TIC

Informe de Ley

SEGUIMIENTO DE LEY DERECHOS DE AUTOR DE SOFTWARE

Oficina de Control Interno

Marzo de 2026

Informe de Ley

TABLA DE CONTENIDO

Informe de Ley

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 genera este 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 2025 de acuerdo con los criterios definidos por la Dirección Nacional de Derechos de Autor - DNDA.

La Oficina de Control Interno - OCI en desarrollo del Programa Anual de Auditoría Interna vigencia 2026 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

2.2. 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 2025, 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.

2.3. Objetivos Específicos

- 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.

- Validar los mecanismos de protección que se han implementado para monitorear la instalación de software en la Entidad, definidos en lineamientos, documentación y en general, en la normativa interna implementada sobre derechos de autor de software confirmando que los controles definidos se hayan ejecutado de acuerdo con lo establecido.

- Validar el estado de las acciones de los planes de mejora definidas en anteriores vigencias.

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 2025 y hasta febrero del 2026, y los mecanismos para dar de baja el software.

4. MARCO NORMATIVO

- Directiva Presidencial 001 de 1999: En la cual el gobierno 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 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, respetando 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 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. RESULTADOS DEL INFORME

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, 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 se realizaron el 9 de febrero de 2026 de la siguiente manera:

Req	Área encargada	Detalles del Requerimiento
1	Oficina de TI	• Indicar con cuántos equipos cuenta la entidad. • Inventario de equipos. • 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. • Relación de Controles de la matriz de riesgos y soportes de ejecución de controles. • Herramientas de monitoreo. • Informar sobre cual es el destino final que se le da al software dado de baja en la entidad. • Aclaración de equipos de alquiler. • Inventario de Contratos de mantenimiento y renovación de licenciamiento. • Reporte de incidentes y requerimientos.
2	Subdirección de Gestión Contractual.	• Listado activo de Contratistas.
3	Subdirección Administrativa	• Listado activo de Planta de Personal.
4	GIT de Administración de Bienes	• Reporte de inventario de activos tecnológicos del año 2025 y lo corrido del 2026.

Tabla 1. Requerimientos solicitados al proceso.

A continuación, se desarrollan los 3 objetivos específicos definidos:

5.1. OBJETIVO ESPECÍFICO 1. 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.

La información aportada permite realizar el correcto registro ante la Dirección Nacional de Derechos de Autor DNDA, contestando las cinco (5) preguntas del formulario con los siguientes datos:

a. ¿Con cuántos equipos cuenta la entidad?

Respuesta: 1227.

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

Respuesta: Si.

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

Respuesta: 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 tiene implementado 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.

- 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.

d. ¿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-MA-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.

e. A parte de diligenciar este aplicativo, las mismas preguntas deben estar relacionadas y contestadas en un informe suscrito por el jefe de Control Interno o quien haga sus veces, el cual debe ser subido al sitio web de su entidad. El link de esta publicación, lo deberá relacionar a continuación.

https://www.mintic.gov.co/portal/inicio/Micrositios/Biblioteca-de-informes/Informe-de-Verificacion-del-Cumplimiento-de-las-Normas-en-Materia-de-Software/

5.2. OBJETIVO ESPECÍFICO 2. Validar los mecanismos de protección que se han implementado para monitorear la instalación de software en la Entidad, definidos en lineamientos, documentación y en general, en la normativa interna implementada sobre derechos de autor de software confirmando que los controles definidos se hayan ejecutado de acuerdo con lo establecido.

5.2.1. Información suministrada por la Oficina de Tecnologías de la Información.

A continuación, se presenta el Requerimiento No. 1 dirigido a la Oficina de Tecnologías de la Información, junto con las respuestas recibidas (no todas explícitas). Por motivos de seguridad de la información, algunas respuestas no se incluyen en este informe. Este requerimiento estuvo compuesto por 10 preguntas.

1. ¿Con cuántos equipos cuenta la entidad?

De conformidad con la Resolución 3066 de 2022, el GIT Administración de Bienes es responsable de administrar el inventario de bienes muebles e inmuebles del MinTIC / FUTIC y, por ende, del control de los equipos propios de la entidad. Conforme a la información reportada, la entidad cuenta con un total de 107 equipos propios (29 servidores y 78 equipos de cómputo). Se cuentan con 1.120 equipos en modalidad de alquiler, estos últimos cubiertos bajo el Contrato No. 1265-2023 el cual inició el 24-11-2023 y finaliza hasta el 31-07-2026.

2. Reporte de los equipos de cómputo.

Se anexa reporte con la totalidad de los equipos de cómputo con los que cuentan el MinTIC/FUTIC, en el cual se discriminan los equipos propios de cada entidad y los equipos en modalidad de alquiler, conforme a lo solicitado.

3. ¿Todo el software instalado y utilizado se encuentra debidamente licenciado?

Sí. La totalidad del software utilizado por la entidad se encuentra debidamente licenciado. Los equipos en modalidad de alquiler se encuentran respaldados mediante el Contrato No. 1265 de 2023, mientras que los equipos propios cuentan con licenciamiento vigente conforme a los procesos de renovación de licencias realizados a través de otros contratos.

4. Mecanismos de control para mitigar la instalación de software no autorizado.

4.1. ¿Qué mecanismos de control se han implementado?

- **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 tiene implementado 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.

- **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.

4.2. ¿Cuál es la documentación aplicable?

La Resolución 2239 de 2024 define lineamientos frente al uso y manejo de la información, se tiene definidas las políticas que: 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 TIC, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del MinTIC 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", específicamente en el 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 "(...) 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.(...)".

De igual manera en el Manual de Políticas de Seguridad y Privacidad de la Información SPI-TIC-MA-001, relacionado con los 6.7. Lineamientos de seguridad de las operaciones Código: SI-6.7.5 - Control de software operacional y Gestión de la vulnerabilidad técnica en su 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 Código: SI-6.6.2 - Equipos y Dispositivos Móviles en el literal x.

La OTI debe establecer los mecanismos técnicos u operativos en aras de garantizar que los computadores portátiles personales, cuenten con software licenciados y antivirus actualizado. En cuanto a los requerimientos que pueden generar los usuarios relacionados con la instalación de un software especifico, se 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.

4.3. Directrices, reglas y políticas de seguridad digital, cómo se validó que se encuentren correctamente implementadas.

Las reglas y políticas implementadas son las siguientes:

Política de Licenciamiento y Gestión de Software:

- Establecimiento de directrices claras sobre el uso de software licenciado, especificando qué versiones, aplicaciones y configuraciones son autorizadas las cuales se encuentran definidas en la línea base.
- Revisión periódica de las licencias de software para asegurar que las instalaciones sean legales y estén alineadas con los acuerdos contractuales.

Directorios Activos (Active Directory):

- Control de acceso: Uso de Active Directory (AD) para gestionar los permisos de acceso a los sistemas y aplicaciones, asegurando que solo usuarios autorizados puedan acceder a software licenciado.
- Grupos de seguridad: Creación de grupos de seguridad específicos para el acceso a software autorizado, restringiendo la instalación de programas no licenciados mediante políticas de seguridad.
- Políticas de auditoría: Activación de auditorías en AD para registrar eventos relacionados con el acceso y uso de software, para identificar cualquier acceso no autorizado o intento de instalación de software sin licencia.

En Firewalls:

- Filtrado de tráfico: Configuración de firewalls para bloquear el tráfico que provenga de fuentes no autorizadas, evitando la descarga o ejecución de software pirata o no licenciado desde redes externas.
- Monitoreo de tráfico: Implementación de reglas específicas en los firewalls para detectar patrones de tráfico que podrían indicar la descarga ilegal o la ejecución de software no licenciado.

- Control de aplicaciones: Uso de firewalls para controlar aplicaciones que se pueden ejecutar en red y bloquear que no están registradas o licenciadas.

Sistemas de Gestión de Información y Eventos de Seguridad:

- Monitoreo en tiempo real: Implementación de herramientas SIEM para correlacionar eventos relacionados con la ejecución de software en la red, permitiendo detectar comportamientos inusuales que sugieran la instalación o uso de software no autorizado a través del servicio de SOC NOC.
- Generación de alertas: Configuración de alertas automáticas ante la detección de la ejecución de software no registrado, mediante el servicio de monitoreo de SOC NOC.

Sistemas de Control de Aplicaciones (Application Control):

- Lista blanca de aplicaciones: Establecimiento de una lista blanca de aplicaciones aprobadas para su ejecución, bloqueando automáticamente cualquier software no autorizado, incluyendo el no licenciado.
- Herramientas de monitoreo de integridad: Implementación de herramientas que revisen la integridad de los archivos de software instalados y verifiquen su autenticidad y licenciamiento.

Control de Dispositivos y Almacenamiento Externo:

- Políticas de uso de dispositivos externos: Restricción del uso de dispositivos de almacenamiento externo (como USBs) para prevenir la instalación de software no licenciado desde dispositivos no autorizados.
- Monitoreo de conexiones externas: Inspección y control del tráfico hacia y desde dispositivos externos y evitar transferencia de software no licenciado.

Los documentos vigentes donde se encuentren definidas estas reglas son:

- Resolución 2239 de 2024.
- Manual de Políticas de SPI SPI-TIC-MA-001.
- Documentos internos de gestión. Manual de Operaciones.

Se valida que se encuentren correctamente implementadas las reglas anteriores:

- Uso del módulo en la herramienta de gestión de servicios que permite el seguimiento y la correcta asignación de licencias de software.
- Implementación de política de control de acceso relacionada con la restricción de derechos de instalación y modificación de software (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.

5. Controles definidos en la Matriz de Riesgos. Matrices de Riesgos y controles definidos.

Se relacionaron las siguientes matrices de riesgos:

- Mapas de Riesgos de SPI GTI-TIC-DI-005 versión 8 y 9.
- Mapas de Riesgos de GTI GTI-TIC-DI-003 versión 7, 8 y 9.

Los controles implementados son:

- Control: A.5.32 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 los Mapas de riesgos SPI. (GTI-TIC-DI-005) GTI versiones 8 y 9 con Periodicidad Trimestral.
- Control: CGTI 20 Verificación del Cumplimiento de Derechos de Autor. Relacionado en el Mapa de Mapa de riesgos de Gestión (GTI-TIC-DI-003), con Periodicidad: “Cada vez que se realice un desarrollo a la medida”.

Adicionalmente, la OTI dispuso de las evidencias y soportes de ejecución de los controles de acuerdo con mapa de riesgos de SPI y de Gestión.

6. Herramientas de monitoreo y control del software instalado.

La herramienta de monitoreo vigente es DEXON. La OTI entregó el respectivo reporte generado.

7. Dar de baja el software. ¿Cuál es el destino final que se le da al software dado de baja en la entidad?

La oficina de TI se encarga de emitir concepto técnico y funcional de los bienes intangibles, y no dar de baja el software de la entidad. La destinación final de los bienes dados de baja está descrita en el Manual de administración de Bienes (GRA-TIC-MA-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.

8.¿Cómo se valida el software licenciado en los equipos de alquiler?

Con base en el modelo de referencia de los equipos en modalidad de alquiler, se realizó la verificación del licenciamiento asociado al momento de la recepción de los equipos, constatando su cumplimiento conforme a las especificaciones del fabricante. La entidad valida que el software esté debidamente licenciado mediante la aplicación de procedimientos para la verificación del licenciamiento del SO Windows, conforme a las directrices del fabricante (documentado en el archivo “Manual para verificar licenciamiento Windows”). Adicionalmente, se tiene la Carta de originalidad de software de equipos

9. Inventario de contratos de mantenimiento y renovación de licenciamientos.

La OTI entregó el Inventario Licencias DataCenter – OTI con la relación de los contratos de mantenimiento y renovación de licenciamientos correspondientes a las vigencias 2025 y 2026, incluyendo las fechas de inicio y finalización.

10. Incidentes detectados con la instalación de software no autorizado.

El Coordinador de la Mesa de Servicios confirma que durante las vigencias 2025-2026 no se han recibido ni gestionado incidentes relacionados con la instalación de software no autorizado o incumplimiento de licenciamiento.

5.2.2. Análisis realizado a la información reportada.

Se realizó la revisión de la totalidad de las evidencias y soportes suministrados y como resultado de este análisis, se identificaron las siguientes fortalezas y prácticas destacadas positivas de gestión:

- **Ejecución de controles y gestión de evidencias.** A nivel general, se observa que la ejecución de los controles se está realizando conforme con las evidencias establecidas para cada una de ellas. Asimismo, se identificó la implementación de los repositorios independientes, que facilita la validación y el seguimiento preciso de la información a cada control. Esta estructura contribuye a una gestión más ordenada y a la reducción de los riesgos de duplicidad de información o de pérdida de evidencias.

- **Herramienta de monitoreo.** Se verificó que los reportes generados por la herramienta de monitoreo presentan una estructura adecuada y permiten realizar un seguimiento puntual del estado de los equipos de la Entidad. Esto promueve el análisis del software instalado y contribuye a la administración del inventario tecnológico y de las condiciones operativas de los equipos.

- **Consistencia entre los reportes de equipos propios y en alquiler.** Los reportes entregados respecto a los equipos de cómputo propios y en alquiler se encuentran consistentes en la información registrada. Esto evidencia un adecuado proceso de consolidación y unificación al interior de la Entidad, lo que fortalece la confiabilidad del inventario tecnológico.

- **Comunicación entre dependencias.** Se identificó la entrega de conceptos técnicos y funcionales de Equipos por parte de la OTI a la Coordinación de Administración de Bienes, para poder definir el tratamiento contable a aplicar (dar de baja del inventario de la Entidad.

- **Verificación del licenciamiento en equipos de alquiler.** Se identificaron soportes que acreditan la gestión de verificación realizada sobre los equipos en

alquiler. Entre los documentos más relevantes se encuentran las fichas técnicas de los equipos, las cartas de originalidad del software instalado, el manual para la confirmación del licenciamiento y el respaldo correspondiente al soporte y licenciamiento contractual (Contrato 1265 de 2023).

- **Sin incidentes o eventos registrados.** El Coordinador de la Mesa de Servicios confirmó que durante las vigencias 2025-2026 no se han recibido ni gestionado incidentes relacionados con la instalación de software no autorizado o incumplimiento de licenciamiento.

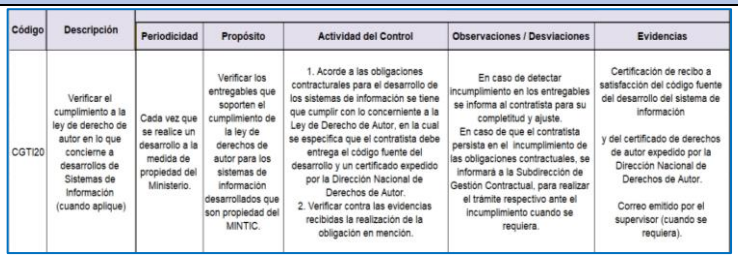
Pese a estas gestiones positivas, se identificaron las siguientes situaciones:

Hallazgo 1. La documentación, evidencias y soportes entregados se encuentran incompletos y/o presentan inconsistencias en la información suministrada.

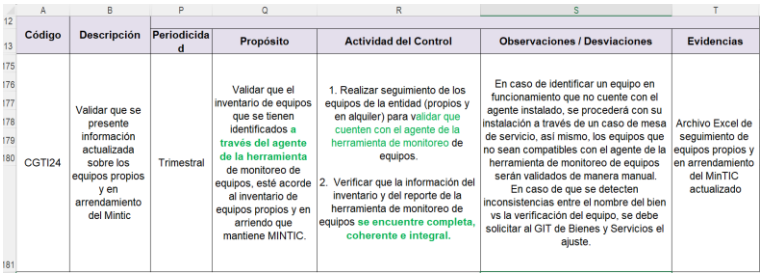
De acuerdo con los diferentes requerimientos realizados, se identificó que algunos de los soportes y evidencias suministrados presentan información inconsistente, incompleta o parcial. Esta situación limita la capacidad de verificación integral del proceso, afecta la trazabilidad de la información evaluada y puede generar riesgos en la confiabilidad de los resultados del análisis.

En la tabla siguiente se presentan cada uno de los casos identificados: el requerimiento con el cual se solicitó la información, las evidencias entregadas y la descripción de la inconsistencia observada.

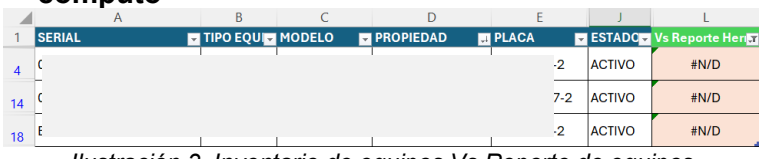
Id	Req	Información entregada	Inconsistencia identificada
1	1.5.3	GTI-TIC-DI-003 Mapa_RiesgosGestiondeTI v8 Certificado de registro DNDA SER 2021.pdf	**Se identifican evidencias parciales.** Se validaron los soportes suministrados relacionados con los controles ejecutados de las matrices de riesgos y se identificó que para la versión 8 del Mapa de riesgos de Gestión GTI-TIC-DI-003 control CGTI20 no se entregó una de las dos evidencias definidas. El control tiene definidas las siguientes evidencias: "Certificación de recibo a satisfacción del código fuente del desarrollo del sistema de información y del certificado de derechos de autor expedido por la Dirección Nacional de Derechos de Autor", sin embargo, solo se entregó el Certificado de registro ante el DNDA. El Certificado de recibo a satisfacción del código fuente del desarrollo del sistema de información no se relacionó dentro de las evidencias.

<table>
<tr><th>Id</th><th>Req</th><th>Información entregada</th><th>Inconsistencia identificada</th></tr>
<tr><td></td><td></td><td></td><td>

<table>
<tr><th>Código</th><th>Descripción</th><th>Periodicidad</th><th>Propósito</th><th>Actividad del Control</th><th>Observaciones / Desviaciones</th><th>Evidencias</th></tr>
<tr><td>CGTI20</td><td>Verificar el cumplimiento a la ley de derecho de autor en lo que concierne a desarrollos de Sistemas de Información (cuando aplique)</td><td>Cada vez que se realice un desarrollo a la medida de propiedad del Ministerio.</td><td>Verificar los entregables que soporten el cumplimiento de la ley de derechos de autor para los sistemas de información desarrollados que son propiedad del MINTIC.</td><td>1. Acorde a las obligaciones contractuales para el desarrollo de los sistemas de información se tiene que cumplir con lo concerniente a la Ley de Derecho de Autor, en la cual se especifica que el contratista debe entrega el código fuente del desarrollo y un certificado expedido por la Dirección Nacional de Derechos de Autor.
2. Verificar contra las evidencias recibidas la realización de la obligación en mención.</td><td>En caso de detectar incumplimiento en los entregables se informa al contratista para su completitud y ajuste.
En caso de que el contratista persista en el incumplimiento de las obligaciones contractuales, se informará a la Subdirección de Gestión Contractual, para realizar el trámite respectivo ante el incumplimiento cuando se requiera.</td><td>Certificación de recibo a satisfacción del código fuente del desarrollo del sistema de información
y del certificado de derechos de autor expedido por la Dirección Nacional de Derechos de Autor.
Correo emitido por el supervisor (cuando se requiera).</td></tr>
</table>
Ilustración 1. Control CGTI20 Mapa de Riesgos de gestión v8

Adicionalmente, con la acción correctiva 2819 se estableció como acción a tomar, el “Incluir un control en la Mapa de riesgos de Gestión del proceso de Gestión de TI que permita presentar información actualizada sobre los equipos propios y en arrendamiento del MinTIC” y para ello, la Oficina de TI indicó que se incluyó el control CGTI24 en el Mapa de riesgos de Gestión del proceso de Gestión de TI versión 8. Pese a lo anterior, no se suministraron soportes de ejecución de este control.

El control CGTI24 establecido es:

<table>
<tr><th>Código</th><th>Descripción</th><th>Periodicidad</th><th>Propósito</th><th>Actividad del Control</th><th>Observaciones / Desviaciones</th><th>Evidencias</th></tr>
<tr><td>CGTI24</td><td>Validar que se presente información actualizada sobre los equipos propios y en arrendamiento del Mintic</td><td>Trimestral</td><td>Validar que el inventario de equipos que se tienen identificados a través del agente de la herramienta de monitoreo de equipos, esté acorde al inventario de equipos propios y en arriendo que mantiene MINTIC.</td><td>1. Realizar seguimiento de los equipos de la entidad (propios y en alquiler) para validar que cuenten con el agente de la herramienta de monitoreo de equipos.
2. Verificar que la información del inventario y del reporte de la herramienta de monitoreo de equipos se encuentre completa, coherente e integral.</td><td>En caso de identificar un equipo en funcionamiento que no cuente con el agente instalado, se procederá con su instalación a través de un caso de mesa de servicio, así mismo, los equipos que no sean compatibles con el agente de la herramienta de monitoreo de equipos serán validados de manera manual.
En caso de que se detecten inconsistencias entre el nombre del bien vs la verificación del equipo, se debe solicitar al GIT de Bienes y Servicios el ajuste.</td><td>Archivo Excel de seguimiento de equipos propios y en arrendamiento del MinTIC actualizado</td></tr>
</table>
Ilustración 2. Control CGTI24 Matriz de Riesgos de gestión v8</td></tr>
<tr><td>2</td><td>1.5.2 y Respuesta el Informe preliminar</td><td>Reporte general de equipos de Mintic, propios y en arrendamiento.

Inventario de equipos de cómputo del MinTIC y FUTIC (Evidencia del Control CGTI24).</td><td>Se valida la integridad, completitud y coherencia de los datos mediante el cruce de información entre el ‘Reporte general de equipos” que se suministró por parte de la OTI y el ‘Inventario de equipos de cómputo’ que genera la herramienta de monitoreo. A partir de esta revisión se identificaron las siguientes debilidades:

• 3 seriales del ‘Reporte general de equipos” no están siendo mapeados en el “Inventario de equipos de cómputo’”

<table>
<tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>J</th><th>L</th></tr>
<tr><td>1</td><td>SERIAL</td><td>TIPO EQU</td><td>MODELO</td><td>PROPIEDAD</td><td>PLACA</td><td>ESTADO</td><td>Vs Reporte Her</td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td><td>-2</td><td>ACTIVO</td><td>#N/D</td></tr>
<tr><td>14</td><td></td><td></td><td></td><td></td><td>7-2</td><td>ACTIVO</td><td>#N/D</td></tr>
<tr><td>18</td><td></td><td></td><td></td><td></td><td>-2</td><td>ACTIVO</td><td>#N/D</td></tr>
</table>
Ilustración 3. Inventario de equipos Vs Reporte de equipos.</td></tr>
</table>

Id	Req	Información entregada	Inconsistencia identificada
			• 63 seriales del "**Inventario de equipos de cómputo**'" no se relacionaron en 'Reporte general de equipos".

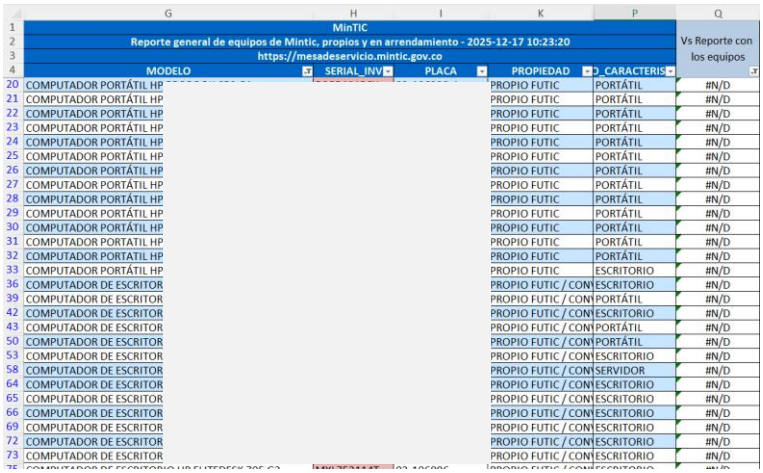


Ilustración 4. Reporte de Equipos de cómputo Vs Inventario

			• Diferentes campos vacíos o inconsistentes del "Inventario de equipos de cómputo'": - 94 registros sin "FECHA_ASIGNACION" - 271 registros sin "TIPO_USUARIO" - 265 registros sin "NOMBRE_RESPONSABLE" - 1 registro sin "TIPO_EQUIPO" - 36 registros sin "PLACA" - Entre otros campos con registros vacíos.

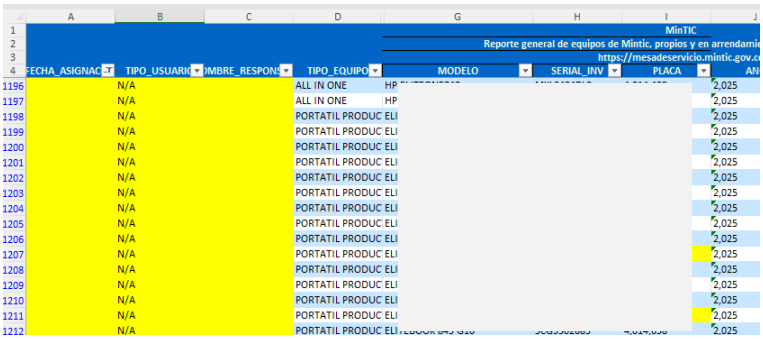


Ilustración 5. Inventario de Equipos sin información.

Tabla 2. Debilidades identificadas

Al respeto el proceso respondió:

Para el Id 1 para el control CGTI20 el proceso indicó que:

> "*En respuesta a la observación preliminar, nos permitimos informar que, de acuerdo con la respuesta adjunta emitida por el proveedor del Contrato No. 799 de 2025, a la fecha no se cuenta aún con la entrega de los derechos correspondientes, teniendo en cuenta que, conforme a lo establecido en el anexo técnico y en la última acta de seguimiento del citado contrato, dichos derechos serán entregados previamente a la liquidación de este. Actualmente, el proceso de liquidación se encuentra en trámite y existe la claridad que el objeto contractual debe cumplirse a cabalidad para que se pueda realizar la liquidación del mismo como lo establece la ley."* (Énfasis fuera de texto),

sin embargo, el control definido no contiene esta desviación ni advierte sobre las condiciones de entrega de las evidencias. Un control debe describir de manera clara y suficiente lo que requiere para funcionar; si falta esta desviación, el diseño del control estaría incompleto, o no se garantiza que quien lo ejecute entienda cuándo o cómo debe activarse y su propósito puede perderse o aplicarse erróneamente. Con lo anterior, el control no cubre adecuadamente el riesgo. Este caso se mantiene en el informe final.

Para el Id 1 para el control CGTI24 el proceso indicó que:

> *"En respuesta a lo asociado a este control, nos permitimos adjuntar en el repositorio las evidencias asociadas al tercer y cuarto trimestre de 2025 y de acuerdo el mapa de riesgos de Gestion de TI Versión 8 y Versión 9 respectivamente. Estas evidencias fueron entregadas y revisadas en el seguimiento que se hace mensualmente desde la OAPES"*,

sin embargo:

- El proceso no entregó la información solicitada en el requerimiento inicialmente realizado. Fue el equipo auditor quien identificó la información que debió haberse proporcionado, evidenciando una omisión por parte del proceso al no tener pleno conocimiento de los controles asociados a los derechos de autor de software.
- Se entregó información sobre la ejecución del control correspondiente a las versiones 8 y 9: ambos soportes son exactamente iguales, presentando los mismos registros y cantidades.
- Tras validar el reporte entregado, se identificaron varias situaciones adicionales, las cuales fueron incluidas en el Id 2 de la "Tabla 2. Debilidades identificadas".

Efectos:

- Evidencia insuficiente o inadecuada que reduce la confiabilidad de las actividades ejecutadas por el proceso.
- Reprocesos por riesgos de incumplimiento de lineamientos.

Causas:

- Falta de verificación de calidad previa a la entrega evidencia (doble revisión).
- Deficiencia en la definición de roles para compilación y validación.

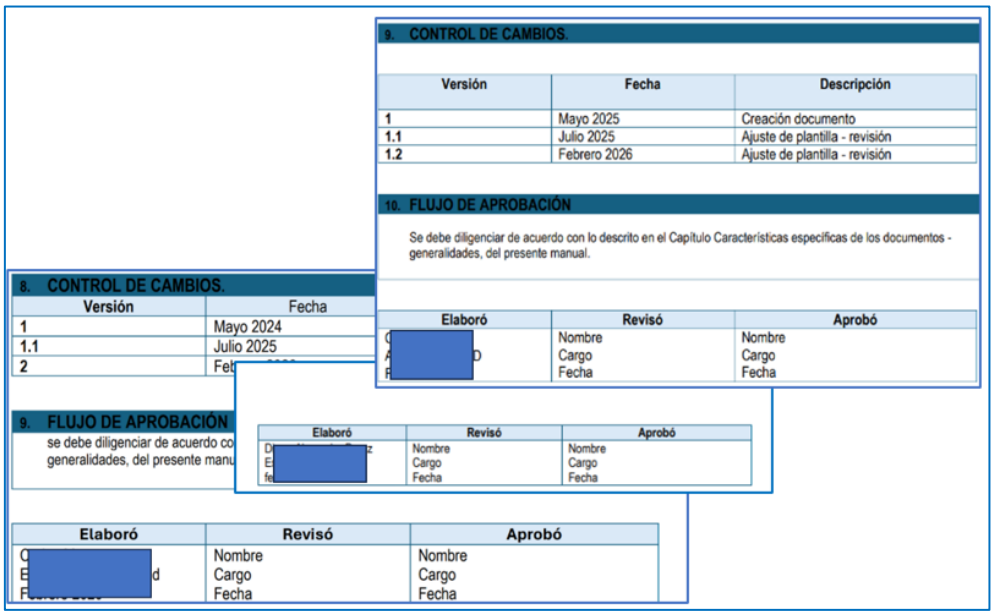
Recomendaciones:

- Implementar listas de verificación de completitud y coherencia antes de la entrega de las evidencias y soportes.
- Mantener centralizadas las evidencias en repositorios.
- Capacitar a los responsables en la entrega de evidencias que sean suficientes y adecuadas.
- Ajustar la redacción de los controles, agregando explícitamente la condición o desviación que hace que el control funcione.
- Mantener actualizado el inventario de equipos de cómputo de MinTIC y FUTIC, propios y en alquiler, con información íntegra, completa y verificable.

Observación preliminar 2. Existencia de documentos internos de gestión con información de carácter reservado que no cuentan con aprobación formal.

Con el requerimiento 1 numeral 4.3. se solicitó se informara sobre las reglas y políticas implementadas en los diferentes dispositivos de seguridad, servicios de control y tráfico de red y cómo asegura la Entidad que estas se encuentran aplicadas correctamente. Al particular, fueron entregados, entre otros, los documentos internos “Manual Administrador AD 2026”, “Manual Administrador Redes 2026” y “Manual Administrador Seguridad Perimetral 2026”, los cuales contienen información clasificada como reservada; sin embargo, estos documentos no han sido aprobados formalmente en la Entidad.

Ilustración 6. Captura de pantalla. Requerimiento 1 Id 4.3



9. CONTROL DE CAMBIOS.

Versión	Fecha	Descripción
1	Mayo 2025	Creación documento
1.1	Julio 2025	Ajuste de plantilla - revisión
1.2	Febrero 2026	Ajuste de plantilla - revisión

10. FLUJO DE APROBACIÓN

Se debe diligenciar de acuerdo con lo descrito en el Capítulo Características específicas de los documentos - generalidades, del presente manual.

Elaboró	Revisó	Aprobó
[redacted]	Nombre Cargo Fecha	Nombre Cargo Fecha

8. CONTROL DE CAMBIOS.

Versión	Fecha
1	Mayo 2024
1.1	Julio 2025
2	Feb

9. FLUJO DE APROBACIÓN

se debe diligenciar de acuerdo co
generalidades, del presente manu

Elaboró	Revisó	Aprobó
[redacted]	Nombre Cargo Fecha	Nombre Cargo Fecha

Elaboró	Revisó	Aprobó
[redacted]	Nombre Cargo Fecha	Nombre Cargo Fecha

Ilustración 7. Control de cambios de documentos internos.

Al particular, el proceso respondió que:

Respuesta:

En relación con la observación preliminar presentada frente a los documentos internos "Manual Administrador AD 2026", "Manual Administrador Redes 2026" y "Manual Administrador Seguridad Perimetral 2026", es importante precisar que dichos documentos corresponden a instrumentos técnicos de **carácter operativo y confidencial**, que contienen información sensible relacionada con la configuración, administración y operación de los controles de seguridad aplicados a la infraestructura tecnológica de la Entidad.

Debido a la naturaleza de la información contenida, estos documentos tienen clasificación de acceso restringido, en cumplimiento de los lineamientos de seguridad de la información, razón por la cual su disponibilidad se encuentra limitada exclusivamente a personal técnico debidamente autorizado, responsable de la administración y operación de los componentes tecnológicos descritos. Esta medida busca prevenir la divulgación no autorizada de información que pueda comprometer la seguridad de la infraestructura tecnológica y de los servicios institucionales.

Así mismo, es importante señalar que estos documentos hacen parte de entregables técnicos asociados a las actividades de ejecución del contrato, los cuales cuentan con validaciones y aprobaciones internas dentro del marco de la supervisión contractual, siendo revisados y constatados por el supervisor del contrato como parte del seguimiento a las actividades mensuales desarrolladas, **razón por la cual se evidencia claramente que cuentan con mecanismos estrictos de control para garantizar su debida revisión y aprobación.**

Adicionalmente, estos manuales corresponden a documentación dinámica de carácter operativo, que requiere actualizaciones y ajustes permanentes derivados de cambios en configuraciones, aplicación de parches de seguridad, implementación de nuevas políticas, ajustes en la arquitectura tecnológica o incorporación de nuevos controles de seguridad. En este contexto, la gestión formal de versiones mediante procesos administrativos de aprobación institucional podría generar cargas operativas adicionales que afectarían la capacidad de respuesta técnica y la actualización oportuna de la documentación, la cual debe mantenerse alineada con el estado real de las configuraciones y controles implementados en la infraestructura. Es asi que, estos documentos se gestionan como documentación técnica controlada dentro del equipo responsable de la operación tecnológica, manteniendo criterios de confidencialidad, acceso restringido y disponibilidad limitada, garantizando que únicamente el personal autorizado pueda consultarlos y utilizarlos en el marco de sus funciones.

Por último, es necesario tener en cuenta que, de acuerdo con las recomendaciones realizadas en el marco de la auditoria de seguimiento 1.2 (ONAC-ISO/IEC 27001:2022). Auditoría del 01 Dic.2025-05. ***Observación No. 5 Acción de mejora. Incorporar actividades de revisión de la normalización de registros con el fin de generar requerimientos al área de control de registros***, ya se tienen previstas las siguientes actividades las cuales se encuentran registradas en el plan de mejoramiento del proceso así:

- **Acción de Mejora 1104: Acción a Tomar**: Realizar el levantamiento del inventario de documentos no formalizados del proceso de Gestión de TI y llevar a cabo una reunión con la OAPES para establecer procedimiento a seguir con el fin de formalizar la documentación en SIMIG. **Descripción de la meta**:

Realizar el levantamiento del inventario de documentos no formalizados del proceso de Gestión de TI y llevar a cabo una reunión con la OAPES para establecer procedimiento a seguir con el fin de formalizar la documentación en SIMIG. **Denominación de la Unidad de medida de la meta**: Inventario y reunión con OAPES **Unidad de medida**: 2 (Inventario, acta de reunión)

En este sentido, es importante resaltar que, como parte del fortalecimiento de los controles asociados a los registros documentales con clasificación reservada generados en la OTI, la acción de mejora correspondiente ya se encuentra en proceso de validación conjunta con la OAPES.

Lo anterior tiene como propósito robustecer los mecanismos de aprobación contemplados en el marco de la supervisión del contrato, no obstante, es pertinente precisar que este mecanismo se enmarca en un ámbito independiente a la aplicación de los controles, reglas y políticas implementadas en los diferentes dispositivos de seguridad.

Haciendo extracción o síntesis de la respuesta del proceso se presenta que:

- Los documentos internos “Manual Administrador AD 2026”, “Manual Administrador Redes 2026” y “Manual Administrador Seguridad Perimetral 2026” son técnicos, operativos y confidenciales, con acceso restringido a personal autorizado.
- Se indica que estos documentos tienen validaciones y aprobaciones internas de acuerdo con el contrato y validados por el supervisor del contrato.
- Se argumenta que son documentos dinámicos que requieren actualizaciones y ajustes frecuentes y que ejecutar un proceso administrativo de aprobación formal de la Entidad genera cargas operativas adicionales que podría afectar la oportunidad.
- Se indica que existe la acción de mejora 1104 (en ejecución), producto de la auditoría de seguimiento ONAC-ISO/IEC 27001:2022 en donde se dejó una observación con el fin de inventariar documentos no formalizados y coordinar con OAPES el procedimiento de formalización en SIMIG.

sin embargo, la respuesta no desvirtúa la situación detectada y se mantiene en el informe final dado que:

- El proceso reconoce explícitamente que no existe aprobación formal de estos documentos, y que para ello tiene en marcha una acción registrada en SIMIG.
- Al momento de la validación de las evidencias suministradas no existía tal aprobación formal y por lo cual, la condición del hallazgo persiste.
- La revisión de un supervisor confirma el cumplimiento contractual y calidad de los entregables, pero no necesariamente equivale a una aprobación formal del documento en la Entidad.
- Por tratarse de documentos sensibles, no debe verse la aprobación formal de estos documentos como un trámite adicional ("cargas operativas adicionales"), dado que esto permite garantizar propiedad, responsabilidad, trazabilidad y controles de cambio, y evita la materialidad de los riesgos presentados.

Efectos: Esta situación genera riesgos asociados a la divulgación no autorizada de información reservada, al uso de documentos no oficiales para la toma de decisiones, a la falta de trazabilidad y posibles incumplimientos de las políticas de seguridad de la información

Causa: Ausencia de controles que garanticen la revisión y aprobación formal antes de la circulación interna del documento, o desconocimiento del procedimiento por parte de los responsables.

Recomendación: Implementar un mecanismo de control que garantice que todos los documentos que contengan información reservada sean revisados y aprobados formalmente antes de su difusión o uso.

5.3. OBJETIVO ESPECÍFICO 3. Validar el estado de las acciones de los planes de mejora definidas en anteriores vigencias.

Observación preliminar 3. Las acciones correctivas 2817 y 2819 se encuentra abiertas y vencidas en SIMIG.

Al realizar la validación en SIMIG de las acciones establecidas para dar atención al Plan de mejoramiento producto del seguimiento de vigencias anteriores, se evidenció que existen 2 acciones vencidas pendientes de cierre, incumpliendo con el procedimiento "Formulación, seguimiento y cierre de acciones de Mejora MIG-TIC-PR-003", específicamente la actividad 15 que indica:

> "*Solicitar la evaluación de eficacia de la acción: El proceso tiene como plazo máximo cinco (5) días hábiles, para carga de seguimiento y evidencias, previos a la fecha de compromiso (terminación) de la acción en la herramienta SiMIG (no se acepta como evidencia links que se redireccionen a aplicativos o páginas web) y solicitar la revisión y pertinencia del cierre de la meta o acción por medio de correo electrónico al auditor y asesor del proceso del GIT de Transformación Organizacional (…).".*

A continuación, se presenta el número de cada acción, su descripción, la fecha de compromiso y los seguimientos registrados:

Acción	Descripción / Fecha de Compromiso	Seguimientos registrados
2819	**Acción a tomar:** Incluir un control en la Mapa de riesgos de Gestión del proceso de Gestión de TI que permita presentar información actualizada sobre los equipos propios y en arrendamiento del Mintic. **Descripción de la meta:** Mapa de Riesgos de Gestión actualizado en SIMIG que incluya un control que permita presentar información actualizada sobre los equipos propios y en arrendamiento del Mintic **Denominación de la Unidad de medida de la meta:** Mapa de riesgos de Gestión del Proceso de Gestión actualizado en SIMIG **Unidad de medida:** 1 **Fecha de compromiso:** 30/nov./2025 **Estado:** Vencida	De acuerdo con lo aclarado por Teams, con relación al control CGTI24 se precisa: 1. La actividad 1 indica que "Realizar seguimiento de los equipos de la entidad (propios y en alquiler) para validar que cuenten con el agente de la herramienta de monitoreo de equipos", sin embargo, no se cuenta con una evidencia definida que concluya cuales equipos se encuentran sin el agente. Se recomienda actualizar la evidencia para conocer i) El 100% de los equipos de la entidad, ii) Los equipos que si tienen el agente instalado, iii) Los equipos que no tienen el agente instalado y el tiquete de solicitud a la Mesa de Servicios de acuerdo con la desviación definida en el control. 2. La actividad 2 indica que "Verificar que la información del inventario y del reporte de la herramienta de monitoreo de equipos se encuentre completa, coherente e integral", y tiene definido como evidencia, un reporte con los equipos y el software instalado, sin embargo, la matriz presentada no sustenta el verbo "Verificar", el cual es un ejercicio de comprobación, implicando confirmar si la información está correcta; para este caso, es validar si el software instalado cuenta con el licenciamiento adecuado. Se identifica que el control creado no cubre a todos los equipos de la entidad, y no valida la información del software instalado. Por lo anterior, no es procedente el cierre de la acción.
2817	**Acción a tomar:** Hacer el seguimiento periódico al cumplimiento a la ejecución de las actividades y evidencias del control "A.5.32 Derechos de propiedad intelectual" del mapa de Riesgos SPI V7. Nota: El Control A.5.32 remplazó al control A.18:1.2 del mapa de Riesgos SPI V5 y ya no está vigente a la fecha. **Descripción de la meta:** Enviar correo trimestral a los responsables, indicando el deber	Se identificaron 2 seguimientos registrados en esta acción: • Del 25/jul./2025: De acuerdo con el seguimiento periódico realizado, se adjuntan las evidencias del mes de Junio/2025. • Del 07/nov./2025: De acuerdo con el seguimiento periódico realizado, se adjuntan evidencias del mes de Septiembre/2025

Acción	Descripción / Fecha de Compromiso	Seguimientos registrados
	de dar cumplimiento a la ejecución de las actividades del control "A.5.32 Derechos de propiedad intelectual" del mapa de Riesgos SPI V7. Consolidar el seguimiento de las evidencias de las actividades de este control en el informe de cada trimestre durante lo que resta del 2025. **Denominación de la Unidad de medida de la meta:** Correo e Informes de Junio, Septiembre y Diciembre 2025. **Unidad de medida:** 3 informes y 3 correos. **Fecha de compromiso:** 31/ene./2026 **Estado:** Vencida	

Al respecto el proceso indicó que:

> **Respuesta:**
>
> **Para la acción 2819**: Se cuenta con la programación de una sesión con OAPES y realizar el ajuste al mapa de riesgos del proceso de Gestión de TI en lo concerniente a la definición de las evidencias del control CGTI24, donde implementaremos un mecanismo para que se verifique el 100% del inventario de equipos de la entidad; teniendo en cuenta el detalle de las actividades asociados a esta operación, entre ellos el estado del Agente en cada máquina.
>
> **Para la acción 2817**: Las evidencias fueron entregadas en diciembre del 2025 al asesor de OAPES como se indica en el repositorio. Sin embargo, aclaramos en este informe, que la tercera evidencia correspondiente al mes de diciembre se registró en SIMIG y se hizo la solicitud el día de hoy del cierre de la acción correspondiente:

sin embargo, la respuesta no desvirtúa la situación detectada sino justifica los motivos por los cuales las acciones se mantienen abiertas y vencidas. Por lo anterior, el hallazgo se mantiene en el informe final.

Efectos:

- Afectación del cumplimiento de planes de mejoramiento institucional.
- Disminución de la eficacia del Sistema de Control Interno y del aseguramiento de la calidad.
- Riesgo de recurrencia de las situaciones que dieron origen a las acciones.
- Incremento de reprocesos por requerimientos adicionales de validación por parte de la Oficina de Control Interno.

Causa:

- Falta de seguimiento oportuno por parte de los responsables designados.
- Ausencia de mecanismos de escalamiento para acciones próximas a vencer.

Recomendación:

- Establecer un plan de choque para dar cierre de estas acciones vencidas.
- Definir la ejecución de seguimientos periódicos más cortos.
- Socializar con los responsables de las acciones los lineamientos vigentes para la gestión de acciones, priorizando las de aquellas de mayor impacto.

6. CONCLUSIONES

- Con la información aportada por parte de los responsables, 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.

- La Entidad tiene implementados mecanismos de control para el monitoreo de la instalación de software en los equipos de cómputo, soportados en políticas, manuales, procedimientos, instructivos y formatos establecidos.

- Existen oportunidades de mejora dentro de la Entidad orientadas a cerrar las brechas identificadas en el seguimiento al cumplimiento de las normas relacionadas con los derechos de autor aplicables al uso de software.

7. RECOMENDACIONES

Al final de cada objetivo y hallazgo se presentaron las recomendaciones asociadas a las oportunidades de mejora del proceso.

Aprobó:

JUAN DIEGO TORO BAUTISTA
Jefe Oficina de Control Interno

Elaboró: Rafael Hernando Calle Cabezas

REGISTRO DE FIRMAS ELECTRONICAS

Informe de Ley - Derechos de Autor 2026

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

Id Acuerdo: 20260317-235814-cc5a38-04185725

Creación: 2026-03-17 23:58:14

Estado: Finalizado

Finalización: 2026-03-18 05:12:50

Escanee el código para verificación

Aprobación: Jefe Oficina de Control Interno

Juan Diego Toro 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 de Ley - Derechos de Autor 2026

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

Id Acuerdo: 20260317-235814-cc5a38-04185725
Creación: 2026-03-17 23:58:14
Estado: Finalizado
Finalización: 2026-03-18 05:12:50

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 Información y las	Aprobado	Env.: 2026-03-17 23:58:16 Lec.: 2026-03-18 05:12:42 Res.: 2026-03-18 05:12:50 IP Res.: 181.53.156.20 Canal: Email