| **FECHA DE EMISIÓN DEL INFORME** | **Día:** | 21 | **Mes:** | 03 | **Año:** | 2025 |
|---|---|---|---|---|---|---|

| | |
|---|---|
| **Aspecto Evaluable (Unidad Auditable):** | Informe Derechos de Autor Software 2024 |
| **Líder de Proceso / Jefe(s) Dependencia(s):** | Carlos Andres Ballesteros Castañeda<br>**Subgerencia de Tecnologías de la Información y las Comunicaciones** |
| **Objetivo de la Auditoría:** | • Teniendo en cuenta el interés del gobierno para la protección de los derechos de autor y los derechos conexos; en relación con la adquisición de programas de computador (software) debidamente licenciados, la Entidad deberá reportar la información de acuerdo con la Directiva Presidencial 02 de 2002 y la ley 1915 de 2018. |
| **Alcance de la Auditoría:** | • El cumplimiento de la normatividad vigente en materia de derechos de autor, se realizará a través del uso adecuado de los programas de computador (Software) a corte del 31 de diciembre de 2024. |
| **Criterios de la Auditoría:** | Directiva Presidencial N° 002 de 2002.<br>Ley 1915 de 2018. |

## ASPECTOS GENERALES

La Dirección Nacional de Derecho de Autor solicita a las entidades u organismos del orden nacional y territorial, diligenciar el informe de uso legal de software en cumplimento de la Directiva Presidencial N° 002 de 2002, en donde se solicita entre otros:

1. Revisar con los encargados de cada entidad, sobre la adquisición de software para que los programas de computador, se encuentren respaldados por los documentos de licenciamiento o transferencia de propiedad según lo que aplique.

2. Validar que la entidad no tenga titularidad del derecho de autor de forma ilegal, sobre los derechos patrimoniales que le hayan sido transferidos, ya sea a través de contratos de cesión o transferencia o porque éstos serán desarrollados por servidores públicos a ellas vinculados, en cumplimiento de las funciones de sus cargos.

PÚBLICA

## ACTIVIDADES DESARROLLADAS

Para la validación de la información que deberá ser reportada se realizaron los siguientes procedimientos de acuerdo con las preguntas determinadas:

1. ¿Con cuántos equipos cuenta la entidad?:

Se validaron los contratos con la entidad Technology World de acuerdo con un checklist que la oficina de control interno de gestión realizó basándose en los manuales de contratación y de supervisión vigentes a la fecha de firma del contrato. Así cómo la validación de la información diligenciada por la Subgerencia de Tecnologías de la Información y las Comunicaciones, para el reporte, la información descrita es como sigue:

| Tipo | Proveedor | Orden de compra | Cantidad | Descripción |
|---|---|---|---|---|
| Alquiler | TECHNOLOGY WORLD GROUP SAS | OC 124251 | 65 | 45 equipos de escritorio y 20 portátiles |
| Alquiler | TECHNOLOGY WORLD GROUP SAS | OC129377 | 54 | 30 equipos de escritorio, 21 portátiles y 3 workstations |
| Propio | Propio de la Entidad | 1 | 1 | 1 equipo de escritorio |
| **Total** | | | **120** | |

Al cierre del 31 de diciembre de 2024, la agencia contó con un total de 120 equipos de cómputo.

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

Se realizó la validación de los soportes sobre los tipos de licenciamiento que tiene la entidad y sobre una muestra de 24 equipos determinada con el 93% de confiabilidad, lo siguiente:

1. Se tiene una política de actualización de los equipos que al momento en que se loguea un nuevo usuario, el equipo se reinicia al estado base, para salvaguardar la información de los otros usuarios que hacen disposición de los equipos.

2. En el proceso de validación, se descartó los programas de Seven y Cactus, dado que son programas a los que se accede a través de un usuario en la nube.

3. Se solicito el soporte de los tipos de licenciamiento que tiene la entidad, en donde validaremos que:

PÚBLICA

- Los equipos tengan el licenciamiento referido por el equipo de TI, de las cuales consta:

**1.** Sistema Operativo Windows 10
**2.**Navegador (Chrome, Firefox)
**3.** 7-ZIP
**4.** Adobe Reader
**5.** Suit Office 365 (Office, OneDrive, Teams, Outlook, OneNote, Copilot)
**6.** ePass2003 Certicamara
**7.** CertiTool
**8.** VeraCrypt
**9.** FortiClient VPN
**10.** Chip - Contaduria
**11.** Microsoft PowerBI Desktop
**12.** SIRECI
**13.** R for Windows
**14.** RStudio
**15.** Python
**16.** QGIS
**17.** VLC Media Player
**18.** Agent Shell, Avaya one-X Agent - 2.5.16
**19.** sipost 4-72 Fuentes de Sipost
**20.** SAP
**21.** Slack
**22.** Módulo Storm
**23.** Zoom Workplace
**24.** Analizador y SDK de MSXML 4.0 SP2
**25.**Prevalidador_Tributario_Informantes_AG2023_v3.1.0-24
**26.** Lightshot-5.5.0.7
**27.** PuTTY release 0.82 (64-bit)
**28.** KeePass Password Safe 2.57

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

En el contexto de la implementación de políticas de seguridad mediante Directivas de Grupo (GPOs), se establecieron reglas que prohíben la instalación de programas o la ejecución de archivos .exe por parte de los usuarios finales. El objetivo de esta medida es prevenir el uso de software no autorizado por la entidad.

Con el fin de evitar la instalación de programas o aplicativos sin la respectiva licencia, la entidad cuenta con las siguientes medidas de seguridad:

- **Control de instalación mediante Microsoft Intune:** Se ha configurado un perfil de administración que restringe la instalación de aplicaciones en los equipos institucionales. Solo los programas autorizados pueden ser instalados, garantizando el cumplimiento de las políticas de software y licenciamiento establecidas por la entidad.

- **A través de nuestra solución de ciberseguridad**, se identifica software no autorizado, malicioso o riesgoso para la entidad, detectando comportamientos anómalos asociados a su uso. Esto permite generar alertas y aplicar restricciones mediante mecanismos de control de acceso a la red y herramientas de gestión de dispositivos, mitigando así posibles vulnerabilidades.

PÚBLICA

Adicional a ello, se tiene establecido en la política de seguridad y privacidad de la información - PO1_TIC, en la sección de Control de acceso lo siguiente:

> *"La instalación de software en los equipos de cómputo en la Agencia será realizada a través del usuario del administrador de la red. Toda solicitud al respecto debe gestionarse a través de la Subgerencia de Tecnologías de la Información y la Comunicación quien aprobará su instalación."*

Y en la sección Seguridad de las operaciones lo siguiente:

> *"Implementar procedimientos para controlar la instalación de software en sistemas operativos"*

La cual es implementada a través de la configuración de usuarios y administración de equipos de cómputo que realiza la Subgerencia TIC.

Para validar el procedimiento, la OCIG hizo prueba de campo, para efectuar la instalación de algún aplicativo .exe, el cual se encuentra documentado en los papeles de trabajo, para constatar los lineamientos establecidos en la política de seguridad y privacidad de la información.

Esta política de seguridad se encuentra publicada en el portal web de la Agencia y es de público conocimiento: https://agenciaatenea.gov.co/sites/default/files/2025-02/PO1_TIC%20Pol%C3%ADtica%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%20V2.pdf

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

Se valido a través de la indagación, con la persona responsable si durante el año se había presentado algún tipo de baja de software, por lo que la respuesta a la pregunta es:

- Durante el año 2024, no se procedió a dar de baja ningún software institucional.

PÚBLICA

| No. | NOMBRE | HALLAZGO | RECOMENDACIÓN | PLAN DE ACCIÓN |
|---|---|---|---|---|
| 1 | Falta de control en la instalación de aplicaciones con rol administrador | De acuerdo con los procedimientos de auditoría desarrollados, se identificó que, de una muestra de 24 equipos, uno de ellos permite la instalación de aplicaciones ya que no cuenta con un mecanismo de seguridad que restrinja la instalación de aplicaciones con privilegios de administrador (Microsoft Intune). De acuerdo con la "PO1_TIC Política de Seguridad y Privacidad de la Información", en la sección "Control de acceso" literal 10 y la sección "Seguridad de las operaciones" literal 11, se establece la obligatoriedad de contar con controles que impidan la instalación no autorizada de software.<br><br>La causa de esta situación radica en la falta de implementación de configuraciones de seguridad adecuadas en el equipo de cómputo, lo que permite que el usuario realice instalaciones sin restricciones administrativas. Como consecuencia, esta brecha de seguridad puede facilitar la instalación de software malicioso o no autorizado, lo que representa un riesgo significativo para la seguridad de la información y la estabilidad de los sistemas corporativos. | Se recomienda dar cumplimiento a la política de Seguridad y Privacidad de la Información, asegurando que solo el área de TI tenga la capacidad de instalar software. | **Medio de verificación**: Asignación de permisos mediante rol administrador local de la máquina.<br><br>**Responsable**: Subgerencia de Tecnologías de la Información<br><br>**Fecha de implementación**: 18/04/2025 |

PÚBLICA

| No. | NOMBRE | HALLAZGO | RECOMENDACIÓN | PLAN DE ACCIÓN |
|---|---|---|---|---|
| 2 | Instalación de software de licenciamiento pago sin autorización de TI | De acuerdo con los procedimientos de auditoría desarrollados, se identificó que, de una muestra de 24 equipos, uno de ellos tiene instaladas aplicaciones de licenciamiento pago sin el conocimiento ni autorización del área de TI. Entre las aplicaciones detectadas se encuentran Biostar, ETB_UC, Express VPN y StrokeScribe.<br><br>Según la Directiva Presidencial N° 002 de 2002 y la Ley 1915 de 2018, toda adquisición e instalación de software con licenciamiento debe ser gestionada exclusivamente por el área de TI, garantizando el cumplimiento normativo y evitando el uso indebido de recursos. Sin embargo, el equipo en cuestión fue utilizado por un usuario con permisos insuficientemente controlados, lo que permitió la instalación de software sin el debido proceso de autorización por parte del área de TI.<br><br>La instalación de software no autorizado con licenciamiento pago puede generar riesgos legales debido al incumplimiento de términos de licencias, costos innecesarios por pagos duplicados y potenciales sanciones por uso indebido de software. Adicionalmente, el uso de herramientas como Express VPN puede comprometer la seguridad de la red corporativa al permitir conexiones no supervisadas, evadiendo los controles establecidos. | Se recomienda dar cumplimiento a la política de Seguridad y Privacidad de la Información, asegurando que solo el área de TI imparta las aprobaciones para la instalación de software de terceros; Así mismo se recomienda que dentro del contrato de arrendamiento con FAMOC DEPANEL S.A.S, se específique a cualquier instalación de software debe ser aprobada por el área de TI, y se debe manifestar por escrito que el software se encuentra debidamente licenciado, con el fin de liberar a ATENEA de cualquier responsabilidad.<br><br>Como control compensatorio y mientras se obtiene la modificación contractual, se recomienda solicitar a FAMOC DEPANEL S.A.S, una certificación respecto al actual licenciamiento instalado en el equipo dispuesto para tal fin. | Solicitar al área administrativa la inclusión de una cláusula contractual con el proveedor FAMOC DEPANEL S.A.S., que especifique que toda instalación de software en los equipos suministrados debe contar con aprobación previa por parte de la Subgerencia de Tecnologías de la Información, conforme a la política de seguridad y privacidad de la información vigente.<br><br>**Responsable**: Subgerencia de Tecnologías de la Información<br><br>**Fecha de implementación**: 30/06/2025<br><br>**Medio de verificación**: Solicitud a la Subgerencia Administrativa para el análisis e inclusión de cláusulas.<br><br>Solicitar a FAMOC DEPANEL S.A.S. una |

PUBLICA

| No. | NOMBRE | HALLAZGO | RECOMENDACIÓN | PLAN DE ACCIÓN |
|---|---|---|---|---|
| | | | | certificación formal que relacione los programas instalados en los equipos asignados, indicando que estos cuentan con licenciamiento vigente y legal, y que fueron instalados conforme a los lineamientos de la entidad<br><br>**Responsable**: Subgerencia de Tecnologías de la Información y Subgerencia Administrativa<br><br>**Fecha de implementación**: 30/06/2025<br><br>**Medio de verificación**: Solicitud de certificación. |

PÚBLICA

| No. | OPORTUNIDAD DE MEJORA | PLAN DE ACCIÓN |
|---|---|---|
| 1 | Durante la sesión de auditoría, se identificó que el área de TI implementa, como buena práctica, un control para la validación de la actividad de uso de las licencias de Microsoft 365 A1, A3 y A5. Este control consiste en monitorear la inactividad de las cuentas y, dependiendo del tiempo transcurrido sin uso, proceder con la inactivación de la licencia y su reasignación a un funcionario que la requiera.<br><br>Si bien esta práctica contribuye a la optimización de los recursos tecnológicos, se evidenció que no se encuentra documentada en un procedimiento formal, lo que podría generar inconsistencias en su aplicación y afectar la trazabilidad de la gestión de licencias.<br><br>Se recomienda formalizar este control mediante su inclusión en un procedimiento documentado, asegurando que contemple criterios claros de inactividad, plazos de validación y el proceso de reasignación de licencias. | Diseñar y documentar lineamientos de monitoreo para la gestión eficiente de licencias Microsoft 365 A1, A3 y A5, que incluya criterios de inactividad y proceso de reasignación de licencias a personal activo<br><br>**Responsable**: Subgerencia de Tecnologías de la Información<br><br>**Fecha de implementación**: 30/09/2025 |
| 2 | Durante la auditoría, se evidenció que el área de TI ha implementado, como buena práctica, un control para la validación del estado de los usuarios con licencias de Microsoft 365. Este control consiste en realizar un cruce de información entre la base de usuarios con licencia y el estado administrativo del personal provisional y contratistas, permitiendo identificar si los usuarios se encuentran activos, inactivos o eliminados.<br><br>Si bien este control contribuye a optimizar la gestión de licencias y evitar costos innecesarios, se identificó que no se encuentra documentado en un procedimiento formal. La ausencia de una guía estructurada podría generar inconsistencias en su aplicación o la pérdida de esta práctica en caso de cambios en el equipo encargado.<br><br>Se recomienda formalizar este control mediante su documentación en un procedimiento que establezca la periodicidad de validación, las fuentes de información a utilizar, los responsables del cruce de datos y las acciones a tomar en cada caso identificado. Esto garantizará su sostenibilidad en el tiempo, mejorará la trazabilidad de la gestión de licencias y fortalecerá los controles internos de la organización. | Documentar los lineamientos de cruce de información entre la base de usuarios con licencias Microsoft 365 y el estado contractual del personal (servidores públicos, provisionales y contratistas), estableciendo la periodicidad del análisis<br><br>**Responsable**: Subgerencia de Tecnologías de la Información<br><br>**Fecha de implementación**: 30/09/2025 |

PÚBLICA

## CONCLUSIONES DE LA AUDITORÍA

Tras la ejecución de la auditoría realizada sobre el cumplimiento de la normatividad vigente en materia de derechos de autor y el uso adecuado de programas de computador (software) en la entidad, ha revelado varios aspectos importantes:

- **Cumplimiento General:** La entidad ha demostrado un cumplimiento general adecuado con respecto a la Directiva Presidencial N° 002 de 2002 y la Ley 1915 de 2018. Todos los equipos de cómputo auditados cuentan con software debidamente licenciado, y se han implementado políticas de actualización y seguridad para salvaguardar la información.
- **Control de Instalación de Software:** Se han identificado mecanismos de control efectivos, como el uso de Microsoft Intune y políticas de seguridad mediante Directivas de Grupo (GPOs), que restringen la instalación de software no autorizado. Sin embargo, se detectaron algunas brechas en la implementación de estas políticas, permitiendo la instalación de software sin la debida autorización en ciertos casos.

La Oficina de Control Interno, concluye que, aunque la entidad ha mostrado un buen nivel de cumplimiento en general, es crucial fortalecer los controles internos y asegurar que todas las políticas de seguridad y licenciamiento se apliquen de manera consistente para mitigar riesgos y garantizar la conformidad normativa.

Para constancia se firma en Bogotá D.C., a los 02 días del mes de abril del año 2025.

| APROBACIÓN DEL INFORME DE AUDITORÍA | | |
|---|---|---|
| **Nombre Completo** | **Responsabilidad** (cargo) | **Firma** |
| Jorge Luis Garzón Tobar | Jefe Oficina Control Interno de Gestión | JORGE LUIS GARZÓN TOBAR Firmado digitalmente por JORGE LUIS GARZÓN TOBAR Fecha: 2025.04.02 14:26:19 -05'00' |
| Ivan Camilo Montoya Valencia | Contratista / Oficina Control Interno de Gestión | Ivan Camilo Montoya Valencia Firmado digitalmente por Ivan Camilo Montoya Valencia Fecha: 2025.04.02 14:28:10 -05'00' |


**Piensa en el medio ambiente, antes de imprimir este documento**.
Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA