

DISTRISSEGURIDAD

Nit: 806.013.404-2

**DISTRISSEGURIDAD
OFICINA DE CONTROL INTERNO**

**INFORME SOFTWARE LEGAL
VIGENCIA 2025**

**NAGIB CHALAVE GONZÁLEZ
ASESOR DE CONTROL INTERNO**

CARTAGENA DE INDIAS DISTRITO TURÍSTICO Y CULTURAL

MARZO DE 2026

1. INTRODUCCIÓN

En cumplimiento de lo ordenado por las Directivas Presidenciales 001 de 1999 y 02 de 2002 del Consejo Asesor del Gobierno Nacional en materia del Control Interno de las entidades del Orden Nacional y Territorial y Circular 027 del 29 de diciembre de 2023 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor; Distrisseguridad, presenta el Informe “Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software”, correspondiente a la vigencia 2025.

2. OBJETIVO

Reportar ante la Dirección Nacional de Derechos de Autor, la información de los equipos de cómputo y software licenciado de Distrisseguridad.

3. ALCANCE

Derecho de Autor sobre software de la vigencia 2025.

4. FUENTE NORMATIVA

- Decreto 1083 de 2015 Art. 2.2.21.4.9 Literal f.
- Directivas Presidencial 001 de 1999.
- Directiva Presidenciales 002 de 2002 del Consejo Asesor del Gobierno Nacional en materia del Control Interno de las entidades del Orden Nacional y Territorial.
- Circular 027 del 29 de diciembre de 2023 de la Dirección Nacional de Derecho de Autor.

5. DESARROLLO DEL INFORME

5.1. ¿Con cuántos equipos cuenta la Entidad?

Actualmente la entidad cuenta con 41 Equipos de cómputo de los cuales 26 se encuentran en funcionamiento (operativos) y 15 se encuentran en desuso para disposición final de baja. A continuación, se relaciona la distribución de los equipos en funcionamiento:

ÍTEM	MARCA DEL EQUIPO	SERIAL MONITOR
1	Thermaltake Clon	0ASVHCPY200550F - 0ASVHCP200746L
2	Thermaltake Clon	0ASVHcPY200635V-0ASVHCPY200674R
3	Thermaltake Clon	OASVHCPY200481R - OASVHCPY200683N

DISTRISSEGURIDAD

Nit: 806.013.404-2

4	Hewlett-Packard	8CC2231203
5	Hewlett-Packard ALL IN ONE 22	8CC22312YX
6	Hewlett-Packard ALL IN ONE PC	8CC223134F 22DF1517LDL
7	Hewlett-Packard PRO MINI 400 g9	GW2480-T / CNK 50519PM
8	DELL	47D-AURX-A05
9	Hewlett-Packard	8CC223133V
10	LENOVO THINKCENTRE	VKN02401
11	Hewlett-Packard ALL IN ONE pc 22-DF1517LA	8CC2231340
12	Hewlett-Packard ALL IN ONE - 22 DF 1XXX	8CC2231340
13	Hewlett-Packard ALL IN ONE	3CR52209M4
14	Hewlett-Packard ALL IN ONE 22	8CC2231308
15	Hewlett-Packard ALL IN ONE 22	8CC223134Q
16	Hewlett-Packard ALL IN ONE 22	N/A
17	DELL	E2222H
18	Hewlett-Packard ALL IN ONE 22	8CC223135P
19	Hewlett-Packard ALL IN ONE	8CN34703YP
20	DELL	E2222H
21	Acer	Portátil
22	Acer	Portátil
23	Acer	Portátil
24	Hewlett-Packard ALL IN ONE	8CN34703YP
25	Hewlett-Packard ALL IN ONE	8CN34703YQ
26	Acer nitro	Portátil model n23q22

5.2. ¿Software instalado en estos equipos se encuentra debidamente licenciado?

El software de los equipos con los que cuenta Distrisseguridad se encuentran debidamente licenciados cumpliendo así con las normativas vigentes en materia de derechos de autor. De acuerdo con lo reportado por el área de TIC de la entidad, se tiene licencia de los siguientes softwares:

Tabla 2. softwares instalados en los equipos de cómputo de Distrisseguridad.

Ítem	Software	Licencia	Vigencia
1	Microsoft Team Enterprise	16	16/sept/2026
2	Microsoft 365 E3	16	16/sept/2026
3	Lumion Pro 1	4	20/jun/2026
4	Revit autodesk	4	09/jul/2026

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

DISTRISSEGURIDAD

Nit: 806.013.404-2

Los 26 equipos funcionales tienen restricción de instalación de software mediante autenticación de usuarios administradores. Dentro de los mecanismos socializados por el área TIC de la entidad, donde manifiestan la implementación de controles específicos implementados, se encuentran los siguientes:

5.3.1 El primer mecanismo consiste en que los PC cuentan con dos usuarios: el primero, Administrador; y el segundo, un usuario estándar, con el fin de que solo el personal de TIC pueda realizar cambios en ellos; sin embargo, como medida adicional en el plan de seguridad y privacidad de la información se dispone de la política que indica que la instalación de software en los equipos de la empresa se encuentra regulada.

En lo que corresponde a la Política de seguridad para los equipos 4.2.5 se tiene:

4.2.5 Política de seguridad para los equipos Distriseguridad, para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al proceso Gestión de TIC.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al proceso Gestión de TIC.

Con respecto al uso adecuado de internet

4.2.6 Política de uso adecuado de internet Distriseguridad consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios

públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

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

De acuerdo a lo manifestado por el área TIC de la entidad, se conoce que el Sistema de gestión de la calidad, específicamente en la caracterización del proceso de infraestructura, tiene contemplado el procedimiento para la baja de bienes. El procedimiento está establecido en el manual de procesos y procedimientos generales Versión 5.0

De otra parte, el software dado de baja en la entidad es desinstalado del equipo donde se encuentre, debido a que las licencias se han adquirido por medios digitales y/o descargados desde la web, no se cuenta con medios físicos de instalación y por ello no se realiza una disposición final como la destrucción física.

Respecto a los computadores, al momento de quedar en desuso se procede a remitir inventariado mediante memorando al PU de Recursos Humanos y Físicos, para que se realice la disposición final de los mismos de acuerdo con las políticas definidas por la entidad.

6. CONCLUSIONES

De acuerdo con el seguimiento realizado por la oficina de Control Interno comunicado mediante memorando 04-0123 de 09 de febrero de 2026, a la información suministrada a través del oficio de 04 de marzo del mismo año por parte del área de TIC de la entidad, y al proceso de verificación realizado por la Oficina de control interno; se pudo establecer que la entidad cuenta con 26 equipos de cómputo en funcionamiento, los cuales cuentan con softwares licenciados activos; por lo que se observa el cumplimiento de las normas en cuanto a los derechos de autor en el tema licenciamiento de software por parte de Distriseguridad.

Así mismo, se observan mecanismos de control establecidos que permiten un control y seguimiento al uso de software dentro de la entidad.

7. RECOMENDACIONES

- Identificar riesgos y diseñar controles relacionados con las fechas de vigencia de las licencias adquirida respectiva en los equipos de cómputo de Distriseguridad, con el objetivo de prevenir la expiración de las licencias.
- Fortalecer los controles de restricción de instalación de software en los equipos de cómputo de la entidad, estableciendo los parámetros técnicos necesarios para garantizar la seguridad y funcionamiento de los mismos.
- Realizar proceso de disposición final para los equipos de cómputo que se encuentran en desuso e inservibles atendiendo los lineamientos establecidos en el programa de gestión ambiental de la entidad relacionados con los residuos de aparatos eléctricos y electrónicos (RAEE).

Atentamente,

NAGIB CHALAVE GONZÁLEZ

Asesor de Control Interno

Proyectó: Donny Marsiglia López - Asesor Externo C.I.