

EMPRESA COLOMBIANA DE PRODUCTOS VETERINARIOS - VECOL S.A.

INFORME DERECHOS DE AUTOR DE SOFTWARE

Presentado a:

LA DIRECCIÓN NACIONAL DE DERECHOS DE AUTOR

Elaboró y Revisó el área de Auditoría Interna

**Andrea López Aranguren
Paula Valentina Escobar**

Marzo de 2026

1. Naturaleza jurídica de la Empresa Colombiana de Productos Veterinarios - Vecol S.A. y aplicabilidad de la normatividad.

VECOL S.A. es una sociedad de economía mixta del orden nacional, con participación estatal representada por el Ministerio de Agricultura y Desarrollo Rural (62,64 %) y el Patrimonio Autónomo de Remanentes de la Caja Agraria en Liquidación (19,98 %), así como participación del sector privado. En consecuencia, la Compañía cuenta con una participación estatal superior al 82 % del capital social, pero inferior al 90 %, razón por la cual no ostenta la naturaleza jurídica de Empresa Industrial y Comercial del Estado. En este sentido, VECOL S.A., en su calidad de sociedad anónima de economía mixta, cuenta con personería jurídica propia y se rige, en el desarrollo de su actividad comercial, por las disposiciones del derecho privado y los lineamientos aplicables a las sociedades comerciales anónimas, de conformidad con la normativa vigente y lo establecido en sus Estatutos Sociales.

2. Aplicabilidad para Vecol S.A:

Vecol S.A., en su calidad de sociedad de economía mixta, deberá atender los requerimientos formulados por los entes de control en materia de derechos de autor de software, con el fin de verificar que las soluciones informáticas utilizadas por la Compañía cuenten con el licenciamiento correspondiente y se encuentren en cumplimiento de la normativa vigente. Para ello, se realizará la revisión y validación de la documentación, así como de la asignación de equipos y los registros asociados al software utilizado en la entidad, verificando su correspondencia con las disposiciones vigentes sobre derechos de autor.

3. Antecedentes

Dando cumplimiento a lo establecido en la Directiva Presidencial N° 002 de 2002 y en la Circular Externa 027 de 2023 de la Dirección Nacional de Derechos de Autor, en las cuales se establece que *“la información que debe contener el reporte corresponde a la verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de Derechos de Autor sobre software”*, el cual debe ser presentado por la Oficina de Auditoría Interna como responsable de verificar el cumplimiento de las disposiciones en esta materia, así como de la remisión de la información relacionada con el inventario, los controles, la instalación y la baja de software. Con fundamento en lo anterior, la función de Auditoría Interna presenta el resultado de la revisión efectuada con corte al 31 de diciembre de 2025, el cual debe ser reportado a través del aplicativo dispuesto por la Dirección Nacional de Derechos de Autor.

4. Objetivos

- Evaluar la información suministrada por el área de Tecnología de la Información, con el fin de verificar el cumplimiento de lo establecido en la Circular 027 del 28 de diciembre de 2023, relacionada con la verificación de la legalidad del software para la vigencia 2025.

- Verificar la existencia y consistencia del inventario de software, mediante la revisión de una muestra representativa de equipos, con el fin de confirmar que los programas instalados correspondan a los activos reportados por el área de Tecnología de la Información.
- Verificar que los programas instalados de manera inicial en los equipos cuenten con las respectivas licencias de uso, validando su estado y vigencia conforme a las disposiciones establecidas por la compañía.
- Evaluar la efectividad de los mecanismos de control implementados por la compañía, con el propósito de confirmar que se restrinja la instalación de aplicaciones por parte de usuarios no autorizados y que no se permitan programas sin el debido licenciamiento.

5. Alcance

La verificación del software se realizó sobre una muestra representativa del inventario total de equipos de cómputo de Vecol S.A., previamente validada con las áreas de Activos Fijos y Tecnología de la Información, con corte al 31 de diciembre de 2025. Para cada equipo seleccionado se efectuó la revisión de los programas instalados y de las licencias en uso, evaluando su estado y vigencia. Adicionalmente, se probó la efectividad de los controles establecidos por la compañía mediante la ejecución de pruebas de instalación de aplicaciones, con el fin de verificar las restricciones para usuarios no autorizados.

6. Normatividad Interna y Externa

1. MAN-DS0-015 – Manual de Seguridad y Privacidad de la Información.
2. PRO-DS0-013 – Instalación de Software en Sistemas Operativos.
3. Directiva Presidencial 001 del 25 de febrero de 1999 – Respeto al Derecho del Autor y a los Derechos Conexos.
4. Directiva Presidencial 002 del 12 de febrero de 2002 – Respeto al Derecho de Autor y a los Derechos conexos, en lo referente a la utilización de programas de ordenador (Software).
5. Circular No. 04 de 2006 del Consejo Asesor del Gobierno Nacional en Materia de Control Interno.
6. Circular No. 12 de 2007 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor.
7. Circular No. 17 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor.
8. Circular No. 027 de 2023 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor.

7. Metodología

Para la elaboración del presente informe se solicitó información a las áreas responsables de la administración del inventario de equipos de cómputo y de las licencias de software adquiridas por la compañía para el desarrollo de sus actividades.

A partir de la información remitida por las diferentes dependencias, el área de Auditoría Interna realizó la verificación de las respuestas y el análisis de la documentación soporte mediante la aplicación de cuestionarios y la revisión física de una muestra de equipos seleccionados. Lo anterior, con el propósito de corroborar el cumplimiento de la normativa aplicable en la implementación y uso de programas, licencias y software, así como de elaborar el reporte correspondiente y realizar el diligenciamiento del formulario ante la Dirección Nacional de Derechos de Autor.

8. Desarrollo del Procedimiento

Con base en la información recopilada y analizada durante el proceso de auditoría, se procedió a revisar los aspectos relacionados con los mecanismos de control implementados por la entidad para prevenir la instalación de programas no autorizados y el procedimiento definido para la gestión del software dado de baja, el licenciamiento del software instalado y el inventario de equipos.

En este sentido, a continuación, se presentan los resultados a las preguntas establecidas en el formulario de reporte de la Dirección Nacional de Derechos de Autor, con el propósito de evidenciar el cumplimiento de las disposiciones en materia de legalidad del software en la entidad.

1. ¿Con cuántos equipos cuenta la entidad?

La compañía cuenta con un total de equipos de cómputo, los cuales se relacionan a continuación:

Resumen Equipos de Computó	Cantidad
Computador de escritorio	43
Computadores portátiles	219
Servidores	6
TOTAL	268

Fuente: Tecnología de la Información

Adicionalmente, se relacionan las Tablet y Celulares asignados a colaboradores:

Resumen Tablet / Celulares	Cantidad
Tablet	52
Celulares	59
TOTAL	111

Fuente: Tecnología de la Información

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

Según el reporte suministrado por el área de Tecnología de la Información, los programas instalados en los equipos cuentan con las licencias correspondientes, tal como se detalla a continuación:

Software	Cantidad de licencias	Estado licenciamiento	Duración de la licencia
Windows 11 Pro	252	Activas	Perpetua
MacOS - Sequoia 15	11	Activas	Perpetua
CCURE 9000 Series P	1	Activas	Perpetua
Hik Central Professional	1	Activas	Perpetua
Microsoft Office (diferentes versiones)	234	Activas	Perpetua
Veam backup and replication 12	1 para 20 equipos	Activas	5 años
VMware v Sphere Client version 8.0.3.00600	3 nodos	Activas	5 años
Windows Svr Datacenter 2022 64Bit español 1 pk DSP OEI DVD 16 Core	1	Activas	Perpetua
Creative Cloud Pro	2	Activas	Anual
Acrobat Pro	12	Activas	Anual
Google Workspace Enterprise Plus	300	Activas	3 años
Manage Engine Vulnerability Manager Plus Enterprise Edition workstation	340	Activas	Anual
Manage Engine Vulnerability Manager Plus Enterprise Edition server	15	Activas	Anual
Antivirus Trellix Protect Plus EDR for Endpoint	280	Activas	3 años

Fuente: Tecnología de la Información

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

La Compañía ha implementado mecanismos de control de carácter técnico y administrativo destinados a mitigar y prevenir la instalación de software que no cuente con el licenciamiento correspondiente. Estos controles son ejecutados por el área de Tecnología de la Información y se describen a continuación:

• **Primer Control:**

- ∞ **Responsable:** Analista de Desarrollo y/o Ingeniero de sistemas e infraestructura.
- ∞ **Frecuencia:** Continua (monitoreo) con revisión de reportes de forma Mensual.
- ∞ **Propósito u Objetivo:** Mitigar el riesgo de instalación de software pirata o malicioso mediante el bloqueo preventivo de descargas desde sitios web no categorizados o prohibidos.

- ∞ **Cómo se lleva a cabo:** A través de la consola centralizada de Trellix (ePO), se configuran políticas de "Web Control" y "Threat Prevention". El sistema analiza el tráfico y bloquea automáticamente las descargas de archivos ejecutables (.exe, .msi, .dmg) provenientes de fuentes no autorizadas.

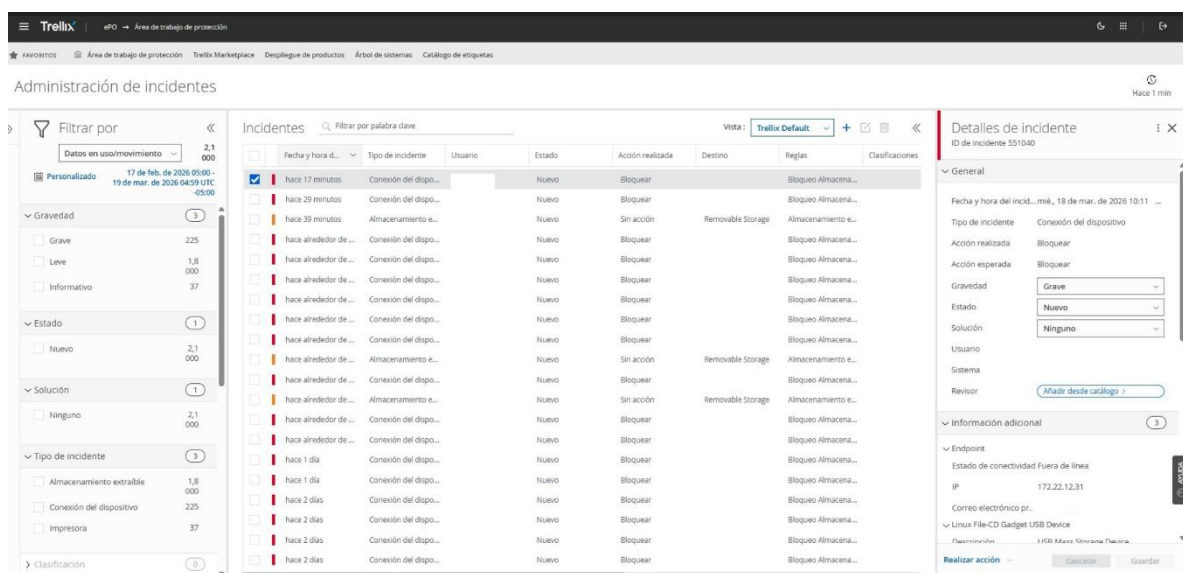
Adicionalmente se realizan bloqueos vía Firewall para evitar la navegación y descarga de software desconocidos y a través de Manage Engine se controlan las actualizaciones de software.

- ∞ **Qué pasa con las desviaciones y/o excepciones:** Si un colaborador requiere un software específico, debe solicitarlo mediante la herramienta interna de Vecol S.A. denominada Mesa de Ayuda Técnica, la cual busca proveer a los usuarios un punto único de contacto mediante el cual se resuelvan y/o canalicen las necesidades relativas al uso de recursos y servicios de plataformas tecnológicas de la empresa. Si se detecta un intento de descarga bloqueado, el sistema genera una alerta que es analizada por el equipo de seguridad para descartar intentos de intrusión.

- ∞ **Evidencia de la ejecución:**

1. Logs generados por la consola de Trellix.
2. Reportes mensuales de actividad de bloqueo de sitios/archivos.
3. Logs de Firewall.
4. Bloqueos de Manage Engine.

El área de auditoría interna efectuó la validación del control y monitoreo continuo de los bloqueos realizados por la consola Trellix mediante la administración de incidentes, según se detalla a continuación, donde se puede concluir que se cumple con la política de seguridad de la información implementada.



The screenshot shows the Trellix ePO interface for incident management. The main window displays a list of incidents with columns for date, type, user, status, action, device, rules, and classifications. A sidebar on the left allows filtering by severity, state, solution, and incident type. A right sidebar shows details for a specific incident, including its date, type, action, and endpoint information.

- **Segundo Control:**

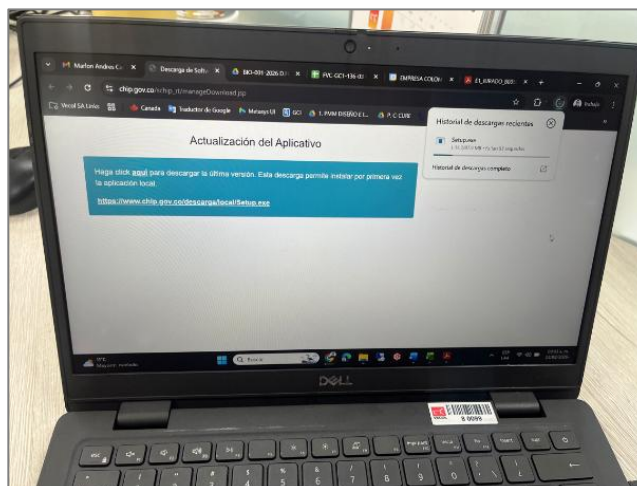
- ∞ **Responsable:** Analista de Desarrollo y/o Ingeniero de sistemas e infraestructura.
- ∞ **Frecuencia:** Permanente (Configuración de base en el dominio).
- ∞ **Propósito u Objetivo:** Garantizar que solo el personal autorizado (con credenciales de administrador) pueda modificar el registro del sistema e instalar aplicaciones, asegurando que todo software cuente con su licencia, previa validación.
- ∞ **Personal autorizado:**
 - Karolain Pineda - Analista de Desarrollo.
 - Diego Vela - Analista de Desarrollo.
 - Geovani Acuña - Ingeniero de Sistemas e Infraestructura.
- ∞ **Cómo se lleva a cabo:** Se aplica una GPO (Group Policy Object) a nivel de Unidad Organizativa (OU) que elimina los privilegios de administrador local a los usuarios estándar. Al intentar ejecutar un instalador, el sistema operativo solicita obligatoriamente el usuario y contraseña de un administrador de dominio o local.
- ∞ **Qué pasa con las desviaciones y/o excepciones:** Las excepciones son mínimas y deben estar documentadas. En caso de que un usuario logre escalar privilegios o instalar software mediante "portables", el antivirus (Trellix) actúa como control compensatorio detectando la anomalía. Siempre está activo el Data Loss Prevention, con excepciones previamente autorizadas.
- ∞ **Evidencia de la ejecución:** Configuración de la directiva en el Editor de Gestión de Directivas de Grupo y resultados del comando gpresult/r en estaciones de trabajo aleatorias.

Con el fin de validar el control relacionado con la restricción en la instalación de aplicaciones, Auditoría Interna seleccionó una muestra de 22 equipos de cómputo y 3 tabletas del total reportado por el área de Tecnología de la Información. Durante la revisión se evidenció que los dispositivos cuentan con controles que restringen la instalación de aplicaciones por parte de colaboradores no autorizados.

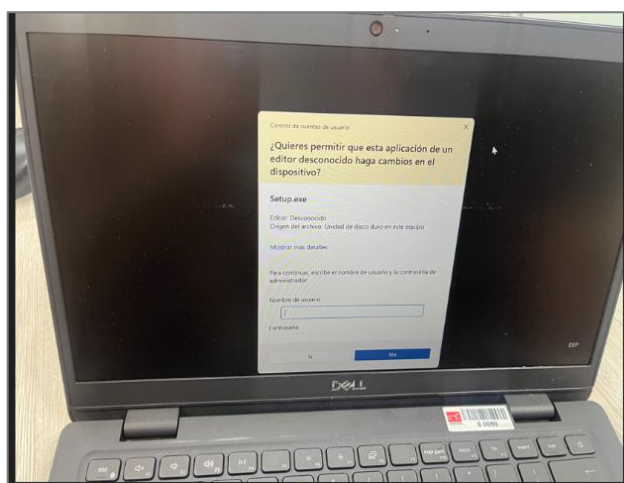
La verificación se realizó mediante la ejecución de una prueba de instalación a partir de un enlace externo; al intentar ejecutar el aplicativo, el sistema generó una alerta y solicitó las credenciales de personal autorizado para permitir la instalación, lo cual confirma la existencia del control. El detalle de la prueba se presenta a continuación:

Se ejecuto el siguiente link: https://www.chip.gov.co/schip_rt/manageDownload.jsp

- Visualización de la ejecución del link externo relacionado, en uno de los equipos validados:



- Solicitud de credenciales solicitando la información de los administradores autorizados por el área de TI, para proceder con la instalación de la aplicación:



Se evidenció que, para los 22 equipos de cómputo evaluados, seleccionados dentro de la totalidad de áreas de la compañía, no fue posible realizar la instalación del software. Al momento de ejecutar la descarga, se observó la activación de un cuadro de diálogo de control de cuentas de usuario que solicita credenciales de administrador para autorizar la instalación, tal como se muestra en la imagen anterior.

En consecuencia, se concluye que los equipos verificados cumplen con las políticas de seguridad implementadas por Vecol S.A., al encontrarse activos y operando adecuadamente los controles establecidos para restringir la instalación de software por parte de usuarios no autorizados.

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

El destino final del software depende de su modelo de licenciamiento. Para el caso específico de los sistemas operativos (Windows) y suites de ofimática (Office) adquiridos bajo la modalidad de licencias perpetuas preinstaladas (OEM), el proceso es el siguiente:

Vínculo con el Hardware:

Las licencias perpetuas están asociadas directamente a la placa base (motherboard) del equipo desde su activación. Por restricciones contractuales del fabricante, estas licencias no son transferibles a otros equipos.

Fin del Ciclo de Vida:

Una vez que el equipo cumple su vida útil, sufre un daño irreparable o queda tecnológicamente obsoleto, la licencia se da de baja de forma simultánea con el activo físico.

Disposición Final:

1. Desincorporación: El equipo se retira del inventario de activos fijos.
2. Destrucción de Datos: Se realiza un borrado seguro de los discos duros para proteger la información institucional.
3. Baja Lógica: Se registra en la matriz de software que dicha licencia ha quedado inactiva y no puede ser reutilizada.
4. Gestión de RAEE: El equipo (y, por ende, la licencia adherida a él) se entrega a un gestor autorizado de Residuos de Aparatos Eléctricos y Electrónicos (RAEE) para su disposición final ambientalmente responsable.

Conclusiones

Con base en la información y los soportes evaluados, se evidenció que los softwares instalados en los equipos de cómputo y adquiridos por la entidad cuenta con las licencias correspondientes, las cuales se encuentran activas y vigentes durante el año 2025 y a la fecha del reporte. En este sentido, la entidad dispone de herramientas y mecanismos de control que permiten verificar la legalidad del software utilizado, dando cumplimiento a las directrices impartidas por la Dirección Nacional de Derechos de Autor en materia de uso autorizado de programas informáticos y los lineamientos internos.

Adicionalmente, a partir de las pruebas realizadas para validar las restricciones establecidas que impiden a los usuarios la instalación de programas o aplicativos no autorizados, se evidenció que los equipos evaluados cuentan con controles de seguridad activos y funcionando adecuadamente. En consecuencia, se concluye que se da cumplimiento a las políticas internas de seguridad de la información establecidas por la compañía y la normatividad aplicable.

A handwritten signature in black ink, appearing to read 'Andrea López Aranguren'.

Andrea López Aranguren
Auditor Interno Vecol S.A.

Anexo 1 - Certificado de Trasmisión a la Dirección Nacional de Derechos de Autor.