AERONÁUTICA CIVIL

**OFICINA DE CONTROL INTERNO**

Informe verificación cumplimiento normas relacionadas con el Licenciamiento de

Software y Derechos de Autor Vigencia 2023

**Bogotá D.C., marzo 2024**

# OBJETIVO.

Dar cumplimiento con lo establecido en la Directiva Presidencial No 002 y la Circular 017 de 2011 de la Dirección Nacional de Derechos de Autor, en donde se ordena a las Oficinas de Control Interno verificar el cumplimiento de las disposiciones en materia de derechos de autor sobre adquisición y utilización de programas de computador (software), así como de la remisión de la información relacionada al inventario, controles de instalación y el aseguramiento para que estos den cumplimiento con los derechos de autor y derechos conexos en la vigencia 2023.

# ALCANCE.

Verificar para la vigencia 2023 y a nivel nacional que el software instalado en los equipos adquiridos por la Entidad, se encuentran debidamente licenciados.

# MARCO NORMATIVO.

Para el desarrollo y la elaboración del presente informe, se tomó como base el siguiente marco normativo:

* Directiva Presidencia 02 del 12 de febrero de 2002, sobre el respeto al derecho de autor y a los derechos conexos en lo referente a utilización de programas de ordenador (software).
* Circular interna 037 UAEAC – SG 05 octubre 2021-Lineamientos de Control para el licenciamiento de Software (perpetuidad, suscripciones, derechos de uso y Derechos de Autor).
* Resolución 3084 de 2015 “por la cual se adopta el manual para el manejo administrativo de los bienes muebles de propiedad de la UAEAC”
* Resolución 04215 de 2019 “por medio de la cual se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), en la UAEAC”
* Circular 04 del 22 de diciembre de 2006, expedida por el Concejo Asesor del Gobierno Nacional en Materia de Control Interno, “Verificación, recomendaciones y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software”.
* Circular 12 del 02 de febrero de 2007 expedida por la Dirección Nacional de Derecho de Autor (DNDA) estableció el procedimiento para el recibo, administración y custodia de dicha información para la verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).
* Circular No. 017 del 01 de junio de 2011, expedida por la Dirección Nacional de Derechos de Autor, donde aclara las condiciones para el recibo de la información y cargue en su página Web para recepcionar la información.
* Circular No. 01 del 04 de abril de 2016 “Vigencia circulares del consejo Asesor del Gobierno Nacional”, expedida por el Concejo Asesor del Gobierno Nacional en materia de control interno.
* Decreto 1008 del 14 de junio de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
* Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
* Manual de Gobierno Digital V6 diciembre 2018.
1. **METODOLOGÍA.**

Se utilizó el modelo de gestión del riesgo y el concepto de controles de las “tres Líneas de Defensa”, evaluando y verificando el cumplimiento de lineamientos normativos en materia de derecho de autor sobre programas de computador (software).

# DESARROLLO DEL INFORME

La responsabilidad, los controles y la gestión de aseguramiento y cumplimiento de directrices establecidas en materia de derecho de autor sobre programas de computador (software) recae en la segunda línea de defensa (Secretaría General – Dirección Administrativa- Grupo de Almacén y Activos Fijos, Grupo de Seguros; la Secretaría de Tecnologías de la Información – Dirección de Infraestructura y Soporte de TI; y la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea).

La oficina de Control Interno, como tercera línea de defensa y desde la fase de evaluación al sistema de control interno implementado en la Entidad en esta materia, solicitó información a la segunda línea de defensa sobre los inventarios de equipos de cómputo, sistemas de información y licencias adquiridas e instaladas. Radicado 2024392040005606
Id: 1240636; del 2024-03-01.

Se constató mediante la información enviada que el control y administración de inventarios es ejercido principalmente por el Grupo de Almacén y Activos fijos. A su vez y de acuerdo con su rol y competencia, la Secretaría de Tecnologías de la Información – Dirección de Infraestructura y Soporte de TI; y la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea, como ordenadoras del gasto y con rubros presupuestales diferentes, adquieren y administran independientemente los equipos PC y licencias para su gestión, evidenciando en la conciliación realizada, que dichas áreas ejercen el control pertinente sobre los equipos adquiridos, distribuidos y puestos en servicio en sus áreas, asegurándose que todo el software instalado tenga el licenciamiento debido.

Una vez analizada y conciliada la información enviada por las áreas, la Oficina de Control Interno procedió, de acuerdo con los criterios del sistema de información de la Dirección Nacional de Derechos de Autor del Ministerio del Interior, a cargar los datos suministrados y registrados en el sistema de información de inventarios del Grupo de Almacén y Activos Fijos, la Dirección de Infraestructura y Soporte de TI y la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea teniendo en cuenta que a estas áreas, de acuerdo con sus roles y competencias, les corresponde la adquisición, ingreso, registro, actualización, seguimiento y

control de los equipos informáticos, sistemas de información y aseguramiento del licenciamiento del Software instalado.

Los computadores (mesa y portátiles) adquiridos institucionalmente tienen asociados el sistema operativo y su inventario es controlado por el Almacén. Igual sucede con las licencias adquiridas, sin embargo, algunas de las licencias de Software adquiridas se hacen por suscripción, las cuales no ingresan al Almacén, se asignan por usuario y no por equipo y su suscripción se hace por un tiempo definido, que al vencerse quedan desactivadas.

**INVENTARIO DE EQUIPOS DE COMPUTO - LICENCIAS – SERVIDORES**



Al corte del presente informe 31/12/2023 el almacén reportó 1060 equipos, entre computadores mesa, portátiles y servidores que se consideran inactivos ya que se encuentran en custodia del almacén y por lo tanto no afectan los reportes de licenciamiento de Software.

Se adjunta al presente informe archivos con el inventario, registros y datos aportados por el Grupo de Almacén y activos fijos, la Dirección de Infraestructura y Soporte de TI y la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea.

En las **POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**, se verificó

* en el numeral 4.19 Hardware y Software, que se tiene establecidos los siguientes mecanismos de control:
* El hardware y software se convierten en la herramienta de trabajo más importante para la Aerocivil y su uso se debe hacer de acuerdo con los siguientes lineamientos:
* El software que se use para la Aerocivil debe estar explícitamente aprobado por el Líder del Proceso.
* La instalación de software sin contar con la autorización del Líder del Proceso y que no tenga el licenciamiento acorde con el Marco Legal y Regulatorio Colombiano, conlleva a un proceso disciplinario.
* Todo el software debe ser adquirido aplicando el Procedimiento para asegurar la adquisición o uso de software original.
* Quien asuma el rol de responsable del software debe cumplir con la debida diligencia para que se garantice el licenciamiento requerido, soporte especializado permanente, mantenimiento y gestión de vulnerabilidades acorde con los requerimientos de seguridad de la información del proceso correspondiente.
* Todo el software instalado en la Aerocivil debe contar con un contrato de soporte que incluya el reporte de las vulnerabilidades acorde con las amenazas cibernéticas a nivel global. El propietario del software debe garantizar los recursos para que las vulnerabilidades reportadas sean remediadas oportunamente para prevenir daños a los intereses de la Aerocivil.
* Todo software instalado en la Aerocivil debe contar con un servicio de detección proactiva de vulnerabilidades con soluciones automatizadas que hagan uso de técnicas acordes con las amenazas cibernéticas a nivel global
* El responsable del software debe definir los requerimientos de seguridad aplicando la guía de gestión de riesgos de la Entidad.
* Todo proveedor de software debe garantizar contractualmente el soporte para la solución de las vulnerabilidades identificadas. Este soporte debe incluir la generación de versiones que corrijan las vulnerabilidades identificadas, complementado con una asesoría para lograr protección con soluciones de seguridad perimetral.
* La Dirección de Informática únicamente puede implementar los requerimientos de seguridad que el responsable del software haya autorizado.
* La Dirección de Informática y las áreas responsables de TI en la Entidad son las únicas áreas autorizadas para instalar, desinstalar, configurar, probar, activar o inactivar en producción cualquier tipo de software.
* La Dirección de Informática y las áreas responsables de TI en la Entidad son las únicas áreas autorizadas para instalar, desinstalar, configurar, probar, activar o inactivar en producción cualquier tipo de hardware.
* La adquisición del hardware debe estar autorizado por la Dirección de Informática y las áreas responsables de TI en la Entidad.
* Todo el hardware utilizado en la Aerocivil debe responder específicamente a las necesidades del software autorizado.
* La Dirección de Informática debe reportar a los propietarios de información correspondiente de la tecnología que administra, los tiempos de obsolescencia para que se tomen las medidas oportunas para la actualización del software y hardware requeridos.
* El uso de software o hardware que no esté explícitamente autorizado debe tratarse aplicando el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
* La disposición de hardware debe contar con un procedimiento de borrado seguro de la información, el cual debe ser solicitado por los propietarios de la información y ejecutado por el Grupo de Soporte Informático.

# Mecanismo de Control para la Instalación Software NO Licenciado.

La Entidad para evitar la instalación de software no licenciado (Software ilegal), por parte de los Servidores Públicos (Usuarios Finales), cuenta con los siguientes mecanismos sistematizados de control:

* Los usuarios finales no cuentan con permisos individuales para la instalación de software en los equipos que tienen asignados.
* A través del directorio activo, se controlan los tipos de acceso y las restricciones asignadas a los usuarios.
* Existen grupos de administradores, que tienen privilegios para instalar software en los equipos
* Los grupos de usuarios estándar no cuentan con el privilegio de instalación de software.
* En la Política de Seguridad, se tiene establecido que el usuario final no actúe como administrador de su equipo de cómputo.
* Cuando un usuario interno, requiere un software de uso libre o licenciado a través de agente externo diferente a la Dirección de Informática, debe solicitar al Grupo de Seguridad de la Información, el respectivo permiso para su verificación, aprobación e instalación a través de la mesa de servicio (linea3000).

Adicionalmente, las páginas de descarga de software no autorizado se encuentran bloqueadas, a través de mecanismos de verificación y control, implementados desde el Grupo de Seguridad de la Información.

# Destino final del Software dado de baja.

Como mecanismo de seguimiento y control, para la baja de las licencias obsoletas, se verificó que la Entidad cuenta con el Protocolo denominado “Baja de Licencias Obsoletas”, el cual se encuentra publicado en el Sistema de Gestión de Calidad de la Entidad (ISOLUCIÓN).

Cuando un software es dado de baja por obsolescencia al cumplir su ciclo de vida útil, el director de Infraestructura y soporte TI solicita al almacén dar de baja y descargar del inventario del cuentadante el software a cargo de la secretaría de TI. Se realiza desinstalación en los equipos y retiro de accesos, si aplica.

Para el software por suscripción, la vigencia de las licencias finaliza cuando no se renueva la suscripción.

**HALLAZGO No 01**

Coordinar la generación y adopción de lineamientos que fortalezcan los controles para la administración y reporte de activos como software y hardware, de tal forma que se minimicen las diferencias en inventarios sobre estos, y los reportes de dicha información guarden correspondencia entre las diferentes dependencias usuarias de dichos activos y responsables.

Realizar la verificación, conciliación y cruce de información generada por el Grupo de almacén sobre el inventario de software y hardware de los cuentadantes responsables para el mantenimiento en el aplicativo de almacén e inventarios la consolidación final con datos iguales y correspondientes.

**Responsables**

Les corresponde a las áreas de Dirección de Infraestructura y Soporte de TI y a la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea de acuerdo con los datos suministrados y registrados en el sistema de información de inventarios del Grupo de Almacén y Activos Fijos.

# 5. CONCLUSIONES y RECOMENDACIONES

Basados en el análisis de la información, la conciliación de los registros enviados y evaluación del sistema de control interno implementado por las áreas que conforman la segunda línea de defensa sobre este tema, se evidenció que la Entidad dispone de los mecanismos de control suficientes para evitar que los servidores públicos (Usuarios) instalen programas no licenciados en los equipos; asegurar que las licencias de software instaladas de la Entidad sean legales y estén actualizadas y constatando documentalmente que la entidad cuenta con procedimientos para dar de baja las licencias obsoletas.

Como oportunidad de mejoramiento se recomienda que la Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea informe y coordine oportunamente un Visto Bueno con la Secretaría de Tecnologías de la Información – Dirección de Infraestructura y Soporte de TI que administra la red Corporativa, para la adquisición de los equipos de cómputo y otros dispositivos de TI para la red de comunicaciones ATN, esto impactaría positivamente para un mejor control sobre los equipos y dispositivos TI que por su naturaleza debería conocer la Secretaría de TI.

Finalmente se concluye que, la AEROCIVIL a través de la primera y segunda línea de defensa se asegura que los equipos, los sistemas de información y el software instalados en la Entidad, cuenten con licencias legales y certificadas por el fabricante respectivo, de acuerdo con lo validado con las diferentes áreas involucradas.

La Dirección Nacional de Derechos de Autor, mediante Certificación de fecha 15- 03-2024, certificó la presentación del informe Software Legal correspondiente a la Vigencia 2023 (Se anexa Certificación).



Atentamente,



# SONIA MARITZA MACHADO CRUZ

Jefe Oficina de Control Interno

Preparo: Anselmo Cañón Pérez.