1. INFORMACIÓN GENERAL

PROCESO O ACTIVIDAD: Auditoría a los habilitadores Seguridad y privacidad de la información - Servicios ciudadanos digitales	**FECHA DE LA AUDITORÍA:** 05 de mayo a 20 de junio de 2025
AUDITOR LIDER: Elías Alonso Nule Rhenals	**EQUIPO AUDITOR:** Diana Elizabeth Patiño Sabogal
AUDITADO:	Oficina de Tecnología de la Información
OBJETIVOS:	**General:** Evaluar el avance de la implementación de la política de Gobierno Digital en el Habilitador Seguridad y Privacidad de la Información y el Habilitador Servicios Ciudadanos Digitales, así como el avance de las Políticas MIPG Gobierno Digital y Seguridad Digital. **Específicos:** • Verificar el cumplimiento normativo y documental de la entidad frente a los lineamientos establecidos en la Resolución 500 de 2021. • Evaluar la implementación de los servicios digitales en la herramienta establecida por el ministerio para la implementación del Servicio Ciudadano Digital de Interoperabilidad.
ALCANCE:	Normativa definida por MINTIC para los Habilitadores de Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales en la Página https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/, MIPG Política Gobierno Digital y Seguridad Digital
CRITERIOS:	**1. Criterios para los trámites objeto de auditoría:** • Resolución 500 de marzo 10 de 2021 «Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital» • DECRETO 620 DE 2020 «Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales» **2. Criterios adicionales:** • Evaluación de riesgos asociados • Información estadística • Estado de los indicadores asociados • Acciones del plan de mejoramiento interno • Autocontrol – autoevaluación • Cumplimiento a las recomendaciones registradas en la auditoría anterior • Monitoreo del cambio • Conflictos de interés

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	05	**Mes**	05	**Año**	2025	**Desde**	05/05/25 DD / MM /AA	**Hasta**	20/06/2025 DD / MM /AA	**Día**	26	**Mes**	06	**Año**	2025

2. ACTIVIDADES DESARROLLADAS

De acuerdo con el Plan Anual de Auditoría de la vigencia 2025, aprobado por el Comité de Coordinación Institucional de Control Interno, se adelantó la Auditoría a los habilitadores Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales. La reunión de apertura se llevó a cabo el 05 de mayo de 2025, a través de la herramienta institucional Microsoft Teams con la participación del jefe de la Oficina de Tecnologías de la Información Y los profesionales de la oficina

La dependencia auditada aprobó el plan de auditoría enviado por el equipo auditor y en consecuencia el líder de la dependencia suscribió el formato EM-FO-06 Carta Salvaguarda el día 05 de mayo de 2025.

La auditoría se realiza aplicando los lineamientos definidos en el Procedimiento Auditoría Interna (código EM-PR-02, versión 13 de 30/12/2024), al igual que los lineamientos generales impartidos por el Departamento Administrativo de la Función Pública en la Guía de Auditoría Interna basada en Riesgos para Entidades Públicas.

En el marco de la presente auditoría se realizaron las siguientes mesas de trabajo:

Tabla 1. Relación de reuniones realizadas entre el equipo auditor y el equipo auditado

FECHA	TEMA
13/05/2025	Identificación de objetivos específicos
29/05/2025	Revisión de las evidencias entregadas
10/06/2025	• Monitoreo de los cambios identificados en el proceso • Conflicto de interés declarados por la Oficina de Tecnologías de la Información. • Autocontrol y autoevaluación

3. FORTALEZAS

Se reconoce el conocimiento técnico del profesional que asistió a todas las reuniones programadas durante el desarrollo de la auditoría, así como su disposición para proporcionar la información solicitada de manera oportuna.

4. REQUISITOS CON CUMPLIMIENTO (CONFORMIDADES)

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
1	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 5. La estrategia de seguridad digital. (…)** Ser aprobada a través de un acto administrativo de carácter general.
DETALLE		
Actualmente, la entidad cuenta con la Resolución N.º 01237 del 21 de julio de 2020, «*Por la cual se deroga la Resolución 106 de 2018, modificada por la Resolución 939 de 2019, y se reglamenta el Comité Institucional de Gestión y Desempeño de la Autoridad Nacional de Licencias Ambientales – ANLA*». En el artículo segundo, "Funciones del Comité Institucional de Gestión y Desempeño", se establece en el numeral 1 lo siguiente: "***Aprobar*** *y hacer*		

seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión – MIPG".
En cumplimiento de lo anterior, el 30 de enero de 2025, el Comité se reunió para aprobar el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI, tal como se evidencia en el numeral 2.1.11, «Plan de Seguridad y Privacidad de la Información», del acta de reunión.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
2	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 5. La estrategia de seguridad digital. (…)** 4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces
DETALLE		

La Oficina de Tecnologías de la Información, durante la vigencia 2024, realizó las siguientes actividades orientadas a promover la cultura de seguridad digital en la entidad:

1. Entre los meses de enero a mayo, se llevaron a cabo capacitaciones sobre seguridad de la información en el marco de las jornadas denominadas "Conociendo la ANLA".
2. El 5 de junio de 2024, se realizó una capacitación sobre los lineamientos de la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información, la cual contó con la participación de 19 profesionales de entidades como ANLA, Ministerio de Ambiente, Codechocó, Corantioquia e Invemar.
3. Se difundieron mensajes informativos a través del correo electrónico institucional, con tips sobre seguridad digital, abordando temas como amenazas digitales, política de seguridad de la información, reporte de eventos o incidentes, uso de repositorios institucionales, entre otros.

En cuanto a la vigencia 2025, se han desarrollado las siguientes acciones:

1. Durante los meses de enero y febrero, se realizaron nuevamente capacitaciones en seguridad de la información en el marco de las jornadas "Conociendo la ANLA".
2. Se enviaron dos (2) boletines informativos mediante correo electrónico, con contenidos relacionados con el uso responsable de Internet y amenazas digitales.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
3	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. (…)** 3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.
DETALLE		

Durante la vigencia 2024, la Oficina de Tecnologías de la Información presentó ante el Comité Institucional de Gestión y Desempeño los resultados del análisis de riesgos y los incidentes de seguridad, según consta en el acta de reunión No. 005 del 10 de julio, en el numeral «*11.2 Socialización de la Oficina de Tecnología de la Información corresponde al monitoreo de Riesgos de Seguridad de la Información y Ciberseguridad donde se informa "presenta ante el comité directivo 20 escenarios de riesgos, de ellos se analizaron los riesgos inherentes, once (11) están en extremos y ocho (8) altos y uno (1) moderado, tras aplicar los controles de la norma, 93 controles en total son escenarios de riesgos que pasaron de alto y externos diecinueve (19), están en zona moderada y uno (1) paso a bajo. En el ejercicio se debe aplicar planes de mejora sobre los diecinueve (19) escenarios en riesgo moderado, sin embargo, no es eficiente, pero se debe optimizar los controles, también en la presentación podemos evidenciar la eficacia de los 64 controles y 23 de memoria, a nivel de evaluación presentan un 85 % de efectividad"*».

En el numeral «*11.3 los incidentes del mes pasado que tienen que ver con seguridad de la información, disponibilidad de servidores que brinden soporte a las aplicaciones y no permitir que están presenten caídas, se reportó 99.01% de disponibilidad, hubo 725 eventos identificados y solucionados por parte de las herramientas antivirus, los cuales fueron alertados y controlados y se identificaron 4 incidentes que afectaron los servicio en junio tal como se muestra en la presentación (…)*», se detalló el comportamiento de la disponibilidad y la gestión de incidentes de seguridad.

Adicionalmente, en el Comité del 20 de noviembre, según consta en el acta de reunión No. 008, en el numeral «*2.8. Incidentes de Seguridad de la Información (…) se ha dado 100% de disponibilidad de los servidores de la entidad, además se han presentado 1.6688 ataques cibernéticos entre los que se encuentran virus troyanos entre otros todos controlados adecuadamente. Asimismo, se reportaron 20 eventos de seguridad gracias al monitoreo del SOC (…)*», se documentaron los eventos de seguridad correspondientes a ese periodo.

Y en el numeral 2.10 Monitoreo de los Riesgos de Seguridad de la Información y Ciberseguridad de indicó *«(…) el monitoreo de los riesgos de seguridad y ciberseguridad, por lo cual inicia describiendo que se presentan 20 escenarios de riesgos de seguridad, en los cuales, 13 son riesgos extremos, seis (6) son riesgos altos, uno (1) en estado moderado y ninguno en bajo. Posterior a la aplicación de controles se obtiene que 17 riesgos pasan a estado moderado y tres (3) en estado bajo. Se implementan 93 controles alineados a la 27001 (…)*»

Lo anterior, permite evidenciar que la Oficina de Tecnologías de la Información mantenerse informada a la alta dirección sobre los riesgos y eventos que afectan la seguridad de la información.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
4	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. (…)** 6. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y sin perjuicio de aquellas tareas que realizan las autoridades de control.
DETALLE		
La Oficina de Tecnologías de la Información hizo entrega a la Oficina de Control Interno mediante correo electrónico, los informes mensuales de seguridad informática y gestión de seguridad de la información que realizan como		

evidencia de los monitoreos del cumplimiento de las políticas, correspondientes a los meses de enero, febrero, marzo y abril de 2025.

En estos se evidencian acciones de monitoreo técnico, tales como:

1. Se documentan incidentes, eventos críticos, vulnerabilidades detectadas y acciones de respuesta. Esto muestra un proceso activo de monitoreo y gestión de riesgos.
2. Se incluyen métricas de control de acceso, ataques bloqueados, incidentes detectados por tipo, vulnerabilidades corregidas, y monitoreo de endpoints y servidores.
3. Se mencionan actividades de fortalecimiento como actualizaciones de firmas de antivirus, aplicación de parches, revisiones de políticas, campañas de concientización y pruebas de vulnerabilidades.
4. Se evidencia que el monitoreo está alineado con políticas internas de seguridad y protocolos establecidos por el área.

Lo anterior, permite evidenciar que mensualmente se ha realizado seguimiento en materia de seguridad de la información.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
5	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. (…)** 10. Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna.

DETALLE

Desde la Oficina de Tecnologías de la Información se ha adelantado la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), para lo cual se han establecido los siguientes documentos:

1. DPI-PL-01 Política del Sistema Integrado de Gestión, la cual establece como objetivos: «Proteger los activos de información de los riesgos que puedan afectar su confidencialidad, integridad, disponibilidad y privacidad» y «Promover la mejora continua a través de la integración del Modelo Integrado de Planeación y Gestión – (MIPG) y los sistemas de gestión implementados por la autoridad».
2. DPI-GU-02 Guía de implementación de la política de seguridad digital – MIPG, que busca «(…) desarrollar las herramientas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital de la entidad, así mismo articular esfuerzos para asegurar su implementación».
3. DPI-MN-01 Manual del Sistema Integrado de Gestión, el cual incluye dentro de su alcance la implementación del SGSI. Asimismo, detalla el seguimiento que debe realizar la Oficina de Tecnologías de la Información en materia de seguridad de software, información y del propio sistema de gestión.

Adicionalmente, se evidencia la gestión del SGSI a través de la implementación de procedimientos específicos como:

- DT-PN-01 Plan de recuperación de desastres
- DT-PR-03 Solicitud de VPN
- DT-PR-04 Gestión de incidentes de seguridad de la información
- DT-PR-06 Gestión de accesos de usuarios
- DT-PR-10 Gestión de medios de almacenamiento removibles
- DT-PR-29 Control e instalación de software

Estos procedimientos son monitoreados mediante los planes de trabajo del SGSI correspondientes a las vigencias 2024 y 2025, donde se definen las actividades, productos entregables y responsables de ejecución. Los avances y resultados son presentados al Comité Institucional de Gestión y Desempeño.

Con base en la documentación y acciones presentadas, se evidencia que la Oficina de Tecnologías de la Información ha implementado un Sistema de Gestión de Seguridad de la Información conforme a los lineamientos establecidos, gestionando de manera estructurada los riesgos de seguridad digital y reportando su seguimiento ante el comité competente.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
6	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	**ARTÍCULO 7. Operaciones seguras.** Los sujetos obligados deben implementar mecanismos de gestión y monitoreo que protejan la infraestructura de TI de amenazas físicas y digitales.
DETALLE		
De acuerdo con la información entregada mediante correo electrónico el día 14 de mayo, por la Oficina de Tecnologías de la Información, se evidencia que se han implementado mecanismos de alta disponibilidad que fortalecen la continuidad del servicio y la protección de la infraestructura tecnológica de la entidad. Esto se refleja en los informes técnicos de pruebas de respaldo y conmutación realizados para el Clúster de SQL Server, el controlador de dominio y los equipos de telefonía Cisco, en los cuales se verificó la operatividad de las soluciones, la correcta ejecución de las pruebas, copias de respaldo, la ausencia de pérdida de servicio y la validación por parte de los responsables técnicos. Lo anterior demuestra la existencia de estrategias de gestión técnica orientadas a proteger los servicios críticos de TI ante eventos de fallo o interrupción, cumpliendo así con el criterio evaluado en lo relacionado con la gestión de amenazas digitales.		

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
7	**Resolución 500 de marzo 10 de 2021** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.	**ARTÍCULO 10. Privacidad de la información.** Los sujetos obligados deben definir una estrategia que permita brindar servicios, controles y condiciones de protección de la privacidad de la información de la Entidad y los ciudadanos acorde con lo exigido en la Ley 1581 de 2012 y los decretos reglamentarios.
	Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.	**Artículo 12. Deber de informar al Titular.** El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo. **Artículo 17. Deberes de los Responsables del Tratamiento.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin

		perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data
	CT-PLE-02 POLÍTICA (ESTRUCTURADA) DE PROTECCIÓN DE DATOS PERSONALES **Versión 5** **Fecha: 24-12-2020**	**7.1.5. Consentimiento de privacidad Previo al tratamiento de datos** se debe solicitar el consentimiento expreso por parte del titular a más tardar en el momento de la recolección de la información, este consentimiento incluirá la información de los datos que serán recolectados, la identificación y datos de contacto del responsable, la finalidad y los derechos como titular. Este consentimiento se solicitará a través de un documento escrito con la firma del titular **y/o mediante clic en la plataforma o herramientas con la marcación de texto por parte del titular en los canales electrónicos o el uso de un párrafo de aceptación de condiciones de uso** y/o un aviso de privacidad visible.

DETALLE

El día 30 de mayo de 2025, se ingresó a la página web de la entidad https://www.anla.gov.co/, específicamente al módulo de “Atención y servicios a la ciudadanía”, en el cual se encuentran los canales dispuestos para la atención de los ciudadanos. A través de estos canales, se recolecta y almacena información sensible de los usuarios. A continuación, se describen los principales canales identificados:

1. Formulación de solicitudes y seguimiento de peticiones, quejas, reclamos, sugerencias y denuncias:

En este formulario se solicitan campos obligatorios como: tipo y número de identificación, nombres, correo electrónico, dirección, información sobre población, entre otros. Por esta razón, se notifica al usuario la política de tratamiento de datos personales, solicitando su aceptación expresa, como se observa en las siguientes imágenes:

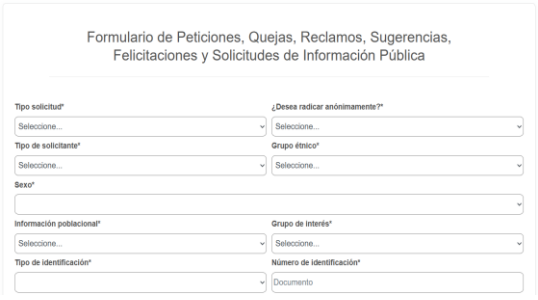
Imagen Nro. 1 Ingreso al formulario de PQRS	Imagen Nro. 2 Solicitud de información formulario de PQRS
	

Imagen Nro. 3 Socialización de política de tratamiento de datos personales

Imagen Nro. 4 Aceptación de política de tratamiento de datos personales

2. <u>Formulario de quejas disciplinarias y denuncias por actos de corrupción:</u>

A través de este canal se pueden realizar denuncias relacionadas con posibles conductas que constituyan faltas disciplinarias o hechos de corrupción cometidos por funcionarios de la entidad. En este caso, también se requiere el diligenciamiento de información personal obligatoria (tipo y número de identificación, nombres, correo electrónico, dirección, entre otros), lo que justifica la notificación de la política de tratamiento de datos personales y la solicitud de aceptación por parte del usuario como en las siguientes imágenes:

Imagen Nro. 5 Solicitud de información formulario del formulario de quejas disciplinarias

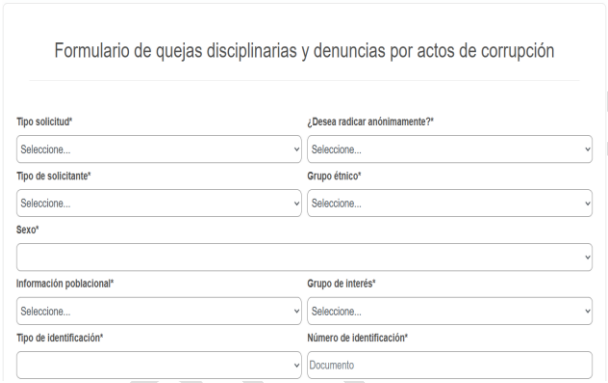
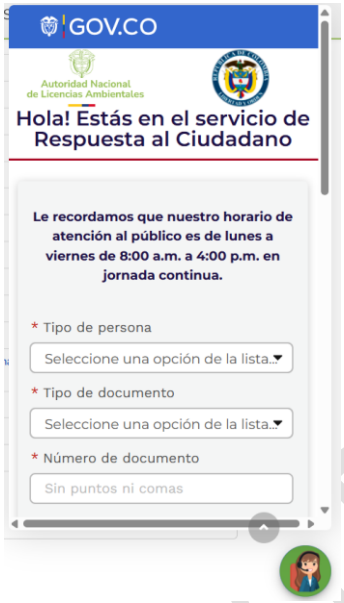


Imagen Nro. 6 Socialización de política de tratamiento de datos personales

Imagen Nro. 7 Aceptación de política de tratamiento de datos personales

3. <u>Canal de respuesta al ciudadano (asistencia virtual)</u>:

Este canal orienta a los ciudadanos sobre los procesos de trámites y permisos. Durante la interacción, se solicitan datos personales sensibles como tipo y número de documento, nombres, apellidos, correo electrónico, entre otros. Por tal motivo, se notifica la política de tratamiento de datos personales y se requiere su aceptación, como se visualiza en la siguiente imágenes:

Imagen Nro. 8 Solicitud de información personal	**Imagen Nro. 9 Aceptación de política de tratamiento de datos personales**
	

4. <u>Canales telefónicos</u>:

Adicionalmente, el día 26 de mayo se realizaron llamadas a las líneas de atención al ciudadano: (601) 2540100, línea gratuita 01 8000 112 998 y línea ética 314 218 8748. Durante las llamadas, se proporciona el siguiente mensaje:

"De acuerdo con la Ley 1581 de 2012, esta llamada será grabada y monitoreada para garantizar la calidad de nuestros servicios. Al continuar, se entienden aceptadas las políticas de seguridad de la información, privacidad y tratamiento de datos personales, disponibles en nuestra página web."

Con base en lo anterior, se evidencia que la entidad cuenta con la Política de Protección de Datos Personales CI-PL-03, versión 5 del 24/12/2020, la cual está publicada en su página web. Esta política es comunicada de manera adecuada a los ciudadanos, y se solicita expresamente su aceptación para el tratamiento de sus datos personales.

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO
8	**DECRETO 1078 DE 2015** «Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones»	**ARTÍCULO 2.2.17.2.1.1. Servicios ciudadanos digitales:** Los servicios ciudadanos digitales se clasifican en servicios base y servicios especiales. 1.1. Servicio de interoperabilidad 1.2. Servicio de autenticación digital 1.3. Servicio de carpeta ciudadana digital

DETALLE

De acuerdo con la información proporcionada por la Oficina de Tecnologías de la Información (OTI), la entidad actualmente dispone de un total de 468 servicios digitales clasificados como “servicios de interoperabilidad”, distribuidos de la siguiente manera:

Tabla 2. Servicios de interoperabilidad

TIPO DE SERVICIO	CANTIDAD DE SERVICIOS
INTERNO	462
EXTERNOS	6

Fuente: Bases de datos entregadas por la OTI

En cuanto al servicio de autenticación digital, se evidenció que la entidad no cuenta con un mecanismo propio implementado, dado que los trámites que requerirían dicho servicio son gestionados directamente por los grupos de valor a través de la plataforma VITAL (Ventanilla Integral de Trámites Ambientales), administrada por el Ministerio de Ambiente y Desarrollo Sostenible.

En relación con el servicio de Carpeta Ciudadana Digital, no ha sido posible su implementación dentro de la entidad, debido a que aún no se ha recibido respuesta por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) sobre si en dicha carpeta deben incluirse trámites asociados a personas jurídicas, las cuales constituyen el único tipo de usuario que realiza trámites ante la entidad.

Sin embargo, esto no es identificado como un incumplimiento ya que la Oficina de Tecnologías de la Información tiene clasificada los servicios ciudadanos digitales.

5. DESCRIPCIÓN DE NO CONFORMIDADES

No.	CRITERIO	DESCRIPCIÓN DEL CRITERIO	NO CONFORMIDAD

1	**Procedimiento DT-PR-04 Gestión de incidentes de seguridad de la información** Versión 4 Fecha: 17/09/2024	7. Desarrollo de actividades Actividad 4: Notificar el evento o incidente de seguridad: Descripción de la actividad: Se notifica a la Alta dirección de la entidad. **Se reporta al CSIRT** y ColCERT Se decide si es necesario reportar a partes interesadas, entes de regulación y autoridades pertinentes	Incumplimiento a lo establecido en el procedimiento de gestión de incidentes de seguridad de la información en la actividad número 4, debido a que los incidentes de seguridad identificados por la Oficina de Tecnologías de la Información no fueron reportados al CSIRT del Gobierno (Equipo de Respuesta a Incidentes de Seguridad Digital) únicamente se registran las lecciones aprendidas.

DETALLE DE LA NO CONFORMIDAD

El 30 de mayo de 2025, el equipo auditor realizó una reunión virtual con los profesionales de la Oficina de Tecnologías de la Información, a través de Microsoft Teams, con el fin de identificar cuántos y cuáles fueron los incidentes de seguridad presentados durante la vigencia 2024. Como resultado, se confirmó la ocurrencia de 6 incidentes.

Se seleccionaron 2 de ellos como muestra, en los cuales se evaluaron los criterios que deben ser implementados para el tratamiento, investigación y gestión de los incidentes de seguridad establecido en la normativa interna y externa evaluada, identificando que:

Tabla 3. Primer incidente de seguridad evaluado

Incidente en la base de datos de la página web	
¿Se encuentra documentado en el formato DT-FO-04 Reporte de incidente de seguridad de la información?	SI
¿Se le ha asignado un responsable para dar solución y respuesta dentro del formato de incidentes?	SI
¿Se describió la situación presentada y la solución del incidentes?	SI
¿fue reportado ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno?	NO
¿Cuenta con la descripción de lecciones aprendidas y se definido un plan de trabajo?	SI

Tabla 4. Segundo incidente de seguridad evaluado

Incidente en la conectividad WAN	
¿Se encuentra documentado en el formato DT-FO-04 Reporte de incidente de seguridad de la información?	SI
¿Se le ha asignado un responsable para dar solución y respuesta dentro del formato de incidentes?	SI
¿Se describió la situación presentada y la solución del incidentes?	SI
¿fue reportado ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno?	NO
¿Cuenta con la descripción de lecciones aprendidas y se definido un plan de trabajo?	SI

De acuerdo con lo anterior, se evidencio que la Oficina de Tecnologías de la Información, no reportaron ninguno de los 2 incidentes ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno a través del formato de reporte establecido por el CSIRT Gobierno La no conformidad se socializó el día 29 de mayo de 2025.
CAUSA
Debilidad en la implementación del procedimiento establecido para el reporte de incidentes ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno.
CONSECUENCIA
Posibles incumplimiento de las obligaciones establecidas en la normativa nacional sobre seguridad digital.

6. NO CONFORMIDADES RECURRENTES

No se presentaron no conformidades recurrentes durante el desarrollo de la auditoría.

7. EVALUACIÓN RIESGOS

En el mapa de riesgos del proceso, no se identifican riesgos relacionados con la seguridad y privacidad de la información - Servicios ciudadanos digitales.

8. OTROS ASPECTOS EVALUADOS

Durante la reunión llevada a cabo el 10 de junio de 2025 con los profesionales de la Oficina de Tecnologías de la Información a través de la plataforma Teams, se llevó a cabo una entrevista detallada para identificar las actividades realizadas en relación con:

8.1 Autocontrol y Autoevaluación

Autocontrol

Se realiza seguimiento a las políticas de Gobierno Digital y Seguridad Digital mediante el cumplimiento de los indicadores establecidos en la herramienta SPIG. Asimismo, dichos indicadores son monitoreados a través del PETI.

Autoevaluación

Para los habilitadores evaluados bajo el enfoque de autoevaluación, los responsables realizan anualmente un autodiagnóstico con el objetivo de identificar el estado actual de la entidad y definir los aspectos en los que se deben implementar planes de trabajo, de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

8.2 Monitoreo del cambio

El Modelo Integrado de Planeación y Gestión –MIPG-, establece la importancia para el Sistema de Control Interno de las entidades de la implementación de actividades de monitoreo y supervisión continua, las cuales tienen el objetivo de valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; y (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública.

De esta forma, la evaluación permanente al estado del Sistema de Control Interno implica el seguimiento al conjunto de dimensiones del modelo, de tal manera que la autoevaluación y la evaluación independiente se convierten en la base para emprender acciones para subsanar las deficiencias detectadas y encaminarse en la mejora continua (COSO, 2013: 143).[1]

Se realizó una reunión por Teams con el auditado, durante la cual se identificó que no existe un cambio relevante.

8.3 Indicadores

Se realizó la verificación del estado de los indicadores relacionados con Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales, con corte a abril de 2025, con el fin de corroborar las metas registradas en la plataforma SPGI.

Proyectos de inversión 32-04-01 y 32-01-04 – Fortalecimiento de la gestión institucional y tecnológica de la Autoridad Nacional de Licencias Ambientales en el territorio nacional.

Tabla 5. Relación de indicadores asociados a la Oficina de Tecnologías de la Información.

DESCRIPCIÓN		AVANCE REPORTADO A ABRIL 2025	OBSERVACIONES
OTI OFICINA			
Adquirir productos y servicios (software y hardware) para la alineación de las tecnologías de la información con las necesidades de la entidad	Procesos de adquisición de equipos de hardware y/o herramientas de software	20%	De los 20 contratos que deben ser gestionados por la Oficina de Tecnologías de la Información para la adquisición de hardware y software para la vigencia 2025, a la fecha de corte se han adelantado únicamente 4 procesos contractuales, lo que representa un avance del 20%. Sin embargo, de acuerdo con la planificación establecida, para el mes de abril se había proyectado un avance del 25%, lo que evidencia un retraso en la ejecución del cronograma y un bajo nivel de cumplimiento frente a la meta propuesta.
Brindar la asesoría tecnológica para la solución de	Porcentaje de Implementación del Plan Estratégico de	44.61%	Hasta marzo, se ha logrado un avance del 44.61%, superando el 30% esperado en la

[1] Manual Operativo MIPG, DAFP, 2021, Pág. 125.

solicitudes de soporte técnico de usuarios de la entidad	Tecnologías de la Información PETI		implementación de los componentes estructurales y transversales. Se verificaron los soportes de avance, observando que son consistentes con la información registrada en las metas durante el periodo de reporte.
	Avance de Implementación de los Planes de seguridad y privacidad de la información, Tratamiento de Riesgos de Seguridad de la Información e Implementación de Tecnologías Emergentes	58.1%	Los planes establecidos conforme al Decreto 612 presentan, con corte a abril de 2025, un avance acumulado del 58,1%, superando el avance esperado del 53,6%. Este resultado está asociado al desarrollo de las 22 acciones programadas para la vigencia, relacionadas con los componentes de transformación digital, seguridad y privacidad de la información, y tratamiento de riesgos. Se verificaron los soportes de avance, observando que son consistentes con la información registrada en las metas durante el periodo de reporte.
	Porcentaje de avance del plan de acción de la política Gobierno Digital para la vigencia	19%	El avance en la ejecución de las actividades definidas en la Política de Seguridad Digital es del 19%, frente a un cumplimiento esperado del 22,75%. Esta diferencia se debe a que dos de las acciones programadas no presentaron evidencias dentro de los tiempos establecidos. Lo anterior evidencia un retraso en la ejecución del cronograma y un bajo nivel de cumplimiento frente a la meta propuesta.
	Porcentaje de avance del plan de acción de la política Seguridad Digital para la vigencia	6.25%	De las cuatro (4) actividades programadas en la Política de Seguridad Digital, solo una (1) inició en el mes de marzo. No obstante, de acuerdo con la proyección establecida en la plataforma del Sistema de Planeación y Gestión Institucional – SPGI, para ese periodo se esperaba un avance del 23%. Sin embargo, únicamente se alcanzó un cumplimiento del 6.25%, lo que evidencia un retraso significativo en la ejecución del cronograma y un bajo nivel de avance frente a la meta propuesta.
	Gestión de incidentes de seguridad de la información y ciberseguridad	33.20%	Desde la Oficina de Tecnologías de la Información se ha dado atención oportuna a los incidentes de seguridad de la información durante la vigencia 2025, con los siguientes registros mensuales: • **Enero:** 466.293 incidentes • **Febrero:** 169.321 incidentes • **Marzo:** 412.104 incidentes • **Abril:** 274.565 incidentes

			Lo anterior evidencia un cumplimiento efectivo de la meta establecida para la gestión de incidentes de seguridad de la información.
	Nivel de conocimiento de competencias del proceso de TI	33.20%	Durante la vigencia 2025, la Oficina de Tecnologías de la Información ha realizado 11 capacitaciones, en las cuales se alcanzó un nivel de apropiación del 95%, de acuerdo con las evaluaciones aplicadas. Esto evidencia un cumplimiento superior a la meta establecida, la cual corresponde al 90%.

8.4 Conflicto de interés

Ninguno de los profesionales y contratistas que hacen parte de la Oficina de Tecnologías de la Información ha declarado algún conflicto de interés que pueda poner en duda la integridad y confidencialidad de la información.

8.5 Evaluación de efectividades

Se reviso en avance de las acciones de la No conformidad 758 con corte al 30 de mayo de 2025, se evidenció que la Oficina de Tecnologías de la Información no ha dado cumplimiento a lo establecido en el Anexo No. 1, numeral 7.3.3 “Plan de tratamiento de los riesgos de seguridad de la información”, específicamente en el lineamiento 4, dado que dicho plan no ha sido aprobado por el Comité de Coordinación Institucional de Control Interno.

Cabe resaltar que esta situación ya había sido identificada previamente en la auditoría interna al Sistema Integrado de Gestión del año 2023, motivo por el cual se generó un plan de mejoramiento asociado a la No Conformidad No. 758. No obstante, de acuerdo con el Acta 032, se ha reprogramado su cumplimiento para el 30 de junio de 2025.

8.6 Evaluación de políticas de MIPG

En el seguimiento realizado a las acciones establecidas en los planes de acción para las políticas de Gobierno Digital y Gobierno de Seguridad Digital del Modelo Integrado de Planeación y Gestión – MIPG durante el primer trimestre de 2024, se ha observado que algunas de sus actividades no han dado inicio, lo que permite evidenciar un avance mínimo. No obstante, se han identificado actividades con bajo cumplimiento como se detalla a continuación:

<u>Política de Gobierno digital</u>

- Documentar las lecciones aprendidas en la ejecución de proyectos TI
- Rediseñar la sede electrónica de la ANLA acorde a la normativa de Gov.co de Min Tic y su integración con la misma

El detalle de la evaluación se puede observar en los Anexo Nro. 2 Seg-Politica GD y Nro. 3 Seg-Politica SD

8.7 Recomendaciones auditoría anterior

Esta auditoría no se llevó a cabo en períodos anteriores.

8.8 Información estadística

Para llevar a cabo esta auditoría, no se necesitan bases de datos para el análisis de información, ya que los productos evaluados son documentos definidos, como manuales, procedimientos, lineamientos, catálogos, entre otros.

9. OBSERVACIONES

9.1 Al revisar los roles y responsabilidades relacionados con la seguridad digital en la entidad, se evidenció que la Resolución Interna N.º 01184 del 7 de junio de 2022 designa al Jefe de la Oficina de Tecnologías de la Información como responsable del Sistema de Gestión de la Seguridad de la Información – SGSI. Situación que generó una No Conformidad en la auditoría externa realizada al Sistema Integrado de Gestión realizada en el año 2024, al no garantizarse la independencia funcional requerida para dicho rol.

Como medida correctiva, la entidad actualizó el Manual Específico de Funciones y de Competencias Laborales mediante la Resolución N.º 2938 del 27 de diciembre de 2024, en la cual se incorpora el cargo de Oficial de Seguridad de la Información y Ciberseguridad, adscrito directamente al despacho del Director General, fortaleciendo así la independencia y nivel estratégico del rol.

Sin embargo, se identificó que la Resolución Interna N.º 01184 de 2022 no ha sido actualizada para reflejar estos cambios, lo cual genera inconsistencias normativas internas. Como fue identificado en el seguimiento realizado por la Oficina de Control Interno el 29 de abril de 2025, a la No Conformidad número 851 formulada por la Oficina de Tecnologías de la Información cuyas acciones eran:

- Solicitar a la OAP el ajuste y actualización de la Resolución 1184 de 2022, en relación con la asignación de funciones del cargo que permitan diferenciar entre el jefe de la OTI y el Oficial de Seguridad de la Información.
- Una vez actualizada la resolución, se generará la respectiva socialización de esta

Razón por la cual, fue calificada como “Inefectiva”, solicitándose a la Oficina de Tecnologías de la Información la reformulación correspondiente.

9.2 Al evaluar el Anexo 2 de la Resolución 2160 del 23 de octubre de 2020, “Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales”, se establece que los servicios digitales implementados por las entidades deben estar integrados en la plataforma de interoperabilidad X-ROAD, definida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional Digital (AND) como el componente tecnológico que soporta el intercambio de datos entre entidades del Estado.

Así mismo, el artículo 2.2.17.7.1 del Decreto 1078 de 2015, sobre la gradualidad en la implementación, indica que «*Las entidades públicas de la rama ejecutiva del orden nacional y los particulares que desempeñen funciones públicas tendrán un plazo de nueve (9) meses contados a partir de la publicación de la Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones*»

En este sentido, la Oficina de Tecnologías de la Información no ha logrado dar cumplimiento a lo establecido, debido a que no ha sido posible realizar la configuración e integración con la plataforma de interoperabilidad X-ROAD, a pesar de múltiples gestiones realizadas ante el MinTIC y la Agencia Nacional Digital, como se evidencia en la siguiente trazabilidad de comunicaciones:

- En el mes de febrero de 2024, se envió mediante correo electrónico una solicitud al MinTIC para la realización de una sesión de contextualización sobre la plataforma X-ROAD como mecanismo de intercambio de información. Esta solicitud se fundamentó en la necesidad de realizar un diagnóstico sobre la implementación de X-ROAD en la ANLA.

- Durante el mes de abril de 2024, se intercambiaron correos electrónicos entre la entidad y el MinTIC con el propósito de obtener soporte técnico sobre el habilitador de Servicios Ciudadanos Digitales, específicamente en relación con Carpeta Ciudadana Digital y X-ROAD. No obstante, el MinTIC informó que no era posible avanzar debido a que el convenio con la Agencia Nacional Digital (AND) aún se encontraba en proceso de perfeccionamiento.

- En los meses de mayo, julio y agosto de 2024, la entidad reiteró al MinTIC la solicitud de soporte técnico sobre la implementación de X-ROAD. Sin embargo, no se obtuvo respuesta por parte del Ministerio.

Adicional a estas gestiones, se realizaron solicitudes formales a través de la plataforma de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD) ante los entes responsables:

Agencia Nacional Digital

El día 23 de diciembre de 2024, se recibió la respuesta al derecho de petición radicado a la Agencia Nacional Digital con número AND-PQRSD-1944-2024 que cita:
«*De manera atenta nos dirigimos a ustedes con el fin de solicitar la revisión en niveles 1,2 y gestión para nivel 3 del servicio "Documento" de la ANLA expondrá a través de XRoad, dado que se requiere en cumplimiento de la normativa para gobierno genera la capacidad de intercambio de información entre entidades públicas en pro de brindar beneficios a los ciudadanos*»

Informado que:
«*Para avanzar al Nivel 2, es necesario radicar la solicitud de servicio a lenguaje@mintic,gov.co y soportecc@mintic.gov.co, acompañada de la evidencia que muestre el correcto uso del estándar de lenguaje notificado en el Nivel 1. Esta evidencia debe incluir el archivo JSON y el proyecto configurado en Postman. Una vez se reciba la información completa, se procederá con la notificación del Nivel 2 del dominio semántico, en el marco del esquema de interoperabilidad.*
Finalmente, para aclarar el Nivel 3 se requiere radicar nuevamente la solicitud de servicio y diligenciar el contrato de descripción del servicio, el cual se encuentra adjunto a este correo»

Ministerio de Tecnologías de la Información y las Comunicaciones

- El día 09 de abril de 2024, se radicó una solicitud formal al en su plataforma de con el número de radicado 241026405 donde se solicitó lo siguiente:
  «*Solicita colaboración para una sesión de contextualización del habilitador de servicios ciudadanos digitales, sobre: carpeta ciudadana digital Y XROAD*»

A lo que el ministerio respondió:
«*Sobre el particular, nos permitimos informarle que actualmente* ***nos encontramos desarrollando el proceso de suscripción del Convenio Interadministrativo con la Agencia Nacional Digital a través del cual durante la vigencia 2024 esperamos realizar el soporte, evolución, mantenimiento y operación para la integración de los Servicios Ciudadanos Digitales (Interoperabilidad, Autenticación Digital, Carpeta Ciudadana Digital), GOV.CO*** *y el soporte y operación de nuestra estrategia "Mi Colombia Digital" que aporta al Estado colombiano la capacidad y eficiencia requerida para el proceso de la transformación digital del país*»

- El día 19 de marzo de 2025, radica ante el Ministerio de Tecnologías de la Información y las Comunicaciones el radicado 251030640 donde solicita:
«*remitosnlos documentos solicitados para avanzar en la aprobación del Nivel 2 para la implementación del servicio de interoperabilidad Xroad: 1. La información solicitada del servicio Sentencia ANH: "Servicio Interconexión" 2. La notificación de Cumplimiento Nivel 1: "Correo_ apro_Xroad_Nivel1" 3. Documento Excel: "CAT-N1-ANLA-Documento*» "SIC"

  Para lo cual, informó el día 07 de abril de 2025 que:
«*Sobre el particular, nos permitimos informarle que* ***actualmente nos encontramos desarrollando el proceso de suscripción del Convenio Interadministrativo con la Agencia Nacional Digital a través del cual durante la vigencia 2025 esperamos realizar el soporte, evolución, mantenimiento y operación para la integración de los Servicios Ciudadanos Digitales (Interoperabilidad, Autenticación Digital, Carpeta Ciudadana Digital)****, GOV.CO y el soporte y operación de nuestra estrategia "Mi Colombia Digital" que aporta al Estado colombiano la capacidad y eficiencia requerida para el proceso de la transformación digital del país. Dentro del cronograma proyectado para tal suscripción se espera iniciar la ejecución del convenio la última semana del mes de abril de 2025, por lo que tomaremos atenta nota de sus datos de contacto para continuar con la implementación del servicio de interoperabilidad X-road*»

Aunque se evidencia que la entidad no ha logrado cumplir con los plazos establecidos en la normativa vigente para la implementación de la plataforma X-ROAD, este incumplimiento no se considera una No Conformidad dado que el equipo auditor constató que la Oficina de Tecnologías de la Información ha adelantado múltiples gestiones y ha mantenido una trazabilidad clara de las solicitudes y requerimientos, demostrando su intención de dar cumplimiento a lo estipulado en la normativa.

10. CONCLUSIONES

10.1 La entidad ha mostrado avances en la implementación del habilitador Seguridad y Privacidad de la Información, evidenciando cumplimiento en varios de los criterios normativos evaluados, particularmente en aspectos relacionados con la gestión documental, el monitoreo de riesgos y la implementación de mecanismos técnicos de seguridad.

No obstante, se identificaron dos no conformidades asociadas a la gestión de riesgos y al reporte de incidentes de seguridad digital, lo que refleja la necesidad de fortalecer la aplicación de procedimientos técnicos y operativos, en concordancia con los lineamientos normativos establecidos.

10.2 En cuanto al habilitador Servicios Ciudadanos Digitales, aunque la entidad no ha logrado completar la integración con la plataforma X-ROAD, esta situación no se considera un incumplimiento, dado que se evidencian gestiones activas y trazabilidad por parte de la entidad ante el MinTIC y la Agencia Nacional Digital, encaminadas a avanzar en su implementación.

10.3 Durante el seguimiento al avance de los planes de acción de las políticas de Gobierno Digital y Seguridad Digital del MIPG, correspondiente al primer trimestre de 2024, se evidenció un cumplimiento limitado, dado que varias actividades no han iniciado y otras presentan un bajo nivel de avance, lo que refleja la necesidad de fortalecer el seguimiento y gestión oportuna de las actividades programadas.

11. RECOMENDACIONES

11.1 Continuar con el seguimiento a las gestiones realizadas ante el MinTIC y la Agencia Nacional Digital, y documentar un plan de acción que incluya cronogramas, responsables y evidencias de avance, con el fin de lograr la integración efectiva de los servicios digitales a la plataforma de interoperabilidad X-ROAD.

11.2 Reforzar el seguimiento de los indicadores, priorizando las actividades con bajo nivel de avance, a fin de asegurar el cumplimiento de las metas establecidas en los plazos definidos.

11.3 Cumplir con las acciones programadas en las políticas de Gobierno Digital y Gobierno de Seguridad Digital del Modelo Integrado de Planeación y Gestión – MIPG, las cuales, hasta la fecha del 30 de marzo de 2025, muestran un nivel de cumplimiento bajo.

11.4 Reevaluar los siguientes indicadores:

- Procesos de adquisición de equipos de hardware y/o herramientas de software
- Porcentaje de avance del plan de acción de la política Gobierno Digital para la vigencia.
- Porcentaje de avance del plan de acción de la política Gobierno Digital para la vigencia.
- Porcentaje de avance del plan de acción de la política Seguridad Digital para la vigencia.

Lo anterior, debido a que dichos indicadores presentaron un bajo nivel de cumplimiento. En caso de considerarse necesario, se recomienda implementar acciones adicionales o establecer un plan de mejoramiento que permita asegurar el cumplimiento de las metas previstas.

ELÍAS ALONSO NULE RHENALS
Jefe de Oficina de Control Interno

Elaboró: Diana Elizabeth Patiño Sabogal
Revisó: Luz Dary Amaya Peña