



INFORME DE SEGUIMIENTO



SEGUIMIENTO DE LEY DERECHOS DE AUTOR DE SOFTWARE

**FECHA DE CORTE:
28 DE FEBRERO DE 2025**

**RESPONSABLES:
ANDRÉS DIAZ MOLINA
Jefe de Oficina de Tecnologías de la Información**

**CRISTIAN DONCEL PERDOMO
GIT de Administración de Bienes**

**ELABORADO POR:
RAFAEL HERNANDO CALLE CABEZAS**

**JUAN DIEGO TORO BAUTISTA
Jefe de la Oficina de Control Interno**

**MARZO DE 2025
OFICINA DE CONTROL INTERNO**



TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS.....	3
2.1. OBJETIVO GENERAL	3
2.2. OBJETIVO ESPECÍFICO	3
3. ALCANCE DEL INFORME.....	3
4. MARCO NORMATIVO	4
5. RESULTADO DEL SEGUIMIENTO	4
6. CONCLUSIONES	12
7. RECOMENDACIONES	13



1. INTRODUCCIÓN

De conformidad con las Directivas Presidenciales 001 de 1999 y 002 de 2002, y las Circulares 07 de 2005, 017 de 2011 y 027 de 2023 expedidas por la Unidad Administrativa Especial de Derechos de Autor, se realiza el presente informe con el cual se ejecutó en la Entidad la verificación, seguimiento y resultados sobre el cumplimiento de las normas en materia de software del 2024 de acuerdo con los criterios definidos por la Dirección Nacional de Derechos de Autor - DNDA.

El propósito de este informe es el de realizar la verificación de cumplimiento de uso de software en la entidad, para lo cual la Oficina de Control Interno - OCI en desarrollo del Programa Anual de Auditoría Interna vigencia 2025 aprobado por el Comité Institucional de Coordinación de Control Interno, solicitó a la Oficina de TI, al GIT de Administración de Bienes, al GIT de Administración de Personal y a la Subdirección de Gestión Contractual, la información y soportes necesarios para analizar, cotejar y contrastar los diferentes aspectos que componen la normatividad relacionada con el licenciamiento de software instalado en los equipos de propiedad del MinTIC/FUTIC.

2. OBJETIVOS

2.1. Objetivo General

Verificar el cumplimiento en la Entidad de las normas en materia de derechos de autor sobre el uso de software para la vigencia 2024, de acuerdo con lo definido en las Directivas Presidenciales 001 de 1999 y 002 de 2002 y las Circulares 07 de 2005, 017 de 2011 y 027 de 2023 expedidas por la Unidad Administrativa Especial de Derechos de Autor.

2.2. Objetivo Específico

Verificar la información remitida por la Oficina de Tecnologías de la Información – OTI y el GIT de Administración de Bienes, con el fin de consolidar y diligenciar el cuestionario dispuesto en la página oficial de la Dirección Nacional de Derechos de Autor - DNDA.

3. ALCANCE DEL INFORME

El alcance incluye la validación de los equipos de cómputo con los que cuenta la Entidad (propios y en alquiler), la verificación de los mecanismos de control de instalación de software implementados en la vigencia 2024 y hasta febrero del 2025, y los mecanismos para dar de baja el software.



4. MARCO NORMATIVO

- Directiva Presidencial 001 de 1999: En la cual el gobierno colombiano es consciente de la creciente importancia de la creación, compra, venta y uso de los bienes protegidos por el derecho de autor y los derechos conexos en el país, dentro de las entidades del estado a todos los niveles y realiza las respectivas consideraciones.
- Directiva Presidencial 002 de 2002: En la cual reitera el interés del gobierno en la protección del derecho de autor y los derechos conexos e imparte instrucciones en relación con la adquisición de programas de computador (software) debidamente licenciados, en donde se respete el derecho de autor de sus creadores.
- Circular 07 de 2005: En la cual el consejo asesor del gobierno nacional en materia de control interno de las entidades del orden nacional y territorial solicitó, de conformidad con lo ordenado en la Directiva Presidencial No. 002 de 2002 respecto al derecho de autor y los derechos conexos, en lo referente a la utilización de programas del ordenador (software), enviar la información relacionada con la "Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software".
- Circular 017 de 2011: En la cual se modifica la circular 12 de 2007, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).
- Circular 027 de 2023: En la cual se modifica la circular 017 de 2011, sobre las recomendaciones, seguimiento resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).

5. RESULTADO DEL SEGUIMIENTO

De conformidad con las Directivas Presidenciales 001 de 1999 y 002 de 2002 y las Circulares 07 de 2005, 017 de 2011 y 027 de 2023 expedidas por la Unidad Administrativa Especial de Derechos de Autor, la Oficina de Control Interno - OCI mediante solicitudes de información, verificación documental y reuniones aclaratorias con los gestores encargados, realizó seguimiento con el fin de determinar el cumplimiento de las normas en materia de derecho de autor de software de acuerdo con los criterios definidos por la Dirección Nacional de Derechos de Autor.

Las solicitudes fueron realizadas el 18 de febrero de 2025 como se detallan a continuación:



INFORME DE SEGUIMIENTO



Tabla 1. Requerimientos realizados.

Id Req	Área encargada	Detalle Requerimiento
1	Oficina de TI	<ul style="list-style-type: none">• Indicar con cuántos equipos cuenta la entidad, incluyendo el inventario de equipos en alquiler.• Indicar si todo el software instalado y utilizado se encuentra debidamente licenciado (Si/No y justificar)• Informar sobre los mecanismos de control para mitigar la instalación de software, detallando los que se hayan implementado, la documentación aplicable, las acciones definidas y las directrices, reglas y políticas de seguridad de la información implementadas.• Informar sobre cual es el destino final que se le da al software dado de baja en la entidad.
2	GIT de Administración de Bienes	Reporte de inventario de activos tecnológicos del año 2024 y lo corrido del 2025.
3	Subdirección Administrativa	Listado Planta de Personal vigente.
4	Subdirección de Gestión Contractual.	Listado Contratistas vigente.

Al respecto, para cada criterio establecido por la Dirección Nacional de Derechos de Autor -DNDA se dieron respuesta en los siguientes términos:

1. ¿Con cuántos equipos cuenta la entidad?

La OTI indicó que *“De acuerdo con la resolución 3066 del 2022 es responsabilidad del GIT Administración de Bienes Administrar el inventario de bienes muebles e inmuebles (tangibles e intangibles) del Ministerio / Fondo Único de TIC, y por ende el control de los equipos propios del MinTIC; con respecto a equipos en alquiler, se cuenta con un total de 990, los cuales se encuentran cubiertos bajo el contrato 1265-2023”*.

Soportes: “Inventario parque computacional.xlsx”

Al respecto, la OCI detectó que no se incluyeron los servidores en este reporte, por lo cual la OTI proyectó un alcance el 28 de febrero de 2025 entregando la relación de 26 servidores en propiedad del MinTIC.

Soportes: “Servidores.xlsx”.

La sumatoria de estas 2 entregas de información da como resultado 1016 equipos (990 alquiler, 26 servidores propios MinTIC).



INFORME DE SEGUIMIENTO



Por otra parte, se solicitó al GIT de Administración de Bienes el "Reporte de inventario de activos tecnológicos" del año 2024-2025 sobre los equipos propios, en donde remitió el reporte de inventario de equipos de cómputo de propiedad del FUTIC e informando que, validado en el módulo de inventarios y activos fijos del aplicativo SEVEN, no registra equipos tecnológicos de propiedad del MinTIC. El conteo de estos equipos suma 166 (83 computadores de escritorio, 42 portátiles y 41 servidores).

Soporte: "Reporte de inventario de activos tecnológicos FUTIC.xlsx".

La oficina de control interno identificó las siguientes diferencias en lo entregado por las anteriores dependencias:

- BD1-OTI: La OTI reportó 26 servidores de propiedad "PropioMinTIC".
- BD2-Bienes: El GIT de Administración de Bienes reportó 41 servidores de propiedad "PropioFUTIC" y ningún servidor de propiedad del MinTIC.

Realizando el análisis de las dos (2) bases de datos anteriores por serial del servidor, se identificaron las siguientes situaciones:

- Entre BD1-OTI y BD2-Bienes cruzan 12 servidores.
- En BD1-OTI hay 14 servidores PropioMinTIC que no están en BD2-Bienes.
- En BD2-Bienes hay 29 servidores PropioFutic que no están en BD1-OTI.

La Oficina de Control Interno conoce que pueden existir varios encargados de la información y que cada uno la administre de manera independiente, sin embargo, el no contar con un responsable único en la Entidad, está generando que los ejercicios de validación al cumplimiento de la Ley de derechos de autor de software, impliquen diferencias sustanciales y un posible impacto en no tener claras las cantidades de equipos en la Entidad.

La situación anterior fue reportada por la Oficina de Control Interno en el informe de seguimiento de marzo de 2022:

"No 7: Por otra parte, aunque la Oficina de TI y la subdirección administrativa (GIT de Administración de Bienes) gestionan, hacen seguimiento y controlan los equipos de cómputo y el software de estos, cada uno maneja de manera independiente su información, implicando falta de un control centralizado y efectivo que le permita al Ministerio conocer y mantener actualizado un único inventario. Tomando como referencia los seguimientos realizados en las vigencias anteriores, en este informe se reitera la importancia de centralizar la responsabilidad sobre el control en los derechos de autor de software en la entidad, por lo cual es necesario que se incluya dentro del plan de mejoramiento, una actividad para definir y establecer este liderazgo."



INFORME DE SEGUIMIENTO



Y que ante esta situación la OTI estableció un plan de mejoramiento con la acción correctiva #1570 en la que definió:

“La Oficina de TI implementará controles que aseguren que el software instalado en los equipos de la entidad se encuentre debidamente licenciado y realizará revisiones semestrales para validar el licenciamiento en los equipos propios y en alquiler, con el fin de mantener un control centralizado. La gestión de entrega de información será centralizada a través de la Oficina de TI, pero es la Subdirección Administrativa la encargada de custodiar el inventario de los equipos de cómputo de propiedad de la entidad, y la Oficina de TI la encargada de custodiar el inventario de los equipos de cómputo en servicio de alquiler. Adicionalmente documentará el control en la hoja de controles del mapa de riesgos de seguridad y privacidad de la información del proceso de TI Descripción de la meta: Archivo actualizado con el inventario de equipos de cómputo de propiedad de la entidad y en servicio de alquiler y su respectivo licenciamiento y el mapa de riesgos de seguridad y privacidad”.

Se recomienda establecer un solo responsable en la Entidad (MinTIC y FUTIC), que garantice que los inventarios de equipos sean precisos e identificables y que los mecanismos de control detallados en los siguientes capítulos, puedan verse correctamente implementados.

Por lo anterior, es necesario establecer un plan de mejoramiento que cuente con una estrategia para mitigar la ocurrencia de la situación anteriormente detectada y mantener un único inventario en la entidad (MinTIC y FUTIC).

Concluyendo la pregunta planteada de este apartado al criterio solicitado por el DNDA, la sumatoria de los equipos con los que cuenta la entidad, excluyendo los seriales que cruzan, es 1170 equipos de cómputo (1016+166-12).

2. ¿El software instalado en estos equipos se encuentra debidamente licenciado?

Al respecto, la OTI indicó que: “Sí, todo el software se encuentra debidamente licenciado, los equipos de alquiler están respaldados mediante contrato 1265-2023 y los equipos propios acorde con la renovación de licenciamiento por medio de otros contratos. Se anexa documento donde se relaciona en la columna “Modalidad contractual” y descripción de licencia, los contratos asociados, cantidad y tipo de licenciamiento con el que cuenta actualmente la entidad”.

Soporte: “Inventario Licencias DataCenter - OTI Diciembre 2024.pdf”.

Lo anterior, corroborado con los mecanismos de control implementados en el siguiente capítulo.



INFORME DE SEGUIMIENTO



3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?

Este criterio del DNDA fue validado por la Oficina de Control Interno en varios aspectos, cada uno de ellos validados individualmente:

- i. Mecanismos de control generales.
- ii. Normatividad, políticas, procedimientos, manuales, guías o instructivos implementados.
- iii. Implementación de mecanismos de control.
- iv. Identificación de riesgos y controles.

i-. Con relación a los mecanismos de control generales (i), la OTI indicó que:

MinTIC ha implementado diferentes mecanismos de control para evitar la instalación de programas no autorizados o que no cuenten con el respectivo licenciamiento así:

- ✓ Políticas de Gestión de Software: Se ha establecido una línea base respecto al software autorizado dentro de la Entidad, la cual se fundamenta en el software efectivamente licenciado y aprobado para su uso. Esta línea base no solo especifica las aplicaciones y herramientas que pueden ser utilizadas, sino que también define las características mínimas que deben cumplirse para asegurar que el software entregado al usuario final cumpla con los estándares de calidad, seguridad y funcionalidad previamente establecidos. De esta manera, se garantiza que todas las versiones del software proporcionado sean compatibles, eficaces y estén dentro de los parámetros legales de licenciamiento. Además, se establece un marco para la gestión y control de las actualizaciones o modificaciones, asegurando la integridad y continuidad de los procesos dentro de la entidad.
- ✓ Controles de acceso: Se tienen implementadas políticas específicas en la GPO (Group Policy Object) para la asignación y gestión de permisos, garantizando que solo los administradores tengan la capacidad de instalar, modificar o eliminar software en los equipos de la red. Estas políticas están diseñadas para fortalecer la seguridad del sistema, restringiendo las acciones críticas relacionadas con el software únicamente a los usuarios con privilegios administrativos. Además, se han configurado restricciones que impiden que usuarios no autorizados realicen cambios que puedan comprometer la integridad del sistema, asegurando que las instalaciones o actualizaciones de software sean controladas de manera centralizada y conforme a las directrices establecidas por la Oficina de TI.



INFORME DE SEGUIMIENTO



- ✓ Listas blancas de Software: Garantiza que únicamente las aplicaciones previamente aprobadas puedan ejecutarse en los dispositivos de la Entidad, la cual permite la ejecución exclusivamente de programas registrados, verificados y autorizados, mientras que bloquea cualquier intento de ejecutar software no autorizado o potencialmente peligroso. Las aplicaciones que no estén explícitamente incluidas en la lista blanca serán automáticamente bloqueadas, lo que reduce significativamente el riesgo de infecciones por malware, el uso de software no licenciado o el acceso a aplicaciones no conformes con las políticas establecidas.
- ✓ Seguridad en la red: A través del firewall, se gestiona de manera efectiva el bloqueo de sitios web que puedan contener software no licenciado, malicioso o potencialmente peligroso para la seguridad de la infraestructura tecnológica de la Entidad. Esta solución de seguridad perimetral permite la filtración de tráfico web en tiempo real, bloqueando el acceso a páginas que estén en listas negras o que se sospeche que puedan distribuir malware, virus, o aplicaciones no autorizadas que puedan comprometer la integridad de los dispositivos y la red. Además, el firewall se configura para identificar y restringir sitios de alto riesgo, como aquellos asociados con actividades ilícitas o que no cumplan con las políticas de seguridad.
- ✓ Controles de acceso físico: Se ha implementado una política de seguridad que bloquea puertos USB con el objetivo de evitar que los usuarios conecten medios extraíbles que puedan contener software no autorizado, malware o cualquier tipo de amenaza cibernética. Esta medida previene la transferencia no controlada de archivos o aplicaciones entre dispositivos, minimizando el riesgo de infecciones o la instalación de software no licenciado en los equipos de la Entidad. Con esta estrategia, se refuerza la seguridad de la infraestructura tecnológica, protegiendo los equipos de posibles vulnerabilidades asociadas con el uso indiscriminado de medios extraíbles.

ii-. La Oficina de Control Interno indagó sobre la normatividad, políticas, procedimientos, manuales, guías o instructivos implementados en la Entidad con relación a Derechos de autor de software, para lo cual la OTI indicó:

Resolución 2239 de 2024: Publicada en el portal web de la Entidad sobre políticas de privacidad ¹. Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones. En esta política se definen los lineamientos frente al uso y manejo de la información, y se tiene definidas las políticas que:

¹ <https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicasy/2627:Politicasy-Privacidad-y-Condiciones-de-Uso>



INFORME DE SEGUIMIENTO



“Aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, aplica a toda la información creada, procesada o utilizada por el Ministerio/Fondo Único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre”.

Lo anterior, específicamente definido en:

- Artículo 10. Política Legal y Cumplimiento “Los funcionarios, contratistas y colaboradores que ejecuten actividades de adquisición o licenciamiento de software tienen el deber de seguir los lineamientos de compra pública e incluir dentro de los estudios previos y pliegos de condiciones, los términos mediante los cuales se acreditará que la forma del licenciamiento, la forma en la que se ejercerán derechos morales y patrimoniales de autor, el número máximo de usuarios o recursos, la forma de instalación y los procedimientos para mantener las condiciones de licencia adecuadas, desechar o transferir software a otros. Igualmente, a través de la Oficial de Datos Personales, se establecerá y comunicará la política específica sobre privacidad y protección de la IIP, que, a efectos de la legislación local, corresponde a la Política de Tratamiento de Datos Personales”
- Artículo 19. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas: que indica que “(...) cualquier software que opere en el Ministerio de Tecnologías de la Información y las Comunicaciones deberá contar con la autorización de la Oficina de Tecnologías de la Información y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro(...)”.

Manual de Políticas de Seguridad y Privacidad de la Información SPI-TIC-MA- 001, relacionado con los Lineamientos de seguridad de las operaciones (capítulo 6.7):

- Código: SI-6.7.5 - Control de software operacional y Gestión de la vulnerabilidad técnica: En el literal k. “La Oficina de Tecnologías de la Información debe realizar de manera periódica una inspección del software instalado en los equipos del Ministerio/Fondo Único de TIC y debe desinstalar el software no autorizado, así como los establecidos en,



INFORME DE SEGUIMIENTO



- Código: SI-6.6.2 - Equipos y Dispositivos Móviles: en el literal x. La Oficina de Tecnologías de la Información, debe establecer los mecanismos técnicos u operativos en aras de garantizar que los computadores portátiles personales, cuenten con software licenciados y antivirus actualizado.

Formatos: En cuanto a los requerimientos que pueden generar los usuarios relacionados con la instalación de un software específico, la entidad cuenta con el formato GTI-TIC-FM-007 Solicitud de autorización de software, donde se relaciona la información necesaria para el análisis, evaluación y autorización por parte del equipo de seguridad de la OTI, con el cual se contemplan los criterios de seguridad necesarios para la autorización o negación de este.

iii-. Sumado a lo anterior, la Oficina de Control Interno indagó sobre cómo se valida que los mecanismos de control anteriores se encuentren adecuadamente implementados, para lo cual la OTI informó sobre el uso del módulo en la herramienta de gestión de servicios que permite el seguimiento y la correcta asignación de licencias de software, para:

- Implementación de política de control de acceso relacionada con la restricción de derechos de instalación y modificación de software, solo para personal autorizado.
- Implementación de listas blancas para el bloqueo de la ejecución de software no registrado y prevenir la instalación de aplicaciones no autorizadas.
- Análisis detallado de los logs generados por los sistemas y aplicaciones, con el objetivo de identificar comportamientos anómalos, accesos no autorizados, o cualquier otra actividad que pueda indicar un incumplimiento de las normativas de seguridad o de funcionamiento.

Soportes: “Evidencia bloqueo de software”, “GTI-TIC-FM-007 Solicitud de autorización de software”, “SPI-TIC-MA-001 Manual de políticas de seguridad y privacidad de la información” y “Documento Word donde se registra capturas de pantalla sobre la gestión del antivirus, seguridad perimetral, inteligencia sobre amenazas y derechos de propiedad intelectual”.

iv-. Por último, la OCI indagó sobre la identificación de riesgos y la implementación de controles internos en el proceso, para lo cual, se confirmó:

- Control: A.18.1.2. Derechos de Propiedad Intelectual: Validar el cumplimiento de los requisitos legales, normativos y contractuales relacionados con los Derechos de propiedad intelectual y el uso de software licenciado. Relacionado en el Mapa de riesgos SPI (GTI-TIC-DI-005) Gestión de Tecnologías de la Información- Versión 5.
- Control: A.5.32 Derechos de propiedad intelectual: Validar el cumplimiento de los requisitos legales, normativos y contractuales relacionados con los



INFORME DE SEGUIMIENTO



Derechos de propiedad intelectual y el uso de software licenciado. Relacionado en los Mapas de riesgos SPI (GTI-TIC-DI-005) Gestión de Tecnologías de la Información - Versiones 7 y 8.

- Control: CGTI 20 Verificación del Cumplimiento de Derechos de Autor. Relacionado en el Mapa de Mapa de riesgos de Gestión (GTI-TIC-DI-003). Relacionado en los Mapas de riesgos SPI (GTI-TIC-DI- 005) Gestión de Tecnologías de la Información - Versiones 5 y 6.

Soportes: “Repositorios de información discriminando las evidencias y soportes de ejecución de los controles de acuerdo al mapa de riesgos de SPI y de Gestión, de acuerdo con su periodicidad y el año de vigencia”.

Por temas de seguridad y privacidad de la información, en este informe no se presentan los datos sensibles de los servidores, equipos de cómputo, software y soportes de ejecución de los controles. Para las situaciones identificadas en este seguimiento que impliquen mejoras en la implementación de mecanismos de control, se gestionarán directamente con las dependencias responsables.

4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?

La destinación final de los bienes dados de baja está descrita en el Manual de administración de Bienes (GRA-TIC-M-002) y el procedimiento de bajas y destinación final de bienes (GRA-TIC-PR-010), lo cual es competencia del Comité de Administración de Bienes autorizar la baja de los estados financieros y su destinación final de acuerdo con lo establecido en dichos manuales y procedimientos, por lo cual, la destinación final de licenciamiento de software es competencia del mencionado comité previo concepto de la Oficina de TI.

6. CONCLUSIONES

La Entidad tiene implementado mecanismos de control para monitorear la instalación de software en los equipos de cómputo por medio de las políticas, manuales, procedimientos, instructivos y formatos.

Se realizó oportunamente por parte de la Oficina de Control Interno el registro ante la Dirección Nacional de Derechos de Autor DNDA de acuerdo con la normativa aplicable.

Al interior de la Entidad se gestionarán las actividades de mejoramiento necesarias para cerrar las brechas identificadas en el seguimiento al cumplimiento en la entidad de las normas en materia de derechos de autor sobre el uso de software.



INFORME DE SEGUIMIENTO



7. RECOMENDACIONES

- Establecer un único responsable en la Entidad (MinTIC y FUTIC), que garantice que los inventarios de equipos sean precisos e identificables y que los mecanismos de control definidos puedan verse correctamente implementados.
- Mantener un repositorio centralizado de información con las evidencias y soportes al cumplimiento de las normas en materia de derechos de autor sobre el uso de software, como la ejecución de controles, y en particular, con el monitoreo que se realiza a los equipos de cómputo de la entidad (MinTIC y FUTIC).

Aprobó:

JUAN DIEGO TORO BAUTISTA
Jefe Oficina de Control Interno

Elaboró: Rafael Hernando Calle Cabezas

REGISTRO DE FIRMAS ELECTRONICAS

Informe Seguimiento Derechos de Autor 2024

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20250321-165616-7c1428-68679481

Creación: 2025-03-21 16:56:16

Estado: Finalizado

Finalización: 2025-03-21 16:59:54



Escanee el código
para verificación

Aprobación: Jefe Oficina de Control Interno

Juan Diego Foro Bautista

79569758

jtorob@mintic.gov.co

Jefe de Oficina de Control Interno

Ministerio de Tecnologías de la Información y las Comunicaciones

REPORTE DE TRAZABILIDAD

Informe Seguimiento Derechos de Autor 2024

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20250321-165616-7c1428-68679481

Creación: 2025-03-21 16:56:16

Estado: Finalizado

Finalización: 2025-03-21 16:59:54



Escanee el código
para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Aprobación	Juan Diego Toro Bautista jtorob@mintic.gov.co Jefe de Oficina de Control Interno Ministerio de Tecnologías de la Informac	Aprobado	Env.: 2025-03-21 16:56:20 Lec.: 2025-03-21 16:59:45 Res.: 2025-03-21 16:59:54 IP Res.: 181.53.156.20