https://sigob.cartagena.gov.co/SeguimientoCorrespondencia?id=EypL9GzBYI1Kdycug6XonaVjlDLmi31IGF%2BLE7RCGu8%3D

Cartagena de Indias D. T y C., agosto 13 de 2025

Oficio **AMC-OFI-0123640-2025**

Doctores:
JOSÉ JOAQUIN POSADA ARRIETA
Secretario General (E)
CAMILO REY SABOGAL
Secretario de Planeación
ERNESTO JOSÉ ROBLES GÓMEZ
Jefe Oficina Asesora Informática

Asunto: Comunicación primer segmento de observaciones - Auditoría Especial a la Implementación del Modelo de Seguridad y Privacidad de la Información - MSPI

Cordial saludo.

Les comunico que en desarrollo de la auditoría referenciada, el equipo auditor formuló y validó las siguientes observaciones, las cuales se discriminan por procesos, así:

Oficina Asesora de Informática.

Observación 1:

En las matrices de riesgos de gestión de los procesos asociados al macroproceso Gestión Tecnología e Informática, no se evidenció la identificación de factores de riesgos, la descripción de los mismos, ni los controles diseñados para mitigar el inadecuado manejo y gestión integral de los residuos de aparatos electrónicos y eléctricos (RAEE), contrariando lo dispuesto en los artículos 2.2.7A.2.3 del Decreto 284 de 2018, 3° de la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), los controles A.8.1.3 – Uso aceptable de los activos, A.8.3.2 - Eliminación de los medios, A.11.2.7 – Eliminación segura de equipos y A.18.1.1 – Identificación de requisitos legales que se encuentran en el Anexo 1 del Modelo de Seguridad y Privacidad de la Información, Vr. 4, 2021, MINTIC, los lineamientos " Gestión Ambiental Institucional" de la política de Fortalecimiento institucional y simplificación de procesos, en lo relacionado con el " ..*Manejo de residuos*.." ; probablemente por debilidades en los controles implementados como primera línea y supervisión como segunda de defensa, generando el incumplimiento de requisitos legales y ambientales, posibles sanciones por parte de entes de control, y la afectación a la imagen institucional por prácticas no sostenibles ni seguras en la disposición de equipos electrónicos obsoletos.

Evidencias: Matrices de riesgos de gestión de los procesos asociados al macroproceso Gestión Tecnología e Informática, Procedimiento baja de activos informáticos, GTIGI04-P004, Vr. 1, 2021 y el programa de disposición final de aparatos eléctricos y electrónicos (RAEE), Vr. 1, de la Alcaldía Distrital de Cartagena de Indias.

Observación 2:

El equipo de seguridad digital de la Oficina Asesora de Informática como segunda línea de defensa, presentó debilidades en la supervisión del cumplimiento de las políticas de propiedad intelectual, toda vez que se evidenció la utilización de software (ArcGIS, AutoCAD Web y Google Earth) sin licencia vigente o suscripción para el uso institucional en la Secretaría de Infraestructura, inobservando los numerales 7 de la Circular 01 de 2000, " Orientación para el cumplimiento de la Ley 603 del año 2000, vinculada con el derecho de autor" y 6.14.2 Derechos de propiedad intelectual, responsabilidades, literal a, del Manual de política de seguridad digital, Vr. 2, 2023, de la Alcaldía Distrital de Cartagena de Indias, los controles A.12.5.1 – Controles sobre el uso del software, A.9.4.4 - Uso de privilegios restringidos, A.18.1.1 – Identificación de requisitos legales aplicables, A.18.1.2 Derechos de propiedad intelectual y A.12.6.2 Restricciones sobre el software instalado, que se encuentran en el Anexo 1 del Modelo de Seguridad y Privacidad de la Información, Vr. 4, 2021, MINTIC, así como las políticas de seguridad digital y control interno en su componente " Actividades de monitoreo" ; posiblemente por debilidades en los controles de supervisión, verificación y acompañamiento a las áreas operativas en relación con el licenciamiento de software, impidiendo garantizar los derechos de propiedad intelectual de terceros, generando posibles sanciones.

Evidencias: Cotizaciones de renovación de licencias de AutoCAD del 14/08/2024 y ArcGIS del 13/08/2024, acta de entrega y recibo a satisfacción de licencias de AutoCAD LT del 9/11/2024, oficios AMC-OFI-0110120-2024 y AMC-OFI-0112393-2024.

Observación 3:

La Alcaldía Mayor de Cartagena cuenta con el documento resultado del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), sin embargo, no se identificaron vulnerabilidades en su implementación a nivel institucional, ni se propusieron acciones de mejora para optimizar procesos y controles, incumpliéndose los lineamientos establecidos en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información, Vr. 4, 2021, MINTIC:

- *" ..Fase de Diagnóstico (p. 21): Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la entidad respecto a la Seguridad y privacidad de la Información…" .*

- *" …Salidas esperadas (p. 21): Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la entidad, y sus acciones de mejora…" .*

- *" …Fase de Mejoramiento Continuo (p. 40), numeral 10.1: Es importante que las entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI…" .*

Lo anterior, posiblemente por debilidades en la ejecución de los controles que garanticen el cumplimiento de los requisitos, a cargo de la Oficina Asesora de Informática en la fase de diagnóstico como primera línea de defensa, lo que podría ocasionar la materialización de los riesgos de disponibilidad, integridad y confidencialidad de la información.

Evidencias: Oficio AMC-OFI-0112214-2025 – Respuesta de la Oficina Asesora de Informática a la solicitud de información.

Observación 4:

La Alcaldía Mayor de Cartagena no ha formalizado mediante acto administrativo el alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), inaplicando el numeral 7.1.3 del documento maestro del MSPI, Vr. 4, 2021, MINTIC, el control A.5.1.1 Políticas para la seguridad de la información del Anexo 1 de la Resolución 500 de 2021, así como las políticas de Seguridad digital y Control interno en cuanto al componente del MECI " Actividades de Control" ; posiblemente por debilidades en la articulación entre las áreas encargadas de realizar dicha gestión, lo que afecta la adherencia del modelo y la transferencia del conocimiento entre el personal en sus diferentes niveles.

Evidencias: Oficio AMC-OFI-0112214-2025 – Respuesta de la Oficina Asesora de Informática a la solicitud de información.

Secretaría de Planeación.

Observación 5:

En los documentos Contexto interno y externo de la Alcaldía Mayor de Cartagena de Indias " *..Implementación Modelo Integrado de Planeación y Gestión, MIPG*.." , versiones 1 y 2 elaborados por el equipo MIPG de la Secretaria de Planeación Distrital, no se identificaron los factores internos y externos que permitan conocer las

características de la entidad y su entorno, para implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas del Distrito, en alineación con los objetivos estratégicos, vulnerando:

- Los numerales 2.2. de la Guía para la gestión por procesos en el marco del Modelo Integrado de Planeación y Gestión (MIPG), Vr. 1, 2020 -DAFP y, 7.1.1. del documento maestro del Modelo de Seguridad y Privacidad de la Información, Vr. 4, 2021, MINTIC.
- El artículo 25, numeral 6 del Decreto Distrital 1600 del 2024.
- El lineamiento " adelantar un diagnóstico de capacidades y entornos" de la política de Planeación institucional en lo referente a " ..*Analizar el contexto interno y externo de la entidad para la identificación de los riesgos y sus posibles causas, así como retos, tendencias y oportunidades de mejora e innovación en la gestión*…" .
- El componente del MECI " Evaluación del riesgo" de la política de Control interno en lo concerniente a " ..*partiendo del análisis del contexto interno, externo de la entidad y el del proceso, se identifican los riesgos para la consecución de sus objetivos en todos los niveles*…" .
- El esquema de líneas de defensa de la séptima dimensión Control interno.

Lo anterior, probablemente por desconocimiento de la primera línea sobre las metodologías existentes para la identificación de contextos, y por debilidades en el acompañamiento de la segunda línea de defensa (Secretaría de Planeación), limitando la capacidad para anticiparse ante amenazas, definir estrategias efectivas y tomar decisiones informadas.

Evidencia: Contexto interno y externo Alcaldía Mayor de Cartagena de Indias PTDDE01- D001 " ..*Implementación Modelo Integrado de Planeación y Gestión, MIPG, Versión 2.0*…" .

En esta observación se vincula a la Secretaría de Planeación, en su rol de primera línea de defensa, como responsable de implementar los controles necesarios para prevenir o mitigar los riesgos de incumplimiento de las disposiciones citadas, con el fin de alcanzar los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta responsabilidad se encuentra definida en las políticas de Planeación institucional y de Control Interno, bajo el esquema de líneas de defensa, así como en la Política de Administración del Riesgo, Vr. 3, 2023, de la Alcaldía Mayor de Cartagena de Indias (Tabla 1. Roles y responsabilidades para la administración del riesgo por procesos), donde se establece que dicha dependencia debe garantizar el mantenimiento efectivo de los controles internos, así como la ejecución de la gestión de riesgos y controles en el desarrollo diario de sus funciones.

Observación 6:

La Oficina Asesora de Informática como líder del proceso y primera línea de defensa presentó las siguientes debilidades en la " Caracterización de usuarios del macroproceso de tecnologías de la información y las comunicaciones" :

1. Desactualización de la caracterización de usuarios y grupos de valor, ya que, en la descripción de la metodología, se observó la aplicación de la Guía de caracterización de usuarios, ciudadanos y grupos interesados, Vr. 3, 2015, OTA y el Manual Operativo del MIPG, Vr. 3, 2019, DAFP, las cuales no corresponden a las versiones vigentes.
2. Entre los objetivos específicos definidos en el alcance no se incluyó la identificación, análisis y determinación de las necesidades o expectativas relacionadas con la implementación del Modelo de Seguridad y Privacidad de la Información-MSPI.
3. En el análisis de la información de las variables caracterizadas, no se estableció el nivel de profundidad (sector, ni segmento) detallado, de los grupos de valor por personas jurídicas para la toma de decisiones.

Lo anterior incumple:

- Los pasos 1 y 4 de la Guía de caracterización de ciudadanía y grupos de valor, Vr. 5, 2022, DAFP.
- El numeral 2.2. de la Guía para la gestión por procesos en el marco del Modelo Integrado de Planeación y Gestión (MIPG), Vr. 1, 2020, DAFP.
- El numeral 7.1.1. del documento maestro del Modelo de Seguridad y Privacidad de la Información, Vr. 4, 2021, MINTIC, así como el lineamiento " ¿Para quién y para qué lo debe hacer?" de la política de Planeación institucional en lo referente a " ..*Es necesario caracterizar, a qué grupo de ciudadanos debe dirigir sus productos y servicios (grupos de valor) y para qué lo debe hacer, es decir, cuáles son los derechos que se deben garantizar, qué necesidades se deben satisfacer, qué problemas se deben solucionar y qué información que debe suministrar*…" .
- El componente del MECI "Actividades de control" de la política de Control interno de la séptima dimensión del MIPG.

Lo anterior, posiblemente por debilidades en la implementación de los controles para la gestión del riesgo a cargo del líder del proceso como primera línea de defensa, y en la verificación y asesoría que le compete a la segunda línea de defensa (Secretaría de Planeación) para asegurar su eficiente administración, lo que impide contar con información detallada para la toma de decisiones, adecuar los servicios, mejorar las estrategias de comunicación y/o facilitar la participación ciudadana, entre otros.

Evidencias: Caracterización de usuarios macroproceso de tecnologías de la información y las comunicaciones

En esta observación se vincula a la Oficina Asesora de Informática, en su rol de primera línea de defensa, como responsable de implementar los controles necesarios para prevenir o mitigar los riesgos de incumplimiento de las disposiciones citadas, con el fin de alcanzar los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta responsabilidad se encuentra definida en la Política de Control Interno, bajo el esquema de líneas de defensa, y en la Política de Administración del Riesgo, Vr. 3, 2023, de la Alcaldía Mayor de Cartagena de Indias (Tabla 1. Roles y responsabilidades para la administración del riesgo por procesos), donde se establece que dicha dependencia debe garantizar el mantenimiento efectivo de los controles internos, así como la ejecución de la gestión de riesgos y controles en el desarrollo diario de sus funciones.

Por otra parte, se vincula a la Secretaría de Planeación, ya que, de conformidad con la política de control interno - esquema de líneas de defensa y la política distrital de Administración del riesgo, le corresponde como segunda línea de defensa monitorear, asesorar y asegurar que los controles y los procesos de gestión del riesgo diseñados por la 1ª línea de defensa sean adecuados y funcionen correctamente.

Secretaría General - Secretaría de Planeación.

Observación 7:

Se identificó que el programa " Seguridad Digital", presentó incoherencia en el avance de las metas y proyectos, con la apropiación y ejecución presupuestal para la vigencia 2025, como se detalla en la siguiente tabla, incumpliendo los principios de planeación, coordinación, viabilidad y coherencia, y lo contemplado en:

- El artículo 3 de la Ley 152 de 1994.
- El artículo 8 de la Ley 819 de 2003 que reglamenta la oportunidad de la ejecución presupuestal, el lineamiento "*programar el presupuesto*" de la política de gestión presupuestal y eficiencia del gasto público en lo referente a " ..*que la entidad examine los resultados obtenidos (información sobre el desempeño) en programas, planes o proyectos*..." .
- El esquema de líneas de defensa de la séptima dimensión Control interno.

Lo anterior, posiblemente por debilidades en los controles diseñados por la primera línea de defensa (Oficina Asesora de Informática y Secretaría General) y porque la segunda línea de defensa (Secretaría de Planeación) no verificó que dichos controles fueran apropiados y funcionaran correctamente, afectando la eficiencia de los recursos

para el logro de las metas del plan de desarrollo:

Programa	Meta Producto	Avance Metas	Proyecto	Porcentaje Avance Proyecto	Asignación Presupuestal	Compromisos	Porcentaje Ejecución Presupuestal
Seguridad Digital	implementar (1) un plan estratégico de tratamiento de riesgo de seguridad y privacidad de la información	10%	fortalecimiento de la seguridad digital institucional en el distrito de Cartagena de indias	1.6% avance	150.000.000	109.354.560 (72.9%)	0%
	implementar (1) un plan estratégico de seguridad y privacidad de la información	10%					
	implementar un (1) cloud data center para la protección y seguridad de la información en el distrito	0%	implementación del Cloud data center en la alcaldía de Cartagena de indias –	0% avance	150.000.000	58.800.000 (39.2%)	0%
Avance Total		**7%**		**0,8%**	**300.000.000**	**168.154.560 (56%)**	**0%**

Evidencias: Plan de acción 2025. Reporte Software Treasury.

Observación 8:

Se evidenció que para la vigencia 2024, la Secretaría General no incluyó en su plan de acción la programación de las metas del programa " Seguridad Digital" , así como tampoco le asignó recursos al proyecto " Fortalecimiento de la seguridad digital institucional en el Distrito de Cartagena de Indias" dentro del presupuesto, a pesar de estar contemplado en el Plan de Seguridad y Privacidad de la Información, contraviniendo:

- El artículo 1 del Decreto 612 de 2018 de la Presidencia de la República.
- El lineamiento "*formular los planes de acción anual*" de la política de Planeación institucional en lo referente a " ..*incluir tanto los aspectos relacionados con el componente misional como con los relacionados con los planes de que trata el Decreto 612 de 2018: plan de seguridad y privacidad de la información*..." .
- El componente "*Actividades de control*" de la política de Control interno relacionado con "*... establecer la planeación estratégica, acciones, responsables, metas, tiempos que faciliten el seguimiento y aplicación de controles...*" .

Lo anterior, posiblemente por falta de articulación entre el Plan Estratégico de TI y el

Plan de Desarrollo, así como por debilidades en el seguimiento por parte del Comité Institucional de Gestión y Desempeño, lo que podría generar la materialización de incumplimientos normativos, dificultades para el logro de los objetivos del MSPI, afectando el Índice de Desempeño Institucional (IDI).

Evidencias: Plan de acción 2024, PETI, POAI, PREDIS, Plan de seguridad y privacidad de la información.

Para las observaciones 7 y 8, se vincula a la Secretaría General, en su rol de primera línea de defensa, como responsable de implementar los controles necesarios para prevenir o mitigar los riesgos de incumplimiento de las disposiciones citadas, con el fin de dar cumplimiento a las metas del plan de desarrollo y adicionalmente en el ejercicio de su función como ordenador del gasto en materia de contratación, de acuerdo con lo dispuesto en el artículo 1 del Decreto 0533 de 2024. Esta responsabilidad se encuentra definida en la Política de Control Interno, bajo el esquema de líneas de defensa, y en la Política de Administración del Riesgo, Vr. 3, 2023, de la Alcaldía Mayor de Cartagena de Indias (Tabla 1. Roles y responsabilidades para la administración del riesgo por procesos), donde se establece que dicha dependencia debe garantizar el mantenimiento efectivo de los controles internos, así como la ejecución de la gestión de riesgos y controles en el desarrollo diario de sus funciones.

Por otra parte, se vincula a la Secretaría de Planeación, ya que, de conformidad con la política de control interno - esquema de líneas de defensa y la política distrital de Administración del riesgo, le corresponde como segunda línea de defensa monitorear, asesorar y asegurar que los controles y los procesos de gestión del riesgo diseñados por la 1ª línea de defensa sean adecuados y funcionen correctamente.

Conforme a lo anterior, les solicito que en el término de tres (3) días hábiles contados a partir del recibo de la presente comunicación, es decir el 19 de agosto de 2025, se pronuncien sobre las observaciones relacionadas, aceptándolas o presentando las evidencias que estimen pertinentes para desvirtuarlas.

De no ser objetadas quedarán en firme y serán consignadas en el informe definitivo y en el plan de mejoramiento.

Atentamente,

https://sigob.cartagena.gov.co/SeguimientoCorrespondencia?id=EypL9GzBYI1Kdycug6XonaVjlDLmi31IGF%2BLE7RCGu8%3D

VERENA LUCÍA GUERRERO BETTÍN
Jefe Oficina Asesora de Control Interno

RESPONSABLE	NOMBRES Y APELLIDOS	CARGO	FIRMA
Proyectó	Tatiana Yaneth Berrio Caraballo Luis Manuel Barreto Hernandez	Asesora Externa Asesor Externo	
Revisó	Rossana Navarro Cure	Profesional Especializado	
Aprobó (si aplica)			
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y/o técnicas vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma del remitente.			