

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 1 de 15

FECHA DE EMISIÓN DEL INFORME	Día:	20	Mes:	03	Año:	2026
-------------------------------------	-------------	-----------	-------------	-----------	-------------	-------------

Aspecto Evaluable (Unidad Auditable):	Informe Derechos de Autor Software 2026
Líder de Proceso / Jefe(s) Dependencia(s):	Carlos Andrés Ballesteros Castañeda Subgerente de Tecnologías de la Información y las Comunicaciones
Objetivo de la Auditoría:	Verificar el cumplimiento normativo y la efectividad de los controles implementados por la entidad para asegurar que el software instalado en los equipos institucionales esté debidamente autorizado y licenciado, y que exista una gestión adecuada del software durante su ciclo de vida (instalación, uso, control, y baja), para lo cual se tendrán en cuenta los siguientes objetivos específicos: - Identificar y validar el inventario de software instalado y en uso en los equipos institucionales, verificando su correspondencia con los registros internos (herramientas de inventario, actas, reportes técnicos) y asegurando la trazabilidad por dependencia, usuario responsable y equipo. - Comprobar la legalidad y uso eficiente del licenciamiento y autorizaciones del software reportado (propietario y/o libre), verificando la existencia de soportes (contratos, facturas, certificados, acuerdos de licencia, términos de uso), la asignación correcta de licencias, y la consistencia entre licencias adquiridas/permitidas y software efectivamente instalado. - Evaluar la suficiencia y eficacia de los controles y procedimientos de gestión del software en todo su ciclo de vida, revisando: mecanismos de autorización de instalación, perfiles y restricciones de administrador, políticas y lineamientos de uso, periodicidad de revisiones/auditorías, gestión de actualizaciones, atención de hallazgos, y procedimientos de desinstalación/baja y disposición cuando aplique, asegurando que se cumpla con la normativa vigente en materia de legalidad de software y se minimicen los riesgos de uso indebido o no autorizado de los mismos

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 2 de 15

Alcance de la Auditoría:	El presente trabajo de evaluación cubrirá el periodo de gestión comprendido entre el 01 de enero de 2025 al 31 de enero de 2026, y tendrá en cuenta lo siguiente: - Contratos de licencia de Software, aplicativos, otros. - Contratos de compra y arriendo de equipos de cómputo. - Seguridad informática en los equipos. - Ciclo de vida del software. - Controles de instalación: perfiles de usuario, administración local, repositorios corporativos, mesa de ayuda y procedimientos. - Documentos internos de la Subgerencia de TIC's (Políticas, procedimientos, manuales, protocolos, entre otros)
Criterios de la Auditoría:	- Directiva Presidencial 01 de 1999 - Directiva Presidencial 02 de 2002 - Circular 04 de 2006 - Ley 1915 de 2018 - Circular 027 de 2023 - M1_TIC Manual de Políticas de Seguridad de la Información

ASPECTOS GENERALES

En cumplimiento de la Directiva Presidencial 002 de 2002, las entidades públicas deben garantizar que el software instalado, utilizado, adquirido, desarrollado o administrado cuente con el debido soporte jurídico, técnico y documental que respalde su uso legal. En este marco, la verificación no se limita a licencias comerciales, sino que abarca también software gratuito o de uso libre, soluciones adquiridas bajo suscripción y desarrollos internos implementados por la Agencia.

En consecuencia, la validación del software debe considerar las particularidades de cada modalidad de uso. Para el software gratuito o de uso libre, es necesario revisar sus condiciones de licenciamiento y uso institucional; para las soluciones bajo suscripción, verificar su soporte contractual, vigencia, alcance y funcionalidades habilitadas; y para los desarrollos internos, confirmar tanto la titularidad institucional como la legalidad de los componentes de terceros que soportan su funcionamiento, tales como librerías, frameworks, APIs o servicios integrados.

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 3 de 15

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, teniendo en cuenta las siguientes preguntas:

1. ¿Con cuántos equipos cuenta la entidad?
2. ¿El software instalado en estos equipos se encuentra debidamente licenciado?
3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?
4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?

Por lo anterior, a continuación, se desarrollan las siguientes actividades, con el fin de dar cumplimiento y verificación a las preguntas referidas por la Dirección Nacional de Derechos de Autor (DNDA)

ACTIVIDADES DESARROLLADAS

En el marco de la verificación de la información requerida para la elaboración del informe de derechos de autor de software, y en atención a los lineamientos y preguntas formuladas por la Dirección Nacional de Derecho de Autor (DNDA), se efectuaron procedimientos de auditoría orientados a obtener evidencia suficiente, competente y pertinente que permitiera sustentar lo solicitado por la entidad.

Dichos procedimientos estuvieron encaminados a validar la existencia, integridad, trazabilidad y consistencia de la información relacionada con el uso, adquisición, licenciamiento, instalación y control del software en la entidad, según correspondiera al alcance de la verificación. Para ello, se aplicaron actividades de revisión documental, análisis de registros, verificación de soportes, consultas a la dependencia responsable y demás pruebas de comprobación que resultaron necesarias, con el fin de emitir una respuesta debidamente fundamentada y soportada.

A continuación, se presenta la validación efectuada a cada aspecto requerido por la DNDA:

1. ¿Con cuántos equipos cuenta la entidad?:

La Agencia cuenta con 197 equipos de cómputo disponibles para su operación. De ellos, 196 se encuentran vinculados mediante contrato de alquiler con el proveedor Sumimmas, en el marco del Contrato Atenea-513-2025, distribuidos en 133 equipos All-in-One, 60 laptops y 3 workstations; adicionalmente, la entidad cuenta con 1 equipo de escritorio de su propiedad.

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 4 de 15

En atención a lo expuesto, y con el fin de verificar las condiciones técnicas de configuración de cada uno de los equipos adquiridos en modalidad de arrendamiento, se efectuó la validación del contrato suscrito con el proveedor, así como la verificación de su ejecución en los términos pactados, teniendo que el mismo fue celebrado mediante el mecanismo de selección abreviada a través de la Bolsa Mercantil de Colombia, de conformidad con la normativa aplicable al sistema de compra pública en Colombia; por tanto, se revisó la existencia del proveedor en la Bolsa Mercantil, así como la concordancia entre los productos ofertados, los contratados por la Agencia y los componentes técnicos incorporados en cada uno de los equipos, verificando de manera particular, como aspecto esencial, que cada uno hubiera sido entregado con el sistema operativo debidamente instalado y licenciado, en cumplimiento de las condiciones técnicas de entrega previstas contractualmente y de los requisitos legales aplicables.

Asimismo, con el propósito de validar la existencia de los equipos y su adecuado registro en la matriz de asignación, se seleccionó una muestra de equipos, a fin de comprobar su existencia física, su correcta ubicación y la respectiva asignación, como se describe a continuación:

Tipo	Proveedor	Contrato	Cantidad	Descripción
Alquiler	Sumimmas	Cto Atenea-513-2025	133	ALL-IN-ONE
			60	LAPTOPS
			3	WORKSTATIONS
Propio	Propio de la Entidad	1	1	Equipo de escritorio
Total			197	

Con base en lo anterior y de conformidad con el plan de muestreo establecido, se definió una muestra de 33 equipos sobre un universo de 197 dispositivos, utilizando un nivel de confianza del 94 % y un error muestral del 9%,.

Las muestras incluidas en la evaluación son las siguientes:

Serie CPU	Tipo de Equipo	Modelo	Ubicación Puesto	Ubicación Física
8CN4520FWR	All in One	HP ProOne 440	17	27
8CN4520M2M	All in One	HP ProOne 440	43	26
8CN4520FZC	All in One	HP ProOne 440	15	25
8CN4520BHW	All in One	HP ProOne 440	16	25
8CN4520M46	All in One	HP ProOne 440	36	25
8CN45209FD	All in One	HP ProOne 440	43	25
8CN4520BM1	All in One	HP ProOne 440	44	25
8CN4520LWM	All in One	HP ProOne 440	45	25
8CN4520BM4	All in One	HP ProOne 440	49	25
8CN4520FW2	All in One	HP ProOne 440	50	25

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 5 de 15

Serie CPU	Tipo de Equipo	Modelo	Ubicación Puesto	Ubicación Física
8CN4520M1S	All in One	HP ProOne 440	22	26
8CN45209GH	All in One	HP ProOne 440	23	26
8CN4520FZW	All in One	HP ProOne 440	27	26
8CN4520LYZ	All in One	HP ProOne 440	28	26
8CN4520FY7	All in One	HP ProOne 440	37	26
8CN4520LYC	All in One	HP ProOne 440	44	26
8CN4520M06	All in One	HP ProOne 440	47	26
8CN4520FVS	All in One	HP ProOne 440	48	26
8CN4520FXJ	All in One	HP ProOne 440	22	27
8CN4520FXC	All in One	HP ProOne 440	26	27
8CN4520FZY	All in One	HP ProOne 440	27	27
8CN45209F5	All in One	HP ProOne 440	28	27
8CN4520LYW	All in One	HP ProOne 440	29	27
8CN45209CP	All in One	HP ProOne 440	35	27
8CN4520LY2	All in One	HP ProOne 440	39	27
8CN4520FX0	All in One	HP ProOne 440	42	26
8CN4520BMH	All in One	HP ProOne 440	23	25
8CN4520BM3	All in One	HP ProOne 440	19	25
8CC13348TW	All in One	HP All-in-One-df0xxx	Sin marcar	26
5CD5436GL3	Portátil	Hp ProBook 4 G1a		26
5CD5436GKH	Portátil	Hp ProBook 4 G1a		26
5CD5436GK8	Portátil	Hp ProBook 4 G1a	34	26
5CD5436GL1	Portátil	Hp ProBook 4 G1a		26

Con fundamento en la revisión efectuada a los equipos de cómputo de la Agencia incluidos en la muestra, se concluye que estos existen materialmente, se encuentran debidamente identificados y referenciados en los registros de control y asignación de la entidad, y cuentan con el licenciamiento correspondiente, de conformidad con el sistema operativo definido en las condiciones contractuales del servicio.

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

De acuerdo con las pruebas de auditoría efectuadas, se determinó que el software instalado en los equipos de la entidad se encuentran debidamente licenciados y autorizados. En la muestra seleccionada, para la validación de existencia de los equipos, se realizaron pruebas de recorrido con el fin de verificar que las aplicaciones instaladas correspondieran exclusivamente a aquellas incluidas en la matriz de control y seguimiento administrada por la Subgerencia TIC. En dicha validación se identificaron tanto las aplicaciones de libre uso y código abierto como aquellas que

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 6 de 15

requieren licenciamiento prepago, con el propósito de confirmar su correspondencia con los registros y controles institucionales.

Con el propósito de adelantar la identificación y comprensión de los equipos validados, se realizó el análisis de los tipos de licenciamiento, sus funcionalidades y su estructura, a efectos de soportar el proceso de verificación. En este sentido, para cada uno de los equipos inspeccionados se validó que los aplicativos instalados correspondieran a los registrados en la matriz de equipos suministrada por la Subgerencia de TIC's, dependencia responsable de su control y administración, así:

Software licenciado sin costo para instalación y uso

NOMBRE	DESCRIPCIÓN
ADOBE	Corresponde a software desarrollado por Adobe, usualmente utilizado para visualizar, crear o editar documentos PDF y otros archivos digitales.
7-ZIP	Es un software de compresión y descompresión de archivos. Es de código abierto y de uso gratuito, y se utiliza como alternativa para manejar archivos comprimidos.
GOOGLE CHROME	Es un navegador web gratuito desarrollado por Google. Se utiliza para acceder a aplicaciones web, portales institucionales y servicios en línea.
MICROSOFT EDGE	Es un navegador web gratuito desarrollado por Microsoft. Generalmente viene integrado con el sistema operativo Windows.
HP INC. (IMPRESORA)	Corresponde al software controlador o utilitario asociado a impresoras HP. Permite que el sistema operativo reconozca el equipo de impresión y habilite sus funciones.
MICROSOFT (VISUAL)	Corresponde generalmente a componentes de Microsoft Visual C++ Redistributable o herramientas asociadas a Visual Studio. Se utiliza para ejecutar aplicaciones desarrolladas en lenguaje C++ que requieren librerías de Microsoft para su funcionamiento.
CERTITOOL – CERTICÁMARA S.A.	Es una herramienta de Certicámara para la instalación, configuración y uso de certificados digitales emitidos en token. Se utiliza para procesos de firma digital, autenticación y uso de certificados electrónicos.
SCHIP / CHIP – CONTADURÍA GENERAL DE LA NACIÓN	Corresponde al Sistema Consolidador de Hacienda e Información Pública (CHIP), administrado por la Contaduría General de la Nación. Se utiliza para el reporte, validación y envío de información financiera, contable y pública por parte de entidades del Estado.
MÓDULO STORM – CONTRALORÍA DE BOGOTÁ / SECRETARÍA DISTRITAL DE HACIENDA	Corresponde a una plataforma para la gestión y envío de formularios, documentos electrónicos y validación de firma digital ante entidades de supervisión o control.
SIRECI – CONTRALORÍA GENERAL DE LA REPÚBLICA	Es el Sistema de Rendición Electrónica de la Cuenta e Informes. Se utiliza para la rendición de cuentas, transmisión de informes y cargue de información ante la Contraloría General de la República.
EPASS2003 – CERTICÁMARA / ENTERSAFE	Corresponde al software o middleware asociado al uso de tokens criptográficos o dispositivos de firma digital. Se utiliza para administrar certificados digitales almacenados en dispositivos seguros y habilitar procesos de autenticación o firma electrónica.
VPN – FORTINET TECHNOLOGIES INC.	Corresponde a una solución de red privada virtual. Permite el acceso seguro y cifrado a redes o recursos institucionales desde ubicaciones externas.
MOZILLA	Es un navegador web libre y gratuito utilizado para navegación y acceso a plataformas web.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 7 de 15

JAVA – ORACLE CORPORATION	Es una plataforma y entorno de ejecución desarrollado por Oracle. Se utiliza para ejecutar aplicaciones que requieren máquina virtual Java o componentes desarrollados en ese lenguaje.
VERACRYPT	Es un software de cifrado de discos, volúmenes y archivos, de código abierto y uso gratuito. Se utiliza para proteger información mediante encriptación, evitando el acceso no autorizado a datos almacenados en equipos o unidades externas.
AM CRYPTO	Corresponde a un software o componente de tipo criptográfico, normalmente usado para procesos de seguridad digital, autenticación, cifrado o firma electrónica.
RSTUDIO / POSIT SOFTWARE	RStudio, actualmente distribuido por Posit Software, es un entorno de desarrollo integrado para el lenguaje R. Se utiliza para análisis estadístico, ciencia de datos, visualización y programación.
ANACONDA	Es una distribución de software para ciencia de datos y programación, que incluye Python y múltiples librerías. Se usa frecuentemente para análisis de datos, desarrollo científico y gestión de entornos de trabajo.
PYTHON – PYTHON SOFTWARE FOUNDATION	Es un lenguaje de programación de código abierto y de uso general. Se utiliza para automatización, análisis de datos, desarrollo de aplicaciones y scripting.
R FOR WINDOWS	Es la distribución del lenguaje y entorno R para sistema operativo Windows. Se utiliza para análisis estadístico, procesamiento de datos y generación de reportes.
QGIS	Es un sistema de información geográfica (SIG) de código abierto. Se utiliza para visualizar, editar, analizar y administrar información geoespacial.
SAP - BOGDATA	Corresponde a software empresarial utilizado para gestión administrativa, financiera, logística o de recursos institucionales. Opera bajo licenciamiento corporativo. Se emplea para soportar procesos de recaudo, impuestos y gestión financiera distrital.
POWER BI	Es una herramienta de Microsoft para análisis de datos e inteligencia de negocios. Permite elaborar tableros, reportes y visualizaciones interactivas.
FUENTES SIPOST / SIPOST VERYTEL	Corresponde a una plataforma de trazabilidad y consulta de envíos postales utilizada para seguimiento operativo y consulta de información de mensajería.
KEEP PASSWORD	Corresponde a un gestor de contraseñas, usado para almacenar credenciales de forma segura. Es un gestor de contraseñas gratuito y de código abierto.
SOFTWARE CÁMARAS RECEPCIÓN	Corresponde a un software utilizado para la visualización, grabación, administración o monitoreo de cámaras de seguridad o recepción.
ZOOM COMMUNICATIONS, INC.	Corresponde a la plataforma Zoom, utilizada para videoconferencias, reuniones virtuales, chat y colaboración remota. Puede operar en modalidad gratuita o bajo licenciamiento institucional.
MESH AGENT	Es un agente de software utilizado para administración remota, soporte técnico o monitoreo de equipos. Normalmente se instala en los equipos para permitir conexión remota segura y gestión centralizada.
FILEZILLA	Es un cliente de transferencia de archivos, usado para conectarse a servidores mediante FTP, FTPS o SFTP. Se emplea para cargar, descargar o administrar archivos en servidores remotos.

Software licenciado con suscripción prepagada

NOMBRE	DESCRIPCIÓN
OFFICE 365 / MICROSOFT 365 (OC 145000)	Es una suite ofimática de Microsoft bajo modelo de suscripción. Incluye herramientas como Word, Excel, PowerPoint, Outlook y otros servicios colaborativos en la nube.
SERVIDOR ORACLE (OC 142939)	Corresponde a software de base de datos empresarial de Oracle, utilizado para almacenar, administrar y consultar información de manera estructurada. En términos técnicos, un servidor Oracle integra la base de datos y al menos una instancia para su operación.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 8 de 15

DIGITAL WARE SEVEN ERP (ATENEA-411-2025)	Es un software ERP de Digital Ware para la planeación y gestión de recursos empresariales. Integra procesos como contabilidad, logística, inventarios, ventas, talento humano y otras áreas de la organización en una sola plataforma.
DIGITAL WARE KAKTUS HCM (ATENEA-410-2025)	Es un software HCM de Digital Ware orientado a la gestión de talento humano y nómina. Permite administrar procesos de recursos humanos como incorporación, compensación, desarrollo, autogestión y retención del talento.
LICENCIA CHATGPT (ATENEA-445-2025)	Corresponde a una suscripción o licencia de uso de la plataforma ChatGPT de OpenAI. Su finalidad es habilitar acceso a funcionalidades de inteligencia artificial generativa para asistencia en redacción, análisis, automatización y productividad.
FUNDSFORNGOS PREMIUM (EE. UU.) (ATENEA-640-2025)	Es una membresía o suscripción de pago orientada a ONG, fundaciones, empresas y personas interesadas en búsqueda de financiación. Proporciona acceso a recursos exclusivos para identificación de convocatorias, donantes, alertas y fortalecimiento de capacidades de fundraising.
NODOKÁ BY MAKAIÁ (COLOMBIA / AMÉRICA LATINA) (ATENEA-640-2025)	Es una solución digital de MAKAIÁ orientada a la movilización de recursos y búsqueda de oportunidades de financiación para organizaciones sociales. Se utiliza para identificar convocatorias, acceder a directorios y fortalecer procesos de formulación y gestión de proyectos en América Latina y el Caribe.
TRIPLEFUNDS BY TRIPLEMINDS (AUSTRIA / INTERNACIONAL) (ATENEA-640-2025)	Es una plataforma de investigación de donantes y oportunidades de financiación desarrollada por TripleMinds, organización con sede en Austria. Ofrece acceso a perfiles de donantes, convocatorias abiertas, webinars y recursos prácticos para organizaciones que buscan financiación internacional.
GRANTSTATION (EE. UU.) (ATENEA-640-2025)	Es una membresía o plataforma especializada en búsqueda de subvenciones y financiadores. Permite consultar bases de datos de grantmakers, oportunidades de financiación y herramientas de planeación para fortalecer programas de consecución de recursos.
CLAUDE CODE (ATENEA-640-2025)	Es una herramienta de Anthropic orientada a apoyar tareas de desarrollo de software con inteligencia artificial. Está diseñada para asistir en flujos de trabajo de programación y puede integrarse en entornos como terminal o VS Code, según la oferta del proveedor.
SISTEMA OPERATIVO - WINDOWS 11 (INCLUIDO DENTRO DEL CONTRATO DE ALQUILER DE EQUIPOS CTO ATENEA-513-2025)	Corresponde al software base que permite el funcionamiento del equipo de cómputo y la ejecución de los demás programas instalados.

De manera complementaria, se efectuó una validación de los desarrollos internos adelantados por la Agencia, con el fin de establecer que los componentes de terceros incorporados en los aplicativos fueran legales y que su uso se encontrara regulado conforme a la modalidad de licenciamiento aplicable. Asimismo, mediante revisión documental de los contratos de prestación de servicios suscritos con los desarrolladores de los sistemas, se verificó la inclusión de cláusulas relacionadas con la cesión de la propiedad intelectual sobre los desarrollos realizados en el marco de sus obligaciones contractuales.

SICORE – POSMEDIA

Es el sistema central de gestión de convocatorias de educación para los ciudadanos. Está compuesto por tres módulos de software, así:

- SICORE_BACK
- SICORE_FRONT

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 9 de 15

- Reportes – Sicore

Se evidencia que SICORE está soportado sobre un conjunto amplio de componentes de terceros, en donde la mayoría corresponden a software open source, bajo licencias como Apache License 2.0, MIT License, LGPL, MPL, Eclipse Distribution License y EPL, entre otras. Esto aplica tanto para componentes del backend como del frontend y de reportes. En consecuencia, se identifica que, en su mayoría de componentes, son de libre uso bajo esquemas open source.

Los componentes de terceros no fueron incorporados como software aislado instalado manualmente por usuarios, sino como dependencias técnicas del desarrollo, integradas al código fuente mediante mecanismos formales como pom.xml en el backend Java/Maven, package.json en el frontend Angular y despliegue conjunto de artefactos compilados en el módulo de reportes. Esto permite establecer que el componente de terceros funcionó como parte de la arquitectura técnica del sistema, bajo integración controlada dentro del desarrollo institucional.

Finalmente, con el fin de verificar la protección de los derechos de propiedad intelectual sobre los desarrollos internos de la Agencia, se revisaron los contratos de los desarrolladores adscritos a la Subgerencia de TIC, con el propósito de constatar la incorporación de cláusulas contractuales específicas en materia de propiedad intelectual, como se muestra a continuación:

No. contrato	Soporte sobre propiedad intelectual / derechos de autor
ATENEA-023-2026	Cláusula Octava – Derechos de autor / Propiedad de la información: los derechos patrimoniales sobre los productos y entregables serán a perpetuidad y 100% de propiedad de ATENEA; si el contratista requiere usar la información derivada del contrato en el futuro, debe contar con autorización previa de la Agencia.
ATENEA-138-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión patrimonial total a favor de ATENEA.
ATENEA-139-2026	Cláusula Octava – Derechos de autor / Propiedad de la información: los productos y entregables son 100% propiedad de ATENEA a perpetuidad; además, el uso posterior por parte del contratista requiere autorización de la Agencia. También aparece Cláusula Vigésima Primera – Confidencialidad, que incluye dentro de la información confidencial la relacionada con propiedad intelectual y derechos de autor.
ATENEA-140-2026	Cláusula Octava – Derechos de autor / Propiedad de la información: cesión patrimonial total a favor de ATENEA.
ATENEA-269-2026	Cláusula Octava – Derechos de autor / Propiedad de la información: los derechos patrimoniales sobre productos y entregables serán 100% de propiedad de ATENEA. Adicionalmente, en la cláusula de confidencialidad se protege la información sobre propiedad intelectual y derechos de autor derivados de actividades de CTI.
ATENEA-270-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión total a favor de ATENEA.
ATENEA-271-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión total a favor de ATENEA.
ATENEA-272-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión patrimonial total a favor de ATENEA.
ATENEA-273-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión patrimonial total a favor de ATENEA; adicionalmente, el contrato incorpora

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 10 de 15

No. contrato	Soporte sobre propiedad intelectual / derechos de autor
	reserva sobre información relativa a propiedad intelectual y derechos de autor en la cláusula de confidencialidad.
ATENEA-275-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión patrimonial total a favor de ATENEA; además, se menciona la confidencialidad sobre información relacionada con propiedad intelectual y derechos de autor.
ATENEA-330-2026	Cláusula Octava – Derechos de autor / Propiedad de la información con cesión patrimonial total a favor de ATENEA.

En consecuencia, se concluyó que tanto el software instalado en los equipos de la Entidad como el software y los componentes requeridos para los desarrollos internos se encuentran debidamente licenciados, autorizados y bajo control institucional.

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

De acuerdo con lo definido en el Manual de Políticas de Seguridad de la Información M1_TIC, se establece que, la Agencia ha implementado controles administrativos y técnicos para evitar que los usuarios instalen programas o aplicativos sin la respectiva licencia. En primer lugar, se tiene establecido que la Subgerencia de Tecnologías de la Información y las Comunicaciones es la única dependencia autorizada para la administración del software, y que todo aplicativo informático o software debe ser adquirido u aprobado por esa Subgerencia para su uso e instalación en la infraestructura de la Agencia; adicionalmente, no se permite el uso de software de acceso remoto no licenciado o no autorizado por la entidad. Esto evidencia un control centralizado sobre la instalación y uso de software institucional.

De igual forma, se establecen restricciones expresas para los usuarios finales, al señalar que los colaboradores no tienen permitido descargar, utilizar e instalar software externo en los recursos tecnológicos institucionales, salvo que sea aprobado e instalado por la Subgerencia TIC. A ello se suma que los equipos son entregados con configuraciones de dominio, restricción de instalación de software y protección contra malware, lo que constituye un mecanismo técnico preventivo frente a instalaciones no autorizadas.

Además, el Manual prevé controles de navegación y monitoreo, indicando que la Subgerencia TIC implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales, y que la Agencia se reserva el derecho de monitorear los accesos, conexiones y descargas de archivos en internet. Estos controles reducen el riesgo de instalación de software sin licencia desde fuentes externas.

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 11 de 15

Finalmente, el citado lineamiento señala que la Subgerencia TIC debe garantizar que todo el software que se ejecute esté protegido por derechos de autor y requiera licencia de uso o sea de libre distribución y uso, además de mantener evidencia de la propiedad del licenciamiento adquirido.

Para la ejecución de las actividades descritas en el manual, la Subgerencia TIC's tiene los siguientes mecanismos:

- **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 la 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.

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 Política de Seguridad de la Información se encuentra publicada en el portal web institucional de la Agencia y puede ser consultada a través del siguiente [enlace](#). Asimismo; el contenido referido en el Manual de Políticas de Seguridad de la Información se encuentra disponible en el siguiente [enlace](#).

Como parte de las actividades de verificación de controles de seguridad sobre los equipos de cómputo, se realizó una prueba de campo a los 33 equipos, referidos anteriormente en la muestra, consistente en el intento de instalación del aplicativo WinRAR.exe, con el propósito de corroborar la efectividad de los controles implementados por la Entidad frente a la instalación de software sin la autorización previa de la Subgerencia de TIC.

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 12 de 15

En desarrollo de esta prueba, se buscó evidenciar la activación del control de privilegios asociado al rol de administrador, de tal manera que cualquier intento de instalación de aplicativos requiriera credenciales o autorización administrativa previa, conforme a los lineamientos de seguridad y administración centralizada definidos por la Entidad.

Es importante precisar que esta actividad no correspondió a una prueba de hacking, intrusión, vulnerabilidad ni explotación de fallas de seguridad, ni implicó acciones orientadas a afectar, alterar, extraer o comprometer la confidencialidad, integridad o disponibilidad de la información contenida en el equipo o en los datos del usuario evaluado. La validación se limitó exclusivamente a comprobar la existencia y funcionamiento del control preventivo de instalación de software no autorizado.

Asimismo, se deja constancia de que el aplicativo utilizado para la prueba corresponde a una herramienta común de compresión de archivos y que su uso en este ejercicio tuvo un carácter estrictamente de verificación, sin generar afectación sobre la operación del equipo ni sobre la información almacenada en este.

Finalmente y como parte del rol de fomento a la cultura del sistema de control interno que realizada por la Oficina de Control Interno, se hizo el recordatorio a cada uno de los colaboradores participantes en la prueba de recorrido, sobre la importancia de tener en cuenta lo estipulado en el Manual de Políticas de Seguridad de la Información, en la sección “5.1 Políticas organizacionales”, la Política de uso de los activos y la Política de uso de los recursos tecnológicos, en donde, la Agencia establece que los activos de información y recursos tecnológicos asignados a sus colaboradores deben ser utilizados exclusivamente para fines institucionales, bajo criterios de uso adecuado, custodia, responsabilidad y seguridad. Asimismo, dispone que su administración, configuración, intervención técnica e instalación de software son competencia exclusiva de la Subgerencia de Tecnologías de la Información y las Comunicaciones, y que cualquier incidente, pérdida, daño o situación que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado oportunamente. En complemento, estas políticas contemplan el monitoreo y auditoría de los activos, el uso legal del software, la protección de la propiedad intelectual y la gestión controlada de cambios sobre los sistemas y recursos tecnológicos.

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

De acuerdo con el Manual de Políticas de Seguridad de la Información, el software dado de baja es retirado de los equipos institucionales bajo control de la Subgerencia TIC, dependencia que es la única autorizada para la administración del software; adicionalmente, el Manual dispone que todo software que se ejecute debe estar protegido por derechos de autor y contar con licencia de uso o corresponder a software de libre distribución y uso, y que se deben ejecutar revisiones periódicas al licenciamiento y desinstalar de los equipos de cómputo el software que no se encuentre

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 13 de 15

licenciado. Asimismo, cuando la baja involucra componentes tecnológicos o medios de almacenamiento, se aplican medidas de borrado seguro, disposición segura y registro de la eliminación, dejando trazabilidad del proceso.

De manera complementaria y según la verificación efectuada, la gestión de aplicaciones y programas se realiza mediante esquemas de licenciamiento de código abierto, software de uso libre y gratuito, y licencias bajo suscripción anual no renovable automáticamente. En ese sentido, el software instalado en los equipos corresponde aproximadamente en un 70% a programas de uso libre y gratuito, mientras que el porcentaje restante corresponde a software licenciado bajo suscripción. Por tanto, una vez finalizado el contrato con el proveedor, deberá efectuarse el análisis sobre la continuidad del servicio y, de no mantenerse su uso, activarse los protocolos definidos en el Manual de Políticas de Seguridad de la Información para su retiro, desinstalación, control de licenciamiento y, cuando aplique, borrado seguro y trazabilidad.

Finalmente, se precisa que, de acuerdo con la información suministrada, durante la vigencia 2025 y lo corrido de la vigencia 2026 no se presentaron bajas de software asociadas a licenciamientos de suscripción prepagada.

Actividades de revisión al plan de mejoramiento

Se efectuó la revisión integral del plan de mejoramiento suscrito por la dependencia como resultado de la evaluación del informe de derechos de autor de software correspondiente a la vigencia anterior, con el propósito de verificar el cumplimiento de las acciones correctivas propuestas frente a las observaciones identificadas, así como su alineación con las causas que les dieron origen, los responsables designados, los plazos establecidos y los mecanismos de seguimiento definidos; de igual manera, se evaluó el nivel de avance y cumplimiento de las acciones implementadas, mediante la validación de los soportes aportados por la dependencia, a fin de determinar su efectividad en la mitigación de los riesgos asociados al incumplimiento de las disposiciones en materia de licenciamiento, uso legal y control del software instalado en los equipos de la entidad, así como su contribución al fortalecimiento del sistema de control interno y al mejoramiento continuo de la gestión institucional.

CONCLUSIONES DE LA AUDITORÍA

1. Como resultado de las pruebas de auditoría efectuada sobre la gestión del software en la Agencia, se concluye que la entidad cuenta con controles administrativos, técnicos y documentales orientados a garantizar el uso legal del software instalado, utilizado, adquirido y desarrollado en su infraestructura tecnológica. En desarrollo de la evaluación, se verificó la existencia y trazabilidad de los equipos de cómputo, la correspondencia del software instalado

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 14 de 15

con los registros administrados por la Subgerencia de Tecnologías de la Información y las Comunicaciones, la existencia de soportes contractuales y de licenciamiento aplicables, así como la incorporación de controles preventivos para restringir la instalación de programas no autorizados.

2. De igual manera, se evidenció que la Agencia mantiene un esquema de administración centralizada del software, soportado en políticas internas de seguridad de la información, mecanismos de restricción sobre privilegios de instalación, monitoreo de los recursos tecnológicos y validación del licenciamiento, lo cual contribuye a mitigar riesgos asociados al uso de software no autorizado o sin respaldo legal. Asimismo, frente a los desarrollos internos, se observó la inclusión de cláusulas contractuales sobre propiedad intelectual y la identificación de componentes de terceros incorporados en la arquitectura tecnológica, permitiendo fortalecer la protección de los derechos patrimoniales de la entidad y la verificación de la legalidad de dichos componentes.
3. A partir de las pruebas de auditoría efectuadas y las evidencias valoradas, se establece que la Agencia presenta cumplimiento frente a las disposiciones aplicables en materia de derechos de autor de software, particularmente en lo relacionado con inventario, licenciamiento, controles de instalación y lineamientos para la baja de software.
4. La Subgerencia de Tecnologías de la Información y las Comunicaciones atendió los comentarios formulados en la revisión realizada en la vigencia anterior y adelantó las acciones definidas en los planes de mejoramiento correspondientes. Lo anterior se evidencia en la implementación de controles para la restricción de instalación de software no autorizado, el fortalecimiento de los mecanismos de administración y licenciamiento de programas, y la adopción de medidas orientadas al cumplimiento de la Directiva Presidencial 002 de 2002 y la Ley 1915 de 2018.
5. Con base en la revisión efectuada al proceso de asignación de licencias de la suite de Office y de acuerdo con la información consolidada en la matriz de control de licenciamiento, se evidenció que, en promedio, la Agencia tiene asignado el 90,16 % de las licencias habilitadas disponibles. Este nivel de uso se considera razonable, en la medida en que refleja un adecuado aprovechamiento del licenciamiento adquirido y, al mismo tiempo, conserva un margen operativo que permite atender oportunamente nuevas vinculaciones de personal, cambios de perfil y necesidades de redistribución conforme a los requerimientos del servicio.
6. De acuerdo con la revisión efectuada sobre las licencias habilitadas y asignadas de los aplicativos Seven ERP, Kaktus HCM, ChatGPT, FundsforNGOs Premium, Nodoká by MAKAlA, TripleFunds, GrantStation y Claude Code, se evidenció que la entidad presenta niveles de

	Formato Informe de Auditoría	CÓDIGO: F4_P1_CIT
		VERSIÓN: 03
	Proceso de Gestión de Control Interno	FECHA: 31/08/2023
		Página 15 de 15

asignación entre el 94 % y el 100 %, lo que refleja un alto grado de utilización del licenciamiento disponible. En particular, se observó asignación total en las herramientas ChatGPT, FundsforNGOs Premium, Nodoká by MAKAlA, TripleFunds, GrantStation y Claude Code.

Para constancia, se firma en Bogotá D.C., a los 20 días del mes de marzo del año 2026.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	Responsabilidad (cargo)	Firma
Carlos Andrés Ballesteros Castañeda	Subgerente de Tecnologías de la Información y las Comunicaciones	
Hector Enrique León Ospina	Jefe Oficina Control Interno de Gestión	
Ivan Camilo Montoya Valencia	Contratista Oficina Control Interno de Gestión	