UNIDAD DE BÚSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS EN EL CONTEXTO Y EN RAZÓN DEL CONFLICTO ARMADO UBPD

INFORME DE SEGUIMIENTO AL CUMPLIMIENTO DE NORMAS DE DERECHOS DE AUTOR Y USO DE SOFTWARE LEGAL – VIGENCIA 2025

BOGOTÁ, D.C. 20 de marzo de 2026

Enlace a la página Web de la UBPD

Dirección de correo electrónico a Servicio al Ciudadano de la UBPD

TABLA DE CONTENIDO

Tabla 1 - Información General del Seguimiento

Tipo de Informe:	Seguimiento de Ley
Título del Informe:	Seguimiento al cumplimiento de normas de derechos de autor y uso de software legal
Fecha	20 de marzo de 2026

1. OBJETIVO

Verificar el estado de licenciamiento del software instalado en los equipos de cómputo que se encuentran puestos al servicio de la Unidad, los controles de seguridad implementados para evitar la instalación de software ilegal, el destino final tecnológico y administrativo dado al software dado de baja en la Unidad y realizar la correlación del Directorio Activo de la Entidad con los directorios existentes de los Servidores Públicos y Contratistas que laboran y prestan servicios en la Unidad de Búsqueda de Personas dadas por Desaparecidas UBPD.

2. ALCANCE

El alcance de la información de los equipos de cómputo y licencias de software en servicio corresponde a la vigencia fiscal 2025, tal como lo señala la circular No. 017 de junio 1 de 2011 de la Dirección Nacional de Derechos de Autor DNDA.

3. MARCO LEGAL

- **Artículo 61 de la Constitución Política de Colombia y Leyes 23 de 1982 y 44 de 1993:** En las cuales se establece que el derecho de autor es una propiedad especial.
- **Directivas Presidenciales No 001 del 25 de febrero de 1999 y No 002 del 12 de febrero de 2002:** Se dan instrucciones a los encargados de cada entidad u organismos públicos de la adquisición de software, para que los programas de computador adquiridos estén respaldados por los respectivos documentos de licenciamiento o transferencia de propiedad.
- **Circular No. 04 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en Materia de Control Interno de las Entidades del Orden Nacional y Territorial:** solicita a los Representantes Legales y Jefes de las Oficinas de Control Interno de las entidades u organismos públicos del orden nacional y territorial, la información relacionada con la “Verificación,

recomendaciones y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre Software.

- **Circular No. 012 del 02 de febrero de 2007 expedida por la Unidad Administrativa Especial, Dirección Nacional de Derechos de Autor:** En la cual se realizan recomendaciones
- **Circular 017 del 01 de junio de 2011:** Modifica Circular 12 del 2 de febrero de 2007, sobre recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software).
- **Decreto 648 del 19 de abril de 2017:** por el cual se modifica y adiciona el Decreto 1083 del 26 de mayo de 2015 Reglamentario Único del Sector de la Función Pública Artículo 2.2.21.4.9 Informe Literal f. De Derechos de autor software.
- **Circular 07 del 28 de diciembre de 2005 del Consejo Asesor del Gobierno Nacional en materia de control interno:** Verificación Cumplimiento Normas Uso de Software. verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software. Informe suscrito por el jefe de control interno y remitido por el Representante Legal a la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor.

4. METODOLOGIA

El 06 de febrero de 2026 mediante correo electrónico, se solicitó al Grupo de Interno de Trabajo de Gestión Tecnológica GITGT dar respuesta a las 4 preguntas requeridas por la Dirección Nacional de Derechos de Autor DNDA, así: "*¿Con cuántos equipos cuenta la entidad?, ¿El software instalado en estos equipos se encuentra debidamente licenciado?, ¿Qué mecanismos de control se ha implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?, ¿Cuál es el destino final que se da al software dado de baja en su Entidad?"*, adicionalmente se solicitó hacer entrega de información relacionada con los inventarios de equipos de cómputo, de licenciamiento instalado, consulta nominal del directorio activo, del estado de registro de los sistemas informáticos propios ante la Dirección Nacional de Derechos de Autor DNDA.

Finalmente, la OACI realizó revisiones y cruces de información entre los soportes de evidencia entregados el 03 de marzo de 2026 por el proceso y efectuó inspecciones físicas de una muestra de 20 equipos de cómputo, con el fin de verificar software, licencias instaladas y controles de seguridad aplicados.

5. RESULTADOS DEL SEGUIMIENTO

5.1. Respuestas para la Dirección Nacional de Derechos de Autor DNDA:

5.1.1. ¿Con cuántos equipos cuenta la entidad?
Respuesta Grupo Interno de Trabajo de Gestión Tecnológica: 882 equipos, distribuidos así por nivel de propiedad:

- Propios: 880
- En Arrendamiento: 2

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

- Respuesta Grupo Interno de Trabajo de Gestión Tecnológica:
  "…Si. El software adquirido por la UBPD y que se encuentra instalado en los equipos propios y arrendados, se encuentra debidamente licenciado. Con lo anterior, las modalidades de licenciamiento utilizado por la Unidad se relacionan a continuación:
  1. Software con licenciamiento de tipo "libre", "fuente abierta", "de dominio público", o que no requiere licenciamiento para su uso. Es posible su instalación y uso, siempre y cuando, exista un requerimiento debidamente formalizado y soportado, de acuerdo con los canales de comunicación internos; la viabilidad soportada en el análisis del tipo de licencia asociado a lo requerido, y que sea aprobado por el grupo de seguridad digital; si aprueba los filtros anteriormente indicados, se procede a actualizar el listado de software permitido en la UBPD (lista blanca) y se procede con la instalación controlada del mismo, la cual, solo la puede realizar la OTIC a través de la Mesa de Servicio.
  Es importante destacar que el procedimiento queda debidamente documentado en la herramienta de gestión de solicitudes (Aranda), en el marco de la prestación del servicio por parte de la Mesa de Servicio, garantizando trazabilidad, control y alineación con las mejores prácticas de ITIL.
  2. El Software que requiere licenciamiento pago o suscripción para su uso, es adquirido obedeciendo a la proyección de necesidades tecnológicas consolidadas por la OTIC y que se registra en el Plan Anual de Adquisiciones. Una vez es adquirido el licenciamiento del software, la asignación e instalación se realiza por medio de la mesa de servicio…" (Sic)

- **Verificación Oficina Asesora de Control Interno:**

Se seleccionó una muestra de 30 equipos de cómputo según el inventario entregado por el Grupo Interno de Trabajo de Gestión Tecnológica. Con el apoyo del servicio de Mesa de Ayuda y a través del agente del software Aranda, se consultaron en la herramienta de administración los nombres y seriales con el fin de obtener el inventario de software instalado, una vez agotado este proceso de verificación, se confirmó que el software instalado en la totalidad de la muestra cumple estrictamente con la normativa de la Unidad.

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

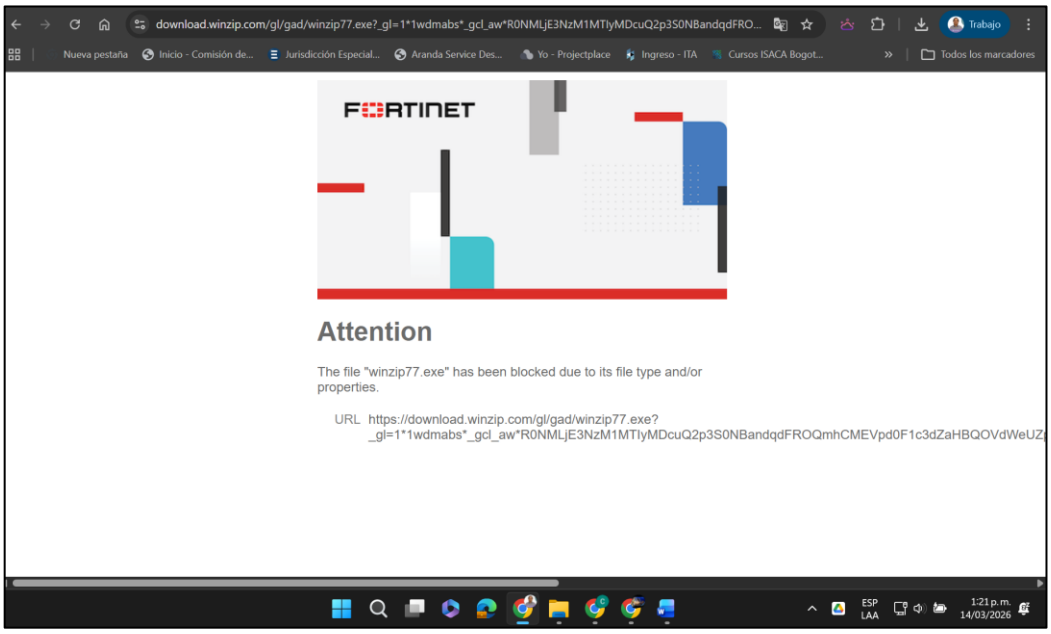
- Respuesta del Grupo Interno de Trabajo de Gestión Tecnológica:
  "…Actualmente, con la implementación de FortiEDR, el control ha evolucionado hacia un enfoque más avanzado y dinámico, propio de una solución XDR (Extended Detection and Response). En lugar de basarse únicamente en la licencia o en listas estáticas, FortiEDR realiza un análisis continuo del comportamiento de las aplicaciones en tiempo real. Si detecta un comportamiento malicioso o anómalo, bloquea automáticamente la aplicación para proteger el sistema.
  Este enfoque permite una detección y respuesta mucho más efectiva ante amenazas nuevas o desconocidas, ya que no depende únicamente de firmas o listas predefinidas, sino que evalúa cómo se comporta el software en el entorno. En caso de que se presente un falso positivo, FortiEDR facilita la revisión y el análisis para permitir la creación de excepciones, asegurando un equilibrio entre seguridad y operatividad.
  Se tiene implementada una política de seguridad en el firewall orientada a restringir y bloquear la descarga de software o aplicaciones no autorizadas en todos los equipos asignados a los usuarios. Esta política actúa como una primera línea de defensa, impidiendo que se realicen descargas que puedan comprometer la seguridad del sistema o facilitar la instalación de software no aprobado, lo cual reduce significativamente el riesgo de infecciones por malware y vulnerabilidades asociadas a programas no verificados.
  Dentro de esta estrategia de control, se han configurado perfiles de navegación web que incorporan un file filter específico para la categoría de "descargas de software". Este filtro bloquea el acceso a sitios web que ofrecen software no autorizado, garantizando que los usuarios no puedan obtener aplicaciones fuera del marco permitido. De esta manera, se asegura que el entorno de trabajo se mantenga protegido contra la instalación o ejecución de software potencialmente dañino o no autorizado.

Con la integración de estas medidas, que combinan el control en el firewall con la gestión de perfiles de navegación y filtros de archivos, se refuerzan las políticas de seguridad organizacional. Esto permite un control integral sobre la descarga e instalación de software, minimizando los riesgos derivados del uso inapropiado de recursos en línea y fortaleciendo la postura de seguridad frente a amenazas internas y externas.
Adicionalmente, se tiene configurado en el Directorio Activo, una política que restringe los usuarios la posibilidad de realizar y/o ejecutar un archivo ejecutable y su respectiva instalación…"

- **Verificación Oficina Asesora de Control Interno:**

La prueba se hizo sobre los 7 equipos de cómputo (6 portátiles y un equipo de escritorio) asignados a Servidores y Contratistas de la Oficina Asesora de Control Interno, verificando si el usuario de red logueado en el equipo contaba con permisos para la descarga e instalación de software, obteniendo los siguientes resultados:

Al ingresar sitio web oficial de proveedores directos de software, como es el caso del compresor de archivos WinZip y al intentar acceder a la descarga gratuita, se muestra una pantalla de bloqueo de descarga del ejecutable, tal como se muestra a continuación:



Fuente: página web del proveedor del software WinZip

Enlace a la página Web de la UBPD

Dirección de correo electrónico a Servicio al Ciudadano de la UBPD

Por otro lado, al intentar descargar software desde paginas no oficiales de descarga, si bien se puede ingresar a estas páginas Web, la descarga también se encuentra bloqueada.

5.1.4. ¿Cuál es el destino final que le da al software dado de baja en su Entidad?

- Respuesta del Grupo Interno de Trabajo de Gestión Tecnológica:

"…con corte al 31 de diciembre de 2025, no se registraron bajas asociadas a software desarrollado por la entidad ni a software con registro de propiedad intelectual a nombre de la UBPD.

No obstante, durante la vigencia 2025 sí se realizaron bajas correspondientes a software comercial adquirido bajo esquemas de licenciamiento tradicional, las cuales obedecen principalmente a procesos de finalización de vigencia, renovación o reemplazo de licencias de uso instaladas en los equipos institucionales, por el mismo tipo de software, pero licenciado por servicios o suscripción, lo cual no implica desinstalación física del software.

Además, se precisa que la entidad también hace uso de herramientas tecnológicas bajo modalidades de servicio o suscripción, las cuales operan mediante esquemas de consumo de servicio y no mediante licenciamiento instalado. En estos casos, al finalizar o renovar el contrato correspondiente, el acceso a la plataforma se desactiva desde el proveedor, sin que implique procesos de baja física del software.

En este contexto, los roles y perfiles de usuario asociados a dichas plataformas no presentan afectación ni pérdida de información, dado que su gestión se realiza a través de servicios tecnológicos administrados y no mediante activación de licencias individuales instaladas en los equipos.

En consecuencia, para la pregunta relacionada con el destino final del software dado de baja, para los casos de software comercial, se actualiza con la renovación de los servicios o se desinstala físicamente en el caso que la entidad no siga utilizando este software bajo otra modalidad de licenciamiento o suscripción. Para el caso del software institucional o desarrollado por la Entidad, considerando que no se efectuaron procesos de baja sobre este tipo de activos durante la vigencia reportada, estos siguen funcionando en los equipos de cómputo de la UBPD…" (Sic)

Enlace a la página Web de la UBPD

Dirección de correo electrónico a Servicio al Ciudadano de la UBPD

- **Verificación Oficina Asesora de Control Interno:**

Al verificar la documentación del proceso en el repositorio del Sistema Integrado de Gestión SIG y/o del Modelo de Operación por Procesos MOP, se observaron documentos relacionados al proceso de baja técnica como lo son:

- Catálogo de Sistemas de Información (GTI-FT-042): Este formato incluye un campo específico para la "Fecha de Inactivación" de los sistemas de información, lo que sugiere un proceso formal para el retiro o baja de un sistema/software.

- Acta de Cierre de Proyecto (GTI-FT-014): Este documento se utiliza para formalizar la finalización de un proyecto. En el contexto de software, un "Cierre de Proyecto" podría ser el paso final para dar de baja un sistema que ha sido desarrollado o implementado.

- Documentos de Borrado Seguro: Estos documentos están relacionados con la eliminación segura de información, que es un paso crucial en el proceso de baja de software o sistemas para asegurar que no queden datos sensibles:
  a) Guía Borrado Seguro (GTI-GU-004)
  b) Solicitud de Borrado Seguro (GTI-FT-031)

Sin embargo, no existe una guía o un documento que establezca de inicio a fin cuales son las actividades y pasos para dar la baja técnica a un software. De igual forma, se carece de un documento que centralice las directrices actuales, por ejemplo:

1. Justificación Técnica y Evaluación de Impacto
2. Criterios y Disparadores de la Baja
3. Procedimientos Técnicos Específicos por Escenario
4. Respaldo y Migración de Datos (Backup)
5. Revocación de Accesos y Licencias
6. Desinstalación Efectiva (Remoción)
7. Destrucción o Custodia de Medios Físicos y Claves
8. Actualización del Inventario (Base de Datos de gestión de Configuración CMDB)
9. Fase de Cierre y Ciberseguridad Final
10. Generación del Acta de Baja Técnica (la evidencia objetiva del destino final y técnico)

6. ESTADO DE REGISTRO DEL SOFTWARE PROPIO

La Unidad dispone actualmente de software desarrollado de forma interna o por terceros, entre los que destacan los sistemas misionales SIM Busquemos, Gestionemos, Tramitemos y el Sistema de Seguridad de la Información. Al consultar al Grupo Interno de Trabajo de Gestión Tecnológica sobre el registro de propiedad intelectual de estas herramientas, se informó que el sistema Gestionemos no se encuentra inscrito ante la Dirección Nacional de Derechos de Autor; no se obtuvo respuesta sobre el estado de los demás aplicativos.

Tabla 2 - Inventario de Sistemas Informáticos Propios

Nombre del Sistema Informático	**Estado de Tramite ante la Dirección Nacional de Derechos de Autor DNDA**
Sistema de Información Misional SIM Busquemos	En trámite desde el 15 de marzo de 2024, con estado actual desconocido.
Gestionemos	En trámite desde el 15 de marzo de 2024, con estado actual desconocido.
Tramitemos	Sin información
Sistema de Seguridad de la Información	Sin información
Sin información de otros sistemas informáticos propios	Sin información

Al respecto, en el seguimiento realizado por la Oficina de Control Interno durante la vigencia 2025, la entonces Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) presentó los soportes de radicación ante la Dirección Nacional de Derechos de Autor. Los trámites corresponden a los sistemas **SIM Busquemos** (radicado 1-2024-27812 del 15 de marzo de 2024) y **Gestionemos** (radicados 1-2024-27725 del 14 de marzo y 1-2024-27806 del 15 de marzo de 2024). Todas estas solicitudes recibieron respuesta el 10 de mayo de 2024, mediante el radicado 2-2024-46151.

CONSULTAR ESTADO DE TRÁMITE

Le invitamos a consultar el estado de su trámite, escogiendo uno de los siguientes filtros:

Número de documento. Número de radicado. Correo electrónico.

Número de documento: 52488878

Número de radicado:

Correo electrónico:

Consultar

Listado de trámites

NÚMERO DE RADICADO	FECHA DE RADICADO	ESTADO
1-2024-27812	marzo, 15-2024	Su comunicación fue atendida en la fecha: mayo, 10-2024 , el número de radicado de salida es: 2-2024-46151 . Verifique el medio por el cual autorizó su respuesta. Para mayor información consulte su trámite ingresando a través de su cuenta de la plataforma de Registro Virtual www.registroenlinea.gov.co
1-2024-27806	marzo, 15-2024	Su comunicación fue atendida en la fecha: mayo, 10-2024 , el número de radicado de salida es: 2-2024-46151 . Verifique el medio por el cual autorizó su respuesta. Para mayor información consulte su trámite ingresando a través de su cuenta de la plataforma de Registro Virtual www.registroenlinea.gov.co
1-2024-27725	marzo, 14-2024	Su comunicación fue atendida en la fecha: mayo, 10-2024 , el número de radicado de salida es: 2-2024-46151 . Verifique el medio por el cual autorizó su respuesta. Para mayor información consulte su trámite ingresando a través de su cuenta de la plataforma de Registro Virtual www.registroenlinea.gov.co

Fuente: Sistema de Consulta de Estado de Trámite.

Es importante resaltar que se identificó que, la cuenta utilizada para el registro está vinculada a los datos de la exservidora Luz Marina Díaz Ramírez. En consecuencia, resulta imperativo recuperar el acceso a dicha cuenta para gestionar la información de los sistemas informáticos ante la Dirección Nacional.

Interior

DNDA Dirección Nacional de Derecho de Autor Ministerio del Interior

Apreciado usuario sus datos son:

Nombre: LUZ MARINA DIAZ RAMIREZ
Correo Principal: LUZMDIAZR@GMAIL.COM
Correo Auxiliar: LDIAZR@UNIDADBUSQUEDA.GOV.CO

Se enviarán sus credenciales de acceso a los correos arriba mencionados.

Si ya no cuenta con acceso a los correos arriba mencionados, debe escribir un correo a info@derechodeautor.gov.co adjuntando una copia del documento de identidad (para validar la propiedad de la cuenta) y los datos a corregir.

Envíar Credenciales

Fuente: Sistema de Recuperación de Credenciales

Finalmente, el Grupo Interno de Trabajo de Gestión Tecnológica no suministró la información requerida sobre los sistemas SIM Busquemos, Tramitemos y el Sistema de Seguridad de la Información y otros sistemas informáticos propios, quedando pendiente la verificación de su estado.

7. RIESGOS

Omitir el registro de software propio ante la Dirección Nacional de Derecho de Autor (DNDA)

El software desarrollado a medida o por terceros representa un activo de información intangible estratégico para la entidad. La ausencia de un registro formal ante la Dirección Nacional de Derechos de Autor (DNDA) vulnera la protección de la propiedad intelectual y genera una exposición a riesgos críticos en materia de control fiscal y seguridad jurídica.

Riesgos Identificados

- Riesgo Legal y de Cumplimiento: Pérdida de la titularidad de los derechos patrimoniales del software. La ausencia de un registro público que otorgue la presunción de titularidad a favor del Estado dificulta la defensa jurídica ante posibles reclamaciones de terceros (ej. excontratistas o desarrolladores que aleguen autoría o uso indebido).

- Riesgo de Fuga de Propiedad Intelectual: Exposición a que el código fuente sea apropiado, comercializado o registrado por terceros sin autorización, lo que conlleva la pérdida del control sobre la confidencialidad, integridad y uso exclusivo de la herramienta.

Consecuencias

- Posible Detrimento Patrimonial (Hallazgo Fiscal): La Contraloría General de la República (CGR) puede tipificar esta omisión como una gestión antieconómica o un detrimento al patrimonio público. Esto se debe a que la entidad invirtió recursos públicos en la creación de un activo que no fue debidamente legalizado, protegido ni incorporado formalmente al patrimonio institucional.

- Sanciones Disciplinarias: La Procuraduría General de la Nación puede iniciar investigaciones contra los ordenadores del gasto, líderes de TI y supervisores de contratos por el incumplimiento de sus deberes de custodia

y protección de los bienes del Estado, bajo el marco de la Ley 1952 de 2019 (Código General Disciplinario).

Debilidad de documentación y procedimientos para la baja técnica de software

El cierre del ciclo de vida del software es una fase crítica tanto en la gestión de servicios de tecnologías de la información (ITIL) como en el Sistema de Gestión de Seguridad de la Información (SGSI). La ausencia de lineamientos documentados para la baja técnica y la disposición final de estos sistemas genera una acumulación de pasivos tecnológicos y vacíos de control administrativo.

Riesgos Identificados

- Riesgo de Privacidad y Fuga de Datos (Habeas Data): Si un software se desactiva (apaga) sin un protocolo de sanitización, migración o destrucción segura de sus bases de datos, existe una alta exposición de datos personales. Esto constituye una vulneración a la Ley 1581 de 2012 y a las circulares externas de la Superintendencia de Industria y Comercio (SIC).

- Obsolescencia y Vulnerabilidades Técnicas: Mantener sistemas "encendidos" sin soporte ni actualizaciones los convierte en puertas de enlace para ciberataques, comprometiendo la integridad de la red institucional.

Consecuencias

- Brechas de Seguridad y Compromiso Institucional: Un incidente de seguridad en software no parchado o en desuso puede paralizar los servicios misionales, afectando directamente al ciudadano y causando un daño reputacional de difícil recuperación.

- Pérdida de Memoria Institucional y Exposición a Daño Antijurídico: La entidad se expone a fallos adversos en procesos judiciales o disciplinarios por la incapacidad de suministrar información histórica. La baja "empírica" (sin protocolos) rompe la cadena de custodia y la trazabilidad de los datos que residían en el software.

Incumplimiento a los criterios de la norma ISO 27001

La Unidad, a través de su Sistema de Seguridad de la Información (SSI), adopta como referente técnico la norma ISO/IEC 27001:2022. Este compromiso se formaliza en la "Declaración de Aplicabilidad", donde la entidad manifiesta el cumplimiento de los 93 controles del Anexo A de la norma precitada.

No obstante, se evidencia una brecha en la aplicación de los controles específicos relacionados con el ciclo de vida del desarrollo seguro y el desmantelamiento de activos, detallados a continuación:

Controles Tecnológicos (Dominio 8)

- **Control 8.25 - Ciclo de vida de desarrollo seguro:** Exige la aplicación de reglas de seguridad en todas las fases del software, incluyendo su retiro o disposición final.
- **Control 8.10 - Eliminación de la información:** Obliga a que los datos en sistemas o medios de almacenamiento sean eliminados de forma segura cuando dejan de ser necesarios, evitando recuperaciones no autorizadas.
- **Control 8.9 - Gestión de la configuración:** Requiere que los estados y configuraciones de los sistemas (incluyendo su baja) sean gestionados, registrados y revisados formalmente.
- **Control 8.2 - Gestión de derechos de acceso:** Mandata la revocación de accesos lógicos (cuentas, roles y conexiones a bases de datos) asociados al software retirado, mitigando el riesgo de "credenciales huérfanas" o puertas traseras.

Controles Organizacionales (Dominio 5)

- **Control 5.9 - Inventario de información y otros activos:** Exige mantener un inventario exacto; la falta de un protocolo de baja impide que el inventario refleje el estado real de los activos.
- **Control 5.33 - Protección de registros:** Dicta que los registros deben protegerse contra pérdida o destrucción, conforme a requisitos legales y de negocio (evidencia histórica).
- **Control 5.14 - Transferencia de información:** En casos donde la baja implique migración, este control exige procedimientos seguros para proteger los datos en tránsito contra intercepción o modificación.

Marco Legal y Vinculación del Modelo de Seguridad (MSPI) con la Norma ISO/IEC 27001

Enlace a la página Web de la UBPD

Dirección de correo electrónico a Servicio al Ciudadano de la UBPD

En el contexto del Estado colombiano, la obligatoriedad no se denomina "cumplimiento de ISO 27001", sino implementación del Modelo de Seguridad y Privacidad de la Información MSPI. Este modelo actúa como un habilitador transversal de la Política de Gobierno Digital (Decretos 1078 de 2015 y 767 de 2022) y es un componente integrante del Modelo Integrado de Planeación y Gestión (MIPG).

Dado que el Modelo de Seguridad y Privacidad de la Información MSPI está fundamentado en un 90% en la familia de normas ISO/IEC 27000 (específicamente la 27001 y 27002), la Unidad, al estar obligada por ley a implementar dicho modelo, asume en la práctica la responsabilidad de operar un Sistema de Seguridad de la Información SSI bajo la estructura de mejora continua (Planear, Hacer, Verificar, Actuar) propia de la norma internacional.

Este compromiso legal se refuerza en la Política de Seguridad de la Información (GTI-PC-001) de la entidad, cuyo marco normativo incluye:

- Resolución 500 de 2021: Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el MSPI como habilitador de Gobierno Digital.
- Resolución 746 de 2022: Fortalece el MSPI y define lineamientos adicionales a los establecidos en la resolución anterior.

8. CALIDAD DE LA INFORMACION

El dato que constituye información de respuesta interna o externa debe cumplir con criterios de calidad (oportunidad, exactitud, completitud, consistencia y credibilidad) y evitar la duplicidad. En este sentido, la Oficina Asesora de Control Interno presenta las siguientes observaciones:

- **Debilidad en Oportunidad y Completitud: Hito 1:** El 06 de febrero de 2026 se realizó la solicitud inicial al Grupo Interno de Trabajo, con fecha de entrega para el 17 de febrero de 2026. **Hito 2:** Al corte del 03 de marzo de 2026, la información no había sido entregada. Se reiteró la solicitud con nuevo plazo al 05 de marzo; no obstante, se recibió una respuesta parcial el mismo 03 de marzo. **Hito 3:** Tras la revisión de la Oficina Asesora de Control Interno, se concluyó que la información carecía de completitud y pertinencia. En consecuencia, se solicitaron ajustes con fecha de entrega para el 13 de marzo de 2026. **Hito 4:** El 16 de marzo de 2026 se recibió una respuesta técnica general que omitió el archivo central "Datos Software UBPD 2025.xlsx"

(requerido desde la solicitud inicial), el cual debía contener los datos de baja, el inventario de software especializado y el inventario de los desarrollos propios.

- **Debilidad en Consistencia:** Una vez verificados los 30 inventarios de software generados desde la herramienta “Aranda” contra el inventario de hardware entregado por el Grupo Interno de Trabajo de Gestión Tecnológica, se observó lo siguiente:

Tabla 3 - Resultados Cruce Información Aranda e Inventarios Hardware

TIPO	SERIAL	NOMBRE COMPLETO	NOMBRE EQUIPO	OBSERVACION
Portátil	5CD451L3DN	MARIA CLEMENCIA PACHECO MARTINEZ	BOG-SAF-069	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
Portátil	5CD451L35R	ROSA MARIA INFANTE RUIZ	BOG-SG-061	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
Portátil	PF1GJY6S		BOG-SGI-054	En Aranda, nombre de equipo distinto.
Portátil	5CD451G54M	LAURA MARCELA CASTILLO VILLEGAS	PEI-SGTT-015	En Inventario el usuario de Office es distinto.
Portátil	5CD451L33P	JUAN DAVID GARZON RINCON	BOG-OTIC-010	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
AIO	MJ06GGA5	MAURICIO BARON VILLA	BOG-SIND-001	Sin inventario en Aranda; en Inventario sin usuario de Office.
Portátil	5CD451L3DD	NURY XIMENA CARABALLO ARCILA	TBOG-SGTT-024	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
AIO	MJ06GG4K	MARIANELLA ISABEL FORERO MORENO	BOG-SGTT-014	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
Portátil	5CD451L3G6	LUIS ALEJANDRO MOYA HERNANDEZ	BOG-OTIC-007	En Aranda, nombre de responsable distinto y nombre equipo distinto; en

TIPO	SERIAL	NOMBRE COMPLETO	NOMBRE EQUIPO	OBSERVACION
				Inventario el usuario de Office es distinto.
Portátil	SCNXCV017748496		BOG-DIS-063	Sin inventario en Aranda.
Portátil	5CD451G4XD	DIANA PATRICIA ORTIZ CAMARGO	PEI-SGTT-016	En Inventario, sin usuario de Office.
Portátil	5CD451L3KQ	CLAUDIA MARCELA MORATO ALARCON	BOG-OTIC-022	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
PC	HY8JQ54	EURIDES TRIANA TRIANA	BOG-SGI-lA01	Sin inventario en Aranda; en Inventario sin usuario de Office.
Portátil	5CD451L33Q	ELIANA CASTELLANOS DIAZ	BOG-OACP-020	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
Portátil	5CD451L3DM	DANIEL CORREA	BOG-SAF-073	En Aranda, nombre de responsable distinto.
AIO	MP2A9FC6	GUSTAVO ARNULFO CAMARGO ABRIL	BOG-SGI-036	En Inventario, sin usuario de Office.
Portátil	5CD451L3LK	LUISA FERNANDA RUGE VELASCO	VVC-SGTT-002	En Inventario, sin usuario de Office.
Portátil	PF1FRFDS	ANDREA YOLANDA JIMENEZ SILVA	FLA-SGTT-019	En Aranda no existe información del equipo; en Inventario, sin usuario de Office.
AIO	MJ06GGA7	ERIKA TIXIANA CABRERA CHAVES	BOG-DPCENF-036	En Aranda sin nombre de responsable; en Inventario sin usuario de Office.
Portátil	5CD451L3BZ	JHON MARIO URBANO MELENDEZ	FLA-SGTT-021	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.
PC	JY8JQ54	EURIDES TRIANA TRIANA	BOG-SGI-lA02	Sin inventario en Aranda; en Inventario sin usuario de Office.
AIO	MJ06GG9W	ANDREA NATALI ROMERO VARGAS	MED-SGTT-042	En Aranda, nombre de responsable distinto; en Inventario el usuario de Office es distinto.

Fuente: 30 Inventarios de Software Aranda e Inventario de Hardware

Enlace a la página Web de la UBPD

Dirección de correo electrónico a Servicio al Ciudadano de la UBPD

Se identificaron inconsistencias en el **73,33%** de la muestra evaluada (22 de 30 equipos), al contrastar la información registrada en la herramienta Aranda frente al inventario de hardware suministrado por el Grupo Interno de Trabajo de Gestión Tecnológica.

9. RECOMENDACIONES

- Recomendación 1: Institucionalizar el Registro Obligatorio y Gestión de Propiedad Intelectual del Software ante la Dirección Nacional de Derechos de Autor DNDA: Se recomienda diseñar e implementar una Política de Gestión de Derechos de Autor que establezca la obligatoriedad del registro ante la DNDA de todo código fuente desarrollado a medida o por terceros. Este procedimiento debe integrarse como un requisito habilitante y obligatorio para la liquidación de contratos y el paso a producción de cualquier aplicativo.

- Recomendación 2: Operacionalizar el Procedimiento de Baja Técnica: Es imperativo oficializar y poner en marcha un Protocolo de Baja Técnica y Disposición Final de Software. Este instrumento debe articularse de manera transversal con el Sistema de Seguridad de la Información (SSI), el Oficial de Seguridad de la Información (OSI) y el Programa de Gestión Documental, garantizando la sanitización de datos y la preservación de la memoria institucional.

- Recomendación 3: Fortalecer los Mecanismos de Autocontrol y Calidad de la Información: Realizar actividades de autocontrol periódicas, que sincronice la gestión de la Mesa de Ayuda con el inventario del Grupo de Gestión Tecnológica. El objetivo es subsanar el margen de error del **73,33 %** identificado y garantizar que la información procesada cumpla con los atributos de exactitud, oportunidad y consistencia.

10. CONCLUSIONES ESTRATEGICAS

- **Priorización en la protección legal de los activos intangibles (Propiedad Intelectual):** La Unidad enfrenta una exposición crítica a riesgos legales, de cumplimiento y de fuga de propiedad intelectual al omitir el registro formal de su software misional (como SIM Busquemos, Gestionemos, Tramitemos y el Sistema de Seguridad de la Información) ante la DNDA. Resulta imperativo institucionalizar este registro como un hito obligatorio en el ciclo de desarrollo y recuperar de manera inmediata el control de las credenciales de acceso que

actualmente se encuentran vinculadas a una exservidora, garantizando así la soberanía de la información institucional.

- **Estandarización de la "baja técnica" para asegurar el cumplimiento y la ciberseguridad:** La ausencia de un procedimiento integral y documentado para el desmantelamiento de software genera un pasivo tecnológico que vulnera la seguridad digital de la entidad. Esta debilidad expone a la Unidad a brechas de seguridad y fugas de datos personales (Ley 1581 de 2012). Es urgente operacionalizar un protocolo de baja técnica alineado con los estándares de la norma ISO/IEC 27001 y el MSPI, que garantice procesos auditables de borrado seguro, revocación de privilegios y gestión de la configuración.

- **Fortalecimiento del Gobierno de TI mediante la exactitud de los inventarios:** Se identificó una debilidad significativa en la calidad de la información tecnológica, evidenciada por una discrepancia del 73,33 % en la muestra evaluada al contrastar la herramienta Aranda con el inventario físico de hardware. A nivel estratégico, esta inconsistencia requiere la implementación de mecanismos de autocontrol periódicos que articulen a la Mesa de Ayuda con el Grupo de Gestión Tecnológica, asegurando que los datos cumplan con los atributos de exactitud, completitud y oportunidad.

11. CONCLUSIÓN GENERAL

Tras el seguimiento realizado, la Oficina Asesora de Control Interno identifica una oportunidad estratégica para fortalecer el Gobierno de TI y blindar el patrimonio intangible de la Unidad. Si bien se evidencian brechas en el registro de propiedad intelectual, la estandarización de bajas técnicas y la consistencia de inventarios (73,33 % de discrepancia), estas situaciones identificadas constituyen la hoja de ruta para elevar los estándares de seguridad y cumplimiento normativo bajo el Modelo de Seguridad y Privacidad de la Información MSPI.

Es imperativo avanzar hacia una gestión tecnológica auditable y soberana, donde el registro sistemático ante la Dirección Nacional de Derechos de Autor DNDA y la adopción de protocolos alineados con la ISO 27001 aseguren la continuidad y protección de la información misional.

Por lo tanto, se exhorta al Grupo de Gestión Tecnológica a liderar un Plan de Mejoramiento dinámico que transforme estas debilidades en fortalezas operativas, garantizando que la infraestructura tecnológica sea un activo confiable, transparente y plenamente protegido para el cumplimiento de nuestra misión institucional.

Cordialmente,

ORIGINAL FIRMADO

DIANA CAROLINA ARBELAEZ ARCINIEGAS
Jefe Oficina Asesora de Control Interno

Tabla 4 - Firmas

Elaborado por:	Carlos Andrés Rico Reina	**Experto Técnico**	FIRMA: ORIGINAL FIRMADO
Aprobado por:	Diana Carolina Arbelaez Arciniegas	**Jefe Oficina Asesora de Control Interno**	FIRMA: ORIGINAL FIRMADO