

Al contestar cite este número:
Radicado DADEP No. 20261100030413
20261100030413

Bogotá D.C, 2026-07-30
OCI 130

MEMORANDO

PARA: LUCÍA BASTIDAS UBATÉ
Directora

DE: ALLAN MAURICE ALFISZ LÓPEZ
Jefe Oficina de Control Interno

ASUNTO: Seguimiento derechos de autor en materia de software 2026

Respetada doctora Lucía.

La Oficina de Control Interno en ejercicio de sus funciones y en especial las conferidas en el literal b), c), d), e) y g) del artículo 12 de la Ley 87 de 1993, los roles asignados en el Decreto 648 de 2017 y en cumplimiento del Plan Anual de Auditoría 2026, se permite remitir los resultados obtenidos de la evaluación independiente efectuada a los derechos de autor en materia de software instalado en los computadores de la entidad, con corte al 30 de junio de 2026.

Atentamente,



ALLAN MAURICE ALFISZ LÓPEZ
Jefe Oficina de Control Interno

Anexos: 21 folios – Informe Seguimiento derechos de autor en materia de software Corte 30 de junio de 2026
Copia: Luisa Fernanda Terraza González – Subdirectora de Gestión Corporativa
Hugo Roberto Hernández Díaz, jefe Oficina de Tecnologías de la Información y las Comunicaciones
Proyectó: Albeiro Rizo Gallardo
Revisó: Allan Maurice Alfisz López
Código de archivo: 1308515

**DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO -DADEP
OFICINA DE CONTROL INTERNO**

**INFORME
SEGUIMIENTO DERECHOS DE AUTOR EN MATERIA DE SOFTWARE
CORTE 30 DE JUNIO DE 2026**

BOGOTÁ, D.C., JULIO DE 2026

Jefe Oficina de Control Interno

ALLAN MAURICE ALFISZ LÓPEZ

Equipo Evaluador

JESÚS ALBEIRO RIZO GALLARDO
Ingeniero de Sistemas - Contratista

TABLA DE CONTENIDO

INTRODUCCIÓN-----	5
1. OBJETIVO GENERAL -----	5
1.1 OBJETIVOS ESPECÍFICOS-----	5
2. CRITERIOS DE SEGUIMIENTO -----	6
3. ALCANCE DEL SEGUIMIENTO -----	6
4. INFORME DETALLADO DEL SEGUIMIENTO -----	6
4.1 Computadores -----	7
4.2 Controles para evitar la instalación de software no autorizado-----	8
4.3 Destino final del software dado de baja en la entidad-----	8
4.4 Listado oficial de software utilizado en la entidad-----	9
4.5 Usuarios con perfil administrador -----	10
4.6 Licencias y software propietario -----	10
4.7 Software libre utilizado en la entidad -----	10
4.8 Muestra y generación de archivos de software instalado en puestos de trabajo (visita) -----	11
4.8.1 Observación Nro. 1 y alerta preventiva: Debilidades en la actualización y control del inventario oficial de software aprobado y autorizado por la OTIC, lo que podría afectar el adecuado seguimiento de dichos activos informáticos. -----	15
4.9 Auditorías para identificar y eliminar software no autorizado -----	15
4.9.1 Observación nro. 2 y alerta preventiva: Incumplimiento en la presentación de los informes de monitoreo y auditoría de software ante la Alta Dirección y el Comité Institucional de Gestión y Desempeño, limitando la disponibilidad oportuna de información para la toma de decisiones y el seguimiento institucional. -----	15
5. ANÁLISIS DE POTENCIALES RIESGOS -----	15
6. SEGUIMIENTO A LAS RECOMENDACIONES SEGÚN INFORME VIGENCIA 2024 -----	16
7. CONCLUSIONES-----	18
8. RECOMENDACIONES-----	20
9. RESUMEN DE HALLAZGOS Y OBSERVACIONES -----	20

Lista de tablas

Tabla Nro. 1. Software por fuente de licenciamiento	9
Tabla Nro. 2. Tipo de aplicación por tipo de licencia	10
Tabla Nro. 3. Tickets de instalación de software libre no incluido en el inventario oficial	11
Tabla Nro. 4. Software de computadores de la muestra, no incluido en el listado oficial	12
Tabla Nro. 5. Seguimiento recomendaciones informe vigencia 2024	16
Tabla Nro. 6. Resumen de Observaciones	20

Lista de imágenes

Imagen Nro. 1. Muestreo Aleatorio Simple	11
--	----

INTRODUCCIÓN

La Oficina de Control Interno del Departamento Administrativo de la Defensoría del Espacio Público (DADEP), en cumplimiento de las directrices del gobierno distrital y del Plan Anual de Auditorías vigencia 2026, efectuó el seguimiento al cumplimiento de la normativa vigente en materia de derechos de autor relacionada con el licenciamiento de software en los equipos de cómputo de la entidad, con corte al 30 de junio de 2026. Lo anterior, en observancia de lo dispuesto en la Directiva Presidencial No. 002 de 2002, la cual establece la obligación de verificar la adecuada adquisición y uso de programas de computador, en el marco de la protección de la propiedad intelectual.

En concordancia con lo anterior, y en atención al requerimiento efectuado por la Dirección Nacional de Derecho de Autor (DNDA), entidad competente en la formulación, dirección y ejecución de la política en materia de derechos de autor y derechos conexos, se realizó la verificación del uso legal del software, de conformidad con el procedimiento definido en la Circular 027 de 2023. En este contexto, la Oficina de Control Interno elaboró el informe de verificación de software y diligenció el instrumento de recolección de información dispuesto por la DNDA, cuyos resultados fueron publicados en el sitio web institucional dentro de los términos legales establecidos.

El presente informe comprende la evaluación del uso e instalación del software adquirido por la entidad, el seguimiento al cumplimiento de las recomendaciones formuladas en el informe de la vigencia 2024, así como el análisis de la gestión de licencias, software libre, licencias dadas de baja y uso de software de terceros y propietario. Adicionalmente, se incorporan los resultados de la verificación física del software instalado en los equipos de cómputo.

Para el desarrollo de esta actividad de auditoría se contó con la colaboración de los procesos Gestión de Recursos y Gestión de la Tecnología y la Información, los cuales suministraron la información y evidencias requeridas para soportar los resultados del presente informe.

1. OBJETIVO GENERAL

Evaluar la gestión y el cumplimiento del licenciamiento del software instalado en el Departamento Administrativo de la Defensoría del Espacio Público, asegurando su uso legal y conforme a los términos de las licencias adquiridas.

1.1 OBJETIVOS ESPECÍFICOS

- Evaluar la efectividad de los controles implementados para prevenir la instalación de software no autorizado en el Departamento Administrativo de la Defensoría del Espacio Público.
- Verificar el cumplimiento del licenciamiento del software instalado en los equipos del DADEP, mediante una visita al puesto de trabajo, según muestra aleatoria.

2. CRITERIOS DE SEGUIMIENTO

Dentro del marco normativo se consideró:

- DADEP, Instructivo Gestión de Recursos Físicos (código SG/MIPG: 127-INSGR-03, versión 14, vigente desde el 10/06/2026).
- DADEP, Política general de seguridad y privacidad de la información (código SG/MIPG: 127-PPPGI-01, versión 9, vigente desde el 12/09/2025).
- DADEP, Políticas operativas específicas de seguridad y privacidad de la información (código SG/MIPG: 127-PPPGI-08, versión 4, vigente desde el 28/07/2025).
- Dirección Nacional de Derecho de Autor, Circular Externa Nro. 027 de 2023.
- Directiva Presidencial Nro. 02 de 2002.
- Directiva Presidencial Nro. 01 de 1999.

3. ALCANCE DEL SEGUIMIENTO

El seguimiento al software existente en la entidad se realizó con corte al 30 de junio de 2026 y la inspección en los puestos de trabajo se llevó a cabo el 22 de julio del mismo año.

4. INFORME DETALLADO DEL SEGUIMIENTO

Recibida la información por parte de la Subdirección de Gestión Corporativa y la Oficina de Tecnologías de la Información y las Comunicaciones, se adelantó el siguiente análisis.

Metodología

Para llevar a cabo el seguimiento se realizaron las siguientes acciones:

- Solicitud de información a la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), mediante radicado DADEP Nro. 20261100026793 del 19/06/2026, y envío de la Carta de Representación para firma del líder del proceso; atendida con el radicado Nro. 20261400028373 del 06/07/2026.
- Solicitud de información a la Subdirección de Gestión Corporativa (SGC), mediante radicado DADEP Nro. 20261100026813 del 19/06/2026, y envío de la Carta de Representación para firma de la líder del proceso; atendida con el radicado Nro. 20264050028353 del 06/07/2026.
- Mediante correo electrónico del 09/07/2026 se solicitó a la OTIC la respuesta faltante a la recomendación del informe vigencia 2024: *"Allegar oportunamente y de manera completa, la información requerida por la Oficina de Control Interno, en pro de garantizar la elaboración y*

publicación del informe en la página web, de conformidad con el Plan Anual de Auditorías 2025. De persistir el incumplimiento en los próximos seguimientos, se configurará el hallazgo correspondiente"; atendida mediante correo del 14/07/2026.

- Mediante correo electrónico del 22/07/2026 se solicitó a la OTIC la respuesta a la pregunta 6: *"Las auditorías periódicas realizadas para identificar y eliminar software no autorizado, como medida de prevención definida por la OTIC; y la documentación de hallazgos y generación de informes para la Alta Dirección y el Comité Institucional de Gestión y Desempeño (CIGD)";* ya que la inicialmente recibida no correspondía a lo solicitado; atendida mediante correo del 22/07/2026.
- Posteriormente, se efectuó la revisión de las evidencias suministradas, así como el cruce de información entre las diferentes bases de datos. De igual manera, se analizó la documentación correspondiente a los procesos de *Gestión de la tecnología y la información*, y *Gestión de recursos*. La información proporcionada por las áreas auditadas fue evaluada en términos de su integridad, cumplimiento de la vigencia requerida y pertinencia de las evidencias y documentos allegados. Adicionalmente, se gestionaron aclaraciones a través de correos electrónicos y visitas a la SGC y OTIC, con el fin de resolver las inquietudes identificadas durante el desarrollo del seguimiento.
- El 22 de julio de 2026, se realizó la inspección física del software instalado en los computadores seleccionados, acompañada con personal de la OTIC, según una muestra aleatoria simple.

4.1 Computadores

Debido a que en el mes de junio de 2026 la entidad recibió 157 computadores de escritorio, se lleva a cabo el proceso de asignación a los funcionarios correspondientes, lo que podría evidenciar algunas diferencias para determinar con mayor certeza la cantidad de equipos existentes a la fecha; por tal motivo, se tomó como punto de partida el valor registrado en el archivo *Equipos y Características Julio 2026.xls*, hoja *Equipos Antiguos*, enviado por la OTIC según correo del 14/07/2026, que como oficina responsable de la configuración e instalación de software, refleja la cantidad de computadores más actualizada hasta el momento. Así las cosas, con corte al 30 de junio de 2026, se identificaron 237 computadores. Cabe aclarar, que este valor se tomó como referencia para calcular la muestra de revisión de software en sitio, y considerando la adquisición del nuevo parque computacional para reemplazar aquellos en estado de obsolescencia, para el próximo seguimiento se contará con la cantidad exacta de computadores en uso por los usuarios finales y/o almacenados en bodega para reasignación o para dar de baja.

En la modalidad de trabajo en casa, se tiene asignado el computador con placa nro. 7132 a un servidor de carrera administrativa, que como se manifestó en la tabla nro. 1, no está conectado a la red institucional.

4.2 Controles para evitar la instalación de software no autorizado

La entidad ha implementado los siguientes controles para evitar la instalación de software ilegal o no autorizado:

- La instalación de software es una función exclusiva de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), quien tiene el control del software autorizado para instalar en los computadores.
- La OTIC, a través de la Mesa de Ayuda, realiza monitoreos periódicos para identificar aplicaciones no autorizadas, ejecuta la limpieza de archivos temporales e historiales de navegación, y procede con la desinstalación de cualquier software que no cuente con licencia institucional o no sea de uso libre.
- Se definen dos (2) perfiles de Administrador; uno, local, con permisos para la instalación y configuración de software y aplicativos, y para la configuración de periféricos. Por consiguiente, los usuarios finales están restringidos para instalar cualquier tipo de software. El otro, es un administrador de red para uso de los funcionarios administradores de la OTIC, que asume las políticas de directorio activo.
- Sólo está permitido el uso de software previamente aprobado y licenciado por la OTIC.
- La instalación de cualquier programa deberá ser solicitada y aprobada mediante el Formato Único de Sistemas (FUS).
- La OTIC realiza auditorías periódicas para identificar y eliminar software no autorizado.

Lo anterior, de conformidad con lo estipulado en el documento: Políticas Operativas Específicas de Seguridad y Privacidad de la Información (código SG/MIPG: 127-PPPGI-08, versión nro. 4, vigente desde el 28/07/2025), numeral 6.1. Política General de Seguridad de la Información:

- Política de estaciones de trabajo.
- Política de derechos de autor y legalidad de software.

4.3 Destino final del software dado de baja en la entidad

Con el concepto técnico dado por la Oficina de Tecnologías de la Información y las Comunicaciones para dar de baja el software, el profesional de recursos físicos y el responsable del almacén, proyectan, revisan y pasan a firmas la resolución de baja de elementos, que se publica en la página web de la entidad, por el tiempo estipulado en la norma, para determinar si alguna entidad pública está interesada en recibirlos. En caso afirmativo, se hace la entrega oficial a través de un acta suscrita entre los responsables del DADEP y sus pares de la entidad interesada.

Se procede luego a realizar la baja de los elementos en el sistema de gestión de bienes muebles e intangibles, se elabora el informe de baja de elementos y se entrega al área de contabilidad para los

registros contables a que haya lugar. Por último, se elabora el acta de entrega de los elementos para disposición final de conformidad con dicho informe.

Lo anterior, de conformidad con lo descrito en el Instructivo Gestión de Recursos Físicos (código SG/MIPG: 127-INSGR-03, versión nro. 13, vigente desde el 31/07/2025, numeral 5.1.12. Baja de elementos).

4.4 Listado oficial de software utilizado en la entidad

Se evidenció el documento *Formato listado oficial Software Autorizado DADEP.xls*, que describe un total de setenta y ocho (78) tipos de software revisados, actualizados, aprobados y definidos por la OTIC en las políticas de restricción, como un control específico para asegurar que en los computadores y servidores se instalen y utilicen únicamente estas licencias autorizadas y vigentes. Todo software no incluido en este listado deberá ser evaluado y aprobado previamente por la OTIC conforme a las políticas institucionales de seguridad de la información y derechos de autor.

En la Tabla Nro. 1, del total del software existente (78), el *Software libre* (7-Zip, Adobe Acrobat Reader, Google Chrome, JAVA JDK, MongoDB Compass, Mozilla Firefox, Notepad++, PowerBI Desktop, Python, Gestion Servicios, Intranet, ORFEO 7, Portal Inmobiliario, Portal Web, entre otros) constituye la mayor fuente de licenciamiento con el 55,13% (43); seguido del *Acuerdo Marco* (Adobe Creative Cloud, Autocad, Fortinet EDR, Office 2019, Office 365, SIGDEP/Visor Observatorio/Visores Geográficos, ArcGIS, ORACLE ORDBMS 19c, ArcGIS Pro, entre otros) con el 15,38% (12) y *Licencia propia* (ECM, Calificador, CAPID, Control de Horario, Inventario Consulta Web, SIDEPE, Sistema de Administración de Cuentas, Sistema de Información Gerencial del Espacio Público, SUMA+ y Gestor de Ficheros DMDEP) con el 12,82% (10).

Tabla Nro. 1. Software por fuente de licenciamiento



Fuente: OTIC – Elaboración OCI

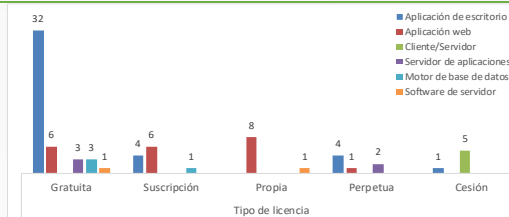
En la Tabla Nro. 2, las aplicaciones de escritorio (Adobe Creative Cloud, Autocad, Fortinet EDR, Office 365, ArcGIS Pro, Office 2019, ROYAL Desktop, Toad for ORACLE, 7-Zip, Adobe Acrobat Reader, FortiClientVPN, Google Chrome, JAVA JDK, Mozilla Firefox, Notepad++, PowerBI Desktop, Python, entre otras) concentran el mayor número de licencias con el 52,56% (41) del total de licencias que posee la entidad (78), y dentro de estas, las *Gratis* son las de mayor utilización (32).

Le siguen las aplicaciones web (SIGDEP/Visor Observatorio/Visores Geograficos ArcGIS, ROYAL, ECM, Gestión servicios, Intranet, ORFEO 7, Portal Inmobiliario, Portal web, CAPID, Control de Horario, Inventario Consulta Web, SIDEPE, Sistema de Administración de Cuentas, Sistema de

Información Gerencial del Espacio Público, SUMA+, entre otras) con el 26,92% (21).

Tabla Nro. 2. Tipo de aplicación por tipo de licencia

Tipo de aplicación	Tipo de licencia					Total	%
	Gratuita	Suscripción	Propia	Perpetua	Cesión		
Aplicación de escritorio	32	4		4	1	41	52,56
Aplicación web	6	6	8	1		21	26,92
Cliente/Servidor					5	5	6,41
Servidor de aplicaciones	3			2		5	6,41
Motor de base de datos	3	1				4	5,13
Software de servidor	1		1			2	2,56
Total	45	11	9	7	6	78	100



Fuente: OTIC – Elaboración OCI

4.5 Usuarios con perfil administrador

Se identificaron siete (7) funcionarios de la OTIC cuyo usuario está configurado con privilegios de Administrador, que le permite realizar instalaciones de software y aplicativos en los computadores.

Por otra parte, se identificaron once (11) formatos únicos de sistemas de los años 2025 y 2026, con solicitudes de acceso a sistemas de información misionales (SIDEF, SAI), sistemas de información geográfica (ArcGIS), sistemas externos (SI-CAPITAL), sistemas de información de gestión (ORFEO), softwares especiales (VUR, SIIC, VUC) y otros sistemas de información (SUMA, ROYAL, MAP).

4.6 Licencias y software propietario

El DADEP posee licenciamiento en productos como: ARCGIS, Microsoft Office 2019 Government, Microsoft Office MacStandard 2019, Microsoft Windows 2016, Microsoft Windows 2016 CAL, Microsoft Windows Profesional, ORACLE/TOAD TM, ROYAL, Software Visual C Profesional 60, Windows 11 y Antivirus. Dentro del software propietario se encuentra: Sistema de Personal de Nómina PERNO, Sistema de Inventarios, Sistema de Contratación, Control de Horario y SIDEF (misional). Cabe anotar, que durante la vigencia 2025 no se realizaron bajas de licencias ni de software en la entidad.

4.7 Software libre utilizado en la entidad

Aunque en la mayoría de los casos el software libre no tiene costo de licenciamiento, es importante que la entidad evalúe el impacto que este puede ocasionar en la infraestructura tecnológica, antes de realizar la instalación. Dada la responsabilidad de la OTIC para instalar software, inclusive para la operación propia, siempre se debe generar el ticket correspondiente para dar cumplimiento a la política de seguridad y privacidad de la información en materia de software.

Se evidenció el archivo *Inventario Software Libre DADEP.xls*, que contiene cuarenta y tres (43) tipos de software autorizados y utilizados para aplicaciones de escritorio, aplicaciones web, motor de bases de datos, servidor de aplicaciones y software de servidor. En lo corrido del año 2026, se observó en el archivo *Casos de instalación software libre.xls*, dieciséis (16) tickets de los cuales seis

(6) solicitaron la instalación del Aplicativo SIIC de Catastro, SIPOS de 4-72 y Fuentes de Word no incluidos en el inventario oficial definido por la OTIC. Ver tabla nro. 3.

Tabla Nro. 3. Tickets de instalación de software libre no incluido en el inventario oficial

Nro. ticket	Software libre no incluido	Fecha de creación	Cerrado
S-202606-13795	Aplicativo SIIC de Catastro	19/06/2026	No
S-202606-13776		17/06/2026	No
S-202606-13739		10/06/2026	16/06/2026
F-202601-3310		22/01/2026	2/02/2026
S-202602-12781	SIPOS de 4-72	5/02/2026	6/02/2026
F-202601-3333	Fuentes de Word	28/01/2026	3/02/2026

Fuente: OTIC – Elaboración OCI

Así las cosas, y teniendo en cuenta lo estipulado en la Política General de Seguridad y Privacidad de la Información, numeral 12. *CONTROL DE INSTALACIÓN Y USO DE SOFTWARE*, medida 1. *Políticas de restricción de instalación*, no se da cumplimiento a lo indicado en la viñeta 2, *Mantenimiento de un listado oficial de software aprobado, el cual será revisado y actualizado periódicamente*. Por lo anterior, es importante que la OTIC defina la periodicidad de revisión del software libre para disponer del inventario debidamente actualizado, resaltando que dicho listado oficial no registra fecha de referencia.

4.8 Muestra y generación de archivos de software instalado en puestos de trabajo (visita)

Para calcular el tamaño de la muestra se aplicó la herramienta generada por la Contraloría General de la República (ver imagen Nro. 1), que permitió por Muestreo Aleatorio Simple estimar una muestra de catorce (14) de los doscientos treinta y siete (237) computadores tomados como población.

Imagen Nro. 1. Muestreo Aleatorio Simple

CONTRALORÍA GENERAL DE LA REPÚBLICA	
AUDITORIA:	
Muestreo Aleatorio Simple para estimar la proporción de una población	
Contraloría Delegada / Gerencia Departamental:	
Sujeto ó Punto de Control:	
Cálculo de la muestra para:	Licencias de software
Período Terminado:	Corte al 30 de junio de 2026
Preparado por:	Albeiro Rizo Gallardo
Fecha:	22/07/2026
Revisado por:	Allan Alfisz
Fecha:	22/07/2026
Referencia de P/T	
INGRESO DE PARÁMETROS	
Tamaño de la Población (N)	237
Error Muestral (E)	5%
Proporción de Éxito (P)	1%
Nivel de Confianza	95%
Nivel de Confianza (Z) (1)	1,960
TAMAÑO DE LA MUESTRA	
Fórmula	15
Muestra Óptima	14
Formula para poblaciones infinitas $n = \frac{Z^2 * P * Q}{E^2}$ Formula para poblaciones finitas $n = \frac{P * Q * Z^2 * N}{N^2 * E^2 + Z^2 * P * Q}$ Z= Valor de la distribución normal estándar de acuerdo al nivel de confianza E= Error de muestreo (precisión) N= Tamaño de la Población P= Proporción estimada Q= 1-P	

Fuente: Contraloría General de la República – Cálculo OCI

Posteriormente, para seleccionar los catorce (14) computadores se realizaron los siguientes pasos:

1. Utilización de la función aleatoria de Excel.
2. Generación de los números aleatorios entre 1 y 237.
3. Selección de los primeros catorce (14) números aleatorios, con base en la identificación del puesto de trabajo.

Con el acompañamiento de la Oficina de Tecnologías de la Información y las Comunicaciones se realizó la inspección física de los computadores seleccionados en la muestra, se verificó en sitio la placa de inventario asociada al puesto de trabajo y se generaron los archivos .txt que contienen el software instalado. Ver tabla nro. 4.

Tabla Nro. 4. Software de computadores de la muestra, no incluido en el listado oficial

Nro.	Puesto de trabajo	Placa de inventario	Dependencia ¹	Software por fuera del listado oficial	Observaciones OCI
1	35	8021	SGIEP	3D Builder, AVG AntiVirus Free, Foxit Phantom, Skype.	• AVG AntiVirus Free no es el antivirus oficial de la entidad. Fortinet Endpoint Detection es el antivirus adquirido por la entidad. • Skype es un software de comunicación. A cambio, la entidad utiliza TEAMS (plataforma digital de comunicación y colaboración que reúne chats, videollamadas y herramientas de trabajo en un solo lugar).
2	55	7171	OTIC	Bizagi Modeler, Eclipse Temurin JDK con Hotspot, Everything voidtools, IrfanView, LibreOffice 7.5.5.2, Postman, Power Automate, Rustdesk, SourceTree, GLPI Agent.	
3	59	7174	OTIC	GLPI Agent	
4	66	9414	Despacho	GLPI Agent	
5	68	7208	OAC	5kPlayer, Armoury Crate, Maxon Cinema 4D, UXP WebView.	
6	72	9415	OAC	GLPI Agent	
7	92	9349	SRI	Sin novedad	Software hace parte del listado oficial
8	117	9450	SRI	GLPI Agent	
9	127	9379	SRI	GLPI Agent	
10	164	8077	SGC	Brave, GoToMeeting, GoTo Opener, Redragon Griffin.	Redragon Griffin es una marca de periféricos (mouse) para videojuegos.

¹ **SGIEP:** Subdirección de Gestión Inmobiliaria y del Espacio Público; **OTIC:** Oficina de Tecnologías de la Información y las Comunicaciones; **OAC:** Oficina Asesora de Comunicaciones; **SRI:** Subdirección de Registro Inmobiliario; **SGC:** Subdirección de Gestión Corporativa; **OJ:** Oficina Jurídica; **OAP:** Oficina Asesora de Planeación.

Nro.	Puesto de trabajo	Placa de inventario	Dependencia ¹	Software por fuera del listado oficial	Observaciones OCI
11	178	9531	SGC	GLPI Agent	
12	182	9399	SGC	GLPI Agent	
13	199	7125	OJ	Sin novedad	Software hace parte del listado oficial
14	203	9502	OAP	GLPI Agent	

Fuente: computadores DADEP - Elaboración OCI

Descripción del software encontrado:

- 3D Builder:** aplicación de software desarrollada por Microsoft que permite a los usuarios crear, imprimir y compartir modelos en 3D.
- 5kPlayer:** software de reproducción multimedia versátil que puede procesar múltiples archivos multimedia, ya sea que estén guardados en formato de video o audio.
- Armoury Crate:** utilidad de software diseñada para proporcionar un control centralizado de los productos de juego ROG compatibles.
- AVG AntiVirus Free:** programa de seguridad informática diseñado para proteger la computadora contra virus, malware, spyware y otras amenazas en línea.
- Bizagi Modeler:** herramienta de modelamiento de procesos de negocio que permite visualizar diagramas, modelar y documentar procesos utilizando el estándar BPMN.
- Brave:** navegador web rápido, privado y seguro para PC, Mac y dispositivos móviles. Se caracteriza por bloquear anuncios y rastreadores automáticamente.
- Eclipse Temurin JDK con Hotspot:** herramienta para cualquier desarrollador que trabaje con aplicaciones Java, proporcionando un entorno robusto y eficiente para la ejecución de programas.
- Everything voidtools:** utilidad de búsqueda de escritorio gratuita para Windows que puede encontrar rápidamente archivos y carpetas por nombre.
- Foxit Phantom:** software de edición de PDF capaz de crear, modificar y colaborar en documentos y formularios PDF.
- GLPI Agent:** diseñado para recopilar y reportar información sobre activos de TI, como computadoras, impresoras, equipos de red y otros periféricos.
- GoToMeeting:** software profesional de reuniones en línea que facilita la conexión con las personas de la forma que desee.

12. **GoTo Opener:** se instala automáticamente con GoToMeeting y le ayuda para iniciarle en las sesiones activas.
13. **IrfanView:** visor y editor de imágenes popular y versátil para Windows.
14. **LibreOffice 7.5.5.2:** suite ofimática de código abierto compatible con Microsoft Office para Windows, Mac y Linux.
15. **Maxon Cinema 4D:** programa profesional de animación y modelado en 3D destinado a diseñadores de animación, generalistas 3D y estudios creativos.
16. **Postman:** herramienta que facilita de forma drástica el diseño, testeo, documentación y automatización de APIs.
17. **Power Automate:** plataforma de automatización que permite crear flujos para conectar aplicaciones y ejecutar tareas automáticamente.
18. **Redragon Griffin:** marca reconocida en el ámbito de los periféricos para videojuegos, que se dedica a ofrecer hardware de alto rendimiento.
19. **Rustdesk:** software de acceso remoto y soporte de código abierto.
20. **Skype:** programa de comunicación por internet que permite hacer videollamadas, llamadas de voz y chats de texto.
21. **SourceTree:** cliente gráfico para GIT (controlador de versiones) que permite realizar la mayoría de las operaciones sin necesidad de escribir comandos.
22. **UXP WebView:** herramienta para desarrolladores que buscan integrar contenido web en sus aplicaciones de Adobe.

Como se registra en la tabla nro. 4, se encontraron estas novedades:

- Veintidós (22) tipos de software no incluidos en el inventario oficial aprobado y autorizado por la OTIC, excepto en el puesto de trabajo 92, placa 9349; y en el puesto 199, placa 7125.
- En el puesto de trabajo 35, placa 8021, está instalado el antivirus AVG, que no corresponde al adquirido por la entidad (Fortinet Endpoint Detection). Adicionalmente, tiene Skype, siendo TEAMS el software adquirido por la entidad.
- En el puesto de trabajo 164, placa 8077, está instalado el software Redragon Griffin, relacionado con hardware para videojuegos.

Por lo expuesto en el numeral 4.7 (donde se identificaron seis (6) tickets para la instalación de tres (3) tipos de software que no están incluidos en el inventario oficial); y en el numeral 4.8, donde se identificaron veintidós (22) tipos de software no registrados en dicho inventario, se configura la observación nro. 1.

4.8.1 Observación Nro. 1 y alerta preventiva: Debilidades en la actualización y control del inventario oficial de software aprobado y autorizado por la OTIC, lo que podría afectar el adecuado seguimiento de dichos activos informáticos.

4.9 Auditorías para identificar y eliminar software no autorizado

Se evidenció el documento: *Resultado Auditoría Gestión de Software.pdf*, ejecutada en la vigencia 2025, cuyo alcance incluyó el proceso de inventario de software que ejecuta OTIC para los equipos de la entidad; la generación del inventario mediante la ejecución de script (.bat/PowerShell) en los equipos de cómputo y la posterior consolidación en una base de datos en Excel; y el inventario de licencias suministrado (Inventario de licencias almacén y certificados de Autodesk), utilizado para contrastar cantidades y tipos de licencias frente al software detectado en los equipos; donde se identificaron oportunidades de mejora para fortalecer la gestión y el cumplimiento normativo.

Aunque la OTIC manifiesta que “...en relación con la socialización y presentación formal de los resultados ante la Alta Dirección y el Comité Institucional de Gestión y Desempeño (CIGD), este proceso está pendiente y se procederá a su trámite correspondiente”, esta oficina considera que no se ha dado trámite oportuno, considerando que a la fecha han transcurrido siete (7) meses del año 2026, y no se ha gestionado la entrega a la Alta Dirección y del CIGD; por consiguiente, no se da cumplimiento a lo indicado en la Política General de Seguridad y Privacidad de la Información, numeral 12. *CONTROL DE INSTALACIÓN Y USO DE SOFTWARE*, medida 3. *Monitoreo y auditoría periódica*, viñeta 2, *Documentación de hallazgos y generación de informes para la Alta Dirección y el Comité Institucional de Gestión y Desempeño (CIGD)*. Por lo anterior, es importante que la OTIC defina una periodicidad de entrega de los informes que permita poner en conocimiento de la Alta Dirección y del CIGD, el estado de la gestión del software. Por consiguiente, se configura la observación nro. 2.

4.9.1 Observación nro. 2 y alerta preventiva: Incumplimiento en la presentación de los informes de monitoreo y auditoría de software ante la Alta Dirección y el Comité Institucional de Gestión y Desempeño, limitando la disponibilidad oportuna de información para la toma de decisiones y el seguimiento institucional.

5. ANÁLISIS DE POTENCIALES RIESGOS

De conformidad con el *Mapa de riesgos institucional 2026 - seguridad de la información*, publicado en la página web el 05/05/2026; no se registran riesgos relacionados directamente con la instalación de software ilegal o no autorizado. Durante la realización de este seguimiento no se presentaron incidentes que favorecieran la materialización de riesgos asociados con programas o licenciamiento de software malicioso.

6. SEGUIMIENTO A LAS RECOMENDACIONES SEGÚN INFORME VIGENCIA 2024

La entidad realizó las siguientes acciones a las recomendaciones del *Informe de Seguimiento Derechos de Autor Software - Vigencia 2024*, remitido a la directora según radicado Nro. 20251100029513 del 31/07/2025. Ver Tabla Nro. 5.

Tabla Nro. 5. Seguimiento recomendaciones informe vigencia 2024

Recomendación	Acción adelantada por el área	Seguimiento OCI
i. Allegar oportunamente y de manera completa, la información requerida por la Oficina de Control Interno, en pro de garantizar la elaboración y publicación del informe en la página web, de conformidad con el Plan Anual de Auditorías 2025. De persistir el incumplimiento en los próximos seguimientos, se configurará el hallazgo correspondiente.	En atención a la recomendación emitida por la Oficina de Control Interno, se informa que como medidas de control y seguimiento acordó con el punto focal de la OTIC, mantener los requerimientos de auditoría de la OCI, en la bandeja de entrada hasta tanto se elabore y remita la respuesta correspondiente y se cierre completamente la gestión requerida. Esta estrategia permite conservar visible el requerimiento junto con su fecha de vencimiento, facilitando el monitoreo permanente de los compromisos adquiridos y reduciendo el riesgo de omisión o entrega extemporánea de la información solicitada.	Se evidenció pantallazo en el sistema ORFEO, que muestra la permanencia del requerimiento de la OCI en la bandeja de entrada, hasta la elaboración y entrega final de la respuesta. Se recomienda constancia en la aplicación del control definido por la OTIC.
ii. Validar la posibilidad de configurar en la red institucional los computadores de propiedad del DADEP asignados para teletrabajo (placas 7132 y 8045), con el fin de prevenir eventuales ataques cibernéticos y disminuir la vulnerabilidad a malware.	Equipo placa 7132: Teniendo en cuenta que este equipo funciona con el internet del funcionario quien trabaja en casa, técnicamente y teniendo la infraestructura con la que cuenta la entidad no es posible configurarlo en el dominio de la red institucional. Sin embargo, cabe aclarar que este equipo tiene configurado el software Forticlient en el cual, mediante una conexión segura por VPN, los usuarios pueden conectarse a las aplicaciones y carpetas compartidas en la red institucional interna de la entidad. Equipo placa 8045: Este equipo se encuentra actualmente en la entidad, sin embargo, vale aclarar que este equipo tiene instalado el software Forticlient.	Aunque técnicamente no es posible configurar el equipo con placa nro. 7132 en el dominio del DADEP, esto puede generar contagio y propagación de virus informáticos en la interacción de archivos con las carpetas compartidas. Cabe resaltar que tener instalado FortiClient a través de VPN, no garantiza que el equipo esté exento de infectarse; por el contrario, puede servir de vehículo en una eventual propagación de virus al interior de la red institucional. Es fundamental mantener actualizado el antivirus del equipo de teletrabajo, para evitar riesgo de propagación de virus informáticos a través del correo electrónico cuando se realice un intercambio de archivos, y riesgos derivados del uso por la utilización de terceros (familiares, amigos, etc.).
iii. Fortalecer las actividades de sensibilización a los usuarios finales y administradores, relacionadas con las prohibiciones y riesgos de instalación de software no licenciado ni autorizado en los computadores y servidores de la entidad.	El 29 de agosto de 2025 se llevó a cabo una capacitación virtual titulada “Ética, Responsabilidad y Uso Legal del Software en el Manejo de la Información”, cuyo propósito fue fortalecer la sensibilización de los funcionarios y contratistas de la entidad en relación con el uso adecuado, ético y legal del software. Adicionalmente, se realizó una capacitación presencial dirigida a los funcionarios encargados de la mesa de ayuda, quienes son el personal autorizado para realizar la instalación de software en los equipos de la entidad, con el fin de reforzar sus conocimientos y asegurar el	Se evidenció la presentación y capacitación virtual de fecha 29/agosto/2025, junto con la lista de asistencia, relacionada con: “Ética, Responsabilidad y Uso Legal del Software en el Manejo de la Información”, dirigida a la entidad. Adicionalmente, se evidenció acta de reunión del 03/junio/2026, llamada: “Capacitación Gestión segura de software”, dirigida al personal OTIC con perfil de administrador.

Recomendación	Acción adelantada por el área	Seguimiento OCI
	cumplimiento de los lineamientos institucionales en esta materia. Evidencia: Material de la capacitación y listas de asistencia en los archivos relacionados a continuación: Etica_Responsabilidad-Uso Legal del Software, Listado asistentes a capacitación, Gestión segura de software - mesa de ayuda y Acta capacitación mesa de ayuda, estos se encuentran en la ruta "\\172.25.1.6\otic-oci\Derechos de autor\Anexos".	
iv. Realizar periódicamente operativos de depuración de software y programas no autorizados, tanto en los computadores como en los servidores de datos de la entidad.	La oficina de tecnologías de información y las comunicaciones del DADEP por medio de un contrato de mantenimiento preventivo y correctivo realiza la revisión tanto física como lógica de todos los equipos de cómputo de la entidad, en este mantenimiento se revisa el software que está instalado en cada máquina como medida de mitigación a la instalación de software no autorizado. Como evidencia de esta actividad se diligencian formatos de mantenimiento preventivo por cada uno de los equipos intervenidos en el mencionado contrato, estos formatos se encuentran almacenados en el expediente físico de este contrato el cual reposa en la oficina de sistemas y puede ser consultado cuando se requiera. Adicionalmente, en el marco del proceso de renovación tecnológica que actualmente adelanta la entidad, se están instalando nuevos equipos de cómputo. Durante este proceso se realiza la validación y verificación del software instalado en cada equipo, garantizando que únicamente se instalen aplicaciones y herramientas autorizadas por la entidad. Esta actividad es ejecutada exclusivamente por usuarios con perfil de administrador, quienes son los únicos que cuentan con los privilegios necesarios para la instalación, configuración y administración del software corporativo, fortaleciendo así los controles para prevenir la instalación de software no autorizado. Adicionalmente se adjunta informe del primer semestre \\172.25.1.6\otic-oci\Derechos de autor\Anexos\ INFORME DE REVISION SOFTWARE NO AUTORIZADO.pdf, con la relación de todos los servidores en los que se validó que efectivamente no se encuentra ningún software no autorizado no instalado.	Se evidenció informe de revisión de software no autorizado, para el primer semestre de 2026, instalado en los servidores de datos, donde no se encontró novedad alguna. Por otro lado, se revisaron dos (2) carpetas físicas del contrato de mantenimiento Nro. 131-628-2024, suscrito con I-comm Solutions, que contiene formatos de mantenimiento preventivo de computadores, con la descripción y cantidad de programas instalados.
v. Revisar las validaciones del aplicativo SAE-SAI, con el fin de verificar la obligatoriedad de almacenamiento de información en los campos Responsable y Área del archivo	Se realizó la revisión de las validaciones del aplicativo SAE-SAI respecto a la obligatoriedad de almacenamiento de la información relacionada con el responsable y el área de los equipos de cómputo.	Se evidenció que el aplicativo SAE/SAI realiza las validaciones correspondientes para que los campos en mención sean de captura obligatoria.

Recomendación	Acción adelantada por el área	Seguimiento OCI
Excel que contiene el informe de equipos de cómputo.	Como resultado de la revisión, se evidenció que el archivo Excel generado por el sistema contiene la información requerida a través de los siguientes campos: CODIGO_DEPENDENCIA_RESPONSABLE, DESC_DEP_RESPONSABLE, IDENTIFICACION_RESPONSABLE, NOMBRE_RESPONSABLE. Por lo anterior, la información del responsable y del área se encuentra disponible dentro del archivo exportado y son campos obligatorios en el sistema de información.	
vi. Registrar los tickets de instalación de software, necesario para que la OTIC elabore las actividades propias de su gestión, con el fin de mantener la trazabilidad del software libre instalado en los computadores de la entidad.	Se adjunta el archivo “\\172.25.1.6\otic-oci\Derechos de autor\listados\Casos de instalación Software libre.xls”, el cual contiene el registro de los tickets relacionados en la mesa de ayuda con las solicitudes de instalación de software libre realizadas por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC). La información consignada en dicho archivo permite evidenciar la trazabilidad de las solicitudes atendidas de software libre en los equipos de la entidad, así como las actividades ejecutadas para su gestión. Este registro sirve como soporte y evidencia del control efectuado sobre la instalación de software, contribuyendo al seguimiento y administración de los recursos tecnológicos institucionales.	Se evidenció archivo Excel que contiene, tanto los tickets de solicitud de instalación de software por parte de usuarios finales, como del personal de la OTIC.

Fuente: OTIC - Elaboración OCI

Revisadas las evidencias y soportes allegados, la entidad dio cumplimiento a las acciones adelantadas para atender las recomendaciones del informe vigencia 2024. Sin embargo, se debe monitorear el computador en calidad de teletrabajo (**placa nro. 7132**), ya que por temas técnicos no está configurado en la red institucional, lo que eventualmente podría servir de vehículo en la propagación de virus informáticos cuando se utilizan las carpetas compartidas o se envían correos, esto teniendo en cuenta que el antivirus es el del equipo en casa y la entidad no tiene control que garantice que está actualizado.

7. CONCLUSIONES

Realizado el seguimiento se concluye:

- Se verificó que la entidad dio cumplimiento a las acciones adelantadas para atender las recomendaciones emitidas en el informe de la vigencia 2024, conforme a las evidencias y soportes revisados. Este resultado refleja un avance positivo en la gestión institucional y en la capacidad de respuesta frente a las observaciones de auditoría, fortaleciendo la cultura de control y el cumplimiento normativo.

- ii. Se evidencia que la entidad ha implementado controles específicos para prevenir la instalación de software ilegal o no autorizado. Medidas adoptadas como la restricción de permisos de instalación a perfiles de administrador, la obligatoriedad de solicitar programas mediante el Formato Único de Sistemas (FUS), la ejecución de monitoreos periódicos y auditorías, así como la desinstalación de aplicaciones no autorizadas, reflejan un fortalecimiento de la política institucional de seguridad informática.
- iii. Se evidenció una debilidad en la gestión y actualización del inventario oficial de software libre de la entidad, toda vez que seis (6) de los dieciséis (16) casos de instalación gestionados hasta lo corrido de la vigencia 2026 corresponden a software que no se encuentra registrado en dicho listado, sumado a veintidós (22) tipos de software detectado en los equipos de la muestra aleatoria. Esta situación refleja incumplimiento de lo establecido en la Política General de Seguridad y Privacidad de la Información respecto al mantenimiento de un listado oficial de software aprobado, actualizado y revisado periódicamente; lo que condujo a la configuración de las observaciones y alertas preventivas 1 y 2.
- iv. La ausencia de una periodicidad formal de revisión y actualización del inventario de software, así como la falta de una fecha de referencia, limita la capacidad de la OTIC para garantizar un control adecuado sobre la instalación y uso de software en la entidad. Esta condición incrementa el riesgo de uso de herramientas no evaluadas o no autorizadas y afecta la efectividad de los controles definidos para la administración de activos de software.
- v. Se evidencia la instalación de software diferente (AVG antivirus y Skype) al oficialmente contratado (antivirus Fortinet y Microsoft Teams) y de programas ajenos a la función institucional (software de videojuegos), lo que refleja debilidades en los controles de instalación y uso de herramientas informáticas. Esta situación incrementa el riesgo de vulnerabilidad en la seguridad de la información y afecta la eficiencia en la gestión tecnológica.
- vi. Se evidencia que en la modalidad de trabajo en casa se dispone de un computador (placa 7132), que por razones técnicas y de gobernabilidad, no mantiene conexión con la red corporativa, lo cual limita la aplicación de controles de seguridad. Esta situación incrementa un eventual riesgo de propagación de virus informáticos ocasionado por la interacción con servicios de la entidad, como el correo y las carpetas compartidas, ya que el antivirus es propiedad del funcionario.
- vii. Se evidencia que no se ha dado trámite oportuno a la socialización y presentación formal de los resultados de las auditorías realizadas por la OTIC durante la vigencia 2025, orientadas a identificar y eliminar software no autorizado. A la fecha, han transcurrido siete (7) meses del año 2026 sin que dichos resultados hayan sido puestos en conocimiento de la Alta Dirección y del Comité Institucional de Gestión y Desempeño (CIGD).

8. RECOMENDACIONES

Realizado el seguimiento se recomienda:

- i. Fortalecer las actividades de sensibilización a los usuarios finales y administradores, relacionadas con las prohibiciones y riesgos de instalación de software no licenciado ni autorizado en los computadores y servidores de la entidad.
- ii. Monitorear permanentemente los equipos utilizados en la modalidad de trabajo en casa de propiedad del funcionario, para que mantengan el antivirus actualizado. Esta medida permitirá reducir el riesgo de propagación de virus informáticos y fortalecer la protección de los servicios de la entidad, incluyendo correo electrónico y carpetas compartidas.
- iii. Incluir en la Política General de Seguridad y Privacidad de la Información periodos de corte para las revisiones periódicas que faciliten la actualización del inventario oficial de software, garantizando que todas las instalaciones se encuentren registradas en el listado institucional aprobado. Adicionalmente, incluir plazos de entrega que garanticen la oportunidad en la comunicación de hallazgos y auditorías realizadas a la Alta Dirección y al Comité Institucional de Gestión y Desempeño.
- iv. Incluir en el listado oficial de software la fecha de realización de la actualización, como periodo de referencia y control periódico, lo que permitirá reducir el riesgo de uso de software no autorizado y depurar la base de datos de programas y software existente.

9. RESUMEN DE HALLAZGOS Y OBSERVACIONES

La Tabla Nro. 6 resume las observaciones derivadas del seguimiento efectuado por la Oficina de Control Interno.

Tabla Nro. 6. Resumen de Observaciones

Observación	
4.8.1	Observación nro. 1 y alerta preventiva: Debilidades en la actualización y control del inventario oficial de software aprobado y autorizado por la OTIC, lo que podría afectar el adecuado seguimiento de dichos activos informáticos.
4.9.1	Observación nro. 2 y alerta preventiva: Incumplimiento en la presentación de los informes de monitoreo y auditoría de software ante la Alta Dirección y el Comité Institucional de Gestión y Desempeño, limitando la disponibilidad oportuna de información para la toma de decisiones y el seguimiento institucional.

Fuente: elaboración OCI

Finalmente, es importante aclarar los conceptos que dan lugar a plan de mejoramiento:

Observación: situación que podría convertirse en un futuro incumplimiento de un requisito (hallazgo) y llegar a tener efectos sobre el cumplimiento de los objetivos, procesos, planes, programas o proyectos. Producto del análisis realizado, es potestativo del líder del proceso acoger las observaciones realizadas por la OCI y sí hay lugar a documentarlas en virtud del autocontrol.

Hallazgo: es el resultado de la comparación de la condición (situación detectada o hechos identificados) con el criterio que se refiere al deber ser (cumplimiento de normas, reglamentos, lineamientos o procedimientos). Los hallazgos deben ser objeto de formulación de acciones tendientes a eliminar de fondo las causas que las originaron, las cuales harán parte del correspondiente plan de mejoramiento que debe formularse en la herramienta tecnológica dispuesta por la entidad.



ALLAN MAURICE ALFISZ LÓPEZ
Jefe Oficina de Control Interno

Anexos: sin anexos
Copia: SGC y OTIC
Proyectó: Albeiro Rizo Gallardo
Revisó y aprobó: Allan Maurice Alfisz López
Fecha: julio de 2026
Código de archivo: 1102703