Control Interno

Distribuido a:

- Diana Patricia Jurado Ramirez
  Gestión de Tecnologías Informáticas y Sistemas de Información

Copias:

- Luis Fernando Gaviria Trujillo.
  Rector.

Emitido por:

- Sandra Yamile Calvo Cataño.
  Director Administrativo Control Interno.

Elaborado por:

- Diego Alejandro García Ceballos.
  Profesional Contratista Control Interno.

Objeto Auditado:

- Software legal 2025.

Áreas Responsable:

- Gestión de Tecnologías Informáticas y Sistemas de Información.

INFORME:

- Software legal 2025.

Informe No. AI-1115-07-2025

Fecha del informe:
20-03-2026

Contenido del informe

Resumen Ejecutivo

Acorde con la información evaluada en el presente ejercicio, se pueden concluir las siguientes fortalezas y debilidades.

Fortalezas

- Controles preventivos para mitigar el riesgo de instalación de software no autorizado o sin licencia, como: Aranda, restricción de privilegios de administrador, control y protección mediante solución de seguridad endpoint, auditorias o controles de software realizadas por GTISI.
- De acuerdo a información de GTISI, no se detectó en la vigencia 2025 software “no Licenciado o ilegal” en equipos de propiedad de la Universidad.
- Procedimiento documentado 135-ASI-15 baja de software.

Debilidades

En el presente informe no se registran observaciones o debilidades; sin embargo, se sugiere realizar las acciones pertinentes frente a las recomendaciones, especialmente las relacionadas con:

- Retomar el control: creación de casos y notificación de soluciones con Mensaje.
- Implementación de lineamientos institucionales sobre el uso de software libre
- Mejora del procedimiento 135-ASI-15 baja de software, respecto a listado y responsabilidades del destino final del software
- Documentar directrices específicas que defina las restricciones sobre la responsabilidad y uso de software no licenciado por parte de los usuarios.

Sandra Yamile Calvo Cataño
Control Interno

Objetivo y Alcance

OBJETIVO

- Evaluar la gestión y controles establecidos por la Universidad frente a la legalidad del software instalado en los equipos, para emitir el informe requerido por la Dirección Nacional de Derechos de Autor - DNDA.

OBJETIVOS ESPECÍFICOS

- Consolidar la información que será reportada a la Dirección Nacional de Derechos de Autor de acuerdo con la Circular Externa No. 027 de 29 de diciembre de 2023 emitida por la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor y en cumplimiento de la Circular No. 04 de 22 de diciembre de 2006.

- Validar los mecanismos de protección del derecho de autor que se utilizan para controlar de manera permanente la instalación de software ilegal.

- Verificar las acciones adelantadas por la Universidad para prevenir el uso no autorizado de programas que no se encuentren debidamente licenciados y el destino final que se le da al software dado de baja en la entidad.

- Verificar las políticas de seguridad informática adoptada y socializada en la Universidad.

- Diligenciar y transmitir oportunamente en la fecha estipulada el informe del software legal en la página web de la Dirección Nacional de Derecho de Autor.

ALCANCE

Licenciamiento de Software, controles para evitar la instalación de software ilegal, a corte al 31 de diciembre de la vigencia 2025.

Riesgos y controles

Los riesgos y controles que se evaluaron son los siguientes:

Tabla 1. Riesgos y controles

RIESGOS		R1	R2	R3
	CALIFICACION RIESGO RESIDUAL	MODERADO	MODERADO	MODERADO
CONTROLES	EFECTIVIDAD	Dar de baja a Software obsoletos o inservibles sin cumplimiento del procedimiento	Instalar sofware no licenciado	No se determina la cantidad de sofware instalado
Procedimiento: 135-ASI-15 baja de software	EFECTIVO	x		
Contraseña o credenciales del usuario administrador - Software de Aranda	EFECTIVO		x	
Network Inventory Advisor	EFECTIVO			x

Fuente: Análisis Control Interno 2026

La matriz anterior muestra la relación entre los riesgos y controles evaluados por Control Interno en el ejercicio de la Auditoría.

Criterios analizados y Metodología empleada

CRITERIOS ANALIZADOS

Los criterios empleados en la auditoría se detallan a continuación:

- Circular Externa No. 027 de 29 de diciembre de 2023 emitida por la Unidad Administrativa Especial Dirección Nacional de Derecho
- Directiva Presidencial No. 02 de 2002
- Circular 12 de 2007 de la Dirección Nacional de Derechos de Autor
- Circular 04 del 22 de diciembre de 2006.

METODOLOGÍA EMPLEADA

La metodología empleada se basó en la aplicación de los siguientes procedimientos de auditoria:

1. **Procedimiento analítico.**
   - Análisis de la información reportada por GTISI en cumplimiento de la solicitud realizada.

2. **Procedimiento de control:**
   - Verificar que las políticas reportadas a través de la información solicitada por la Oficina de control Interno se encuentran vigentes.
   - Verificar la operación y aplicación de los controles reportados por GTISI para la prevención de instalación de software no licenciado.

Muestra:

Se realizó verificación de algunos de los controles en los equipos de la Oficina de Control Interno

Resultados de la evaluación

A continuación, se presentan de forma detallada los resultados del trabajo de evaluación. Cada uno hace referencia a los riesgos y controles evaluados. Cada observación está asociada a un nivel de prioridad de solución (criticidad) cuyo significado es el siguiente:

Tabla 2. Prioridad de las observaciones según el riesgo

Prioridad	**Descripción**
Alta	El hallazgo implica que las debilidades evidenciadas requieren intervenciones o ajustes significativos y deben ser atendidas en el corto plazo
Media	El hallazgo implica que las debilidades evidenciadas requieren intervenciones o ajustes en el mediano plazo.
Baja	El hallazgo implica que las debilidades evidenciadas, requieren intervenciones o ajustes menores.

Fuente: Análisis de Control Interno

5.1. Resultado de los aspectos evaluados.

Gestión de Tecnologías Informáticas y Sistemas de Información[1], mediante memorando 02-135-32 del 12 de marzo de 2026, remitió la información requerida por la Oficina de Control Interno para el desarrollo de la evaluación de la gestión realizada por la Universidad frente a la legalidad del software instalado en los equipos y la actualización de inventarios, así:

5.1.1. Inventario equipos de cómputo.

Al 31 de diciembre de 2025, la Universidad Tecnológica de Pereira, cuenta con un total de 5.062 equipos de cómputo desglosados por: equipos de uso docentes 1.930 (38.13%), administrativo 610 (12.05%), estudiantes 2.522 (49.82%).

Tabla 3. Inventario de equipos de cómputo existentes en la Universidad a corte 31 de diciembre de 2025 discriminado por uso.

Descripción	Cantidad
Equipos uso docentes:	1,930
Equipos uso administrativo:	610
Equipos uso estudiantes:	2,522
TOTAL	5,062

Fuente: GTI&SI

[1] En adelante GTI&SI

5.1.2. Inventario de software.

De acuerdo al inventario de software remitido por GTI&SI, con corte a 31 de diciembre de 2025, se encuentra relacionado un total de 261 productos de software licenciados, así: Desarrollo propio 192 (73.56%) con uso destinado para la administración y 69 software adquirido (26.44%) con uso para administración (48), Investigación (3) y docencia (18).

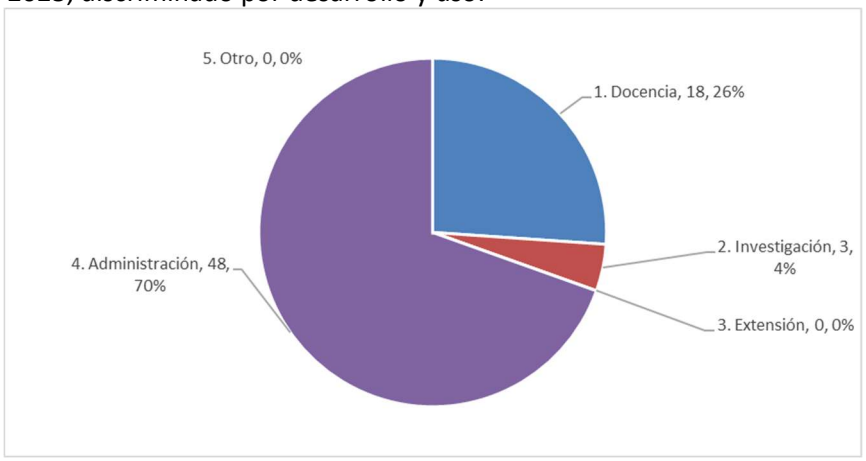
Tabla 4. Inventario de software en la Universidad a corte 31 de diciembre de 2023, discriminado por desarrollo y uso.

Tipo y uso del software	Total
DESARROLLO PROPIO	**192**
Uso Administración	192
DESARROLLO ADQUIRIDO	**69**
Uso Administración	48
Uso Investigación	3
Uso Docencia	18
Otro	0
Total, inventario software licenciado	261

Fuente: GTI&SI. Tabla: Elaboración propia.

La Universidad cuenta con un total de 2926 licencias, 2734 corresponden a desarrollo adquirido y 192 a desarrollo propio.

Gráfica 1. Inventario de software en la Universidad a corte 31 de diciembre de 2025, discriminado por desarrollo y uso.



Fuente: GTI&SI. Gráfico: Elaboración propia.

El inventario de software licenciado presenta un incremento entre las vigencias 2024 y 2025, pasando de 226 a 261 registros, lo que representa un crecimiento del 15,5 %. Este aumento se explica principalmente por el incremento del software adquirido, que pasó de 34 a 69 registros, mientras que el software de desarrollo propio se mantiene estable en 192 registros.

En cuanto a las categorías de uso, el software destinado a procesos administrativos continúa concentrando la mayor participación, aumentando de 192 a 236 registros, mientras que el software utilizado en docencia y en investigación también presenta incrementos.

5.1.3. Políticas sobre el uso y restricción de uso de software licenciado y no licenciado

Las políticas, procedimientos, herramientas y/o mecanismos implementados en la entidad para controlar la instalación de software, están contempladas en las directrices de seguridad la información, las cuales se pueden consultar en:

https://gestioncalidad.utp.edu.co/iso-27001/286/manual-de-directrices/

Las directrices especificas contempladas en el manual son:

- Dispositivos móviles. "*Los dispositivos móviles institucionales deben ser usados exclusivamente para labores institucionales y sistemas operativos y software totalmente licenciado*"
- Protección contra software malicioso: ***"Administración de Servicios Informáticos:*** Es responsable de proveer e instalar las herramientas necesarias como antivirus, antimalware, antispyware y antispam que permitan reducir el riesgo de contagio de software malicioso en los equipos de cómputo, como también de *garantizar que dichas herramientas cuenten con su licencia de funcionamiento* y la disponibilidad de actualización tanto del software como de sus bases de datos."
- Desarrollo seguro de software: *"Todo el software usado en el desarrollo de aplicaciones debe estar licenciado o contar con la debida autorización del proveedor."*

No obstante, las directrices no establecen un apartado especifico en el cual se declare las restricciones sobre la responsabilidad y uso de software No Licenciado en los equipos de cómputo u otros dispositivos institucionales por parte de los usuarios.

La Universidad cuenta con el siguiente marco normativo interno, sobre aspectos de derechos de autor y uso de software:

- Acuerdo del Consejo Superior No. 32 del 6 de junio de 2017, por medio del cual se adopta el Estatuto de Propiedad Intelectual.
- Resolución 5101 del 06 abril de 2020 en la cual se adopta el Manual de Administración, Uso y Control de Bienes Muebles

- Resolución de Rectoría No. 6123 de 05 de diciembre de 2017 por medio de la cual se adopta el manual general de directrices del sistema de gestión de seguridad de la Información.
- Resolución de Rectoría no. 7332 de 21 de noviembre de 2018 por medio de la cual se incorpora al manual de directrices de seguridad de la información de la Universidad, la directriz de uso de la red de datos institucional.

GTISI aclara que la Universidad no cuenta con políticas, lineamientos o directrices sobre uso de software Libre.

5.1.4. Medidas o controles preventivos automatizados establecidos para evitar el uso de software ilegal y prevenir que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva.

Conforme a lo informado por GTISI, se mantiene operativo el software de Aranda que permite controlar la instalación de software, Además, indican los siguientes aspectos de control:

- Gestión de privilegios locales: Se mantiene control sobre las cuentas con privilegios de administrador local en la mayoría de los equipos institucionales, con el fin de limitar la instalación de software por parte de usuarios finales.

- Políticas de restricción a nivel de dominio: Se aplican políticas de seguridad y restricción de software (GPO) en el dominio asigtisi.utp.edu.co, orientadas a impedir que los usuarios instalen aplicaciones sin la autorización previa del área de Administración de Servicios Informáticos.

- Control y protección mediante solución de seguridad endpoint: Se implementan controles a través de la solución Kaspersky Endpoint Security, que permite la detección, bloqueo y control de software potencialmente malicioso o no autorizado, fortaleciendo la protección de los equipos institucionales.

- Se realizaron 500 mantenimientos preventivos donde se revisa que los equipos tengan instalados software licenciado según contrato 5879-2025.

- Inventario de software a través del Network Inventory Advisor quien determina la cantidad de software instalados.

- Auditorias o controles de software realizadas por Gestión de Tecnologías Informáticas y Sistemas de Información.

- Creación de casos y notificación de soluciones a un requerimiento en la parte de observaciones se tiene el siguiente mensaje: "Tenga en cuenta que en los computadores no se debe instalar software ilegal o no autorizado por la Universidad.

5.1.5 Controles establecidos para la baja de Software

La Universidad a través de GTISI tiene documentado en el sistema integral de calidad el procedimiento 135-ASI-15 Baja de Software, el cual se encuentra publicado en el siguiente link: https://app4.utp.edu.co/calidad_bibi/ver/?iddoc=43142&tipo=10606 , este procedimiento tiene por objetivo "Dar de baja a Software obsoletos o inservibles" este procedimiento establece que GTISI emite un concepto técnico para verificar la obsolescencia técnica y tecnológica" En caso de dar de baja un software se remite a Gestión Contable la información.

De otra parte, GTISI informa que:

- Cada responsable del software determina la baja de los mismos y su destino final.
- Para la vigencia 2025 no hay un listado de baja software (En el procedimiento se determina el formato consolidado de software o licencias a dar de baja).

5.1.6 Información sobre detección No licenciado por parte de GTISI

De acuerdo con lo informado por GTSI mediante el memorando No. 02-135-32 del 12 de marzo de 2026, y conforme a lo evidenciado en el Anexo denominado "4.+Informe+de+Software+Legal+2025.xls", específicamente en el numeral 13. "Medidas correctivas en caso de instalación de software no licenciado o ilegal en equipos de la Universidad", dicha área manifiesta no tener conocimiento, ni haber detectado la instalación de software no licenciado o ilegal en los equipos de propiedad institucional.

De igual manera informa que si se detectara por parte de GTISI este tipo de software, procedería a indicar al usuario sobre la importancia de no hacerlo y realizaría la solicitud de desinstalación inmediata del software. Agrega que, pasado un tiempo vuelve a revisar y si reincide el usuario, se reporta a la Oficina de Control Interno Disciplinario para lo de su competencia.

5.2 Evaluación de efectividad de las medidas o controles preventivos

Se presenta los resultados de la prueba realizada el 17-03-2026 de la evaluación de efectividad de los controles implementados para prevenir la instalación de programas o aplicaciones sin la licencia correspondiente y así evitar el uso de software ilegal.

a. Software Aranda:

Prueba realizada: Se verifica en los PC de la Oficina de Control Interno el día 17/03/2026 dando como resultado la siguiente tabla:

Tabla 5. Prueba de instalación de software

Equipo	Software de prueba	Resultado	Cumplimiento
326226	Python	Solicita permiso de soporte técnico	Efectivo

Equipo	Software de prueba	Resultado	Cumplimiento
326226	ChatGPT	Se deja instalar, el software es libre	Conforme a lo que indica GTISI mediante correo remitido el 17 de marzo de 2026, remitido por raton@utp.edu.co: ¨…es importante aclarar que no todo el software que se ejecuta en Windows requiere una instalación con privilegios de administrador. Las políticas de seguridad establecidas en los equipos de la Universidad impiden que los usuarios estándar realicen instalaciones que modifiquen el sistema operativo (archivos del sistema, registro, servicios, etc.)…. En estos casos, Windows permite su ejecución sin solicitar credenciales de administrador. Específicamente: ChatGPT se utiliza como aplicación web o como aplicación de usuario, sin realizar modificaciones al sistema operativo. ¨
333896	Spotify	Se deja instalar, el software es libre	Conforme a lo que indica GTISI mediante correo remitido el 17 de marzo de 2026, remitido por raton@utp.edu.co: ¨…es importante aclarar que no todo el software que se ejecuta en Windows requiere una instalación con privilegios de administrador. Las políticas de seguridad establecidas en los equipos de la Universidad impiden que los usuarios estándar realicen instalaciones que modifiquen el sistema operativo (archivos del sistema, registro, servicios, etc.)…. En estos casos, Windows permite su ejecución sin solicitar credenciales de administrador. Específicamente: Spotify es una aplicación incluida o distribuida a través de componentes integrados de Windows, que solo requiere activación para su uso.
333896	Acrobat	Solicita permiso de soporte técnico	Efectivo
333983	Certitool	Solicita permiso de soporte técnico	Efectivo
334007	GameLoop	Solicita permiso de soporte técnico	Efectivo
333991	TeamViewer	Solicita permiso de soporte técnico	Efectivo
333859	Acrobat	Solicita permiso de soporte técnico	Efectivo

Fuente: Pruebas realizadas por Control Interno

El aplicativo Aranda para restricción de instalación de software que requiere licencia funcionó como se esperaba, requiriendo la autorización de un administrador para proceder con la instalación. Esto

valida la configuración de seguridad del sistema operativo y su contribución al control general. Salvo para dos aplicaciones que son gratuitas.

b. Gestión de privilegios locales

Prueba realizada: Se intenta ingresar con el usuario de Soporte Técnico al PC 326226, lo anterior dado como resultado que esta restringido el acceso a dicho usuario.

Cuando un usuario con privilegios estándar intenta acceder al sistema operativo utilizando credenciales de administrador o soporte técnico, el sistema requiere la autenticación mediante contraseña. Si la contraseña ingresada no es válida, el sistema deniega el acceso; además no permite el restablecimiento de la misma.

IMAGEN 1.VERIFICACIÓN CONTROL DE ACCESO USUARIO SOPORTE TÉCNICO

Imagen tomada el 17/03/2026 – PC 333891

c. Control y protección mediante solución de seguridad endpoint:

Se verifica la instalación en los equipos de la Oficina de Control Interno de la solución Kaspersky Endpoint Security.

IMAGEN 2.VERIFICACIÓN DE KASPERSKY ENDPOINT SECURITY EQUIPO 333891

Imagen tomada el 17/03/2026 – PC 333891

d. Auditorias o controles de software realizadas por Gestión de Tecnologías Informáticas y Sistemas de Información

Se evidencia reporte en el Excel donde se indica fecha de realización de la auditoria, nombre de programa, cantidad y equipo.

Archivo excel: Auditoria+de+software+Octubre+16+2025+por+titulo+de+sw

e. Mantenimientos preventivos

Se evidencia el contrato de prestación de servicios No. 5879 DE 2025 suscrito con DESARROLLO ORGANIZACIONAL LÓGICO FUNCIONAL AVANZADO S.A.S.
Objeto: Prestación de servicios para realizar el mantenimiento preventivo- predictivo a 500 equipos de cómputo y 50 impresoras de tipos 2,3 o 4 de la UTP…
Fecha suscripción: 07/05/2025
Duración: término de 4 meses

f. Inventario de software a través del Network Inventory Advisor

El control no fue probado.

g. Creación de casos y notificación de soluciones con Mensaje

No se evidencia el mensaje "Tenga en cuenta que en los computadores no se debe instalar software ilegal o no autorizado por la Universidad." en la creación de casos y notificación de soluciones a un requerimiento en la parte de observaciones.

De acuerdo a lo informado por GTISI, mediante correo remitido el 18 de marzo de 2026, remitido por raton@utp.edu.co: "*Con respecto a su solicitud, informamos que la plantilla de notificación de Aranda fue ajustada como parte del proceso de implementación del portal Aranda Web, como acción de mejora de la mesa de ayuda, mediante el cual los usuarios pueden registrar solicitudes de soporte, consultar el estado de sus casos y acceder a guías de autoayuda.*
Como resultado de este ajuste, de manera inadvertida el mensaje referente a la prohibición de instalación de software ilegal o no autorizado dejó de mostrarse en los correos de notificación.
Esta situación ya fue corregida y actualmente la plantilla vuelve a incluir el mensaje en el cuerpo del correo que reciben los usuarios con la solución de su solicitud de servicio...".

5.3 Seguimiento plan de mejoramiento

En seguimiento del Plan de Mejoramiento Software Legal 2024 Informe No. AI-1115-01-48, Gestión de Tecnologías Informáticas y Sistemas de Información, mediante memorando 02-135-58 del 6 de mayo de 2025, informa lo siguiente:

"Dando respuesta al memorando 02-1115-201 me permite informar que esta oficina no presentará un plan de mejoramiento en relación con las recomendaciones contenidas en el informe final de la

Auditoría de Software Vigencia Legal 2024. Lo anterior, teniendo en cuenta que la información correspondiente ya fue incluida en el Plan de Mejoramiento de la vigencia 2024 y según las anotaciones realizadas por Control Interno, se evidencia el cumplimiento de la totalidad de las acciones previstas en dicho informar."

Aunque GTISI no planteó acciones de mejoramiento respecto a las recomendaciones dadas en el informe No. AI-1115-01-48, Control Interno, presenta en la siguiente tabla una evaluación, sobre las recomendaciones realizadas, respecto a implementación o mantenimiento de los controles planteados.

Tabla 6. Seguimiento plan de mejoramiento Informe No. AI-1115-01-48

No.	OBSERVACIÓN DE AUDITORÍA	ACCION DE MEJORA DEFINITIVA	FECHA DE CUMPLIMIENTO	ACLARACIONES	ESTADO DE LA ACCION DE MEJORA DEFINITIVA AL 18.03.2026
1	Recomendaciones Generales 1: Realizar auditoría de software en la vigencia 2025.	NA	NA	GTISI indica Mediante memorando 02-135-58 del 6 de mayo de 2025 que no implementará Plan de Mejora.	Se evidencia soporte de auditoría realizada por GTISI
2	Recomendaciones Generales 2: Capacitar periódicamente a los usuarios sobre las políticas de seguridad y los riesgos asociados con la instalación de software no autorizado.	NA	NA	GTISI indica Mediante memorando 02-135-58 del 6 de mayo de 2025 que no implementará Plan de Mejora.	No se evalúa dado que no se validó, ni solicito evidencia respecto a temas de capacitación en la auditoría
3	Recomendaciones Generales 4: Revisar y actualizar periódicamente las políticas de seguridad relacionadas con la instalación de software con el propósito de asegurar que se ajusten a las necesidades y riesgos actuales.	NA	NA	GTISI indica Mediante memorando 02-135-58 del 6 de mayo de 2025 que no implementará Plan de Mejora.	No se evidencia la implementación de la recomendación, puesto que las directrices y la normatividad no presentan cambios
4	Recomendaciones Generales 5: Construir un normograma que contenga las normas externas, como leyes, decretos, acuerdos, circulares, resoluciones que afectan la gestión de la entidad sobre el tema de software legal, y las normas internas, como resoluciones, acuerdos, directrices manuales y, en general, todos los actos administrativos relacionados con software legal y que permita	NA	NA	GTISI indica Mediante memorando 02-135-58 del 6 de mayo de 2025 que no implementará Plan de Mejora.	No se evidencia la implementación de la recomendación, puesto que no se tiene un documento que compile la normatividad relacionada, lo que ocasiona que en los reporte se citen normas derogadas

No.	OBSERVACIÓN DE AUDITORÍA	ACCION DE MEJORA DEFINITIVA	FECHA DE CUMPLIMIENTO	ACLARACIONES	ESTADO DE LA ACCION DE MEJORA DEFINITIVA AL 18.03.2026
	conocer la vigencia y aplicabilidad a la Universidad.				
5	Recomendaciones Generales 6: Continuar con la ejecución de acciones para incorporar en base de datos todos los equipos de cómputo, software adquirido y desarrollado en la Universidad."	NA	NA	GTISI indica Mediante memorando 02-135-58 del 6 de mayo de 2025 que no implementará Plan de Mejora.	Se evidencia controles frente a los equipos y software instalados en equipos de la Universidad

Fuente: Construcción Propia

5.4 Concepto General

Con base en la verificación realizada para la vigencia 2025, se evidencia que la institución cuenta con controles preventivos para mitigar el riesgo de instalación de software no autorizado o sin licencia, destacándose herramientas como Aranda, la restricción de privilegios de administrador, control y protección mediante solución de seguridad endpoint, auditorias o controles de software realizadas por GTISI, lo que contribuye a un control adecuado sobre la instalación de aplicaciones, sin embargo el control Inventario de software a través del Network Inventory Advisor, no fue posible su validación y el control creación de casos y notificación de soluciones con Mensaje, para la presente vigencia no fue aplicado.

De otra parte, se identifican oportunidades de mejora relacionadas con la ausencia de lineamientos institucionales sobre el uso de software libre, la implementación de un listado consolidado de software dado de baja, y el hecho de que las directrices existentes no establecen un apartado específico que defina las restricciones sobre la responsabilidad y uso de software no licenciado por parte de los usuarios en equipos de cómputo u otros dispositivos institucionales.

5.5. Publicación de informe software legal

5.5.1 Reporte del registro de informe de software legal en la Dirección Nacional de Derecho de Autor (DNDA)

En el link: https://controlinterno.utp.edu.co/informes-de-evaluacion-y-seguimiento/135/software/ se evidencia el recibo a satisfacción del registro de informe de Software Legal por parte de la Dirección Nacional de Derecho de Autor (DNDA) sobre la vigencia 2025.

5.5.2 Link de la publicación en su entidad del Informe de Software en los términos de la Circular 04 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en materia de Control Interno.

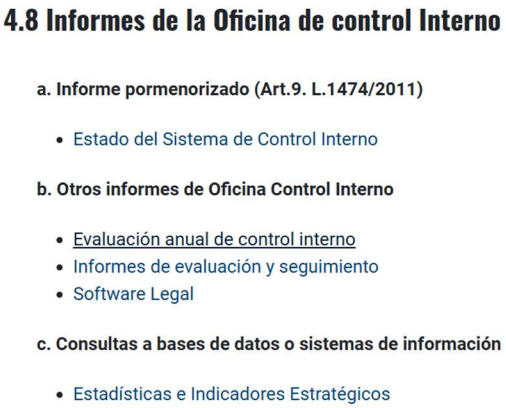
La Oficina de Control Interno, siguiendo la función de evaluador independiente y atendiendo los requisitos normativos, verifica, consolida y publica los certificados anuales de reporte de software

legal en la página web institucional referenciada a través del siguiente link: https://controlinterno.utp.edu.co/informes-de-evaluacion-y-seguimiento/135/software/ .

5.5.3 Página de transparencia y acceso a la información pública

Así mismo, el informe de software legal de encuentra publicado en la página de transparencia y acceso a la información pública en el ítem 4.8 Informes de la Oficina de Control Interno; link: https://atencionalciudadano.utp.edu.co/transparencia-y-acceso-a-informacion-publica/

IMAGEN 3. PANTALLAZO MICROSITIO TRANSPARENCIA Y ACCESO A LA INFORMACIÓN



Fuente: https://atencionalciudadano.utp.edu.co/transparencia-y-acceso-a-informacion-publica/
Fecha de consulta: 18-03-2025

Recomendaciones

Recomendaciones generales:

1. Formalizar lineamientos institucionales sobre el uso de software libre, definiendo criterios de uso, validación, autorización y control, con el fin de mitigar riesgos asociados a seguridad, legalidad y compatibilidad tecnológica.

2. Establecer y mantener un registro consolidado de software dado de baja, conforme a lo definido en los procedimientos institucionales (135-ASI-15 Baja de Software), que permita garantizar la trazabilidad del ciclo de vida del software y la adecuada disposición final. Así mismo, documentar en el procedimiento, conforme a lo reportado por GTISI, quien tiene la autoridad y responsabilidad frente la determinación del destino final que se le da al software dado de baja.

3. Incorporar en las directrices institucionales un apartado específico sobre la responsabilidad de los usuarios frente a la instalación y uso de software no licenciado, incluyendo restricciones, obligaciones y posibles consecuencias, con el fin de fortalecer la cultura de legalidad y el control preventivo, de manera que respondan a los riesgos actuales y a la evolución del entorno tecnológico institucional

4. Verificar periódicamente la correspondencia entre el software instalado y las licencias adquiridas, mediante cruces entre herramientas de inventario, registros contractuales y reportes institucionales.

5. Generar estrategias periódicas de sensibilización dirigida a los usuarios sobre el uso adecuado del software, los riesgos asociados al uso de software no autorizado y no licenciado y las responsabilidades institucionales frente al cumplimiento normativo.

6. Construir y mantener actualizado un normograma sobre software legal, que integre la normativa externa e interna aplicable, facilitando su trazabilidad, vigencia, consulta y aplicación.

Limitaciones

Durante el desarrollo de este proceso no se presentaron limitaciones.

Plan de mejoramiento

De acuerdo a la observación establecida en el presente informe por Control Interno, recomendamos que se implementen las acciones de mejoramiento a que haya lugar.

El plan de mejoramiento deberá ser presentado por el auditado en el formato Plan de Mejoramiento (1115-F03-01) quince (15) días hábiles después de la entrega del informe de evaluación y en él se deberá acordar los seguimientos acerca de las acciones implementadas que permitirán evidenciar la mejora en los puntos evaluados y que presentaron debilidades.

Es así, que el Plan de Mejoramiento presentado será parte integral del presente informe.

Fecha de presentación del Plan de Mejoramiento - 1115-F03-01:

_____ _____ _____
DD / MM / AA

Responsable del Plan de Mejoramiento 1115-F03-01:

Responsable del Seguimiento de Plan de Mejoramiento 1115-F03-01:
Oficina de Control Interno

Firmado digitalmente por Sandra Yamile Calvo Cataño
Fecha: 2026.03.20 09:48:25 -05'00'

SANDRA YAMILE CALVO CATAÑO
Director Administrativo Control Interno.
Universidad Tecnológica de Pereira

Diego Alejandro Garcia Digitally signed by Diego Alejandro Garcia
Date: 2026.03.20 09:30:59 -05'00'

Elaboró: Diego Alejandro García Ceballos.
Profesional Contratista Control Interno.

ANEXO No. 1. Confirmación presentación de informe software legal vigencia 2025

CONFIRMACIÓN PRESENTACIÓN INFORME SOFTWARE LEGAL VIGENCIA 2025

Respetado(a) Usuario(a):
SANDRA YAMILE CALVO CATAÑO
UNIVERSIDAD TECNOLÓGICA DE PEREIRA
Pereira (Risaralda)

Le informamos que luego de verificar en nuestros archivos, se encontró que efectivamente el 20-03-2026 usted remitió ante la Dirección Nacional de Derecho de Autor, con éxito el informe de software legal, con los siguientes datos:

Orden	Nacional
Sector	Educación
Departamento	Risaralda
Municipio	Pereira
Entidad	UNIVERSIDAD TECNOLÓGICA DE PEREIRA
Nit	891480035-9
Nombre funcionario	SANDRA YAMILE CALVO CATAÑO
Dependencia	OFICINA DE CONTROL INTERNO
Cargo	DIRECTOR ADMINISTRATIVO
1.Con cuantos equipos cuenta la entidad	5062
2. El software se encuentra debidamente licenciado?	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?	Información remitida por GTISI mediante memorando No. 02-135-32 de 2025: 1. Software de Aranda que permite controlar la instalación de software, Además, indican los siguientes aspectos de control: 2. Gestión de privilegios locales: Se mantiene control sobre las cuentas con privilegios de administrador local en la mayoría de los equipos institucionales, con el fin de limitar la instalación de software por parte de usuarios finales. 3. Políticas de restricción a nivel de dominio: Se aplican políticas de seguridad y restricción de software (GPO) en el dominio asigtisi.utp.edu.co, orientadas a impedir que los usuarios instalen aplicaciones sin la autorización previa del área de Administración de Servicios Informáticos. 4. Control y protección mediante solución de seguridad endpoint: Se implementan controles a través de la solución Kaspersky Endpoint Security, que permite la detección, bloqueo y control de software potencialmente malicioso o no autorizado, fortaleciendo la protección de los equipos institucionales. 5. Inventario de software a través del Network Inventory Advisor quien determina la cantidad de software instalados. 6. Auditorias o controles de software realizadas por Gestión de Tecnologías Informáticas y Sistemas de Información. 7. Se realizaron 500 mantenimientos preventivos donde se revisa que los equipos tengan instalados software licenciado según contrato 5879-2025. -- Normas reguladoras internas: ● Acuerdo del Consejo Superior No. 32 del 6 de junio de 2017, por medio del cual se adopta el Estatuto de Propiedad Intelectual. ● Resolución 5101 del 06 abril de 2020 en la cual se adopta el Manual de Administración, Uso y Control de Bienes Muebles ● Resolución de Rectoría No. 6123 de 05 de diciembre de 2017 por medio de la cual se adopta el manual general de directrices del sistema de gestión de seguridad de la Información. ● Resolución de Rectoría no. 7332 de 21 de noviembre de 2018 por medio de la cual se incorpora al manual de directrices de seguridad de la información de la Universidad, la directriz de uso de la red de datos institucional.
4. ¿Cuál es el destino final que se le da al software dado de baja en su entidad?	Cada responsable del software determina la baja de los mismos y su destino final de acuerdo a lo establecido en el procedimiento 135-ASI-15 Baja de Software, siendo su disposición final la eliminación. (Información remitida por GTISI mediante memorando No. 02-135-32 de 2025)

Ingrese el Link de la publicación en su entidad del Informe de Software en los términos de la Circular 04 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en materia de Control Interno	https://controlinterno.utp.edu.co/informes-de-evaluacion-y-seguimiento/135/software/

Cualquier otra inquietud estaremos atentos a responderla a través del número telefónico +57 (601) 7868220 ext. 1114, o al correo electrónico info@derechodeautor.gov.co

Se ha enviado una copia al correo registrado: controlinterno@utp.edu.co