FONCEP-FONDO DE PRESTACIONES ECONOMICAS CESANTIAS Y PENSIONES
Al contestar cite Radicado :3-2026-02021
Folios :3 Anexos :1 Fecha: 2026-03-10 16:47
Dependencia Remitente:Oficina Asesora de Control Interno
Destino :SERGIO CORTES RINCON +8
Serie :26 - informes
SubSerie :13 - informes de evaluación y seguimiento

BOGOTÁ

COMUNICACIÓN INTERNA

PARA: **SERGIO CORTES RINCON**
Director General
Dirección General

MANUEL FERNANDO ISAZA GONZALEZ
Subdirector - Subdirección Financiera y Administrativa

ANDREA MARCELA RINCON C
Subdirectora - Subdirección de Prestaciones Ecónomicas

ANA MARIA CORTES TAMAYO
Subdirectora Juridica - Subdirección Jurídica

HUGO ALBERTO POVEDA CASTAÑEDA
Gerente - Gerencia de Pensiones

IVAN ENRIQUE QUASTH TORRES
Gerente - Gerencia de Bonos y Cuotas Partes

JOAQUIN MANUEL GRANADOS RODRIGUEZ
Jefe Oficina - Oficina Asesora de Planeación

TANIA KRUSKAYA LEON PATIÑO
Jefe Oficina - Oficina de Informática y Sistemas

ANDREA MAYERLY RIOS LAGOS
Asesora - Grupo Comunicaciones y Servicio al ciudadano

DE: **SAUL DIAZ LADINO**
Jefe Oficina
Oficina Asesora de Control Interno

ASUNTO: Informe de verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derechos de autor de software - diciembre 2025.

En cumplimiento al plan anual de auditorías de la vigencia 2026, la Oficina de Control Interno realizó seguimiento al cumplimiento de las normas en materia de derechos de autor de software, en cuanto al hardware, software, controles y disposición final de equipos de cómputo, para la presentación de su resultado en el aplicativo dispuesto por la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor, con corte al 31 de diciembre del año 2025, en cumplimiento de lo dispuesto en la circular 027 de 2023.

A partir de la verificación realizada por la Oficina de Control Interno respecto al cumplimiento de las disposiciones de derechos de autor de software, se observó que el sistema de control interno es adecuado, sin embargo, se presentan las siguientes recomendaciones para la mejora del proceso.

- Actualizar y mantener un plan de revisión de placas de identificación de equipos de cómputo y sus periféricos.
- Establecer un plan para garantizar el funcionamiento del total de los equipos biométricos de la entidad.
- Fortalecer las revisiones periódicas sobre los equipos de cómputo que permitan identificar archivos o contenidos ingresados a través de memorias USB, CD u otros medios externos, que puedan resultar contrarios a las políticas de seguridad de la información establecidas por la entidad.
- Programar durante la vigencia 2026 socializaciones o capacitaciones enfocadas a la aplicación de las disposiciones de derechos de autor y propiedad intelectual a todos los colaboradores de FONCEP.
- Fortalecer el control "*Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad)"* con el fin de mantener los equipos protegidos con antivirus y complementarios durante los 365 días del año.
- Adelantar la documentación de los controles de acuerdo con lo establecido en el Manual de gestión de riesgo.

En caso de tener observaciones frente al contenido del presente informe, se solicita que se comuniquen dentro de los tres días siguientes a la radicación del presente informe, mediante radicado SIDEAF. En caso de no recibirse observaciones, se procederá a publicar el informe en la página web de FONCEP y realizar el reporte a la DNDA.

Cordialmente,

Firmado Electrónicamente
por SAUL DIAZ LADINO
Fecha: 2026-03-10 16:47
3d0544502e0683b9bb29aa56b57d932844b4a929a391ef9228a472f445471958

SAUL DIAZ LADINO
Jefe Oficina
Oficina Asesora de Control Interno

Actividad	Nombre	Cargo	Dependencia	Firma
Revisó	CESAR AUGUSTO FRANCO VARGAS	Contratista	Oficina Asesora de Control Interno	
Proyectó	GLADYS PARRA GIL	Tecnico Operativo	Oficina Asesora de Control Interno	

Documento producido automáticamente por el Sistema de Gestión de Documentos Electrónicos de Archivo del FONCEP - SIDEAF, en plena conexidad con la Resolución DG - 00024 del 14 de Abril de 2023.

FONDO DE PRESTACIONES ECONOMICAS, CESANTIAS Y PENSIONES - FONCEP

OFICINA DE COTROL INTERNO

INFORME DE SEGUIMIENTO A DERECHOS DE AUTOR DE SOFTWARE

PLAN ANUAL DE AUDITORÍA 2026

SAÚL DÍAZ LADINO
Jefe Oficina Control Interno

CESAR AUGUSTO FRANCO V
Auditor Oficina de Control Interno

Bogotá D.C, Marzo de 2026

Tabla de contenido

INFORME DE VERIFICACIÓN, RECOMENDACIONES, SEGUIMIENTO Y RESULTADOS SOBRE EL CUMPLIMIENTO DE LAS NORMAS EN MATERIA DE DERECHOS DE AUTOR DE SOFTWARE

1. INTRODUCCIÓN

En el marco del Plan Anual de Auditoría 2026, la Oficina de Control Interno (OCI) del Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP realizó el seguimiento al a la verificación, recomendaciones, y resultados sobre el cumplimiento de las normas en materia de derechos de autor de software conforme a lo dispuesto al numeral 2 de la Directiva presidencial 02 de 2002 "*Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software*)", en complemento con la Circula Externa 027 de la Unidad Administrativa de Derechos de Autor, mediante la cual se establecen las instrucciones para el reporte anual de verificación del uso legal de software en las entidades públicas.

Este informe se elabora en cumplimiento de los informes a cargo del jefe de Control Interno, entre ellos el informe de derechos de autor de software, previsto en el Decreto 1083 de 2015, artículo 2.2.21.4.9, literal f (adicionado por el Decreto 648 de 2017), el cual remite a lo señalado en el artículo 2.8.4.8.2 del Decreto 1068 de 2015. Adicionalmente, se sustenta en las funciones de evaluación independiente y asesoría asignadas a la OCI por el artículo 12 de la Ley 87 de 1993.

El seguimiento se orienta a verificar la implementación de las medidas distritales aplicables a la legalidad de software, a cuantos equipos tienen la entidad, a los controles implementados para prevenir software ilegal y los mecanismos que se tienen para la baja del software cuando deja de ser funcional para la entidad.

Adicionalmente constituye un insumo para la Alta Dirección y las líneas de defensa, al identificar avances, oportunidades de mejora y riesgos.

2. OBJETIVO

Verificar el cumplimiento de las disposiciones vigentes en materia de derechos de autor sobre software en el FONCEP, en especial las contenidas en la Directiva Presidencial 02 del 12 de febrero del 2002, y en el marco de los informes a cargo de la Oficina de Control Interno previstos en el Decreto 648 de 2017, así mismo, verificar el reporte de la vigencia 2025 en el aplicativo dispuesto por la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, de conformidad con la Circular Externa 027 de 2023.

3. ALCANCE

El seguimiento comprende la verificación del hardware, el software instalado, los mecanismos de control implementados para prevenir el uso de software no autorizado y la disposición final de los equipos de cómputo y licencias dadas de baja en el FONCEP, con corte a 31 de diciembre de 2025, a fin de evaluar el cumplimiento de las disposiciones vigentes en materia de derechos de autor de software y formular las recomendaciones a que haya lugar.

4. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA

- Decreto 1083 de 2015 “Reglamentario Único del Sector de la Función Pública” que dispone en el artículo 2.2.21.4.9 los informes que debe presentar la OCI (adicionado por el Decreto 648 de 2017).
- Directiva Presidencial 02 del 2002 “Respeto al derecho de autor y los derechos conexos, en lo referente a la utilización de programas de ordenador (software).
- Circular externa 027 de 2023 “Modificación circular 017 del 01 de junio de 2011, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador “Software”
- Circular 17 del año 2011 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor “Modificación circular 12 del 12 de febrero de 2007, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derechos de autor sobre programas de computador /software)
- Circular 12 del 2 de febrero 2007 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor “Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derechos de autor sobre programas de computador software”
- Circular 04 de 2006 “Verificación cumplimiento normas de uso de software”.

5. METODOLOGÍA

Para el desarrollo del seguimiento y la elaboración del presente informe, la Oficina de Control Interno aplicó técnicas de auditoría y verificación, tales como revisión documental, observación, inspección en sitio, verificación selectiva de equipos de cómputo y análisis de la información suministrada por las dependencias responsables. Así mismo, se efectuó verificación sobre una muestra no estadística de equipos, con el fin de validar aspectos relacionados con hardware, software instalado y mecanismos de control.

Como fuente de información se tuvieron en cuenta las respuestas remitidas por la Subdirección Financiera y Administrativa mediante radicado 3-2026-01301 del 10 de febrero de 2026, y por la Oficina de Informática y Sistemas (OIS) mediante radicados 3-2026-01293 del 10 de febrero de 2026 y 3-2026-01766 del 2 de marzo de 2026. Con base en esta información y en las

verificaciones realizadas por la Oficina de Control Interno, se formularon las observaciones, conclusiones y recomendaciones del presente informe.

6. RESULTADOS

Mediante Directiva Presidencial 02 de 2002 se ordenó a las Oficinas de Control Interno, en desarrollo de las funciones de control y en el marco de sus visitas, inspecciones o informes, verificar que los programas de computador que se adquieran estén respaldados por los documentos de licenciamiento o transferencia de propiedad respectivos, entre otros aspectos.

Así mismo, mediante circulares 012 de 2007, 017 de 2011, y la circular externa 027 de 2023 la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor - DNDA dispuso que, a más tardar el tercer viernes del mes de marzo de cada año, el representante legal de la entidad y el jefe de la oficina de Control Interno deberán presentar el reporte de "*verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derechos de autor de software*", y se cargue en la página web www.derechosdeautor.gov.co el link del informe de control interno con la verificación de esos aspectos, entre los que incluye las siguientes preguntas:

1. ¿Con cuántos equipos cuenta la Entidad?
2. ¿El software instalado en estos equipos se encuentra debidamente licenciado?
3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?
4. ¿Cuál es el destino final que se le da al software dado de baja en su Entidad?

Para dar cumplimiento a los establecido en la normatividad sobre el reporte a la DNDA, la Jefe de la Oficina de Informática y Sistemas (OIS) certificó la información que es requerida por la DNDA mediante el radicado 3-2026-01766 del 02 de marzo de 2026, como se detalla a continuación:

6.1 ¿Con cuántos equipos cuenta la Entidad?

La Oficina de Informática y Sistemas (OIS) certificó los equipos de cómputo con que cuenta la entidad, distribuidos de la siguiente forma:

RESUMEN EQUIPOS DE ESCRITORIO	
DELL INC. OPTIPLEX 7010	*8*
Hewlett-Packard	*121*
PC Smart	*21*
Computadores HP nuevos	*62*
TOTAL PC ESCRITORIO	***212***

RESUMEN EQUIPOS DE ESCRITORIO	
PORTATILES	
DELL INC.	*3*
HEWLETT PACKARD	*22*
HEWLETT PACKARD NUEVOS	*24*
TOTAL PORTATILES	***49***
TOTAL COMPUTADORES	***261***

Servidores Físicos	**Cantidad**
Dell on premise	4
HP PROLIANT on premise	1
IBM on premise	1
Blade on premise	8
Servidores virtuales	**Cantidad**
Máquinas virtuales OnPremise 24	24
Oracle OCI-Nube Pública 51	51
TOTAL, SERVIDORES FONCEP	**89**

Se evidenció, con base en el inventario de hardware certificado por la jefe de la Oficina de Informática y Sistemas (OIS), que la entidad cuenta con registro y control de 261 equipos de cómputo, 14 servidores físicos y 75 servidores virtuales y/o en nube. Así mismo, se observó que durante la vigencia 2025 se dieron de baja 10 equipos de cómputo por obsolescencia, de conformidad con lo registrado en la Resolución DG-000083 del 18 de diciembre de 2025.

Por otra parte, la Oficina de Control Interno realizó la verificación del hardware de la entidad a partir de la información remitida por la Oficina de Informática y Sistemas (OIS) y la Subdirección Financiera y Administrativa (SFA), mediante inspección efectuada el 23 de febrero de 2026 sobre una muestra no estadística de 21 equipos de cómputo, equivalente al 8% del total, con el fin de verificar la actualización del plaqueteo, la identificación física y la asignación de usuarios.

Como resultado de esta verificación, se evidenció correspondencia entre el listado de equipos, los usuarios asignados y la relación remitida por las dependencias. No obstante, se identificó deficiencia en el plaqueteo y en la visibilidad de algunas identificaciones, especialmente en periféricos como mouse, teclados y pantallas, lo que dificulta su asociación con el equipo de cómputo respectivo, particularmente en algunos de los computadores de escritorio incorporados recientemente al inventario. En consecuencia, se **reitera la recomendación** de actualizar y mantener un plan de revisión periódica de las identificaciones de los equipos y sus periféricos, con el fin de asegurar su adecuada trazabilidad y control.

Durante la vigencia 2025 no se evidenció adquisición de nuevos equipos.

6.2 ¿El software instalado en todos los equipos se encuentran debidamente licenciado?

La jefe de la Oficina de Informática y Sistemas (OIS) certificó mediante radicado N° y 3-2026-01766 de 2 de marzo de 2026: "*La suscrita jefe de la Oficina de Informática y Sistemas del FONCEP,* ***CERTIFICA*** *que la Entidad cuenta con las licencias de sistema operativo, antivirus, Office y demás aplicaciones que deban estar licenciadas, para todos los equipos de propiedad del FONCEP."*

La Oficina de Control Interno verificó el ingreso de nuevas licencias durante la vigencia 2025 y evidenció que, de acuerdo con la información suministrada por la Oficina de Informática y Sistemas y el área administrativa, durante dicha vigencia se adquirieron tres licencias y/o actualizaciones, respecto de las cuales se corroboró su ingreso al almacén, lo anterior en cumplimiento de la política de operación del procedimiento de almacén: "*11. Cuando se realice la adquisición de licencias y/o software, estas deberán ser legalizadas con el ingreso al almacén, exceptuando las adquisiciones, actualizaciones, renovaciones o software cuya vida útil sea igual o inferior a 360 días. Cuando se trate de una licencia y/o software adquirido bajo un contrato de prestación de servicios, está por su naturaleza no tienen ingreso al almacén*".

Así mismo, en visita de inspección realizada el 23 de febrero de 2026, conjuntamente con un funcionario de la Oficina de Informática y Sistemas, la Oficina de Control Interno verificó el software adquirido y el software instalado en una muestra no estadística de 21 equipos de cómputo, evidenciando que, en todos los casos revisados, los equipos contaban con software licenciado de acuerdo con el inventario suministrado por la OIS, así como con software libre o de uso permitido, entre ellos Adobe Acrobat Reader, FortiClient VPN, AnyDesk, Java, Mozilla Firefox, Microsoft Edge, FileZilla y controladores de impresión administrados por dicha oficina.

No obstante, en la muestra verificada se evidenció que un equipo de cómputo no contaba con antivirus instalado y que otros tres equipos no tenían actualizada la última versión del antivirus Kaspersky. Aunque esta situación fue corregida durante la inspección, se observó debilidad en la efectividad del control denominado *"Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad)",* asociado al riesgo de *"Pérdida de integridad de los activos de información de los procesos del FONCEP*". En consecuencia, **se recomienda** revisar, fortalecer y adecuar dicho control, con el fin de asegurar la protección permanente de los equipos y reducir la exposición a virus, software malicioso u otras amenazas que puedan comprometer la información de la entidad.

De otra parte, en cinco equipos de la muestra seleccionada se realizó una prueba de descarga de programas y aplicaciones, evidenciándose que no era posible su instalación por parte del usuario final, debido a las restricciones implementadas por las herramientas de seguridad (PCSECURE) y a la exigencia de credenciales de administrador. Lo anterior permite concluir

que la instalación de software se encuentra restringida y controlada por la Oficina de Informática y Sistemas.

Finalmente, en lo que corresponde al contrato realizado en el año 2025 "*OIS-212-Contratar en el marco del proyecto de inversión No. 8030 para el cumplimiento de la meta No. 3. "Renovar el 100% del programa tecnológico y de gobierno digital", adquirir, implementar y puesta en funcionamiento de un sistema de seguridad física (sistema biométrico, cámaras) y sistema lógico de monitoreo para el FONCEP*" la OCI observó que están instalados los sistemas biométricos en los diferentes pisos y oficinas del FONCEP, que permanecen activos, y que para algunas dependencias tienen reconocimiento facial y funcionan para el ingreso, adicionalmente y de acuerdo con los documentos contractuales y soportes de ingreso se pudo establecer la entrega de los equipos, pero no se pudo evidenciar el completo funcionamiento y adecuación para todas las oficinas e instancias de la entidad por lo que **se recomienda** tomar las medidas necesarias que garanticen el completo funcionamiento y uso de los equipos biométricos configurándolos con el software actualizado y garantizando el control de ingresos mediante estos equipos

6.3 ¿Los mecanismos de control que se han implementado en la entidad para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?

La Oficina de Informática y Sistemas certificó: *"Durante el 2025, mantuvo y soporto el mecanismo de control de acceso mediante la restricción de los privilegios de administración para los usuarios del dominio y la política por Active Directory (Directorio Activo) asigna los roles y permisos a cada usuario de acuerdo con lo establecido por el jefe del área en el Formato de Acceso o Retiro de Servicios de TI. Adicionalmente, se mantuvo el licenciamiento de la herramienta PCtechSoft SAS2023, la cual permite un control centralizado sobre las estaciones de trabajo o servidores".*

La Oficina de Control Interno evidenció en la inspección realizada que los controles se encuentran funcionando. Así mismo, se evidenció que en los equipos de la muestra no había archivos MP3, MP4 o de video descargados por vía internet, sin embargo se evidenció que hay equipos que permiten ingresar memoria USB o CD donde se podrían hacer las descargas de archivos de reproducción Mp3 o Mp4, pero según indicó el ingeniero que acompaño la visita son solo autorizados con objetivos misionales o de entrega de información a entes externos **se recomienda** Mantener revisiones periódicas que garantice la revisión de archivos que puedan resultar lesivos o en contra de las políticas establecidas en la entidad.

Con respecto a las políticas acerca de los permisos para el uso de los computadores, los privilegios para algunos funcionarios, prohibiciones, autorizaciones y cuidado de los equipos se encuentran en el Manual de modelo de seguridad y privacidad de la información código MOI-APO-GTI-006 versión 2 de 12 de febrero de 2026 y en el procedimiento gestión mesa de ayuda: PDT-APO-GTI-001versión 004 de 15 de diciembre de 2025.

Durante el año 2025 se realizaron las siguientes piezas y capacitaciones para dar a conocer y actualizar sobre seguridad de la información:

- Sensibilización en Seguridad de la Información junio de 2025.
- Información importante para mantener la seguridad de la información FONCEP al Día. Edición 111 del 27 de octubre de 2025
- Información sobre autenticación correos para usuarios FONCEP Edición 115 del 24 de noviembre de 2025.
- Aviso revisión de Software y mantenimiento lógico FONCEP al Día Edición 116 del 01 de diciembre de 2025.
- Capacitación ciberseguridad, y uso de IA para gestión de pensiones convocada por FONCEP al Día. Edición 116 del 01 de diciembre de 2025.
- Tips Conciencia Digital FONCEP al Día. Edición 119 del 22 de diciembre de 2025.
- Invitación capacitaciones Gobernanza de Datos FONCEP al Día. Edición 117 del 09 de diciembre de 2025

Teniendo en cuenta que se debe fortalecer la información relacionada con derechos de autor y propiedad intelectual, **se recomienda** que durante la vigencia 2026 se contemple las socializaciones o capacitaciones enfocadas al tema de derechos de autor y propiedad intelectual, para reforzar el conocimiento respecto a este tema específico a los servidores de FONCEP.

6.4 Explicar cuál es el destino final que se le da al Software dado de baja en la entidad

De acuerdo con lo establecido en el procedimiento de almacén, capítulo Baja de bienes o elementos, que describe la actividad 1. Identificar posible necesidad de baja de bienes:

“Nota 1: Cuando se trate de software o licencias el responsable de dichos bienes deberá informar al responsable de almacén acerca del vencimiento de vida útil mediante correo electrónico o comunicación interna, donde indiquen si el bien se debe dar de baja y recomendar su destino final, el cual puede ser destrucción en el caso de medios magnéticos (se debe verificar si se requiere aplicar tratamiento sobre residuos peligrosos).”

“Nota 4: Los elementos tecnológicos, periféricos, software, licencias y/o similares, que sean devueltos por parte de la Oficina Informática y Sistemas, para ser dados de baja, o uso como repuesto, deberán ser entregados adjuntando el concepto técnico, que justifica y recomiende el destino final de los mismos. Este debe contener como mínimo la siguiente información: Nombre del elemento, placa, marca, tipo, serie, referencia, modelo, descripción del estado actual del elemento y destino si es para baja; en la situación que el bien dado de baja sea utilizado como como repuesto se deberá indicar el valor estimado para dar ingreso en el módulo de control de inventario.”

En este sentido, la Oficina de Informática y Sistemas **certificó** que, de acuerdo con los procedimientos internos, el concepto técnico de baja es remitido al área administrativa, la cual adelanta el proceso correspondiente. Tratándose de software o licencias, por su naturaleza intangible y al no ser recibidos físicamente en almacén, la baja se materializa mediante el retiro definitivo de los registros correspondientes en las bases de datos administrativas y en los registros contables de la entidad.

Durante la vigencia 2025 se evidenció que la baja de bienes tecnológicos fue aprobada mediante la Resolución DG-000083 del 18 de diciembre de 2025, "Por medio de la cual se ordena el retiro de bienes de las bases de datos y la baja en cuentas contables del Fondo de Prestaciones Económicas, Cesantías y Pensiones – FONCEP y se establece su disposición final". Esta decisión se sustentó en el concepto técnico emitido por la Oficina de Informática y Sistemas y fue presentada ante el Comité Institucional de Gestión y Desempeño, según consta en el Acta No. 6 del 29 de octubre de 2025.

Entre los bienes tecnológicos dados de baja durante la vigencia se encuentran:

- 5 PORTATILES TABLET HP PRO X2 + TECLADO CASE HP PRO X2 CON CONVERTIDOR HDMI + OFFICESTD 2013 OLP NI GOV 021-10271.
- 4 COMPUTADORES PORTATILES
- 1 COMPUTADOR DE ESCRITORIO
- 3 LICENCIAS

6.5 Verificación de las disposiciones vigentes respecto a la política de derechos de autor

La OCI observó que FONCEP cuenta con la política de derechos de autor, la cual se encuentra publicada en la página web de la entidad en el enlace https://www.foncep.gov.co/politica-de-derechos-de-autor, atendiendo a lo establecido en la resolución 1519 de 2020 del MinTic. En dicha política se establecen lineamientos sobre el alcance del uso del sitio web, la autorización para el uso de contenidos y sus limitaciones, la política de datos abiertos, las responsabilidades de los usuarios frente al contenido publicado, las prohibiciones aplicables y el canal dispuesto para notificaciones y reclamaciones por presunta vulneración de derechos de autor.

De otra parte, se procedió a verificar la aplicación de las disposiciones respecto a transferencia de derechos patrimoniales del desarrollo de software teniendo en cuenta lo establecido el numeral 3 de la Directiva Presidencial 02 de 2002 en la cual se indica lo siguiente: "*3. En el evento de que la entidad vaya a detentar la titularidad del derecho de autor sobre tales programas en razón de que los derechos patrimoniales le vayan a ser transferidos ya sea a través de contratos de cesión o transferencia o porque éstos serán desarrollados por servidores públicos a ellas vinculados, en cumplimiento de las funciones de sus cargos, la titularidad de esos derechos deberá constar en el respectivo contrato o manual de funciones*".

Para la verificación, la OCI tomó una muestra no estadística de 10 contratos del año 2025 de los que tienen a su cargo desarrollos de software, mantenimiento de este, o que pueden generar algún tipo de creación o invención de información para las diferentes áreas de la entidad, observando que todos los contratos de la muestra tienen la siguiente cláusula de protección de los derechos de autor y traslado para la propiedad a favor del FONCEP:

> *DERECHOS DE AUTOR Y CONFIDENCIALIDAD: EL (LA) CONTRATISTA será responsable de los conceptos que emita en desarrollo y ejecución del presente contrato, así como de mantener la reserva y confidencialidad de la información que obtenga como consecuencia de las actividades que desarrolle para el cumplimiento del objeto del mismo. De conformidad con las normas de Derechos de Autor, la información y demás documentos que resulten en desarrollo del objeto del presente contrato, gozan de protección legal y serán de propiedad del FONCEP, quien podrá publicarlos, divulgarlos o en cualquier forma usarlos.*

7. EVALUACIÓN DE LOS CONTROLES DE RIESGOS

Revisada la plataforma Suite Visión Empresarial (SVE) y teniendo en cuenta del alcance del presente informe, se evaluaron los controles asociados a los siguientes riesgos:

Tipo de riesgo	Riesgo	Control
Operacional	Recursos tecnológicos gestionados incumpliendo los objetivos del proceso.	Garantizar la definición de los requisitos adecuados.
		Asegurar el adecuado seguimiento a los requerimientos e incidencias de software e infraestructura, pcs y periféricos
		Asegurar la calidad y los tiempos del servicio prestado
		Asegurar la adecuada definición de necesidades y requerimientos
		Asegurar la asignación de los recursos
		Asegurar la gestión del conocimiento
Seguridad de la información	Pérdida de confidencialidad de los activos de información de los procesos de FONCEP.	Asegurar que la gestión de seguridad en la red (antivirus, firewall y demás software que soportan la seguridad) estén instalados, actualizados y funcionen correctamente en todos los equipos y sistemas de la entidad.
		Garantizar que los requerimientos de ajustes y cambios tecnológicos sean aprobados a través del Comité Primario de la Oficina de Informática y Sistemas, para así proceder con su implementación.

Tipo de riesgo	Riesgo	Control
		Verificar la protección contra vulnerabilidades técnicas en la infraestructura tecnológica de la entidad.
		Garantizar el acceso a la información, permisos y accesos a los sistemas de información, documentos y bases de datos únicamente a los colaboradores del área, de acuerdo con sus respectivos roles.
		Garantizar el establecimiento de los lineamientos que aseguren la confidencialidad y no divulgación de la información sensible de los procesos.
Seguridad de la información	Pérdida de disponibilidad de los activos de información de los procesos de FONCEP	Asegurar el correcto funcionamiento de los sistemas, aplicativos o herramientas utilizadas por los procesos.
		Garantizar la implementación del Plan de Recuperación de Desastres Tecnológicos (DRP) y Análisis de Impacto de Negocios (BIA) definido para los sistemas, herramientas y aplicaciones del FONCEP.
		Garantizar la correcta definición de permisos y roles de acceso a los activos de información del proceso el acceso a la información, permisos y accesos a los sistemas de información, documentos y bases de datos únicamente a los colaboradores del área, de acuerdo con sus respectivos roles.
		Validar la adecuada asignación de roles, permisos y accesos a los sistemas de información, documentos y bases de datos de los usuarios de cada dependencia.
		Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad) .
		Verificar la protección contra vulnerabilidades técnicas en la infraestructura tecnológica de la entidad.
		Garantizar la correcta implementación de los procedimientos de Gestión de Backup y Gestión de Bases de Datos y Aplicaciones.
		Garantizar la implementación de los requerimientos de ajustes y cambios tecnológicos.
Seguridad de la información	Perdida de la integridad de los activos de información de los procesos de FONCEP	Validar la adecuada asignación de roles, permisos y accesos a los sistemas de información, documentos y bases de datos de los usuarios de cada dependencia.

Tipo de riesgo	Riesgo	Control
		Garantizar la correcta definición de permisos y roles de acceso a los activos de información del proceso el acceso a la información, permisos y accesos a los sistemas de información, documentos y bases de datos únicamente a los colaboradores del área, de acuerdo con sus respectivos roles.
		Garantizar el cumplimiento de los lineamientos de operación para resguardo, administración y correcta disposición de los activos de la información almacenados en expedientes físicos y digitales.
		Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad) .
		Verificar la protección contra vulnerabilidades técnicas en la infraestructura tecnológica de la entidad.
		Garantizar la correcta implementación de los procedimientos de Gestión de Backup y Gestión de Bases de Datos y Aplicaciones.
		Garantizar la implementación de los requerimientos de ajustes y cambios tecnológicos.

Fuente: Plataforma SVE

En cuanto a los atributos de eficiencia e informativos de los controles, se relaciona lo observado por la OCI:

Atributos	Criterios	Observación OCI
Eficiencia	Tipo: Preventivo, detectivo o correctivo	Se registra que los 26 controles son preventivos
	Implementación: Automático o manual	Todos los controles verificados se ejecutan de forma manual
Informativos	Documentado o sin documentar	Hay 6 controles documentados, y 20 controles se encuentran sin documentar. Teniendo en cuenta que la mayoría de los controles se encuentran sin documentar **se recomienda** adelantar la documentación de los controles de acuerdo con lo establecido en el Manual de gestión de riesgo.
	Frecuencia continua o aleatoria de ejecución	La ejecución de los controles verificados se realiza de forma continua
	Evidencia con registro o sin registro	Se evidenció registros de ejecución en el monitoreo realizado con fecha de corte 15 de enero de 2026 con los soportes de validación correspondientes.

Fuente: SVE

Como resultado de la verificación adelantada en el marco del presente informe, se evidenció debilidad en la efectividad de los controles relacionados con la actualización y funcionamiento

de las herramientas de seguridad en red, en particular los denominados *"Asegurar que la gestión de seguridad en la red (antivirus, firewall y demás software que soportan la seguridad) esté instalada, actualizada y funcione correctamente en todos los equipos y sistemas de la entidad*" y *"Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad)",* asociados a los riesgos de pérdida de confidencialidad, disponibilidad e integridad de los activos de información del FONCEP, según corresponda.

Lo anterior, toda vez que en la revisión efectuada se evidenció que un equipo de cómputo no contaba con antivirus instalado y tres equipos presentaban desactualización del software de protección. Aunque esta situación fue corregida durante la inspección, la condición observada permite concluir que los controles requieren fortalecimiento para garantizar una cobertura efectiva y permanente sobre la totalidad de los equipos de la entidad. En consecuencia, **se recomienda** revisar, ajustar y fortalecer dichos controles, de manera que aseguren la protección continua de los equipos de cómputo durante toda la vigencia.

8. CONCLUSIONES

A partir de la verificación realizada por la Oficina de Control Interno al cumplimiento de las disposiciones de derechos de autor de software, se observó que el sistema de control interno es adecuado, sin embargo, se presentan recomendaciones para la mejora del proceso.

En cumplimiento de las disposiciones vigentes, se realizará el reporte de que trata la circular 027/2023 en la plataforma dispuesta por la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor – www.derechodeautor.gov.co.

La información suministrada por los responsables de proceso y verificada por la OCI en desarrollo del presente informe, permitió cumplir el objetivo y el alcance propuesto.

9. RECOMENDACIONES

- Actualizar y mantener un plan de revisión de placas de identificación de equipos de cómputo y sus periféricos.
- Establecer un plan para garantizar el funcionamiento del total de los equipos biométricos de la entidad.
- Fortalecer las revisiones periódicas sobre los equipos de cómputo que permitan identificar archivos o contenidos ingresados a través de memorias USB, CD u otros medios externos, que puedan resultar contrarios a las políticas de seguridad de la información establecidas por la entidad..
- Programar durante la vigencia 2026 socializaciones o capacitaciones enfocadas a la aplicación de las disposiciones de derechos de autor y propiedad intelectual a todos los colaboradores de FONCEP.

- Fortalecer el control "*Asegurar la actualización y correcto funcionamiento de la seguridad en la red (antivirus, firewall y demás software que soportan la seguridad)"* con el fin de mantener los equipos protegidos con antivirus y complementarios durante los 365 dias del año.
- Adelantar la documentación de los controles de acuerdo con lo establecido en el Manual de gestión de riesgo.

Actividad	Nombre	Cargo	Dependencia	Firma
Revisó y aprobó	Saul Díaz Ladino	Jefe Oficina	Oficina de Control Interno	
Proyectó	Cesar Augusto Franco V	Contratista	Oficina de Control Interno