



Informe de *software* **2025**



Introducción

En cumplimiento de lo dispuesto en la **Directiva Presidencial No. 02 del 12 de febrero de 2002** emitida por la Presidencia de la República de Colombia, y de las normas vigentes en materia de derecho de autor y derechos conexos, en especial aquellas relacionadas con el uso, adquisición y administración de programas de computador (software), el presente informe correspondiente al **año 2025** tiene como propósito presentar de manera integral las acciones, controles y procedimientos implementados por **Rotorr** para garantizar el uso legal, seguro y eficiente del software institucional.

La Directiva Presidencial establece lineamientos orientados a asegurar que las entidades adopten prácticas responsables frente al licenciamiento, la instalación, el inventario y la verificación del software, previniendo el uso de programas no autorizados o sin la debida habilitación legal. En este marco, Rotorr reafirma su compromiso con el respeto a la propiedad intelectual, la transparencia administrativa y la gestión adecuada de los recursos tecnológicos.

Durante la vigencia 2025, Rotorr desarrolló actividades sistemáticas de **verificación, monitoreo y control**, orientadas a:

- Validar el cumplimiento de las condiciones de licenciamiento del software instalado en los equipos institucionales.
- Mantener actualizado el inventario de activos tecnológicos y de software.

- Evaluar riesgos asociados al uso indebido, obsolescencia o vulnerabilidades derivadas de herramientas informáticas no autorizadas.
- Fortalecer los mecanismos de control interno relacionados con la gestión de tecnologías de la información.

Asimismo, se ejecutaron acciones de **seguimiento y mejora continua**, incluyendo revisiones periódicas, cruces de información, actualización documental y socialización de lineamientos internos dirigidos a promover el uso adecuado del software por parte de los servidores y colaboradores.

Este informe presenta un análisis detallado del estado de cumplimiento, los resultados obtenidos en las actividades de control, las situaciones identificadas y las **medidas correctivas y preventivas** adoptadas. De igual forma, se formulan recomendaciones orientadas a optimizar la gestión del software, fortalecer la cultura de legalidad tecnológica y asegurar la sostenibilidad de los controles implementados.

Con ello, Rotorr no solo da cumplimiento a las disposiciones normativas aplicables, sino que también consolida buenas prácticas en materia de administración tecnológica, protección de derechos de autor y mitigación de riesgos operativos, legales y reputacionales asociados al uso de software.

Objetivo General

Garantizar, durante la vigencia 2025, el cumplimiento de la normativa aplicable en materia de derechos de autor y derechos conexos relacionados con el uso de programas de computador (software) en Rotorr, mediante la implementación de actividades de verificación, monitoreo y control, asegurando el uso legal, adecuado y eficiente de las herramientas informáticas institucionales, así como la protección de la propiedad intelectual y la mitigación de riesgos legales, operativos y tecnológicos.

Objetivos Específicos

- Verificar el cumplimiento del licenciamiento del software instalado en los equipos y sistemas de Rotorr, asegurando que todas las herramientas informáticas cuenten con autorización legal vigente.
- Mantener actualizado el inventario de software y activos tecnológicos, garantizando la trazabilidad, control y consistencia de la información.
- Evaluar y gestionar los riesgos asociados al uso de software, incluyendo riesgos legales, de seguridad de la información, obsolescencia y vulnerabilidades.
- Fortalecer los controles internos relacionados con la adquisición, instalación, actualización, retiro y auditoría del software institucional.

- Promover la cultura de legalidad y uso responsable del software, mediante actividades de sensibilización y socialización de lineamientos internos.
- Implementar acciones correctivas y preventivas derivadas de hallazgos identificados en los procesos de verificación y seguimiento.
- Asegurar la alineación normativa con la Directiva Presidencial No. 02 de 2002 y demás disposiciones aplicables en materia de derechos de autor.
- Optimizar la gestión tecnológica institucional, fomentando buenas prácticas en administración de licencias y seguridad digital.

Marco Legal

- Directiva Presidencial 01 de 1999.
- Directiva Presidencial 02 de 2022.
- [Circular 04 de 2006 CAGNCI](#)
- [Circular 027 de 28 dic 2023 sobre Informe de Software](#)

Preguntas

1. ¿Con cuántos equipos cuenta la entidad?

La corporación Rotorr cuenta con 13 equipos portátiles suministrados por aliados estratégicos.

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

Respuesta: SI.

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

Con el propósito de garantizar que los usuarios no instalen programas o aplicaciones que no cuenten con la licencia respectiva, Rotorr ha fortalecido durante la vigencia 2025 un conjunto integral de controles administrativos, técnicos y preventivos. Estos mecanismos están orientados a prevenir el uso de software no autorizado, proteger los derechos de autor, salvaguardar la seguridad de la información y asegurar el cumplimiento de la normativa vigente en materia de propiedad intelectual. Los principales controles implementados son:

- **Política Interna de Uso y Gestión de Software:** Se mantiene vigente y socializada una política institucional que establece lineamientos claros sobre la solicitud, evaluación, adquisición, instalación, actualización y retiro de software. Esta política define

responsabilidades, restricciones, buenas prácticas y consecuencias frente al incumplimiento, asegurando que todo software utilizado en la entidad cuente con licenciamiento válido y verificable.

- **Gestión centralizada de instalaciones:** La instalación, configuración y desinstalación de software se realiza exclusivamente a través del área de tecnología o mediante herramientas de gestión remota. Este esquema limita la capacidad de los usuarios para instalar aplicaciones sin autorización previa, garantizando que únicamente se implementen soluciones tecnológicas aprobadas y legalmente licenciadas.
- **Control de accesos y privilegios:** Se aplican principios de mínimo privilegio y segregación de funciones, restringiendo los permisos administrativos en estaciones de trabajo. Solo el personal expresamente autorizado puede ejecutar instalaciones o cambios críticos, reduciendo significativamente el riesgo de incorporación de software no permitido.
- **Herramientas de inventario y gestión de activos (ITAM/SAM):** Rotor utiliza mecanismos de inventario automatizado para mantener actualizado el registro de software instalado, versiones, licencias asociadas y niveles de uso. Estas herramientas facilitan auditorías internas, conciliaciones de licenciamiento y detección de desviaciones o instalaciones no autorizadas.
- **Controles de seguridad perimetral y filtrado:** Se implementan soluciones como firewalls, proxies y filtros web que restringen el acceso a sitios no confiables o repositorios que distribuyen software sin licencia. Asimismo, se aplican políticas de descarga segura para

minimizar la introducción de aplicaciones potencialmente ilegales o maliciosas.

- **Monitoreo y detección de software no autorizado:** Se ejecutan procesos periódicos de escaneo y monitoreo en la red institucional para identificar aplicaciones no aprobadas, versiones obsoletas o riesgos de seguridad. Ante hallazgos, se activan procedimientos de validación, bloqueo o desinstalación controlada.
- **Capacitación y sensibilización a colaboradores:** Durante 2025 se fortalecieron las actividades de formación orientadas a promover el uso legal y responsable del software. Estas jornadas incluyen información sobre riesgos legales, impactos reputacionales, ciberseguridad y buenas prácticas en el uso de herramientas tecnológicas.
- **Procedimientos de auditoría y control interno:** Se realizan verificaciones internas periódicas para evaluar el cumplimiento de políticas, validar inventarios y revisar la consistencia del licenciamiento. Estos ejercicios permiten identificar oportunidades de mejora, implementar acciones correctivas y fortalecer el sistema de control interno tecnológico.

En conjunto, estos mecanismos consolidan un entorno de control robusto que contribuye a la legalidad tecnológica, la protección de la propiedad intelectual, la eficiencia operativa y la mitigación de riesgos asociados al uso indebido del software en Rotorr.

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

El destino final del software dado de baja en Rotorr se gestiona conforme a las políticas institucionales de administración de activos tecnológicos, los lineamientos de seguridad de la información y la normativa vigente en materia de derechos de autor y propiedad intelectual. Durante la vigencia 2025, el proceso de baja se ejecutó bajo criterios de legalidad, trazabilidad y control, contemplando las siguientes acciones:

- **Desinstalación controlada y saneamiento de registros:** Todo software declarado en baja es desinstalado de manera centralizada por el área de tecnología, garantizando su eliminación completa de los equipos, servidores o entornos virtuales. Paralelamente, se actualizan y depuran los registros en las herramientas de inventario (ITAM/SAM), directorios y bases de datos institucionales, evitando inconsistencias o permanencia de instalaciones no autorizadas.
- **Eliminación segura de copias digitales:** Las copias digitales, instaladores, imágenes y respaldos asociados al software dado de baja son eliminados aplicando protocolos de borrado seguro definidos en las políticas de seguridad de la información. Este procedimiento minimiza riesgos de reutilización indebida, fugas de información o exposición a vulnerabilidades.
- **Gestión de medios físicos (cuando aplique):** En caso de existir soportes físicos (discos, unidades externas u otros medios), estos son destruidos o dispuestos mediante procedimientos que aseguren la imposibilidad de recuperación. La destrucción se documenta mediante actas o registros de disposición final.

- **Revisión de licencias y soporte contractual:** Se verifica el estado de las licencias vinculadas al software dado de baja, registrando su cancelación, vencimiento, transferencia o no renovación, según corresponda. Cuando es procedente, se notifica al proveedor o fabricante para mantener la coherencia contractual y evitar obligaciones innecesarias.
- **Evaluación de reutilización o reasignación:** Si la baja obedece a renovación tecnológica, actualización o cambios operativos, se analiza la posibilidad de reasignar licencias disponibles o reutilizar el software dentro de la entidad, siempre bajo estricta observancia de los términos de licenciamiento y restricciones legales.
- **Control de riesgos y cumplimiento normativo:** El proceso incorpora validaciones orientadas a prevenir usos posteriores no autorizados, riesgos legales o hallazgos de auditoría. Todas las actuaciones se desarrollan en alineación con la normativa sobre derechos de autor, garantizando la protección de los derechos de los desarrolladores y el uso legal del software institucional.
- **Trazabilidad y evidencia documental:** Cada baja de software cuenta con soportes verificables (solicitudes, aprobaciones, registros de desinstalación, actas, actualización de inventarios), asegurando transparencia, control interno y disponibilidad de evidencia ante revisiones o auditorías.

De esta manera, Rotorr asegura que el retiro o baja de software se realice bajo principios de legalidad, seguridad, eficiencia administrativa y fortalecimiento del sistema de control interno tecnológico.