía No.6 del Modelo de Seguridad de la Información (MSPI), esto permite la protección de activos de información físicos, digitales y electrónicos por medio de políticas, procedimientos, controles e indicadores. No obstante, el Proceso de Gestión Tecnológica no aportó evidencias que permitieran evidenciar la integración del Modelo de Seguridad (MSPI) con el Sistema de Gestión Documental de la SDHT. En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Planificación	Integración del MSPI, con el sistema de gestión documental de la entidad	Evidencias de integración entre el MSPI con el sistema de gestión documental de la entidad entre el 1 de enero de 2019 y 31 de julio de 2020	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos
La falta de integración entre el el Modelo de Seguridad de la Información (MSPI) con el Sistema de Gestión Documental podría generar riesgos relacionados con la perdida de documentos, archivos, carpetas e información en general.

Frente a la matriz de riesgo del proceso de gestión documental se tienen identificados los siguientes riesgos:

- Pérdida de documentos
- Pérdida alteración, deterioro y/o destrucción de documentos para favorecimiento de intereses particulares

Los controles definidos para estos riesgos respectivamente son:

- Control del préstamo documental
- Control de acceso a las zonas destinadas para archivo
- Aplicación del procedimiento de préstamo y consulta de documentos

No obstante, estos controles deben ser alineados con los controles definidos en la norma ISO 27001:2013 específicamente con el control A.18.1.3 de Protección de registros.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía No.6 de Referencia sobre Gestión Documental Versión 1 del 11 de marzo de 2016 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Observación N°5. Ausencia de los Mapas de Riesgos de Seguridad Digital de los procesos de la SDHT

Se evidenció que la SDHT cuenta con el Procedimiento PG03-PR06 de Administración de Riesgos de Gestión, Corrupción y Seguridad Digital del 30 de abril de 2020, con el instructivo PG03-IN55 Versión 1 del 9 de agosto de 2019 para el diligenciamiento del Formato PG03-F0401 Mapa de riesgos Versión 6 para la identificación de riesgos de seguridad digital de los procesos de la entidad. No obstante, aún no se ha terminado con el levantamiento completo de los mapas de riesgos de seguridad digital para cada uno de los procesos de la entidad.

Esta situación presentada impide identificar, analizar y valorar claramente los riesgos de seguridad digital para así continuar con el diseño, implementación y ejecución de los respetivos controles. La entidad se encuentra expuesta a que se presenten y materialicen incidentes, amenazas y vulnerabilidades en el entorno digital.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Planificación	Identificación, Valoración y tratamiento de riesgo	Documento con la metodología de gestión de riesgos.	**Cumple:** con la entrega de: Procedimiento PG03-PR06 de Administración de Riesgos de Gestión, Corrupción y Seguridad Digital del 30 de abril de 2020, Instructivo PG03-IN55 Versión 1 del 9 de agosto de 2019, Formato PG03-F0401 Mapa de riesgos Versión 6.

Fase	Criterio	Entregable	Estado
Fase de Planificación	Identificación, Valoración y tratamiento de riesgo	Mapas de riesgos de seguridad digital por cada proceso de la SDHT con corte a 31 de julio de 2020 de acuerdo con los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas.	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos
Al no tener claramente identificados los mapas de riesgos de seguridad digital para los procesos de la entidad se pueden presentar incidentes, amenazas y vulnerabilidades en el entorno digital.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía para la administración del riesgo y el diseño de control en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital Versión 4 del Departamento Administrativo de la Función Pública (DAFP) octubre de 2018.
- Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones y Departamento Administrativo de la Función Pública (DAFP) 2018.

Observación N°6. Falta de planeación y ejecución de las actividades definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y en el Plan de Seguridad y Privacidad de la información para las vigencias 2019 y 2020.

En los Planes de Acción de la SDHT para las vigencias 2019 y 2020 se incluyó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la información, no obstante, el proceso de Gestión Tecnológica no aportó evidencias que soporten o permitan evidenciar la ejecución de las actividades definidas en estos planes. Adicionalmente se observa que hay una falta de articulación entre estos planes y el resultado del diagnóstico de la implementación del Modelo de Seguridad de la información (MSPI) descrito en la Observación No.1, lo que no permite la articulación del ejercicio de implementación del Modelo como se detalla en la Guía Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Planificación	Identificación, Valoración y tratamiento de riesgo	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencias 2019 y 2020	**Parcialmente cumple:** Se presentó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencias 2019 y 2020, estos no obedecen a una planeación coherente de este componente ya que algunas actividades no corresponden a este Plan como por ejemplo Analizar la Arquitectura Empresarial, formular el proyecto de IPv4 a IPv6.
Fase de Planificación	Identificación, Valoración y tratamiento de riesgo	Plan de Seguridad y Privacidad de la información Vigencias 2019 y 2020	**Parcialmente cumple:** Se presentó el Plan de Seguridad y Privacidad de la Información Vigencias 2019 y 2020 integrado a los Planes de Acción de la entidad, estos no obedecen a una planeación coherente de este componente ya que por ejemplo no se incluyeron actividades relacionadas con la implementación del MSPI.
Fase de Implementación	Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Evidencias de la realización e implementación de las actividades descritas en el marco del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la SDHT Vigencias 2019 y 2020	**No Cumple** No presentó avance
	Implementación del Plan de Seguridad y Privacidad de la información	Evidencias de la realización e implementación de las actividades descritas en el marco del Plan de Seguridad y Privacidad de la Información de la SDHT Vigencias 2019 y 2020	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos

Al no planear y ejecutar correctamente los Planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información es posible y probable que no se logre la implementación completa del Modelo de Seguridad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.2 Fase de Planificación y 8.3 Fase de Implementación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.

Observación N°7. Ausencia del Plan de Control Operacional.

El plan de Control Operacional establece las actividades para la implementación de los requisitos, controles y buenas prácticas de seguridad de la información y hace parte de la Fase de Implementación del Modelo de Seguridad de la Información (MSPI). Actualmente la SDHT no cuenta con un plan de control operacional por lo cual la implementación del Modelo no ha sido completa.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Implementación	Planificación y Control Operacional	Plan de control operacional de seguridad de la información en la SDHT Vigencia 2019 y 2020	**No Cumple** No presentó avance
		Copia del acta de aprobación por parte de la alta dirección del Plan de control operacional de seguridad de la información en la SDHT Vigencia 2019 y 2020.	**No Cumple** No presentó avance
		Evidencias de la implementación de las actividades descritas en el Plan de Control operacional de las vigencias 2019 y 2020	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos
El no contar con una estrategia de planificación y control operacional impide que el Modelo de Seguridad de la Información sea implementado en su totalidad en la entidad.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.3 Fase de Implementación.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.

Observación N°8. Ausencia de Plan de revisión y seguimiento a la implementación del MSPI.

Se evidenció que el Proceso de Gestión Tecnológica no cuenta con el Plan de Revisión y Seguimiento a la Implementación del MSPI de la Fase de Evaluación y Desempeño, este plan debe contemplar la revisión de los controles establecidos, la revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles, seguimiento al alcance e implementación del MSPI, seguimiento a los incidentes de seguridad de la información al interior de la entidad y seguimiento a los indicadores de gestión del MSPI.

En resumen, se observó lo siguiente:

Fase	Criterio	Entregable	Estado
Fase de Evaluación y Desempeño	Plan de Revisión y Seguimiento a la Implementación del MSPI	Plan de seguimiento, mejoramiento continuo y revisión de la implementación del MSPI en la SDHT Vigencia 2019 y 2020.	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos

El no contar con un plan de revisión y seguimiento a la implementación del MSPI genera problemas para medir y evaluar el desempeño del sistema contra la política.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 29 de Julio de 2016 – 8.4 Fase de Evaluación y Desempeño.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía No.16 de Evaluación del Desempeño Versión 1 del 16 de febrero de 2017 del Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Observación No.9 Incumplimiento en la realización y ejecución de las acciones de mejoramiento PMI 147, PMI 148, PMI 149 y PMI 150 correspondientes a la Auditoria de Seguridad de la Información año 2018

En el año 2018 se desarrolló por parte de Control Interno una auditoría de la implementación del Modelo de Seguridad de la Información, a partir de la misma se generaron las acciones de mejora: PMI 147, PMI 148, PMI 149 y PMI 150 del Plan de Mejoramiento Institucional. Estas acciones tenían inicialmente como fecha de cierre el 31 de diciembre de 2018. Dado que estas acciones no fueron finalizadas en la fecha acordada, el 22 de marzo de 2019 se realizó una reunión entre la Subdirección Administrativa y Control Interno donde se levantó un acta con el fin de realizar un seguimiento oportuno y concreto para cada una de las acciones. Desde esa fecha hasta el momento el Proceso de Gestión Tecnológica no ha cerrado completamente dichas acciones de mejora y las cuales se reiteran en la presente auditoría. Esto también constituye un incumplimiento a la Fase de Mejora Continua del Modelo de Seguridad de la Información (MSPI).

En resumen, se observó lo siguiente:

PMI	Avance Corte Octubre 2020	Fase	Acción	Estado
PMI 147	75%	Fase de Planificación	Alinear el procedimiento de Gestión Documental para articularse con el Modelo de Seguridad y Privacidad de la Información (MSPI).	**No Cumple** No presentó avance
PMI 148	25%	Fase de Implementación	Gestionar la revisión y aprobación de los documentos pertinentes a la fase de implementación	**No Cumple** No presentó avance
			Garantizar la articulación e integración de los procesos de Gestión Documental y Activos de Información de la entidad	**No Cumple** No presentó avance

PMI	Avance Corte Octubre 2020	Fase	Acción	Estado
PMI 148	25%	Fase de Implementación	Definir el documento "*Métricas e indicadores para medir el SGSI*" y validar que este se encuentre revisado y aprobado por la alta dirección (Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones y su socialización.	**No Cumple** No presentó avance
PMI 149	0%	Fase de Evaluación y Seguimiento	Elaborar el plan de auditorías y revisiones independientes al MSPI, revisado y aprobado por la alta dirección (Comité de Seguridad y de las tecnologías de la información).	**No Cumple** No presentó avance
			Presentar el plan de seguimiento y revisión del MSPI, revisado y aprobado por la alta dirección Comité de Seguridad y de las tecnologías de la información.	**No Cumple** No presentó avance
			Capacitar a todos los funcionarios y colaboradores de la entidad, frente a las medidas y procedimientos de seguridad de la información que se van a implementar.	**No Cumple** No presentó avance
PMI 150	20%	Fase de Mejora Continua	Verificar los resultados del plan de revisión y seguimiento a la implementación del MSPI.	**No Cumple** No presentó avance

PMI	Avance Corte Octubre 2020	Fase	Acción	Estado
PMI 150	20%	Fase de Mejora Continua	Analizar los resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	**No Cumple** No presentó avance
			Aplicar las lecciones aprendidas de las experiencias de seguridad de la propia entidad, tanto de los cambios internos, así como los externos del entorno y la de los incidentes ocurridos.	**No Cumple** No presentó avance
			Modificar controles e implementar las mejoras identificadas en las revisiones del SGSI, de acuerdo con las decisiones sobre los cambios requeridos para mejorar el proceso**.**	**No Cumple** No presentó avance

Análisis de los controles frente a los riesgos

El no ejecutar las acciones de mejoramiento a la implementación del Modelo de Seguridad de la Información (MSPI) puede generar retrasos en la implementación.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tienen identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación.

Por lo tanto, se recomienda establecer riesgos asociados y los puntos de control pertinentes que permita mitigar la ocurrencia del riesgo inherente.

Criterios de auditoría

- Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC Versión 3.0.2 del 26 de Julio de 2016.
- Anexo 3 Segmentación Elementos Habilitadores: Seguridad de la Información Manual de Gobierno Digital Versión 7 de abril de 2019.
- Plan de Mejoramiento Institucional SDHT.

IV. RECOMENDACIONES

1. El Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) expedirá en los próximos días una Resolución y un Anexo Técnico con la actualización de la nueva versión del Modelo de Seguridad y Privacidad de la Información MSPI, se recomienda que las acciones de mejora que sean planteadas en el marco de esta auditoría y que sean incluidas en el Plan de Mejoramiento Institucional (PMI) estén alineadas a esta nueva versión para una mejor sinergia.
2. Se recomienda que los procedimientos, formatos y manuales relacionados con el Modelo de Seguridad de la Información (MSPI) sean transversales a todos los procesos entidad y no únicamente al Proceso de Gestión Tecnológica. Como se encuentran actualmente pueden generar confusión en su diseño e implementación, ya que el proceso de Gestión Tecnológica podría llegar a ser juez y parte al mismo tiempo. Los únicos procedimientos, formatos y manuales que deben pertenecer al Proceso de Gestión Tecnológica son aquellos relacionados con Seguridad Informática.
3. Se recomienda que por medio de un acto administrativo se nombre formalmente a una persona de planta en carrera administrativa como Oficial de Seguridad de la Información de la SDHT, quien también será el Responsable de Seguridad Digital. Para no ser juez y parte, este rol debe pertenecer a un proceso diferente al de Gestión Tecnológica siguiendo la recomendación 1 y como se indica en el Manual de Gobierno Digital sección 1.6 ¿Quiénes ejecutan la política? apartado "*Responsable de Seguridad de la información*". Cabe mencionar que actualmente este rol en la SDHT es realizado por un contratista en la modalidad de contrato de prestación de servicios profesionales en el Proceso de Gestión Tecnológica. Adicionalmente se genera una interrupción de las actividades cuando se termina el contrato y se realiza la recontratación. Esta interrupción se evidenció en el primer semestre de 2020 donde no había un encargado formal del tema y no se avanzó lo suficiente en la implementación del Modelo de Seguridad de la Información (MSPI) como se observó en el marco de esta auditoría.
4. Se recomienda que en las capacitaciones que se realizan a los funcionarios y contratistas de la entidad se explique claramente la diferencia entre Seguridad de la Información, Seguridad Informática y Seguridad Digital ya que al no tener claros estos conceptos se pueden generar confusiones en los alcances y responsabilidades que cada uno tiene al interior de la entidad.
5. Se recomienda fortalecer y mantener el equipo de trabajo para la implementación de la Política de Gobierno Digital en la SDHT, incluyendo el personal necesario para implementar el Modelo de Seguridad de la Información (MSPI).
6. Se recomienda incorporar elementos de seguridad de la información, seguridad informática y seguridad digital en los diferentes sistemas de Información de la entidad, si bien este tema no fue del alcance de esta auditoría, en las auditorías específicas a los sistemas de información de la entidad se ha evidenciado que los controles no son homogéneos entre los sistemas de información, por tal razón se recomienda implementar el Dominio de Arquitectura de Seguridad del Modelo de Arquitectura Empresarial del Marco de Referencia de Arquitectura V 2.0 con los lineamientos:

    - MAE.LI.AS.01 Auditoria y Trazabilidad de Componentes de Información
    - MAE.LI.AS.02 Protección y privacidad de componentes de información
    - MAE.LI.AS.03 Seguridad y privacidad de los sistemas de información
    - MAE.LI.AS.04 Auditoría y Trazabilidad de los Sistemas de Información
    - MAE.LI.AS.05 Análisis de Riesgos
    - MAE.LI.AS.06 Seguridad Informática

EQUIPO AUDITOR

NOMBRE	TEMA AUDITADO	FIRMA
Julián Andrés Ruiz Méndez	Modelo de Seguridad de la Información MinTIC	**ORIGINAL FIRMADO**

AUDITOR LIDER

NOMBRE	FIRMA
Viviana Roció Bejarano Camargo	**ORIGINAL FIRMADO**

Para constancia se firma en Bogotá D.C., a los 11 días del mes de diciembre del año 2020.