

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Informe de Evaluación Independiente Final	Fecha de Expedición	26	11	2019
--	----------------------------	----	----	------

Proceso (s) y/o proyecto auditado:	Gestión Tecnológica / Gobierno Digital – Habilitador Transversal Arquitectura TI
Responsable proceso y/o proyecto auditado:	Subsecretaría de Gestión Corporativa y Control Interno Disciplinario
Objetivo de la Auditoría:	Evaluar el nivel de implementación de la Política de Gobierno Digital (Habilitador Transversal Arquitectura TI) en su alcance correspondiente 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 la Política de Gobierno Digital en el Habilitador Transversal de Arquitectura TI, así como al cumplimiento de las actividades y controles de los procedimientos que sean objeto de muestra de auditoría relacionados con el proceso de Gestión Tecnológica de la Secretaría Distrital del Hábitat de aquí en adelante SDHT, correspondiente a la vigencia 2018 hasta el 31 de agosto de 2019. Adicionalmente se realizará el seguimiento al nomograma del proceso auditado en cumplimiento del Plan Anual de Auditoría 2019.
Criterios de la Auditoría:	<ul style="list-style-type: none"> • Caracterización de Proceso PS05-CP01, Proceso de Gestión Tecnológica. • Decreto 415 de 2016. "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones". • 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". • 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 Gobierno Digital Versión 7 de abril de 2019. • Documentos Marco de Referencia Arquitectura TIC Colombia.
Metodología	Técnicas de auditoría basados en los métodos de observación, confrontación, revisión y comparación. De acuerdo con las normas internacionales de auditoría, la presente es una auditoría de cumplimiento legal, es decir se verificará el cumplimiento del sistema, procedimientos, registros, instructivos y demás documentos que soporten el sistema

Reunión de Apertura					Ejecución de la Auditoría					Reunión de Cierre					
Día	16	Mes	09	Año	2019	Desde	17/09/2019	Hasta	18/11/2019	Día	18	Mes	11	Año	2019
						D / M / A		D / M / A							

Representante Alta Dirección	Asesor de Control Interno	Auditor (es)
Giovanni Salgado Rubiano	Viviana Rocío Bejarano Camargo	Julián Andrés Ruiz Méndez

I. FICHA TÉCNICA

Para la ejecución de la auditoría se realizó reunión de conocimiento del área los días 18 y 20 septiembre de 2019, así mismo mediante memorandos internos, fueron realizadas las solicitudes de información con el fin de determinar la muestra y realizar el desarrollo de la auditoría como se muestra a continuación:

- ✓ Memorando interno con radicado SDHT 3-2019-07076 dirigido al Subsecretario de Gestión Corporativa y CID Giovanni Salgado Rubiano, donde se realiza la solicitud de información de los 6 dominios del Marco de Referencia de Arquitectura Empresarial: Estrategia de TI (Documentos referentes a los lineamientos LI.ES.01, LI.ES.02, LI.ES.03, LI.ES.04, LI.ES.06, LI.ES.11, LI.ES.12, LI.ES.13), Gobierno de TI (Documentos referentes a los

lineamientos LI.GO.01, LI.GO.02, LI.GO.03, LI.GO.04, LI.GO.05, LI.GO.06, LI.GO.12), Información (Documentos referentes a los lineamientos LI.INF.01, LI.INF.03, LI.INF.05, LI.INF.06, LI.INF.07, LI.INF.08), Sistemas de Información (Documentos referentes a los lineamientos LI.SIS.01, LI.SIS.02, LI.SIS.03, LI.SIS.04, LI.SIS.05, LI.SIS.12, LI.SIS.18, LI.SIS.20, LI.SIS.21, LI.SIS.22, LI.SIS.23), Servicios Tecnológicos (LI.ST.01, LI.ST.03, LI.ST.06, LI.ST.07, LI.ST.08, LI.ST.09, LI.ST.10, LI.ST.11, LI.ST.12, LI.ST.13, LI.ST.14, LI.ST.15), Uso y apropiación (LI.UA.01, LI.UA.02, LI.UA.03, LI.UA.05, LI.UA.06).

- ✓ Memorando interno con radicado SDHT 3-2019-07688 dirigido a la Subdirectora Financiera Marysol Méndez Cortés donde se realiza solicitud de información sobre el Sistema de Información JSP7.
- ✓ Memorando interno con radicado SDHT 3-2019-07689 dirigido a la Subdirectora de Información Sectorial (e) Shirley Andrea Zamora Mora donde se realiza solicitud de información sobre el Sistema de Información Portal GIS.
- ✓ Memorando interno con radicado SDHT con radicado SDHT 3-2019-07690 dirigido a la Subsecretaria de Inspección, Vigilancia y Control de Vivienda Leslie Diahann Martínez Luque donde se realiza solicitud de información sobre el Sistema de Información Portal SIDIVIC.

Finalmente, para la ejecución de las pruebas de auditoría y resolución de inquietudes se realizó una reunión con el designado por parte de los responsables el martes 29 de octubre de 2019.

NOTA IMPORTANTE: Antes de leer las observaciones, se recomienda leer la recomendación 1, en las tablas resumen finales en cada observación se dejaron los nombres de los antiguos lineamientos de acuerdo al alcance de la auditoría, pero referenciado con los entregables actualizados con base en el nuevo MRAE.

Universo:

Documentos relacionados para cada uno de los 93 lineamientos, correspondientes a los 6 dominios del Marco de Referencia de Arquitectura Empresarial, de aquí en adelante MRAE, del habilitador Arquitectura TI de la Política de Gobierno Digital de la siguiente forma:

- **Estrategia de TI:** Se encarga de apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las entidades públicas, para lograr que esté alineada con las estrategias organizacionales y sectoriales. Este dominio cuenta con 13 lineamientos definidos.
- **Gobierno de TI:** Se encarga de brindar directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector. Este dominio cuenta con 15 lineamientos definidos.
- **Información:** Se encarga de definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma. Este dominio cuenta con 15 lineamientos definidos.
- **Sistemas de Información:** Se encarga de planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución. Este dominio cuenta con 24 lineamientos definidos.
- **Servicios Tecnológicos:** Se encarga de gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones. Este dominio cuenta con 16 lineamientos definidos.
- **Uso y apropiación:** Se encarga de definir la estrategia y prácticas concretas que apoyan la adopción del MRAE que requiere la institución para implementar la Arquitectura TI. Este dominio cuenta con 10 lineamientos definidos.

Población objeto:

Documentos relacionados para cada uno de los 93 lineamientos, correspondientes a los 6 dominios del Marco de Referencia de Arquitectura Empresarial, de aquí en adelante MRAE, del habilitador Arquitectura TI de la Política de Gobierno Digital de la siguiente forma:

- **Estrategia de TI:** Se encarga de apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las entidades públicas, para lograr que esté alineada con las estrategias organizacionales y sectoriales. Este dominio cuenta con 13 lineamientos definidos.

- **Gobierno de TI:** Se encarga de brindar directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector. Este dominio cuenta con 15 lineamientos definidos.
- **Información:** Se encarga de definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma. Este dominio cuenta con 15 lineamientos definidos.
- **Sistemas de Información:** Se encarga de planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución. Este dominio cuenta con 24 lineamientos definidos.
- **Servicios Tecnológicos:** Se encarga de gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones. Este dominio cuenta con 16 lineamientos definidos.
- **Uso y apropiación:** Se encarga de definir la estrategia y prácticas concretas que apoyan la adopción del MRAE que requiere la institución para implementar la Arquitectura TI. Este dominio cuenta con 10 lineamientos definidos.

Muestra de Auditoría:

A criterio del auditor se seleccionaron **49 lineamientos, que corresponden al 52,68% de los 93 lineamientos** del MRAE, para los 6 dominios de la siguiente forma:

- **Estrategia de TI:** Se seleccionó una muestra de 8 lineamientos (LI.ES.01, LI.ES.02, LI.ES.03, LI.ES.04, LI.ES.06, LI.ES.11, LI.ES.12, LI.ES.13), que corresponden al 61.53% sobre el total de lineamientos (13) para este dominio.
- **Gobierno de TI:** Se seleccionó una muestra de 7 lineamientos (LI.GO.01, LI.GO.02, LI.GO.03, LI.GO.04, LI.GO.05, LI.GO.06, LI.GO.12), que corresponden al 46,66% sobre el total de lineamientos (15) para este dominio.
- **Información:** Se seleccionó una muestra de 6 lineamientos (LI.INF.01, LI.INF.03, LI.INF.05, LI.INF.06, LI.INF.07, LI.INF.08), que corresponden al 40% sobre el total de lineamientos (15) para este dominio.
- **Sistemas de Información:** Se seleccionó una muestra de 11 lineamientos (LI.SIS.01, LI.SIS.02, LI.SIS.03, LI.SIS.04, LI.SIS.05, LI.SIS.12, LI.SIS.18, LI.SIS.20, LI.SIS.21, LI.SIS.22, LI.SIS.23), que corresponden al 45,83% sobre el total de lineamientos (24) para este dominio.
- **Servicios Tecnológicos:** Se seleccionó una muestra de 12 lineamientos (LI.ST.01, LI.ST.03, LI.ST.06, LI.ST.07, LI.ST.08, LI.ST.09, LI.ST.10, LI.ST.11, LI.ST.12, LI.ST.13, LI.ST.14, LI.ST.15), que corresponden al 75% sobre el total de lineamientos (16) para este dominio.
- **Uso y apropiación:** Se seleccionó una muestra de 5 lineamientos (LI.UA.01, LI.UA.02, LI.UA.03, LI.UA.05, LI.UA.06), que corresponden al 50% sobre el total de lineamientos (10) para este dominio.

Por cada uno de los lineamientos seleccionados se solicitaron documentos específicos como se puede observar en el documento "Lista de Verificación".

Herramientas Utilizadas:

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

- Manual de Gobierno Digital Versión 7 de abril de 2019.
- Guía técnica G.ES.01 Guía del dominio de Estrategia TI Versión 1.2 del 17 de julio de 2017.
- Guía técnica G.ES.03 Guía del dominio de Estrategia: Definición y diseño de una política de TI Versión 1.1 del 15 de mayo de 2017.
- Guía técnica G.ES.04 Guía del dominio de Estrategia TI: Definición del catálogo de servicios de TI Versión 1.1 del 11 de julio de 2017.
- Guía técnica G.ES.06 Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI 1.0 del 30 de marzo de 2016.
- Guía Técnica G.GEN.03 Guía General de un Proceso de Arquitectura Empresarial. Versión 1.3 del 31 de Mayo de 2016.
- Guía Técnica G.GOB.01 Guía del dominio de Gobierno TI Versión 1.0 del 30 de diciembre de 2014
- Guía Técnica G.INF.01. Guía básica del dominio de Información Versión 1.0 del 30 de diciembre de 2014

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

- Guía Técnica G.INF.07 Guía como construir el catálogo de Componentes de Información Versión 1.0 del 21 de diciembre de 2016.
- Guía Técnica G.SIS.01 Guía del dominio de Sistemas de Información Versión 1.0 del 30 de diciembre de 2014.
- Guía Técnica G.SIS.02 Guía Técnica de Sistemas de Información – Trazabilidad Versión 1.0 del 30 de diciembre de 2014.
- Guía Técnica G.SIS.03 Guía para la construcción del catálogo de Sistemas de Información Versión 1.0 del 6 de Julio de 2018.
- Guía Técnica G.ST.01 Guía del dominio de Servicios Tecnológicos Versión 1.0 del 30 de diciembre de 2014.
- Guía Técnica G.UA.01 Guía del dominio de Uso y Apropiación Versión 1.0 del 30 de diciembre de 2014.
- Requerimientos para obtener el sello de excelencia en la categoría de capacidades de gestión de TI.

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 auditoría, así como la atención, importancia y respeto hacia el auditor.
- ✓ Se entregó la información solicitada por parte de la Subsecretaría de Gestión Corporativa y CID para la presente auditoría en los plazos establecidos.
- ✓ Se evidenció que la entidad a través de la Resolución Interna 874 de 2018 y ya se tiene institucionalizado y estableció el Comité Institucional de Gestión y Desempeño donde existe un Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones donde ha sido presentado el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) y ha sido aprobado.
- ✓ Se resalta el esfuerzo en cuanto a la actualización de los procedimientos que hacen parte del Proceso de Gestión de Tecnologías.
- ✓ Se evidenció que el área tiene conocimiento en el aplicativo FOREST y genera capacitaciones permanentes sobre el mismo al interior de la entidad.

III. RESULTADOS DE LA AUDITORÍA

Observación N°1. Inconsistencias, debilidades y deficiencias en el documento Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC)

Esta observación consolida la evaluación de los siguientes lineamientos:

- Entendimiento Estratégico (LI.ES.01)
- Evaluación de la gestión de la estrategia de TI (LI.ES.12)
- Tablero de Indicadores (LI.ES.13)

Se evidenció que el Proceso de Gestión de Tecnología tiene 2 Planes Estratégicos de Tecnologías de la Información: uno aprobado bajo el nombre Plan Estratégico de Tecnologías de la Información (PETI) según el acta No.4 del Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones del 17 de diciembre de 2018 y el cual no tiene registro oficial en el Sistema Integrado de Gestión (SIG) ni alineado a las Tablas de Retención documental y el otro denominado Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) el cual hace parte del Plan de Acción SDHT 2019 Versión 4 de Mayo de 2019. Si bien ambos documentos tienen varios elementos en común, al comparar los dos documentos no dicen lo mismo y no tienen la misma estructura, siendo el PETIC incluido en el Plan de acción una versión simplificada, resumida e incompleta que no permite al lector abordar o entender de forma completa la estrategia de TI que va a implementar la SDHT. Un ejemplo de esta situación se evidenció en el Portafolio de Proyectos del PETI donde aparecen 19 proyectos, mientras que en el PETIC incluido en el Plan de Acción aparecen 20 proyectos, el proyecto agregado en el PETIC fue el de la Auditoría al Sistema Integral de Vivienda Efectiva – SIPIVE, sin que exista una justificación clara del porque este proyecto fue agregado en el Plan de Acción 2019 al PETIC y sin la aprobación del Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones.

Se precisa que en el Decreto 612 de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, el Departamento Administrativo de la Función Pública – DAFP aclaró lo siguiente: ***“el decreto no pretende agrupar instrumentos ni metodologías para la formulación de los diferentes planes, solamente unifica su fecha de presentación y su propósito es orientar a las entidades a que de manera articulada definan todo lo necesario para hacia la consecución de los objetivos y metas institucionales, de modo tal que los responsables puedan desagregar cada uno de los temas en rutas de acción detalladas, de forma articulada y orientada al direccionamiento estratégico de la entidad”***.¹ Por lo que independiente de la alineación del PETIC con el Plan de Acción a 31 de enero de cada año, debe existir un documento PETIC independiente y formalizado que cumpla con los criterios dados en la nueva Guía Técnica G.ES.06 Guía para la Construcción del PETI – Planeación de la Tecnología para la Transformación Digital de Julio de 2019 expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Entrando en el contenido del PETI, se evidenció que la situación actual para la percepción de TI estuvo basada en pruebas de vulnerabilidades, diagnósticos de la norma ISO 27001 realizados previamente y enfocados principalmente a aspectos relacionados con Seguridad de la Información. Para el análisis de la situación actual, se dejaron de revisar y analizar aspectos importantes relacionados con la arquitectura de negocio, el plan estratégico institucional actual y los servicios y trámites de la SDHT; para así orientar el PETI hacia la generación de valor público ciudadano. Es importante separar los aspectos de Seguridad Digital, Seguridad Informática y Seguridad de la Información en los diferentes planes de la entidad como lo son el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Adicionalmente de los 19 proyectos listados en el Portafolio de Proyectos de TI: 13 proyectos corresponden al dominio de Servicios Tecnológicos (68,42%), 5 proyectos al dominio de Sistemas de Información (26,31%) y 1 proyecto al dominio de Información (5,27%). No se encontraron proyectos relacionados con los dominios de Estrategia de TI (0%), Gobierno de TI (0%) y Uso y apropiación (0%). Si bien los servicios tecnológicos son el fundamento y la base de la Arquitectura de TI de cualquier entidad, no se pueden enfocar todos los esfuerzos en este dominio, se deben crear proyectos específicos para los dominios no contemplados.

No se observó una clara alineación de TI con los procesos de la SDHT, un mapa de ruta o un plan maestro definido que permita identificar los hitos más importantes para la evolución de las tecnologías de la información en la SDHT. Adicionalmente se

carece de un modelo operativo, un modelo de planeación con la estructura de las actividades estratégicas, el plan maestro, el presupuesto, el plan de intervención de los sistemas de información, el plan de proyectos de servicios tecnológicos, el plan del proyecto de inversión; que a su vez estos contengan una matriz de indicadores que estén relacionados directamente con los objetivos y metas establecidos en el PETI y que permita la generación de un tablero de control de TI. Para evaluar los lineamientos LI.ES.12 y LI.ES.13, el Proceso de Gestión Tecnológica mencionó que para la vigencia 2018 no se definió una Matriz de indicadores directamente relacionados con los objetivos y metas establecidos en el PETI y tampoco se definió un Tablero de control de TI relacionado con el PETI.

Se evidenció que no existe un proceso o procedimiento formalizado dentro del Sistema Integrado de Gestión (SIG) que permita realizar la formulación, el diseño y concepción de la estrategia de TI en la SDHT, a través de un entendimiento estratégico, que como resultado entregue un Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI).

En resumen, se observó lo siguiente:

Lineamiento	Estado	Entregable Nuevo MRAE
Entendimiento Estratégico (LI.ES.01)	No cumple	Estrategia de TI en PETI
Evaluación de la gestión de la estrategia de TI (LI.ES.12)	No presentó avance (No cumple)	Medición de los Indicadores de logro definidos en la estrategia de TI y planes de acción asociados a las mediciones por fuera de los rangos aceptables
Tablero de Indicadores (LI.ES.13)	No presentó avance (No cumple)	Tablero de Indicadores de TI

Análisis de los controles frente a los riesgos

El posible riesgo identificado que se puede ocasionar desalineación entre la misionalidad frente a las inversiones de tecnología. Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

MRAE: G.ES.06 Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI 1.0 del 30 de marzo de 2016 y Guía técnica G.ES.01 Guía del dominio de Estrategia TI Versión 1.2 del 17 de julio de 2017.

Observación N°2. Ausencia de una Arquitectura Empresarial Actual, Arquitectura Empresarial Objetivo y documentación de Arquitecturas de Transición

Esta observación consolida la evaluación de los siguientes lineamientos:

- Definición de la arquitectura empresarial (LI.ES.02)
- Mapa de Ruta de la Arquitectura Empresarial (LI.ES.03)
- Proceso para evaluar y mantener la arquitectura empresarial (LI.ES.04)

El proceso de Gestión Tecnológica remitió el Plan y Estrategia de Transición de IPV4 a IPV6, PS05-IN06 Instructivo para definir arquitectura de software V1, Plan de continuidad de negocio SDHT, carpeta Reuniones con encuestas de implementación de la política digital diligenciada por los responsables de SIPI, Habitaten Cifras, SIDEC y base de datos geográfica y carpeta de Arquitectura de referencia de SW con actas y listados de asistencia a 3 reuniones donde se explica la Política de Gobierno Digital y MSPi y se diligencia la encuesta sobre principios y servicios ciudadanos; si bien estos documentos pueden ser parte de un proceso de identificación para la realización de un ejercicio de Arquitectura Empresarial, no están directamente relacionados y no corresponden a lo solicitado por el auditor, el único documento relacionado es el Instructivo PS05-IN06 para

¹ <https://bit.ly/2JMouWp>

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

definir arquitectura de software V1, el cual se encontró que está formalizado en el Sistema Integrado de gestión (SIG), más sin embargo se evidenció que no es aplicado por las áreas responsables de los sistemas de información y no corresponde a una arquitectura objetivo para el dominio de Sistemas de Información.

En resumen, se encontró lo siguiente:

Lineamiento	Estado	Entregable Nuevo MRAE
Definición de la arquitectura empresarial (LI.ES.02)	No cumple	Documento de Arquitectura Empresarial en donde describa la arquitectura objetivo para cada uno de los dominios.
Mapa de ruta de la arquitectura empresarial (LI.ES.03)	No cumple	Hoja de ruta de Arquitectura Empresarial
Proceso para evaluar y mantener la arquitectura empresarial (LI.ES.04)	No cumple	Proceso o procedimiento de arquitectura empresarial aprobado e implementado.

Análisis de los controles frente a los riesgos

El posible riesgo identificado que se puede ocasionar desalineación entre la misionalidad frente a las inversiones de tecnología. Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

G.GEN.03 Guía General de un Proceso de Arquitectura Empresarial del 31 de mayo de 2016.

Observación N° 3. Incumplimiento de los requisitos en el Catálogo de Servicios de TI y en las Políticas y Estándares para la gestión y gobernabilidad de TI

Esta observación consolida la evaluación de los siguientes lineamientos:

- Políticas y estándares para la gestión y gobernabilidad de TI (LI.ES.06)
- Catálogo de servicios de TI (LI.ES.11)

En el marco del LI.ES.06, se evidenció que la SDHT tiene el Manual de Políticas del Subsistema de Gestión de Seguridad de la Información adoptado bajo el código PS05-MM13 Versión 4 del 26 de septiembre de 2018 en el SIG. En este manual se observa la política general de seguridad de la información y 20 políticas específicas. Se encuentra que todas las políticas hacen parte del MSPI, sin embargo, no hay políticas relacionadas con los dominios del MRAE, como son: gestión de la información, adquisición tecnológica, desarrollo e implementación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios.

También para LI.ES.11, se evidenció el Catálogo de Servicios de la SDHT con fecha 30 de mayo de 2018, donde se evidencian 13 servicios. Para cada servicio se describe su nombre, descripción, objetivo, característica del servicio, alcance del servicio, canal de prestación, beneficiario e indicador. No obstante, el catálogo de servicios no cumple con los criterios de calidad y no contiene todos los elementos descritos en la Guía Técnica G.ES.04 Guía del dominio de Estrategia TI- Definición del catálogo de servicios de TI del 11 de julio de 2017.

En resumen, se encontró lo siguiente:

Lineamiento	Estado	Entregable Nuevo MRAE
Políticas y estándares para la gestión y gobernabilidad de TI (LI.ES.06)	Parcialmente cumple	Catálogo de Servicios de TI
Catálogo de servicios de TI (LI.ES.11)	Parcialmente cumple	Políticas de TI

Análisis de los controles frente a los riesgos

El posible riesgo identificado que se puede ocasionar debilidades en el proceso de contratación de tecnología y aumento de los casos en la mesa de servicios.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

G.ES.03 Guía para la definición y diseño de una política de TI del 15 de mayo de 2017, G.ES.04 y Guía del dominio de Estrategia TI- Definición del catálogo de servicios de TI del 11 de julio de 2017.

Observación N° 4. Falta de Gobierno de TI al interior de la SDHT

Esta observación c la evaluación de los siguientes lineamientos:

- Alineación del gobierno TI (LI.GO.01)
- Apoyo de TI a los procesos (LI.GO.02)
- Conformidad (LI.GO.03)
- Cadena de valor de TI (LI.GO.04)
- Optimización de las compras de TI (LI.GO.06)
- Evaluación del desempeño de la gestión de TI (LI.GO.12)

Respecto al dominio de Gobierno de TI, y el cumplimiento del lineamiento LI.GO.01, se evidenció que mediante la Resolución 874 del 21 de diciembre 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*"², existen varios comités que pueden apoyar la alineación del Gobierno de TI con la SDHT, como son: 1) El Comité Institucional de Gestión y Desempeño, 2) El Comité de Seguridad de la Información y de Tecnologías de la Información y las Comunicaciones y 3) El Comité de Transparencia, Antitrámites y de Gobierno Digital. Dada la gran cantidad de comités e instancias implementadas en la SDHT, puede generar desarticulación y por lo tanto debilidades en lo relacionado con la dirección, evaluación y monitoreo eficiente de las TI dentro de la SDHT.

Adicionalmente para el cumplimiento del lineamiento LI.GO.02, no se pudo evidenciar el resultado completo del ejercicio de consolidación de proyectos para el PETIC 2020, solo se observó una matriz de Excel con una pestaña llamada "Proyectos 2019" donde hay 17 proyectos identificados por un valor total de \$2.495.400.105, donde 9 aparecen como si ejecutados (52,94%) y 6 de ellos como no ejecutados (35,29%) y de estos 3 se piensan contratar en noviembre de 2019. La otra pestaña se llama "Cronograma" y hay 11 proyectos referenciados en una tabla sin más información.

² <https://bit.ly/2Q1PpGx>

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Para el cumplimiento del lineamiento LI.G.O.03, se entregó copia del Contrato de Prestación de Servicios No.477 de 2019 con fecha del 26 de Junio de 2019, cuyo objeto es "Implementar los módulos necesarios en el sistema de información JSP7 que permitan la articulación de las herramientas de planeación institucional con la actividad contractual" por valor de \$59'500,000, este documento no corresponde al entregable solicitado "Plan de Automatización" o " Plan de acción y evidencias de seguimiento de acciones para la atención de aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo".

En el marco del lineamiento LI.G.O.04, de acuerdo con la información remitida, no se evidenció cadena de valor de TI.

Para el lineamiento LI.G.O.06 se encontró que la SDHT cumple y hace uso de los Acuerdos Marco de Precio de Colombia Compra Eficiente con 4 órdenes de compra principalmente enfocados a la contratación de servicios de alojamiento de la infraestructura tecnológica en un centro de datos para la SDHT, prestar los servicios de conectividad para la SDHT, adquisición de productos Microsoft y Adquisición de computadores y periféricos.

En el lineamiento LI.G.O.12 se encontró que se cumple ya que se tienen los anexos técnicos junto con los Acuerdos de Niveles de Servicios (ANS) para las 4 órdenes de compra realizadas por la SDHT por Colombia Compra Eficiente.

Lineamiento	Estado	Entregable Nuevo MRAE
Alineación del gobierno TI (LI.G.O.01)	Parcialmente cumple	Esquema de Gobierno de TI, alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión (MIPG), que estructure y direcciona el flujo de las decisiones de TI. El esquema de Gobierno de TI deberá identificar los roles, los procesos y los recursos necesarios para habilitar las capacidades de TI.
Apoyo de TI a los procesos (LI.G.O.02)	Parcialmente cumple	Catálogo de hallazgos asociados a los procesos de la entidad.
Conformidad (LI.G.O.03)	No cumple	Plan de acción y evidencias de seguimiento de acciones para la atención de aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo.
Cadena de valor de TI (LI.G.O.04)	Parcialmente cumple	Estructurar e implementar un macroproceso de gestión de TI.
Optimización de las compras de TI (LI.G.O.06)	Cumple	Órdenes de compra realizadas.
Evaluación del desempeño de la gestión de TI (LI.G.O.12)	Cumple	Resultados de las encuestas para medir la gestión de TI a nivel interno de la entidad y uso de los ANS de Colombia Compra Eficiente.

Análisis de los controles frente a los riesgos

El posible riesgo identificado puede conllevar a un fenómeno conocido como "Anarquía de TI", lo que dificulta tener un Gobierno de TI.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

Criterio de auditoría

G.G.O.B.01 Guía del dominio de Gobierno TI 30 de diciembre de 2014

Observación N° 5. Incompatibilidad de las funciones del Equipo de TI con la Política de Gobierno Digital

Esta observación consolidada la evaluación del lineamiento Capacidades y recursos de TI (LI.G.O.05).

Se observó que en el PETI aparece una organización propuesta para el área de Gestión Tecnológica, sin embargo, esta propuesta deja en cabeza del rol de Gestión de Seguridad de TI los temas relacionados con Gobierno en Línea ahora Política de Gobierno Digital, mientras que los demás roles tienen temas relacionados con la política de Gobierno Digital y el MRAE, pero no están de forma explícita. Adicionalmente se informó que en otras áreas de la entidad existen Ingenieros que realizan labores técnicas sobre los Sistemas de Información, pero de forma autónoma y desarticulada del proceso de Gestión Tecnológica. Solo hay articulación cuando se deben disponer de los servicios tecnológicos o de infraestructura para desplegar los sistemas de información o bases de datos.



Ilustración 4, organización propuesta para el desarrollo de las actividades del área de gestión tecnológica.

Imagen extraída del PETI Página 12

Se revisaron los contratos y los 3 últimos informes de actividades de los 7 contratistas que actualmente apoyan el Proceso de Gestión Tecnológica

- Las obligaciones en cada uno de los contratos no están alineadas con los roles definidos en las guías de MRAE.
- No existe un contratista, profesional o rol que apoye las labores de Estrategia de TI y Gobierno de TI.
- Es importante que el rol de Administración de aplicativos y bases de datos sea separado, dada la especialidad exigida por el MRAE en los dominios de Información y Sistemas de Información.
- Las funciones no están alineadas con lo descrito en el Decreto 415 de 2016
- Las obligaciones están relacionadas con soporte técnico preventivo y correctivo.
- Se recomienda personas independientes que realicen las labores de la mesa de servicios de TI.

En resumen:

Lineamiento	Estado	Entregable Nuevo MRAE
Capacidades y recursos de TI (LI.G.O.05)	Parcialmente cumple	Mapa de Capacidades de TI.

Análisis de los controles frente a los riesgos

El posible riesgo identificado puede ocasionar falta de capacidades y recursos de TI apropiados para apalancar el MRAE.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

Criterio de auditoría

G.GOB.01 Guía del dominio de Gobierno TI 30 de diciembre de 2014

Observación N° 6. Ausencia de Arquitectura de Información y de criterios unificados para la Gestión de Información al Interior de la SDHT

Esta observación consolida la evaluación de los siguientes lineamientos:

- Responsabilidad y gestión de componentes de información (LI.INF.01)
- Gobierno de la Arquitectura de Información (LI.INF.03)
- Definición y caracterización de la información Georreferenciada (LI.INF.05)
- Lenguaje común de intercambio de los componentes de Información (LI.INF.06)
- Directorio de servicios de los componentes de información (LI.INF.07)
- Publicación de los servicios de intercambio de componentes de información (LI.INF.08)

Respecto al lineamiento LI.INF.01 se observó que la SDHT no tiene una estrategia unificada de gestión de la información, tampoco existe un responsable de este tema y no se observó un portafolio de proyectos para la gestión de información.

Para el lineamiento LI.INF.03 se observó que la SDHT tiene: Formato PG 04-F0561 la cual es una matriz para la creación, actualización y eliminación de usuarios de la base de datos geográfica y recursos SIG SDHT, Formato PG 04-F0562 Registro de Copia de Seguridad de la Base de datos Geográfica de SDHT, Modelo Entidad Relación para las áreas de la SDHT, Formato PG 04-F0554 Acuerdo de confidencialidad y buen uso de la información de la SDHT y el procedimiento PG 04-PR09 para la administración, actualización y mantenimiento de la Base de datos geográfica y empresarial de la SDHT. Si bien estos documentos permiten evidenciar que se avanza en una Arquitectura de Información para los datos geográficos de la SDHT, no contempla todos los datos e información que gestiona la SDHT.

En el lineamiento LI.INF.05 se evidenció que se tiene un catálogo con información georreferenciada y cumple los criterios de identificación de la información georreferenciada.

Para los lineamientos LI.INF.06, LI.INF.07 y LI.INF.08 el Proceso de Gestión Tecnológica no entregó información, por lo que no cumple con los criterios dados en el MRAE.

En resumen:

Lineamiento	Estado	Entregable Nuevo MRAE
Responsabilidad y gestión de componentes de información (LI.INF.01)	No presentó avance (No cumple)	Matriz CRUD de entidades de información vs Sistemas de Información y Matriz CRUD de entidades de información vs Procesos
Gobierno de la Arquitectura de Información (LI.INF.03)	Parcialmente cumple	Documento con la definición de arquitectura de información. Vistas de la Arquitectura de Información. Vista de Gobierno de Arquitectura de Información.
Definición y caracterización de la información Georreferenciada (LI.INF.05)	Cumple	Catálogo de componente de información identificando información georreferenciada
Lenguaje común de intercambio de los componentes de Información (LI.INF.06)	No presentó avance (No cumple)	Servicios web publicados en el directorio de servicios de Intercambio de Información del MINTIC. Certificación Nivel 3 del Lenguaje
Directorio de servicios de los componentes de información (LI.INF.07)	No presentó avance (No cumple)	Catálogo de componentes de información.
Publicación de los servicios de intercambio de componentes de información (LI.INF.08)	No presentó avance (No cumple)	Publicación de los servicios de intercambio de Componentes de información.

Análisis de los controles frente a los riesgos

El posible riesgo identificado puede ocasionar duplicidad de información.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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

G.INF.01 Guía Técnica Básica de Información y G.INF.07 Guía Cómo construir el catálogo de Componentes de Información.

Observación N° 7. Ausencia de una Arquitectura de Sistemas de Información y criterios unificados para la gestión de los Sistemas de Información

Esta observación consolida la evaluación de los siguientes lineamientos:

- Definición estratégica de los sistemas de Información (LI.SIS.01)
- Catálogo o Directorio de sistemas de información (LI.SIS.02)
- Arquitecturas de referencia de sistemas de Información (LI.SIS.03)
- Arquitecturas de solución de sistemas de Información (LI.SIS.04)
- Metodología de referencia para el desarrollo de sistemas de información (LI.SIS.05)

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

- Análisis de requerimientos de los sistemas de Información (LI.SIS.12)
- Estrategia de mantenimiento de los sistemas de Información (LI.SIS.18)
- Plan de calidad de los sistemas de información (LI.SIS.20)
- Criterios no funcionales y de calidad de los sistemas de información (LI.SIS.21)
- Seguridad y privacidad de los sistemas de Información (LI.SIS.22)
- Auditoría y trazabilidad de los sistemas de Información (LI.SIS.23)

Para los lineamientos LI.SIS.01, LI.SIS.03, LI.SIS.20, LI.SIS.23 el Proceso de Gestión Tecnológica no presentó soportes.

Para el lineamiento LI.SIS.02 se evidenció que el Proceso de Gestión Tecnológica tiene un archivo en Excel con el listado de 13 Sistemas de Información, cual es la dependencia que lo tiene, quien es el Administrador y un número de celular para contactar al administrador. Este Directorio de Sistemas de Información no cumple con lo establecido en la Guía Técnica G.SIS.03 Guía para la construcción del catálogo de Sistemas de Información.

Para el lineamiento LI.SIS.04 se observó la siguiente información para cada Sistema de Información:

Sistema de Información	Información Entregada
Aula Virtual	Manual de administradores, Manual de Instalación Moodle, Manual para usuario, Proceso de Migración, Pruebas de migración de infraestructura.
Forest	Manual de operación Forest BPM S.
Habitapp	Documento Análisis de Habitapp, Documento de diseño de Habitapp, Acta de Reunión de presentación primer prototipo Habitapp, Documento de Instalación de la Aplicación Habitapp.
Hábitat a la Vista	Manual de Instalación SIDIVIC y Hábitat a la Vista (Geovisor Web), Manual del usuario de Hábitat a la Vista.
Hábitat en Cifras	Documento de Arquitectura de Alto nivel, Manual de trabajo operativo Hábitat en Cifras, Manual de Usuario Componente Estadístico de SIHAB, Manual Técnico Componente Estadístico del SIHAB, Matriz de Excel de objetos del bus dimensional, Documento de diseño de la Bodega de datos de SIHAB.
Intranet	Diagrama de base de datos de Drupal 8 y Información y manuales de drupal 8.
JSP7 (ERP)	La información es confidencial ya que es un sistema propietario.
Mesa de Ayuda GLPI	Manual de GLPI Versión 0.85.
PortalGIS	Catálogo de Objetos Geográficos Mapa de Referencia para el Distrito Capital, Matriz con Documentación del Catálogo de Objetos Geográficos de la Secretaría Distrital del Hábitat, Instructivo para la Catalogación de Objetos Geográficos del UA ECD, Formato PG 04-F0561 la cual es una matriz para la creación, actualización y eliminación de usuarios de la base de datos geográfica y recursos SIG SDHT, Formato PG 04-F0562 Registro de Copia de Seguridad de la Base de datos Geográfica de SDHT, Modelo Entidad Relación para las áreas de la SDHT, Formato PG 04-F0554 Acuerdo de confidencialidad y buen uso de la información de la SDHT y el procedimiento PG 04-PR09 para la administración.
SIDEC	Documento general Aplicativo SIDEC (Sistema de Información de Declaratorias), Documento con descripción general de la Arquitectura y lineamientos técnicos, Manual de instalación y configuración de aplicativo SIDEC, Manual de usuario aplicativo SIDEC, Diagrama entidad relación de SIDEC.
SIDIVIC	Manual de Instalación de SIDIVIC, Manual de Usuario de SIDIVIC 2, PM 05-MM34 Manual del Sistema de Información Distrital de Inspección, Vigilancia y Control de Vivienda SIDIVIC, Especificación de casos de uso.
SIPI	Arquitectura de SIPI V1 y Manual Técnico de Instalación SIPI.
SIPIVE	Documentación detallada de: 1. Inventario de servicios, 2. Diagrama de despliegue físico, 4. Guía de Estilo y Usabilidad, 5. Estándar de codificación del lenguaje, 6. Estándar de normalización de la base de datos, 7. Patron de diseño, 9. Documento de Arquitectura de la Solución, 11. Diagrama de componentes, 13. Modelo de datos, 14. Diccionario de datos, 16. Diagrama de servicios transversales, 18. Metodología de referencia, 19. Metodología de análisis y levantamiento de requerimientos, 20. Documento de especificaciones

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

	funcionales, 21.Documento de especificaciones no funcionales, 22.Documentación de los procesos de gestión del cambio.
VUC	Casos de uso, Código Fuente, Diseño, Arquitectura VUC, Diseño Técnico, Manual de Administrador, Manual VUC Ciudadano, Manual VUC Funcionarios, Modelo de datos, Modelo Entidad Relación.
VUC Website	Código Fuente, Glosario, Service classes and features, Documentación Drupal 7, Arquitectura Drupal7.
Web Histórico	Arquitectura Joomla, Guía de desarrollo Joomla, Joomla Guía de Desarrollo, Modelo Entidad Relación.
Web Histórico II	Arquitectura Joomla, Guía de desarrollo Joomla, Joomla Guía de Desarrollo, Modelo Entidad Relación.
Website	Diagrama bases de datos drupal7, Drupal7 Architecture, Tecnologías web utilizadas.

Como se puede observar para todos los sistemas de información de la SDHT la información no es homogénea, el sistema de información que tiene la información más completa es SIPIVE.

Para el lineamiento LI.SIS.05 se observaron documentos relacionados con la metodología de referencia utilizada para el mantenimiento del sistema de información SIPIVE y las guías de desarrollo de Joomla para el histórico de la página web, no obstante, la SDHT carece de una metodología de referencia para el desarrollo de Sistemas de Información.

En el lineamiento LI.SIS.12 se evidenció que el Sistema de Información SIPIVE realizó el levantamiento de requerimientos con base en el proceso Instrumentos de financiación para el acceso a la vivienda. No obstante, la SDHT carece de un Proceso claro de especificación de requerimientos donde se realice la identificación, la especificación, la validación y aprobación de los requerimientos para todos los sistemas de información de la SDHT.

Para el lineamiento LI.SIS.18 se observó que existe un procedimiento de gestión de cambios para el sistema de información SIPIVE utilizando GIT y GITHUB, sin embargo, no se evidenció que exista un procedimiento de gestión de cambios que sea común para todos los sistemas de información de la SDHT.

En el lineamiento LI.SIS.20 y para el lineamiento LI.SIS.23 se requieren tener para cada sistema de Información no se remitió información.

Para el lineamiento LI.SIS.21 se observó la identificación de Requerimientos no funcionales para el sistema de información SIPIVE, no obstante, no todos los Sistemas de Información de la SDHT tienen identificados los requerimientos no funcionales.

Para el lineamiento LI.SIS.22 se observó un diagrama de alto nivel de los servicios web, pero no se identificó el Sistema de Información pertenece este diagrama.

En resumen:

Lineamiento	Estado	Entregable Nuevo MRAE
Definición estratégica de los sistemas de Información (LI.SIS.01)	No presentó avance (No cumple)	Documentos de Arquitecturas de Software.
Catálogo o Directorio de sistemas de información (LI.SIS.02)	No cumple	Catálogo de sistemas de información.
Arquitecturas de referencia de sistemas de Información (LI.SIS.03)	No presentó avance (No cumple)	Documento con la definición de arquitectura de sistemas de información.
Arquitecturas de solución de sistemas de Información (LI.SIS.04)	Parcialmente cumple	Documentos de Arquitecturas de Solución.
Metodología de referencia para el desarrollo de sistemas de información (LI.SIS.05)	No cumple	Proceso de desarrollo de software
Análisis de requerimientos de los sistemas de Información (LI.SIS.12)	No cumple	Proceso de especificación de requerimientos en donde se realice

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

		la identificación, la especificación, la validación y aprobación de los requerimientos
Estrategia de mantenimiento de los sistemas de Información (LI.SIS.18)	No cumple	Proceso documentado y formalizado de gestión de cambios.
Plan de calidad de los sistemas de información (LI.SIS.20)	No presentó avance (No cumple)	Plan de Calidad.
Criterios no funcionales y de calidad de los sistemas de información (LI.SIS.21)	No cumple	Documentación de los requerimientos no funcionales de los sistemas de información de la entidad y la forma en la que se garantizan.
Seguridad y privacidad de los sistemas de Información (LI.SIS.22)	No cumple	Riesgos asociados a las aplicaciones.
Auditoría y trazabilidad de los sistemas de Información (LI.SIS.23)	No presentó avance (No cumple)	Mecanismos de auditoría y trazabilidad en las aplicaciones

Análisis de los controles frente a los riesgos

El posible riesgo identificado puede ocasionar sobrecostos, debilidades en la seguridad de los sistemas de información.

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene 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: G.SIS.01 Guía del dominio de Sistemas de Información y G.SIS.03 Guía para la construcción del catálogo de Sistemas de Información.

Observación N° 8. Debilidades en los Servicios Tecnológicos – Infraestructura Tecnológica

Esta observación consolida la evaluación de los siguientes lineamientos:

- Directorio de servicios tecnológicos (LI.ST.01)
- Gestión de los Servicios tecnológicos (LI.ST.03)
- Alta disponibilidad de los Servicios tecnológicos (LI.ST.06)
- Capacidad de los Servicios tecnológicos (LI.ST.07)
- Acuerdos de Nivel de Servicios (LI.ST.08)
- Mesa de servicio (LI.ST.09)
- Planes de mantenimiento (LI.ST.10)
- Control de consumo de los recursos compartidos por Servicios tecnológicos (LI.ST.11)
- Gestión preventiva de los Servicios tecnológicos (LI.ST.12) (Este lineamiento fue eliminado)
- Respaldo y recuperación de los Servicios Tecnológicos (LI.ST.13)
- Análisis de vulnerabilidades (LI.ST.14)
- Monitoreo de seguridad de infraestructura Tecnológica (LI.ST.15)

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Para el lineamiento LT.ST.01 se observó el Catálogo de Servicios de TI, sin embargo, se solicitó el Catálogo o Directorio de Servicios tecnológicos e infraestructura.

En el lineamiento LI.ST.03, se evidenció que el Proceso de Gestión Tecnológica manifestó que solo cumplía con la Gestión de la continuidad para lo cual entregó 3 documentos: Documento de Análisis de Impacto del negocio V1, PS05-IN56 Instructivo para definir la Arquitectura de Software y el Procedimiento PS05-PR06 para control de cambios de la Infraestructura tecnológica

Para los lineamientos LI.ST.06, LI.ST.07 y LI.ST.10 no se presentaron evidencias.

En los lineamientos LI.ST.08 y LI.ST.09 se observaron 2 documentos que son: Procedimiento PS05-PR01 de soporte técnico a usuarios y un listado con los casos atendidos; no aplica para todos los servicios tecnológicos e infraestructura tecnológica

Para los lineamientos LI.ST.11 y LI.ST.12 se observó que se tiene el Procedimiento PS05-PR20 Procedimiento de Monitoreo de los Recursos de Procesamiento y Almacenamiento de Información con el cual se anuló el Procedimiento PS05-PRS Monitoreo del uso de los medios de procesamiento de información. Si bien este procedimiento muestra que se realiza monitoreo para la solución de incidencias sobre los Sistemas de Información y/o almacenamiento, no aplica para todos los servicios tecnológicos e infraestructura tecnológica y no solo de forma reactiva sino también de forma preventiva cuando no se presentan incidencias, fallas o errores. Adicionalmente se observaron alarmas de las máquinas virtuales que pueden ayudar a complementar el procedimiento.

En el lineamiento LI.ST.13 se observó la entrega del Procedimiento PS05-PR16 de respaldo y restablecimiento de información (BACKUP) de aplicativos y/o infraestructura el cual informa el Proceso de Gestión Tecnológica se encuentra en actualización, sin embargo, se observa que cumple, se recomienda ser específico hacia la infraestructura crítica de TI.

Para el lineamiento LI.ST.14 se observó que se han realizado pruebas de ethical hacking, hay informes de seguridad, de pentesting, pruebas al firewall y verificación de correos. Se recomienda que se continúen realizando, pero con un énfasis más profundo hacia la infraestructura tecnológica.

Finalmente, para el lineamiento LI.ST.15 se observó la matriz de inventario de activos de información, el procedimiento PG03-PR06 de administración de Riesgos de gestión, corrupción y seguridad digital y el procedimiento PS05-PR05 de clasificación y etiquetado de información. No obstante, se evidenció que la infraestructura tecnológica se encuentra en la matriz de inventario de activos de información, pero no se identifican los controles que se aplican a esta infraestructura para evitar que se puedan presentar problemas de seguridad.

En resumen:

Lineamiento	Estado	Entregable Nuevo MRAE
Directorio de servicios tecnológicos (LI.ST.01)	No cumple	Documento con la definición de arquitectura de infraestructura tecnológica. Catálogo de elementos de infraestructura.
Gestión de los Servicios tecnológicos (LI.ST.03)	Parcialmente cumple	Proceso de despliegue o paso a producción.
Alta disponibilidad de los Servicios tecnológicos (LI.ST.06)	No presentó avance (No cumple)	Plan de disponibilidad.
Capacidad de los Servicios tecnológicos (LI.ST.07)	No presentó avance (No cumple)	Plan de capacidad de la infraestructura de TI.
Acuerdos de Nivel de Servicios (LI.ST.08)	Parcialmente cumple	Acuerdos de nivel de servicio firmados con los contratistas que ofrecen servicios de infraestructura de TI

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

Mesa de servicio (LI.ST.09)	Parcialmente cumple	Estructuración mesa de servicio y evidencias de las mesas de servicios.
Planes de mantenimiento (LI.ST.10)	No presentó avance (No cumple)	Cronograma de los mantenimientos planeados e Informes de los mantenimientos realizados
Control de consumo de los recursos con partidos por Servicios tecnológicos (LI.ST.11)	Parcialmente cumple	Registros de monitoreo de la infraestructura de TI
Gestión preventiva de los Servicios tecnológicos (LI.ST.12)	Parcialmente cumple	Sistemas de monitoreo de recursos tecnológicos con alertas configuradas y definición de umbrales y generación de alertas.
Respaldo y recuperación de los Servicios Tecnológicos (LI.ST.13)	Parcialmente cumple	Proceso de respaldo de la infraestructura de TI crítica
Análisis de vulnerabilidades (LI.ST.14)	Cumple	Riegos de elementos de infraestructura.
Monitoreo de seguridad de infraestructura Tecnológica (LI.ST.15)	Parcialmente cumple	Controles de seguridad.

Análisis de los controles frente a los riesgos

Frente a la matriz de riesgo del Proceso de Gestión Tecnológica se observa que relacionado con el cumplimiento del dominio auditado el riesgo asociado es:

Interrupción de los servicios, sistemas de información, telecomunicaciones y Data Center

El cual se plantea mitigar mediante los controles:

- ✓ Plan de Mantenimiento Sistema de Alimentación no Interrumpido (UPS) que proporciona el tiempo para un apagado controlado de los dispositivos tecnológicos y las estaciones de trabajo.
- ✓ Plan de mantenimiento de equipos.
- ✓ Monitoreo del Servidor físico que aloja el sistema de información (Espacio en disco, memoria, RAM, procesador y red consumida, entre otros).

Debido a lo anterior y como resultado de esta auditoria se concluye que ninguno de los cuatro (04) controles fue efectivo en su totalidad, toda vez que se generan las condiciones para materializar el riesgo identificado.

Criterios de auditoría

G.ST.01 Guía del dominio de Servicios Tecnológicos del 30 de diciembre de 2014.

Observación N° 9. Ausencia de una estrategia de Uso y Apropiación al interior de la entidad.

Esta observación consolida la evaluación de los siguientes lineamientos:

- Estrategia de Uso y Apropiación (LI.UA.01)
- Matriz de interesados (LI.UA.02)
- Involucramiento y compromiso (LI.UA.03)
- Plan de formación (LI.UA.05)
- Preparación para el cambio (LI.UA.06)

El proceso de Gestión Tecnológica indicó que no tiene información ni avances referentes a los lineamientos LI.UA.01, LI.UA.02, LI.UA.03 y LI.UA.06.

Para el lineamiento LI.UA.05 se observó que la SDHT tiene un Plan Institucional de Capacitación donde se realizan capacitaciones para el aplicativo FOREST (mayo, junio, julio y septiembre), OFFICE 365 (agosto y septiembre) y prácticas digitales (julio). Se evidencia por cada una de ellas se han realizado actividades de capacitación con los funcionarios y contratistas.

En resumen:

Lineamiento	Estado	Entregable Nuevo MRAE
Estrategia de Uso y Apropriación (LI.UA.01)	No presentó avance (No cumple)	Plan de uso y apropiación de los servicios de TI.
Matriz de interesados (LI.UA.02)	No presentó avance (No cumple)	Matriz de interesados o de grupos de interés.
Involucramiento y compromiso (LI.UA.03)	No presentó avance (No cumple)	Plan de Uso y apropiación con estrategia de sensibilización según grupo de interés.
Plan de formación (LI.UA.05)	Cumple	Cronograma con las actividades de formación programadas.
Preparación para el cambio (LI.UA.06)	No presentó avance (No cumple)	Procedimiento documentado de gestión del cambio y plan de gestión del cambio.

Análisis de los controles frente a los riesgos

Frente a la matriz de riesgo del proceso de gestión tecnológica, no se tiene identificado este riesgo y, por lo tanto, no se tienen controles para su mitigación. No obstante, en la matriz de riesgo del proceso de talento humano existe el riesgo:

Capacitación deficiente o insuficiente

El cual se plantea mitigar mediante los controles:

- ✓ Seguimiento al cumplimiento del cronograma de actividades establecido en el PIC.

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

Criterios de auditoría

G.UA.01 Guía del dominio de Uso y Apropriación del 30 de diciembre de 2014

IV. RECOMENDACIONES

1. Mientras se desarrollaba esta auditoría, el Ministerio de Tecnologías de la Información y las Comunicaciones expidió 3 nuevos documentos relacionados que son:

- **Documento Maestro del Modelo de Arquitectura Empresarial – MAE.G.GEN.01 Versión 1.0 del 31 de octubre de 2019:** Proporciona un entendimiento detallado de la estructura del Modelo de Arquitectura Empresarial, el cual debe ser implementado para mejorar las capacidades institucionales mediante el uso adecuado de las TIC y su alineamiento con las necesidades de la entidad, logrando ofrecer de esta forma mejores servicios ciudadanos y el cumplimiento de la política de Gobierno Digital en su habilitador transversal de Arquitectura. En la página 46 se encuentra la tabla de equivalencias respecto al MRAE anterior. Este documento puede ser consultado en la URL: https://www.mintic.gov.co/arquiturati/630/articulos-9401_pdf_00.pdf
- **Documento Maestro del Modelo de Gestión de Proyectos TI – MGPTI.G.GEN.01 Versión 1.0 del 31 de octubre de 2019:** Brinda orientación para administrar los proyectos de tecnologías de la información de forma adecuada y ofrecer mejores servicios a los ciudadanos cumpliendo con la política de gobierno digital. En la página 41 se encuentra la tabla de equivalencias respecto al MRAE anterior. Este documento puede ser consultado en la URL: https://www.mintic.gov.co/arquiturati/630/articulos-9401_pdf_01.pdf
- **Documento Maestro del Modelo de Gestión y Gobierno de TI – MGGTI.G.GEN.01 Versión 1.0 del 31 de octubre de 2019:** Brinda orientación para gestionar y gobernar las Tecnologías de la Información (TI) de forma adecuada y de esta forma ofrecer mejores servicios a los ciudadanos cumpliendo con la Política de Gobierno Digital. En la página 47 se encuentra la tabla de equivalencias respecto al MRAE anterior. Este documento puede ser consultado en la URL: https://www.mintic.gov.co/arquiturati/630/articulos-9401_pdf_02.pdf

Se recomienda que el plan de mejoramiento que la SDHT construya con base en los resultados de esta auditoría se realiza teniendo en cuenta estos nuevos documentos, los nuevos lineamientos y con las tablas de equivalencias de lineamientos referenciadas. Esto con el fin de generar valor en las mejoras que la entidad y alinear los nuevos enfoques y lineamientos que el Ministerio de Tecnologías de la Información y las Comunicaciones se encuentra expidiendo para fortalecer los Habilitadores Arquitectura, Servicios Ciudadanos y Seguridad de la Información. Especialmente esta recomendación aplica para las observaciones 1 y 2.

2. Para la observación 1 en el marco del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) de la SDHT, se recomienda seguir el nuevo instrumento **G.ES.06 Guía para la Construcción del PETI – Planeación de la Tecnología para la Transformación Digital de Julio de 2019 expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)**, en la que se reestructura la versión anterior de la guía, se incorpora una metodología y se actualiza el contenido para la construcción del PETI con un enfoque de Arquitectura en la planeación de la Tecnología para la Transformación Digital.
3. Verificar, revisar y fortalecer el diligenciamiento de la herramienta de autodiagnóstico de la Política de Gobierno Digital en el indicador de cumplimiento Arquitectura³, ya que según la última medición realizada de forma incompleta se encontró que la SDHT se encuentra en un nivel Medio bajo en Arquitectura con una escala entre 20 y 40 puntos.
4. Tener en cuenta los criterios dados en el "**Sello de Excelencia en Capacidades de Gestión de TI**"⁴ para los niveles 1, 2 y 3, para la elaboración del plan de mejoramiento producto de esta auditoría interna. Este sello contiene los requisitos, criterios y evidencias por cada dominio del MRAE.
5. Se recomienda a la SDHT, elaborar un **Plan de Transformación Digital**, enfocado en el fortalecimiento institucional y en la creación de una estrategia de ciudad y territorio inteligente, que contenga la hoja de ruta con los proyectos

³ <https://autodiagnosticogobdigital.gov.co/>

⁴ <https://bit.ly/2qED8wS>

INFORME DE EVALUACIÓN INDEPENDIENTE Y SEGUIMIENTO

de transformación sobre los procesos, las personas y los recursos tecnológicos, aplicando el artículo 147 del Plan Nacional de Desarrollo.

6. Se recomienda independizar los temas de Seguridad de la Información del Proceso de Gestión Tecnológica, ya que no es objetivo ser juez y parte ante estos temas, en este sentido el Proceso de Gestión Tecnológica sería el responsable y liderar la implementación de la Seguridad Informática dentro de la SDHT, mientras que otras áreas liderarían el tema de Seguridad Digital y Seguridad de la información.

7. Para la observación 2, se recomienda crear el Grupo de Trabajo de Arquitectura Empresarial en la SDHT ya que el Manual de Gobierno Digital Versión 7 de abril de 2019, en la "**Sección 1.6 ¿Quiénes ejecutan la política?**" Subsección "**Otros roles e instancias importantes**" menciona que: "*Dentro de los procesos de transformación digital de las entidades públicas, se recomienda la creación de algunas instancias técnicas, para definir y tomar decisiones operativas y técnicas con relación a la arquitectura empresarial de la entidad. Estas instancias deben actuar en coordinación con el comité institucional de gestión y desempeño para la toma de decisiones. Entre estas se encuentran: - Grupo de trabajo de Arquitectura empresarial⁵, este grupo se encarga de: "actúa como un comité técnico de arquitectura empresarial, que evalúa los impactos de cualquier decisión de inversión, adquisición o modernización de sistemas de información e infraestructura tecnológica en la entidad. Asimismo, tiene funciones de gobierno sobre la arquitectura empresarial de la entidad y debe remitirse al Comité Institucional de Gestión y Desempeño cuando se requieran tomar decisiones de alto nivel. Es importante tener en cuenta que este grupo se conforma dependiendo de la necesidad y madurez de la entidad en materia de arquitectura empresarial y **aunque es deseable, no es obligatorio**. Este grupo de trabajo de Arquitectura Empresarial debe estar conformado por el director de Tecnologías de la Información y las Comunicaciones (CIO) o quien haga sus veces, el director de planeación, profesionales encargados de las arquitecturas de sistemas de información y arquitectura de infraestructura tecnológica, el líder de gestión o información o arquitecto de información de la entidad y líderes de las áreas funcionales y de procesos cuando se requiera"*⁶.

EQUIPO AUDITOR

NOMBRE	TEMA AUDITADO	FIRMA
Julián Andrés Ruiz Méndez	Habilitador Transversal Arquitectura TI de la Política de Gobierno Digital	ORIGINAL FIRMADO

AUDITOR LIDER

NOMBRE	FIRMA
Viviana Rocio Bejarano Camargo	ORIGINAL FIRMADO

Para constancia se firma en Bogotá D.C., a los 26 días del mes de noviembre del año 2019

⁵ <https://bit.ly/2Q2fWn2>

⁶ <https://bit.ly/2Q2fWn2>