INFORME OCI-2025-30

SEGUIMIENTO AL CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL

SEGUNDO SEMESTRE DE 2025.

OFICINA DE CONTROL INTERNO

DICIEMBRE DE 2025

UNIDAD DE RESTITUCIÓN DE TIERRAS

DESTINATARIOS:

- **Rangel Giovani Yule Zape**, Director General.
- **Jaqueline Campos Rincón**, Secretaria General.
- **Aura Patricia Bolívar Jaime,** Subdirectora General.
- **Paula Andrea Villa Vélez,** Directora Jurídica.
- **Virgelina Moreno Rodríguez,** Directora Territorial sede Chocó.
- **Wilson Zapata**, Jefe Oficina Asesora de Planeación.
- **Carlos Alberto De la Ossa Hurtado**, Jefe Oficina de Tecnologías de la Información.

RESPONSABLE DEL INFORME:

- **Claudia Marcela Pinzón Martínez**, Jefe Oficina de Control Interno.

EQUIPO AUDITOR:

- **Carlos Alberto Quiñones Cárdenas,** Contratista de la Oficina de Control Interno.

OBJETIVO(S):

Evaluar las actividades realizadas por la Oficina de Tecnologías de la Información de la URT, respecto al cumplimiento de la implementación de la Política de Gobierno Digital durante el segundo semestre del 2025.

ALCANCE:

- Verificación del avance en la implementación del Marco de Referencia de Arquitectura Empresarial del Estado Colombiano, de conformidad con la brecha identificada en el informe de seguimiento del primer semestre de 2025.
- Verificación del estado de implementación del Modelo de Seguridad y Privacidad de la Información, de acuerdo con las disposiciones.

Nota: El establecimiento de esta fecha de corte no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos posteriores que, por su grado de materialidad deban ser revelados.

LIMITACIÓN:

El proceso auditor no presentó limitaciones, dado que abordó todas las actividades previstas dentro del programa de auditoría.

CRITERIOS:

- Decreto 1078 de 2015 *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.*

- Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".*
- Resolución 500 de 2021 (MinTIC) *"Por medio del cual se realiza la adopción del MSPI como habilitador de la Política de Gobierno Digital, el cual establece los lineamientos y estándares para la estrategia de seguridad digital en Entidades públicas, adoptando el Modelo de Seguridad y Privacidad de la Información como parte de la política de Gobierno Digital".*
- Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- Resolución 1978 de 2023 *"Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones",* expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnologías de la información y las Comunicaciones (MRAE.DM DOCUMENTO MAESTRO) – MINTIC 2023.
- Plazos para la implementación del Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnologías de la información y las Comunicaciones (MRAE.ADM.1) – MINTIC 2023.
- Resolución 2277 de 2025 (MinTIC) *"Por medio del cual se realiza la actualización del Anexo 1 de la Resolución 500 de 2021*", reemplaza y actualiza los lineamientos técnicos del MSPI.

DESCRIPCIÓN DEL TRABAJO REALIZADO

1. MARCO DE REFERENCIA DE ARQUITECTURA EMPRESARIAL (MRAE).

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, a través de la política de Gobierno Digital, desarrolló el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE) con el propósito de fortalecer la gestión institucional mediante la adopción de la Arquitectura Empresarial (AE). Esta práctica estratégica permite a las Entidades Públicas alinear su visión, gestión y tecnología de manera estructurada y sostenible, impulsando su transformación hacia organizaciones de alto desempeño.

Desde su creación en 2014, el MRAE ha evolucionado para responder a las necesidades del sector público. En 2019 se publicó la versión 2.0, que incorporó tres modelos fundamentales: el Modelo de AE (MAE), el Modelo de Gestión de Proyectos de TI (MGPTI) y el Modelo de Gestión y Gobierno de TI (MGGTI). Posteriormente, el Decreto 767 de 2022 reforzó la obligación de integrar la estrategia tecnológica en el Plan Estratégico de TI (PETI) de cada Entidad. En 2023 se lanzó la versión 3.0 del MRAE, actualizando sus componentes y guías para facilitar su adopción y apoyar la transformación digital del Estado.

El documento *"MRAE.ADM.1 Plazos para la implementación del Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC 2023",* en su numeral 2.3, establece que, para la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD) el plazo para cumplir el 100% de los lineamientos es de 25 meses contados a partir de la entrada en vigencia de la Resolución 1978 de 2023, la cual comenzó a regir el 26 de mayo de 2023, por lo que el término venció el 27 de junio de 2025.

Mediante el *"Informe OCI-2025-15 seguimiento al cumplimiento de la política de gobierno digital – primer semestre de 2025",* la Oficina de Control Interno (OCI) de la UAEGRTD identificó dieciséis (16) lineamientos parcialmente implementados y ocho (8) lineamientos no implementados. En consecuencia, el presente seguimiento se realizó de manera específica sobre estos veinticuatro (24) lineamientos que estaban pendientes por cumplir en el corte al 30 de junio de 2025, frente a lo cual se concluyó que la Oficina de Tecnologías de la Información (OTI) ha realizado acciones para su implementación, de los cuales diecisiete (17) cumplen con el respectivo lineamiento, y frente a los siete (7) restantes, si bien se ajustan a las disposiciones de MinTic, presentaban observaciones para su formalización, fortalecimiento y/o mejoramiento. Las recomendaciones específicas se presentan a continuación, las cuales fueron socializadas previamente con la OTI:

Tabla No. 1 Resultado de evaluación del Marco de Referencia de Arquitectura Empresarial

No.	ID Y DESCRIPCIÓN DEL LINEAMIENTO	RESULTADO	RECOMENDACIÓN OCI
Modelo de Arquitectura Empresarial – MAE.			
1	MAE.LI.PA.03 - Gobierno y capacidad de Arquitectura Empresarial - Las Entidades de la administración pública deben instaurar la capacidad para planear, desarrollar, mantener y evolucionar la Arquitectura Empresarial mediante la definición e implementación de la cadena de valor de la AE compuesta por: el proceso, la estructura organizacional para llevarlo a cabo, las instancias y órganos de gobierno. La Entidad deberá contar con un Grupo de trabajo o Profesional que se encargue de liderar y/o ejecutar el proceso, y para la toma de decisiones con un Comité de AE conformado por las diferentes áreas interesadas.	Cumple con observaciones	Los documentos proyectados para el cumplimiento de este lineamiento se encuentran en fase de revisión por parte de la Oficina Asesora de Planeación, por lo cual se recomienda hacer seguimiento y gestión hasta su aprobación e incorporación en el SIPG.
2	MAE.LI.PA.05 - Definición de la Arquitectura Empresarial - Las Entidades de la administración pública deben definir la Arquitectura Empresarial mediante la ejecución de los ejercicios de AE establecidos en la etapa de planeación de la AE. Para cada ejercicio de AE y en el marco del desarrollo de los dominios de la arquitectura, se debe plantear la situación objetivo con la que se espera lograr los objetivos estratégicos de la Arquitectura y a partir del análisis de brecha con respecto a la situación actual, cerrar el ejercicio con la identificación de las iniciativas y soluciones que harán parte de la hoja de ruta de la Arquitectura Empresarial.	Cumple	Sin observaciones
3	MAE.LI.PA.08 - Repositorio AE - Las Entidades de la administración pública deben contar con un repositorio de Arquitectura Empresarial que les permita almacenar y hacer la gestión sobre la documentación, los modelos, los artefactos y demás componentes que describen la Arquitectura Empresarial y sus ejercicios. Se recomienda que el repositorio sea gestionado mediante una herramienta de Arquitectura Empresarial o similar que facilite el acceso y consulta por parte de los interesados y que esté estructurado de tal manera que se pueda navegar desde vistas estratégicas y conceptuales de alto nivel dirigidas a los interesados no técnicos, hasta las vistas arquitecturales con detalle técnico de bajo nivel dirigidas a los arquitectos y técnicos.	Cumple	Se recomienda la estructuración completa del repositorio para acceder a la capacidad de ofrecer vistas estratégicas y técnicas navegables a las carpetas, categorías, vistas estratégicas y técnicas de la AE.

No.	ID Y DESCRIPCIÓN DEL LINEAMIENTO	RESULTADO	RECOMENDACIÓN OCI
4	MAE.LI.AIN.02 - Modelo capacidades institucionales - Las Entidades de la administración pública deben realizar mediante la definición de un modelo de capacidades, el entendimiento de las capacidades institucionales para identificar las capacidades actuales y objetivo de la Entidad. Las capacidades de la Entidad pueden ser clasificadas en estratégicas, misionales y de apoyo, las que a su vez se pueden subdividir según el detalle requerido en la Entidad y para facilitar su entendimiento.	Cumple	Se recomienda fortalecer la evidencia soporte para que incluya la situación actual y objetivo de las capacidades institucionales, articulando con la Oficina Asesora de Planeación para el suministro, concertación y organización de evidencias articuladas con el MRAE y el análisis de brechas entre las capacidades actual y objetivo.
5	MAE.LI.AIN.03 - Modelo operativo institucional - Las Entidades de la administración pública deben realizar el entendimiento preciso, claro y documentado de la situación actual y objetivo del Modelo operativo de la Entidad, que contemple los procesos, cadena de valor, instancias de decisión y la estructura orgánica con sus respectivos roles, actores y recursos, que habilitan cada una de las capacidades institucionales.	Cumple	Se requiere articular con la Oficina Asesora de Planeación para adjuntar la evidencia de la documentación de la situación actual y objetivo del modelo operativo, y la integración explícita de roles, actores y recursos en relación con las capacidades institucionales.
6	MAE.LI.AIN.04 - Modelo de servicios institucionales - Las Entidades de la administración pública deben, mediante el análisis del portafolio servicios de la Entidad, identificar la situación actual de los servicios impactados por el ejercicio de AE y establecer la situación objetivo en función de los requerimientos y los objetivos estratégicos que se desean alcanzar según las definiciones dadas en la visión de la AE.	Cumple con observaciones	Se recomienda que, a partir del portafolio de servicios institucionales, en la fase de implementación de los ejercicios de AE, se genere un documento con el inventario del portafolio de servicios institucionales, indicando cuáles son impactados por la AE, el análisis de la situación actual y situación objetivo de dichos servicios, alineado con los objetivos estratégicos y la visión de AE, el mapa o modelo de servicios institucionales que muestre la relación entre los servicios, procesos y capacidades , y las actas o informes de los subcomités donde se evidencie la discusión y definición de la situación objetivo.
7	MAE.LI.AI.04 - Modelo de Información Institucional - Las Entidades de la administración pública deben contar con un Modelo de Información Institucional acordado con los interesados, que proporcione una vista común y coherente de la información; sirviendo como base y guía para cualquier modelo de datos particular o proyecto de datos que se desarrolle.	Cumple	Para fortalecer las evidencias, se sugiere incluir un mapa visual integral que muestre la relación entre categorías de información, sistemas y flujos, validado por los responsables, garantizar que el modelo y sus artefactos estén publicados en repositorios oficiales (intranet, portal institucional) para facilitar su consulta y actualización continua. Se sugiere además, en la implementación y madurez del lineamiento, realizar actividades de socialización y validación del modelo con las áreas misionales y Entidades externas para demostrar el acuerdo con los interesados, incorporar métricas de efectividad (por ejemplo, nivel de interoperabilidad, calidad de datos, uso de servicios) y evidenciar su seguimiento en informes periódicos.
8	MAE.LI.AT.01 - Catálogo de elementos de infraestructura - Las Entidades de la administración pública deben contar con un catálogo actualizado de sus elementos de infraestructura tecnológica, que le sirva de insumo para administrar, analizar y mejorar la infraestructura tecnológica de la Entidad. Las Entidades cabeza de sector adicionalmente deben consolidar y mantener actualizado el catálogo de elementos de infraestructura tecnológica compartidos por las Entidades del sector.	Cumple	Se recomienda definir o integrar en procedimientos establecidos una metodología para mantener actualizado el catálogo, incluyendo revisiones con los grupos técnicos y responsables de infraestructura, e integrar indicadores de desempeño que permitan analizar la utilización, capacidad y estado de los elementos para facilitar la toma de decisiones sobre estos elementos, su seguridad y la mejora continua.
9	MAE.LI.AT.02 - Plataforma de interoperabilidad del Estado - Las Entidades de la administración pública deben incluir dentro de su arquitectura de Infraestructura Tecnológica los elementos necesarios para poder realizar el intercambio de información entre las áreas de la institución y las Entidades externas a nivel sectorial y nacional mediante la plataforma de interoperabilidad definida en el Marco de Interoperabilidad.	Cumple	Para el grado de madurez, se recomienda relacionar reportes de disponibilidad, con tiempos de respuesta y volúmenes de intercambio de datos para evidenciar la operación efectiva, e incorporar planes de contingencia para garantizar la resiliencia del servicio.

No.	ID Y DESCRIPCIÓN DEL LINEAMIENTO	RESULTADO	RECOMENDACIÓN OCI
10	MAE.LI.AT.03 - Continuidad y disponibilidad de los Elementos de infraestructura - Las Entidades de la administración pública deben incluir en el diseño de la arquitectura de infraestructura tecnológica los mecanismos que garanticen la continuidad y disponibilidad de la infraestructura tecnológica, así como la capacidad de atención y resolución de incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios de la Entidad.	Cumple	Para la implementación, se recomienda incluir evidencias de pruebas periódicas de recuperación ante desastres y simulacros que demuestren la efectividad de los mecanismos implementados.
11	MAE.LI.AT.04 - Arquitecturas de referencia tecnológica de la Entidad - Las Entidades de la administración pública serán las responsables de definir y evolucionar las arquitecturas de referencia en lo referente a los componentes de arquitectura tecnológica, con el propósito de orientar el diseño de cualquier arquitectura de solución bajo parámetros, patrones y atributos de calidad definidos por la Entidad, teniendo en cuenta los principios de diseño de servicios digitales, los componentes estructurales y su comportamiento con otros subsistemas e interfaces, definidos en el Manual de Gobierno digital.	Cumple con observaciones	El documento proyectado para el cumplimiento de este lineamiento se encuentra en fase de revisión por parte de la Oficina Asesora de Planeación, por lo cual se recomienda hacer seguimiento y gestión hasta su aprobación e incorporación en el SIPG.
12	MAE.LI.AS.01 - Catálogo de servicios de seguridad de la información y ciberseguridad - Las Entidades de la administración pública deben contar con un catálogo de servicios de seguridad que comprende una lista de servicios que proporcionan funciones específicas de seguridad para los sistemas de información y una lista de servicios institucionales relacionados con seguridad de la información y ciberseguridad.	Cumple con observaciones	Se recomienda incorporar el documento en el marco del SIPG para garantizar su actualización periódica, incluyendo fecha de última revisión y responsable.
13	MAE.LI.AS.02 - Análisis de Impacto del negocio - Las Entidades de la administración pública deben realizar el análisis de impacto de negocios que debe convertirse en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.	Cumple	Se recomienda implementar las recomendaciones mencionadas el informe BIA, y actualizar periódicamente el análisis de impacto al negocio.
14	MAE.LI.AS.03 - Arquitectura de Seguridad - Las Entidades de la administración pública deben definir, evolucionar y aplicar una arquitectura de seguridad sobre la infraestructura tecnológica, los sistemas de información y los datos durante la ejecución de los ejercicios de arquitectura empresarial.	Cumple	Se recomienda analizar la incorporación del catálogo en el SIPG para garantizar su formalización y actualización. Y a futuro, para la implementación, se recomienda incluir los resultados de pruebas de penetración, registros de incidentes y acciones correctivas para demostrar la efectividad de la arquitectura de seguridad.
Modelo de Gestión de Proyectos de TI – MGPTI.			
1	MGPTI.LI.CES.04 - Grupo de gestión de proyectos de TI - Las Entidades de la administración pública deben establecer un equipo o grupo de trabajo que coordine y articule esfuerzos para gestionar el portafolio de programas y proyectos de TI; este grupo de trabajo tiene entre otras tareas estandarizar y optimizar los procesos de la gestión de proyectos.	Cumple con observaciones	Se evidenció lineamientos para la gestión de proyectos, el banco de proyectos y un equipo de gerencia de proyectos en la OTI, no obstante, se recomienda la integración de los instrumentos al Sistema Integrado de Planeación y Gestión (SIPG), y para la implementación y evaluación del nivel de madurez, incorporar evidencias que soporten la plena operación del grupo como una Oficina de Gestión de Proyectos (PMO).
2	MGPTI.LI.EJC.03 - Gestión de riesgos - Las Entidades de la administración pública durante el ciclo de vida del proyecto deben identificar, analizar, evaluar continuamente la exposición y dar respuesta a los riesgos, de acuerdo con el apetito de riesgo y los procesos que para tal fin defina la Entidad.	Cumple con observaciones	Se recomienda formalizar la integración al SIPG los formatos de riesgos adoptados, y para la implementación, se recomienda suministrar registros del control efectivo realizado en los proyectos (incorporando estados, responsables, fechas, tendencia, riesgo residual) y documentación de las respuestas a riesgos materializados en proyectos TI concretos.

No.	ID Y DESCRIPCIÓN DEL LINEAMIENTO	RESULTADO	RECOMENDACIÓN OCI
3	MGPTI.LI.EJC.04 - Involucramiento de interesados - Las Entidades de la administración pública deben involucrar de manera temprana y proactiva a los interesados, definir en el plan de gestión del proyecto cómo gestionarlos, mantener activa comunicación con ellos y gestionar sus preocupaciones e intereses para que contribuyan al éxito del proyecto.	Cumple	Sin observaciones
Modelo de Gestión y Gobierno de TI – MGGTI.			
1	MGGTI.LI.ES.09 - Diseño impulsado con el usuario - La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe involucrar activamente a los ciudadanos en la definición de trámites y servicios digitales, con el fin de asegurar que el resultado final satisfaga las necesidades de los usuarios.	Cumple	Para reforzar los soportes del cumplimiento del lineamiento, se recomienda documentar los casos concretos donde la retroalimentación ciudadana haya generado cambios en trámites o servicios digitales (por ejemplo, ajustes en plataformas, simplificación de procesos).
2	MGGTI.LI.SI.03 - Guía de estilo y usabilidad - La dirección de tecnologías y Sistemas de la información o quien haga sus veces debe definir, adoptar y/o adaptar una guía de estilo y usabilidad para la institución. Esta guía debe incorporar los lineamientos de gov.co y elementos de accesibilidad web.	Cumple con observaciones	Se recomienda analizar la incorporación del manual de usuario del portal Web en el SIPG para garantizar su formalización y actualización. De manera complementaria, se recomienda fortalecer dicho manual, incluyendo las referencias de estilo de gov.co, accesibilidad web (WAI/WCAG), aspectos de diseño visual, idEntidad corporativa y usabilidad.
3	MGGTI.LI.ST.02 - Gestión de los servicios de TI - La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe gestionar la operación y el soporte de los servicios tecnológicos, en particular, durante la implementación y paso a producción de los servicios de TI, se debe garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad.	Cumple	Se recomienda definir métricas de desempeño y acuerdos de nivel de servicio (SLA) para cada servicio, y para la implementación incorporar evidencia del plan de capacidad y su seguimiento, mostrando cómo se proyecta la demanda y se garantiza la disponibilidad de recursos ante incrementos de carga, realizar reportes periódicos de monitoreo y análisis de riesgos operativos.
4	MGGTI.LI.ST.06 - Capacidad de los servicios tecnológicos - La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe velar por la prestación de los servicios de TI, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para un óptimo funcionamiento.	Cumple	Se recomienda incluir en la documentación un plan formal de gestión de capacidad.
5	MGGTI.LI.ST.10 - Monitoreo de recursos TI - La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe monitorear los recursos y servicios de TI y controlar el nivel de consumo de los recursos críticos que son compartidos por los Servicios Tecnológicos a fin de garantizar su disponibilidad.	Cumple	Para la implementación se recomienda incluir evidencias de los reportes e informes de análisis de los monitoreos realizados.
6	MGGTI.LI.ST.12 - Disposición de residuos tecnológicos - La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, siguiendo las directrices de las áreas administrativas debe gestionar la correcta disposición de residuos tecnológicos de acuerdo con el Plan Institucional de Gestión Ambiental y teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional.	Cumple	Para la implementación se recomienda incorporar registros actualizados de ejecución (actas de disposición final, reportes de gestores, fotografías de puntos ecológicos y centros de acopio) para demostrar la aplicación práctica del programa, indicadores específicos para RAEE: Incluir métricas diferenciadas para residuos tecnológicos (cantidad gestionada, porcentaje reciclado, reducción anual), y capacitación y sensibilización.
7	MGGTI.LI.ST.13 - Gestión de problemas de TI - La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe definir e implementar un procedimiento para la gestión de incidentes, los cuales sean analizados periódicamente para identificar posibles patrones los cuales, a su vez, sean tratados como problemas para identificar causa raíz y soluciones definitivas.	Cumple	Para la implementación y evaluación de madurez se recomienda incorporar reportes que muestren análisis de tendencias, casos cerrados y soluciones implementadas, para evidenciar la ejecución del procedimiento, y como oportunidad de mejora se recomienda analizar si los problemas críticos se relacionan con escenarios de planes de continuidad y riesgos operativos, fortaleciendo la gestión preventiva.

Fuente: Construcción propia del equipo auditor a partir de los reportes y evidencias suministradas por la Oficina de Tecnologías de la Información (OTI).

Nota: El detalle de la verificación realizada por parte de la Oficina de Control Interno se encuentra en el *"Anexo No. 1 – Marco de Referencia de Arquitectura Empresarial "*.

2. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La evaluación presentada en este informe se realizó conforme a lo dispuesto en la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la cual establece los lineamientos y requisitos para la implementación y gestión del Modelo de Seguridad y Privacidad de la Información en las Entidades públicas. Este marco normativo se aplicó en este corte de revisión de la OCI considerando que este era el vigente al momento de la planeación de las actividades de la Oficina de Tecnologías de la Información (OTI) durante la vigencia 2025.

En atención a las actualizaciones normativas emitidas por MinTIC, particularmente la Resolución 2277 de 2025, mediante la cual en julio de la presente vigencia se actualizó el MSPI, incorporando la última versión de la norma internacional ISO/IEC 27001 y otras disposiciones, los informes de seguimiento que se elaboren a partir del primer semestre de 2026 se regirán por este nuevo criterio.

Tabla No. 4 Resultado de evaluación del instrumento del Modelo de Seguridad y Privacidad de la Información – MSPI.

No.	DOMINIO	CALIFICACIÓN ACTUAL (%)	CALIFICACIÓN OBJETIVO (%)
A.5	Políticas de seguridad de la información	100	100
A.6	Organización de la seguridad de la información	96	100
A.7	Seguridad de los recursos humanos	93	100
A.8	Gestión de activos	90	100
A.9	Control de acceso	83	100
A.10	Criptografía	90	100
A.11	Seguridad física y del entorno	96	100
A.12	Seguridad de las operaciones	93	100
A.13	Seguridad de las comunicaciones	100	100
A.14	Adquisición, desarrollo y mantenimiento de sistemas	87	100
A.15	Relaciones con los proveedores	100	100
A.16	Gestión de incidentes de seguridad de la información	86	100
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	80	100
A.18	Cumplimiento	95	100
Resultado: Promedio de evaluación de controles		**92**	**100**

Fuente: Construcción propia del equipo auditor a partir de los reportes y evidencias suministradas por la Oficina de Tecnologías de la Información (OTI).

Este resultado, permite concluir que, se ha logrado un avance de implementación del 92 % de los controles previstos en el MSPI, conforme al reporte suministrado por la OTI y revisado por la OCI.

Este nivel de cumplimiento refleja un compromiso con la protección de los activos de información, la infraestructura TI y la privacidad de los datos, alineado con los objetivos de seguridad digital para fortalecer la confianza y agilidad en la prestación de servicios públicos.

Teniendo en cuenta la nueva resolución emitida por el MinTIC, este resultado se considera un punto de partida para la formulación de un plan de trabajo que permita dar cumplimiento a los nuevos requerimientos normativos, asegurando la continuidad del proceso de mejora y la adaptación a los estándares actualizados.

Como resultado de la verificación realizada por la OCI, a continuación, se presentan las observaciones y recomendaciones específicas de la sección de levantamiento de información del instrumento MSPI, las cuales fueron socializadas previamente con el Oficial de Seguridad de la OTI:

1. La sección de nivel de madurez y el componente del ciclo PHVA están pendientes por diligenciar.
2. Del numeral 4 *"Mapa de Procesos",* se recomienda actualizar el link referenciado, debido que este direccionaba a la sección de Misión, Visión y Propósito superior institucional.
3. Del numeral 12 *"Procedimientos de control documental del MSPI"*, se observó que el documento *"MC-GU-01 Elaboración de Documentos del SIPG",* no es suficiente para dar cumplimiento al requisito de gestión de información documentada del MSPI establecido por MinTIC. Aunque dicho documento define lineamientos generales para la elaboración y control de documentos dentro del SIPG, el MSPI exige un procedimiento específico que garantice la identificación, versionamiento, trazabilidad, control de cambios y disposición final de la información relacionada con seguridad y privacidad, conforme a la Resolución 02277 de 2025, el Documento Maestro del MSPI y la Guía 6 – Gestión Documental. Por lo tanto, la Entidad debe complementar el marco general con un procedimiento alineado a estos lineamientos para asegurar el cumplimiento normativo.

   Se recomienda implementar un procedimiento específico para la gestión de información documentada del MSPI, alineado con los lineamientos establecidos por MinTIC en la Resolución 02277 de 2025, el Documento Maestro del MSPI y la Guía 6 – Gestión Documental. Este procedimiento debe garantizar la identificación, codificación, versionamiento, trazabilidad, control de cambios, publicación, acceso y disposición final de los documentos relacionados con seguridad y privacidad de la información. De esta manera, se asegura el cumplimiento normativo y la adecuada integración del subsistema de seguridad y privacidad dentro del Sistema Integral de Planeación y Gestión (SIPG).
4. Del numeral 18 *"Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes"*, se observó que dentro de las actividades generales de las líneas de formación en Tecnologías de la Información (TI) se incluyen acciones orientadas a la seguridad de la información, tales como: sensibilización sobre los riesgos de ciberataques, fortalecimiento de la seguridad en entornos de trabajo híbrido con almacenamiento en la nube, e implementación de prácticas seguras (uso adecuado de contraseñas, gestión de almacenamiento y aplicación de políticas de privacidad). Se evidenció que la última actualización de estas actividades corresponde a agosto de 2023, por lo que se recomienda evaluar la pertinencia y necesidad de su actualización, con el fin de garantizar

su vigencia y alineación con los riesgos actuales y las mejores prácticas en seguridad de la información.

5. Del numeral 20 *"Inventario de activos de información clasificados, de la Entidad, revisado y aprobado por la alta dirección"*, se observó que se cuenta con el archivo de inventario de activos de información, no obstante, este documento es un Excel sin la codificación de documentos del SIPG, por lo cual no es posible determinar si su estructura y contenidos han sido aprobados por la instancia correspondiente al interior de la Entidad. Adicionalmente, el corte de la información publicada es de la vigencia 2024, pero la OTI realizó un ejercicio de actualización en el 2025, el cual no se ve publicado. Se recomienda establecer un formato en el SIPG para el inventario de activos de información y actualizar la información de acuerdo con el resultado del ejercicio realizado en esta vigencia.
6. Del numeral 21 *"Inventario de áreas de procesamiento de información y telecomunicaciones"*, no se evidenció un documento con el inventario de áreas de procesamiento de información y telecomunicaciones.
7. Del numeral 24 *"Inventario de partes externas o terceros a los que se transfiere información de la Entidad"*, no se evidenció documento con el inventario de partes externas o terceros a los que se transfiere información de la Entidad. Se recomienda revisar la documentación que maneja la Oficina Asesora de Planeación respecto a Entidades a las cuales se les transfiere información (reportes), y complementar con otro tipo de interacción que incluya transferencia de información.
8. Del numeral 26 *"Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden"*, no se evidenció dicho inventario.
9. Del numeral 28 *"Plan de continuidad de la Entidad aprobado"*, se observó que se cuenta con el *"PLAN DE PREPARACIÓN DE TI PARA LA CONTINUIDAD DEL NEGOCIO"* (GT-ES-10), pero se recomienda analizar la posibilidad y necesidad de actualizar este documento, teniendo en cuenta que su última actualización es de septiembre de 2020 y a partir de esta fecha se han aplicado cambios (por ejemplo, en infraestructura de TI) que pueden afectar el plan.
10. Del numeral 29 *"Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información"*, en la sección Normatividad de la intranet institucional, se presentan las funciones de la Oficina de Tecnología, pero no se publica la normatividad vigente. Esto impide evidenciar que se encuentran identificadas las obligaciones legales, estatutarias, reglamentarias y normativas relacionadas con la seguridad de la información, especialmente las más recientes, como la Resolución MinTIC 02277 de 2025 (que modifica la Resolución 500 de 2021 sobre el Modelo de Seguridad y Privacidad de la Información) y el Documento Maestro del MSPI, entre otras disposiciones aplicables. Se recomienda actualizar la información en las diferentes secciones donde se referencie normograma de la Entidad, en especial las relacionadas con seguridad de información.
11. Del numeral 31 *"Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea."*, en el reporte suministrado no se referencia cuales dichos documentos con que cuenta la UAEGRTD relacionados con

seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.

12. Del numeral 32 *"Indicadores y métricas de seguridad de la información definidos"*, en el reporte suministrado se referenció el acceso al sistema de información STRATEGOS, pero no se aportó la relación de cuáles son los Indicadores y métricas de seguridad de la información definidos. Para la vigencia 2025 los indicadores establecidos son: GT-2-2025 *"Porcentaje de avance del plan de seguridad y privacidad de la información. PESI"* y GT-3-2025 *"Porcentaje de avance del plan de tratamiento de riesgos de seguridad y privacidad de la información – PTRSI"*, no obstante no se logra identificar la medición de los indicadores recomendados por MinTic, tales como:

    - Porcentaje de activos de información clasificados (MSPI – Documento Maestro / ISO 27001 (Control A.5.9)).
    - Número de incidentes de seguridad reportados y gestionados (MSPI – Guía de Gestión de Incidentes / ISO 27035).
    - Nivel de cumplimiento del plan de tratamiento de riesgos (MSPI – Guía de Gestión de Riesgos / ISO 27005).
    - Grado de implementación de controles del Anexo A ISO 27001 (MSPI – Documento Maestro / ISO 27001).
    - Porcentaje de personal capacitado en seguridad de la información (MSPI – Lineamientos de Capacitación / Política GD).
    - Tiempo promedio de respuesta a incidentes críticos (MSPI – Guía de Incidentes / ISO 27035).
    - Porcentaje de sistemas con controles de acceso implementados (MSPI / ISO 27001 (Control A.9)).

13. Del numeral 33 *"Declaración de aplicabilidad"*, no se evidenció el documento con la Declaración de aplicabilidad de los controles del MSPI.

14. Del numeral 34 *"Aceptación de los riesgos residuales por parte de los dueños de los riesgos"*, en la respuesta diligenciada en el instrumento se referenció el sistema de información de planeación y gestión STRATEGOS para el monitoreo de riesgos de gestión y corrupción, sin embargo, esto no permite inferir que la Entidad define la aceptación de los riesgos residuales por parte de los responsables de los riesgos. Se recomienda fortalecer la respuesta, por ejemplo, indicando que en los documentos "POLÍTICA DE ADMINISTRACIÓN DEL RIESGO" (MC-ES-04), "GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO" (MC-GU-02) y "MONITOREO DE RIESGOS STRATEGOS (MC-IN-02), se establece que la aceptación de riesgos residuales es una decisión explícita de los responsables del proceso, bajo criterios definidos en la política y la guía metodológica. La *"Guía para la Administración de Riesgos"*, en la sección 8.14 *"Tratamiento del Riesgo"*, indica que el riesgo puede ser aceptado cuando cumple con los criterios de aceptación y se encuentra en zona de calificación baja, siempre que los controles existentes se mantengan con la misma rigurosidad. Asimismo, la *"Política de Administración de Riesgo"*, en la sección 5.1 *"Niveles de aceptación del riesgo"*, señala que la aceptación se da cuando no se requieren medidas adicionales y el riesgo residual

está en zona baja, mientras que riesgos de corrupción, fiscales y de seguridad de la información son inaceptables en zonas moderadas, altas o extremas. En ambos documentos se precisa que esta decisión corresponde a los líderes de proceso (primera línea de defensa), quienes deben considerar la probabilidad, impacto y relación costo-beneficio de las medidas adicionales, garantizando monitoreo permanente.

15. Del numeral 35 *"Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección"*, en las evidencias se hizo referencia al Plan de Seguridad y Privacidad de la Información, y al Plan de Tratamiento de Riesgos, sin embargo, estos documentos no dan cumplimiento al requisito del documento de la estrategia de planificación y control operacional, que se encuentra en la Cláusula 8.1 de ISO 27001 y en el Documento Maestro del MSPI.
16. De los numeral 38 *"Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección"* y 41 *"Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección"*, no se evidenció el documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
17. Del numeral 40 *"Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección"*, se observó que en la evidencia se relacionó el documento *"PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"* (GT-ES-14), sin embargo, no se hace referencia al resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.

Nota: El detalle de la verificación realizada, reposa en los papeles de trabajo custodiados por la Oficina de Control Interno.

RECOMENDACIONES

- Respecto al Marco de Referencia de Arquitectura Empresarial (MRAE), se sugiere realizar un análisis de las recomendaciones específicas emitidas para los diferentes lineamientos, con el fin de garantizar su alineación con la estrategia de Gobierno Digital. Este análisis debe servir como base para la planeación de actividades orientadas a la implementación progresiva de los componentes del modelo y al incremento del nivel de madurez de la arquitectura empresarial.
- Respecto al Modelo de Seguridad y Privacidad de la Información (MSPI), teniendo en cuenta que el resultado alcanzado en la implementación del MSPI fue del 92 %, se recomienda cerrar las brechas identificadas mediante la ejecución de acciones específicas que garanticen el cumplimiento total de los controles establecidos. Adicionalmente, se debe generar o actualizar el plan de trabajo orientado a la adopción de la actualización del MSPI conforme a la 2277 de 2025 emitida por el MinTIC, asegurando la incorporación de los nuevos requerimientos normativos.
- Se recomienda realizar el reporte de la infraestructura crítica de ciberseguridad conforme a los lineamientos y plazos establecidos por el MinTIC en el Decreto 338 de 2022, que adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, asegurando el cumplimiento del plazo definido en la normativa vigente, el cual establece como fecha

límite el 17 de diciembre de 2025. Para ello, se sugiere adelantar las actividades necesarias para la identificación, clasificación y documentación de los activos críticos, así como la validación de la información requerida, con el fin de garantizar la entrega oportuna y evitar riesgos asociados al incumplimiento regulatorio.

Notas:

- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.
- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por los responsables de atender el proceso auditor, a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- Es discrecional de Entidad determinar si se acogen las recomendaciones elevadas por la Oficina de Control Interno ante las situaciones observadas, no obstante, se invita a que las mismas sean consideradas en el establecimiento de los planes de mejoramiento a que haya lugar.

CLAUDIA MARCELA PINZON MARTINEZ

Firmado digitalmente por CLAUDIA MARCELA PINZON MARTINEZ
DN: T=JEFE DE OFICINA ASESORA CODIGO 0137 GRADO 22, SN=PINZON MARTINEZ, STREET="Calle 13A #29-24 BARRIO ED ALLIANZ", S=BOGOTA D.C., OU=TOKEN VIRTUAL, SERIALNUMBER=2280032, OID.1.3.6.1.4.1.23267.2.3=900498799, OID.1.3.6.1.4.1.23267.2.2=53077880, OID.1.3.6.1.4.1.23267.2.1=364, O=UNIDAD DE RESTITUCION DE TIERRAS, L=BOGOTA D.C., G=CLAUDIA MARCELA, C=CO, CN=CLAUDIA MARCELA PINZON MARTINEZ
Razón: Yo soy el autor de este documento
Ubicación:
Fecha: 11/12/2025 10:39:17 -05'00'

CLAUDIA MARCELA PINZÓN MARTÍNEZ
Jefe Oficina de Control Interno

Anexos: Anexo No. 1 – Marco de Referencia de Arquitectura Empresarial

Elaboró: Carlos Alberto Quiñones Cárdenas, líder de auditoría, Oficina de Control Interno.

Revisó: Maicol Stiven Zipamocha Murcia, contratista, Oficina de Control Interno.