ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA GENERAL

INFORME EJECUTIVO
AUDITORIA A LA GESTIÓN DE LA ESTRATEGIA DE TECNOLOGIA DE INFORMACIÓN Y LAS COMUNICACIONES

1. **Objetivo General:** Evaluar la eficacia de los controles aplicables al proceso Estrategia de Tecnologías de la Información y las Comunicaciones de la entidad, verificar el estado de avance y cumplimiento de las metas del proyecto de Inversión 1081-Rediseño de la arquitectura de la plataforma tecnológica en la Secretaría General, así como el cumplimiento de la normativa y directrices internas y externas aplicables, entre ellas, los requisitos establecidos en la NTC ISO 9001:2015.

2. **Alcance:** Verificar la efectividad de los controles establecidos por la OTIC sobre la Estrategia de la Información y Comunicaciones para el período comprendido entre septiembre 2018 (fecha de actualización de la caracterización del proceso) y marzo 2019. Así como realizar seguimiento al cumplimiento de los planes de acción definidos para la atención de observaciones y no conformidades derivadas de auditorías internas.

3. **Principales criterios**

- Anexo operativo del Decreto 1499 de 2017 - MIPG
- Modelo de privacidad y seguridad de la información Vs.3.0.2 del MINTIC
- Planes de acción definidos durante la vigencia 2018: Sistema Integrado de Gestión para las No Conformidades #34 y #35 generadas por la OCI y #52 generada por la OAP.
- Procedimientos del proceso 4204000-PO-051 Estrategia de Tecnologías de la Información y las Comunicaciones Vs. 11:

  - Procedimiento 2213200-PR-116 Vs.10 – Elaboración del Plan Estratégico de TI Basado en la Arquitectura Empresarial de TI
  - Procedimiento 2213200-PR-106 Vs.11 - Análisis, Diseño, Desarrollo e Implementación de Soluciones
  - Procedimiento 2213200-PR-187 Vs. 06: Inventario, Clasificación, etiquetado de información, protección de datos personales, evaluación de riesgos y planes de tratamiento a los Activos de Información.

- Manuales y Guías referenciadas en los procedimientos mencionados:
  - 4204000-MA-031 Vs.01: Manual del Sistema de Seguridad de la Información

  - 2213200-GS-004 vs.07: Guía para el inventario, clasificación, etiquetado de información, protección de datos personales y análisis de riesgos de los Activos de Información.

  - 2211700-OT-048 vs.02: Lineamientos para la implementación y sostenibilidad del Sistema de Gestión de Seguridad de la Información.

  - 2211700-OT-043 vs.05: Plan Estratégico de Tecnologías de Información PETI 2016-2020

- Mapa de Riesgos del proceso publicada en el Sistema Integrado de Gestión.
- G-ES-06 Guía Técnica para la elaboración del PETI de MinTIC vs.2.0 del 30 de abril 2018

- G-ES-06 Guía Técnica para la estructuración del PETI del MINTIC vs 1.0 del 30 de marzo de 2016

Conclusión General:

Resultado de las verificaciones realizadas, se confirmó de manera parcial la efectividad de las actividades de control relacionadas con la actualización, aprobación y publicación del PETI, la identificación del inventario de Activos de Información de la Entidad, y la adquisición de tecnología enmarcada en el Plan de Adquisiciones Anual de la OTIC, sin contemplar lo pertinente a la oportunidad en la actualización y aprobación del PETI, la diferenciación de controles para un proceso de adquisición de software nuevo, mantenimiento de software, adquisición de hardware, licencias y/o infraestructura, y finalmente la inclusión de todas las dependencias de la Entidad para la identificación de sus Activos de Información.

En lo referente al avance y cumplimiento de las metas del proyecto de inversión 1081, se observó al I trimestre del año 2019, un avance (magnitud acumulada) del 7%, con una ejecución presupuestal de $ 1.784 MM (17%) y un cumplimiento de la gestión contractual programada del 13%, debido a que no se observa un avance significativo se recomienda que se tomen todas las medidas para que se cumplan todas las actividades programadas para el cumplimiento de las metas en la vigencia 2019.

En consideración de las oportunidades de mejora, debilidades de control y/o gestión, se precisan las principales recomendaciones:

- Fortalecer y actualizar el mapa de riesgos del proceso evaluado, incluyendo riesgos relacionados con la contribución del PETI en el cumplimiento de los objetivos estratégicos de negocio, y con los Activos de Información, así como implementar nuevos controles según aplique con la definición de los riesgos y aprovechar el proceso de actualización de mapa de riesgos que se está realizando, para alinear los controles establecidos en los procedimientos e implementar nuevos controles según aplique a nuevos riesgos.

- Dar celeridad a las gestiones conducentes a realizar la liquidación de los contratos que culminaron su ejecución a finales del 2018 o inicios del 2019, y que se encuentran próximos a cumplir el plazo para realizar su liquidación, evitando una posible pérdida de competencia de la entidad para liquidar, según los términos definidos en la ley 1150 de 2007 art 11 para el cumplimiento de los términos de liquidación.

- Realizar la actualización de las metas para el proyecto 1081- Rediseño de la arquitectura de la plataforma tecnológica en la Secretaría General, específicamente la meta “Cumplir El 80 % Del Plan De Trabajo Para La Implementación Del ERP En La Secretaría General”, la cual no presenta avances en su ejecución y de acuerdo con lo informado por la OTIC requiere ser modificada. Asimismo, finalizar la suscripción de los contratos faltantes conducentes a dar cumplimiento a las metas definidas.

- Realizar monitoreo periódico del cumplimiento de las metas del Proyecto 1081 en instancia de los Subcomités de autocontrol, verificando que aquellas que requieren de mayor esfuerzo de ejecución presupuestal y avance en magnitud, dispongan de los recursos necesarios y/o

se encuentren en el estado de implementación esperado para su finalización en los términos previstos.

- Ajustar el procedimiento 2213200-PR-106 Vs. 11 - Análisis, Diseño, Desarrollo e Implementación de Soluciones y/o implementar nuevos procedimientos, diferenciando las actividades para los diferentes tipos de requerimientos tecnológicos como son: desarrollos nuevos, mantenimientos de software y adquisiciones de hardware, licencias y/o infraestructura tecnológica.

- Como medida de control definir un monitoreo periódico para verificar la efectividad de los controles definidos por cada área de negocio para la protección de sus Activos de Información, y ajustar tanto el procedimiento e incluir lo como parte de los controles clave que se establecen en el mapa de riesgos del proceso.

- Revisar y ajustar los controles que actualmente se encuentran establecidos en el formato FT-367, asegurando que los mismos mitiguen el riesgo relacionado al Activo de Información.

- Revisar y ajustar el formato FT-367 Identificación, valoración y planes de tratamiento a los Activos de Información, asegurando que exista coherencia entre el control definido y el riesgo que mitiga para la protección del Activo de Información, asegurando que el control definido incluya la acción a realizar, la periodicidad y el responsable de su ejecución. Al igual, asegurando que el mencionado formato se encuentra completamente diligenciado en la totalidad de sus campos.

- Fortalecer el procedimiento 2213200-PR-187 Vs.06 Inventario, Clasificación, Etiquetado de Información, Protección de Datos Personales, Evaluación de Riesgos y Planes de Tratamiento a los Activos de Información, incluyendo la responsabilidad de cada área de negocio frente a la implementación y ejecución del control, así como una actividad de monitoreo que permita evaluar periódicamente la efectividad de los controles definidos por cada área.