Al contestar por favor cite este número
Radicado N° 202601300006473

COMUNICACIÓN INTERNA

Bogotá D.C, Miércoles, 18 de Marzo de 2026

PARA: Liliana Morales
Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Oficina de Tecnologías de la Información y las Comunicaciones

ASUNTO: Informe de la Auditoría de Cumplimiento "Verificación del cumplimiento de las normas en materia de Derechos de Autor de software en la Región Metropolitana Bogotá-Cundinamarca".

Respetada Ingeniera Liliana,

En cumplimiento de lo establecido en la Plan Anual de Auditoría de la vigencia 2026, la Oficina de Control Interno realizó durante los meses de febrero y marzo de 2026, la auditoría de cumplimiento denominada "Verificación del cumplimiento de las normas en materia de Derechos de Autor de software en la Región Metropolitana Bogotá-Cundinamarca".

Las conclusiones de la verificación se describen en el numeral 8 del informe que se anexa a la presente comunicación.

Agradecemos el apoyo brindado en el marco de la auditoría y esperamos que los resultados contribuyan a continuar fortaleciendo el Sistema de Control Interno en la Región Metropolitana Bogotá-Cundinamarca.

Finalmente precisamos que (i) Teniendo en cuenta que el sistema de correspondencia SIGMA se encuentra en etapa de desarrollo de acuerdo con la respuesta remitida a la Oficina de Control Interno mediante correo electrónico de fecha 24 de noviembre de 2025 [1] , por la Subdirección de Gestión Corporativa – PQRSD [2] se remite al líder del proceso, a fin de que pueda conocer en primera instancia de los resultados y pueda analizar las conclusiones del informe y en informados a la Subdirección de Gestión Corporativa (quienes acompañaron el ejercicio de evaluación independiente como proceso transversal el cual se ilustra en el informe adjunto) y a los Miembros del Comité Institucional de Coordinación de Control Interno; y,

(ii) Además se remitirá el memorando e informe a través de correo electrónico a fin de garantizar lo señalado en el parágrafo No. 1 del artículo 2.2.21.4.7. del Decreto 1083 de 2015 [3] y Resolución Regional No. 112 de 2025 "*Por medio de la cual se crea, integra y se establece el reglamento de funcionamiento del Comité Institucional de Coordinación de Control Interno de la Región Metropolitana Bogotá – Cundinamarca*"; teniendo en cuenta que, el SIGMA – Sistema de

Correo institucional: contactenos@regionmetropoilitana.gov.co
NIT: 901665578-7
Dirección: Avenida Calle26 #57-83, Edificio CEMSA Torre 8 / Piso 15
Teléfono Commutador: +57 (601) 7431943

Correspondencia de la Región Metropolitana Bogotá Cundinamarca no permite la asignación de varios usuarios como destinatario principal, dado que se encuentra en desarrollo.

---

[1] *Se destaca del correo: "En atención al correo que antecede, nos permitimos informar que, de acuerdo con la revisión realizada, el sistema SIGMA actualmente no cuenta con el desarrollo que permita asignar múltiples remitentes en la generación y envió.* ***Conforme a los parámetros definidos, cada comunicación queda asociada únicamente al responsable del proceso, mientas que los demás actores se gestionan como informados dentro del mismo trámite***". (Negrilla fuera de texto).
[2] Usuario: dmahecha@regionmetropolitana.gov.co

[3] *"(....) PARÁGRAFO 1. Los informes de auditoría, seguimiento y evaluaciones* ***tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva****, y deberán ser remitidos al nominador cuando este lo requiera*". (Negrilla fuera del texto).

Cordialmente,

REYES SAAVEDRA AURORA ANDREA
Firmado digitalmente por REYES SAAVEDRA AURORA ANDREA

Aurora Andrea Reyes Saavedra
Jefe Oficina de Control Interno
OFICINA DE CONTROL INTERNO
Anexos: Informe Final de Auditoría en formato PDF
Copia: Luis Felipe Lota - Director y Presidente del Comité Institucional de Coordinación de Control Interno, Luis Alberto Colorado Aldana – Jefe de la Oficina de Asesora de Planeación Institucional - miembro del Comité Institucional de Coordinación de Control Interno, Laura Lucía Cárdenas - Jefe de la Oficina Jurídica (e) y miembro del Comité Institucional de Coordinación de Control Interno (e) – Resolución No. 057 del 12 de marzo de 2026, Ángela Marcela Cárdenas Mora - Jefe de la Oficina Asesora de Comunicaciones y Participación Ciudadana - miembro del Comité Institucional de Coordinación de Control Interno, Luz Dary Garzón Guevara - Jefe de la Oficina de Control Disciplinario Interno - miembro del Comité Institucional de Coordinación de Control Interno, Henry Ortiz Saavedra- Subdirector de Gestión Corporativa- miembro del Comité Institucional de Coordinación de Control Interno, Gisela Paola Ladrador Araújo - Subdirectora de Planeación Metropolitana y Regional -miembro del Comité Institucional de Coordinación de Control Interno, Diego Díaz del Castillo Fernández - Subdirector de Gestión de Proyectos - miembro del Comité Institucional de Coordinación de Control Interno.
Proyectó: Crhistian Augusto Amador León - Contratista OCI - OFICINA DE CONTROL INTERNO

Correo institucional: contactenos@regionmetropoilitana.gov.co
NIT: 901665578-7
Dirección: Avenida Calle26 #57-83, Edificio CEMSA Torre 8 / Piso 15
Teléfono Conmutador: +57 (601) 7431943

Oficina de Control Interno

INFORME DE AUDITORÍA DE CUMPLIMIENTO

Verificación del cumplimiento de las normas en materia de Derechos de Autor de software en la Región Metropolitana Bogotá-Cundinamarca

Vigencia 2025

Marzo de 2026

Contenido

1. Objetivo

Evaluar el cumplimiento de las normas en materia de derechos de autor de software por parte de la RMBC, mediante la verificación del inventario de software instalado, su licenciamiento, uso y mecanismos de administración y control asociados, en los sistemas administrativos y de soporte, como elementos que contribuyen a garantizar el uso de software legal en la entidad.

2. Alcance

La verificación y análisis de información se realizó respecto de información comprendida en el periodo de tiempo del 1 de enero al 31 de diciembre de 2025.

3. Criterios Normativos

Los criterios de la verificación se encuentran sustentados, en la siguiente normatividad externa e interna sobre la materia:

- **Ley 87 de 1993.** *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".*
- **Decreto 1083 de 2015. "***Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública***".**
- **Directiva Presidencial 01 de 1999**, *"Asunto: Respeto al derecho de autor y a los derechos conexos."*
- **Directiva Presidencial 02 de 2002**, *"Asunto: Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software)."*
- **Circular 04 del 22 de diciembre de 2006**, expedida por el Consejo Asesor del Gobierno Nacional, *"Asunto: "verificación cumplimiento normas de uso de software."*
- **Circular 012 de 2 de febrero de 2007** expedida por la Dirección Nacional de Derechos de Autor, asunto: *"Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre programas de computador (software)."*
- **Circular 017 de 1 de junio de 2011** expedida por la Dirección Nacional de Derechos de Autor, *"Asunto: Modificación 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)."*
- **Circular Externa No. 027 de 2023** de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, *por la cual se modifica la Circular 017 del 1 de junio de 2011 y se habilita un nuevo campo en el micrositio del Informe de Software, en el cual se deberá subir el link que permita acceder al Informe*

"Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software".

- Comunicación publicada en el micrositio 'Informe de Software' de la DNDA, donde se indica el plazo para rendición del informe (consulta en línea). *Enlace DNDA*

Y la demás normatividad interna y externa aplicable con el fin de lograr el objetivo y alcance de la presente auditoría.

4. Metodología [1]

En el marco del presente seguimiento, se realizaron entre otras las siguientes actividades:

- Análisis de los criterios normativos aplicables para la Región Metropolitana Bogotá-Cundinamarca de acuerdo con los lineamientos establecidos por la Dirección Nacional de Derechos de Autor – DNDA, Directivas Presidenciales, Circular del Consejo Asesor del Gobierno Nacional.
- Con comunicación interna No. 202601300004183 del 12 de febrero de 2026, remitido a través de SIGMA, se notifica, solicita información y se comunican los criterios normativos a la Oficina de Tecnologías de la Información y las Comunicaciones, para la ejecución de la auditoría de seguimiento a la verificación del cumplimiento de las normas en materia de derechos de autor de software vigencia 2025 en la Región Metropolitana Bogotá-Cundinamarca.
- Mediante comunicación interna No. 202601600004213 del 12 de febrero la OTIC informa el equipo delegado para atender la auditoría, solicita la reprogramación de la reunión de apertura de la auditoría y remitió la Carta de Salvaguarda y/o Representación debidamente diligenciada y firmada.
- El día 17 de febrero de 2026 se llevó a cabo la reunión de apertura de la auditoría de seguimiento a la verificación del cumplimiento de las normas en materia de derechos de autor de software vigencia 2025 en la Región Metropolitana Bogotá-Cundinamarca. Durante la reunión se comunicaron el objetivo, el alcance, el marco normativo aplicable y las fechas previstas para la realización de la auditoría, así mismo se otorgó plazo para la entrega de la información solicitada.
- Mediante comunicaciones internas No. 202601600004403 y 202601600004423 del 17 de febrero, la OTIC realizó solicitud de información para dar respuesta a la solicitud de la OCI a la Subdirección de Gestión Corporativa y a la Oficina Jurídica.

[1] Las actividades que se enuncian en el siguiente numeral se encuentran soportadas en los papeles de trabajo de la auditoría, los cuales reposan en el archivo de gestión de la OCI de acuerdo con el tiempo señalado en la TRD vigente

- Mediante comunicación interna No. 202604000004963 del 24 de febrero de 2026 la Subdirección de Gestión Corporativa dio respuesta a la OTIC de la solicitud de la información. Así mismo, mediante comunicación interna No. 202601400004833 del 20 de febrero de 2026 la Oficina Jurídica dio respuesta a solicitud de información de la OTIC.
- Mediante comunicación interna No. 202601600004983 del 25 de febrero de 2026 remitido a través de SIGMA, la Oficina de Tecnologías de la Información y las Comunicaciones dio respuesta a la solicitud efectuada por la OCI.
- Mediante correo electrónico del 06 de marzo de 2026, la Oficina de Control Interno socializó el informe preliminar, otorgando plazo hasta el 11 de marzo de 2026 para la remisión de comentarios u observaciones por parte de las áreas involucradas.
- Mediante correo electrónico del 11 de marzo de 2026, la Oficina de Tecnologías de la Información y las Comunicaciones remitió observaciones al informe preliminar. Así mismo, la Subdirección de Gestión Corporativa, mediante correo electrónico de la misma fecha, presentó comentarios relacionados con la observación referente a la baja o desinstalación de software.

  Una vez revisadas las observaciones recibidas, se procedió a la elaboración del presente informe final, incorporando los ajustes pertinentes con base en los comentarios remitidos por la Oficina de Tecnologías de la Información y las Comunicaciones y por la Subdirección de Gestión Corporativa.

  En particular, teniendo en cuenta la información suministrada, algunos aspectos inicialmente planteados como observaciones fueron reclasificados como recomendaciones orientadas al fortalecimiento documental de los controles existentes.
- Mediante mesa de trabajo se realizó el cierre de la auditoría el día 16 de marzo de 2026 en donde se socializó los resultados finales del ejercicio de auditoría contando con la participación de la Subdirección de Gestión Corporativa y la Oficina de Tecnologías de la Información y las Comunicaciones.

5. Desarrollo del Informe

La Oficina de Control Interno efectuó la verificación del cumplimiento de las disposiciones relacionadas con los Derechos de Autor de Software en la Región Metropolitana Bogotá-Cundinamarca (RMBC), con el propósito de analizar diferentes aspectos asociados a la gestión y administración de los recursos tecnológicos de la entidad.

En este sentido, se revisó la confiabilidad, integridad y actualización del inventario institucional de equipos de cómputo (hardware), considerando los movimientos registrados durante la vigencia 2025, tales como altas, bajas y asignaciones. De igual

manera, se evaluó la situación del licenciamiento de software, verificando su correspondencia con los equipos en operación y su respaldo mediante contratos, acuerdos o instrumentos vigentes que acrediten el uso legal de las herramientas tecnológicas implementadas por la entidad.

Finalmente, se examinó la existencia, implementación y aplicación de políticas, procedimientos, lineamientos y controles establecidos por la entidad para garantizar el cumplimiento de la normativa en materia de derechos de autor de software, así como la efectividad de dichos mecanismos para prevenir la instalación o uso de software no autorizado dentro de la infraestructura tecnológica institucional.

5.1. Inventario de equipos de cómputo (hardware).

Para el desarrollo del presente análisis, la Oficina de Control Interno solicitó la información relacionada con el inventario institucional de equipos de cómputo de la Región Metropolitana Bogotá-Cundinamarca (RMBC). En este sentido, mediante memorando No. 202601600004403 del 17 de febrero de 2026 se requirió por parte de la OTIC a la Subdirección de Gestión Corporativa el envío del inventario actualizado de los activos tecnológicos asociados a estaciones de trabajo y equipos de cómputo utilizados por la entidad.

En respuesta a dicha solicitud, la Subdirección de Gestión Corporativa remitió la información mediante memorando No. 202604000004963, indicando que con corte al 31 de diciembre de 2025 la entidad contaba con noventa y nueve (99) equipos de cómputo, los cuales se encontraban registrados dentro del inventario institucional con su respectiva identificación y asignación. De igual manera, se adjuntó el inventario detallado como soporte para la verificación de la información reportada.

De acuerdo con la información suministrada por la dependencia responsable y con base en el archivo remitido, el inventario de equipos de cómputo de la entidad se encuentra distribuido de la siguiente manera:

INVENTARIO DE COMPUTADORES		
ITEM	**2025**	**TOTAL**
EQUIPOS PORTÁTILES (LAPTOP)	65	**99**
EQUIPOS DE ESCRITORIO TIPO ALL-IN-ONE	34	
	TOTAL	**99**

Tabla 1. Inventario de equipos de cómputo y servidores – Vigencia

El inventario remitido contiene información relevante para la identificación y trazabilidad de los activos tecnológicos, incluyendo variables como tipo de equipo, dependencia responsable, funcionario o contratista asignado, cargo, jefe de área, descripción del

equipo, marca y modelo. Esta información permite evidenciar la asignación institucional de los equipos y facilita el control administrativo sobre los activos tecnológicos utilizados por las diferentes dependencias de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

5.2. Equipos de Cómputo Adquiridos - Vigencia 2025

Durante el desarrollo del presente seguimiento, la Subdirección de Gestión Corporativa remitió mediante memorando No. 202604000004963 el inventario detallado de equipos de cómputo (hardware) correspondiente a la vigencia 2025. El archivo aportado contiene la relación de los equipos registrados en el inventario institucional, incluyendo información asociada a su identificación, características técnicas y asignación dentro de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

De acuerdo con la información suministrada por el proceso, los equipos adquiridos durante la vigencia 2025 corresponden a los mismos registros incluidos en el inventario institucional aportado, razón por la cual la verificación se realizó sobre dicha base de datos, la cual consolida la información de los activos tecnológicos asociados a estaciones de trabajo y equipos portátiles utilizados por la entidad. En este contexto, se recomienda mantener mecanismos de identificación o trazabilidad dentro del inventario que permitan distinguir de manera clara las incorporaciones realizadas en cada vigencia.

5.3. Software dado de Baja - Vigencia 2025

En el marco del seguimiento realizado por la Oficina de Control Interno, mediante memorando No. 202601600004403 se solicitó a la dependencia competente la información relacionada con el software dado de baja durante la vigencia 2025. En respuesta a dicha solicitud, la Subdirección de Gestión Corporativa, mediante memorando No. 202604000004963, informó que durante el periodo evaluado no se realizó la baja de ningún software, razón por la cual no existe inventario asociado a software retirado o desincorporado durante dicha vigencia.

En consecuencia, para el periodo objeto de verificación no se evidenciaron registros de software dado de baja dentro de la Región Metropolitana Bogotá-Cundinamarca (RMBC), de acuerdo con la información suministrada por el proceso responsable.

5.4. Contratos de mantenimiento y renovación de licenciamiento - Vigencia 2025

En atención al requerimiento relacionado con el inventario de contratos de mantenimiento y renovación de licenciamiento con los que cuenta la entidad, se solicitó información mediante memorando No. 202601600004423 por parte de la OTIC. En

respuesta, la Oficina Jurídica remitió mediante comunicación interna con radicado No. 202601400004833 del 20 de febrero de 2026 el listado de contratos asociados a la adquisición y renovación de licencias de software vigentes en la entidad.

De acuerdo con la información suministrada, durante la vigencia 2025 se suscribieron contratos relacionados con la adquisición y renovación de licenciamiento de software y servicios tecnológicos, entre los cuales se encuentran contratos asociados a herramientas Microsoft, software especializado para diseño institucional, AutoCAD, licenciamiento ArcGIS Enterprise, certificados de firma digital y cifrado SSL, renovación del ERP–HCM institucional y herramientas de colaboración Microsoft 365 y antivirus.

Estos instrumentos contractuales soportan la operación de los sistemas de información y servicios tecnológicos de la Región Metropolitana Bogotá-Cundinamarca.

En relación con el plan y cronograma de mantenimiento preventivo de equipos de cómputo de usuario final solicitado para la vigencia 2025, el proceso informó que dichas actividades fueron programadas y ejecutadas durante los primeros meses de la vigencia 2026, remitiendo como soporte el plan de trabajo y cronograma correspondiente. Dicho plan contempla actividades orientadas a la consolidación del inventario de equipos, validación de información con el área de almacén, estandarización de activos tecnológicos, control de software y hardware, actualización del sistema operativo y fortalecimiento de herramientas de gestión de activos, incluyendo el uso de la plataforma GLPI como repositorio de control de activos tecnológicos.

En este sentido, se observa que la entidad ha venido adelantando acciones orientadas al fortalecimiento del control y gestión de los activos tecnológicos, particularmente en lo relacionado con la organización del inventario y el seguimiento a los sistemas y herramientas institucionales. No obstante, se recomienda continuar consolidando en un punto único de control la información asociada a los contratos de licenciamiento y servicios tecnológicos, incorporando variables como objeto contractual detallado, valor, plazo de ejecución, fecha de inicio y terminación, supervisor designado y estado del contrato, con el fin de facilitar la trazabilidad, seguimiento y control integral del licenciamiento tecnológico institucional.

5.5. Mantenimiento correctivo de servidores, sistemas de información y bases de datos - Vigencia 2025

En atención al requerimiento relacionado con el informe de mantenimiento correctivo de servidores, sistemas de información y bases de datos realizados durante la vigencia 2025, la Oficina de Tecnologías de la Información y las Comunicaciones informó que durante dicho periodo no se presentaron eventos que requirieran la elaboración de informes de mantenimiento correctivo por parte del proceso.

De acuerdo con lo indicado por la OTIC, la infraestructura tecnológica de la entidad

opera bajo modalidades de servicios en la nube, principalmente Software as a Service (SaaS) y Platform as a Service (PaaS), por lo cual las actividades asociadas al mantenimiento de infraestructura tecnológica, motores de bases de datos, aplicación de parches de seguridad, respaldos y disponibilidad del servicio se encuentran incluidas dentro de los contratos de prestación del servicio y son responsabilidad directa de los proveedores, conforme a los respectivos acuerdos de nivel de servicio (ANS) establecidos.

En este sentido, las actividades relacionadas con el mantenimiento correctivo de infraestructura tecnológica y motores de bases de datos no son ejecutadas directamente por la OTIC, sino que forman parte de las responsabilidades asumidas por los proveedores en el marco de la prestación del servicio. En consecuencia, durante la vigencia 2025 no se evidenciaron situaciones que requirieran la gestión interna de mantenimientos correctivos por parte del proceso, reportándose que los sistemas administrados directamente por la OTIC operaron con normalidad durante el periodo evaluado.

En escenarios donde los servicios tecnológicos se encuentran soportados en modelos de computación en la nube, el control institucional se orienta principalmente al seguimiento de los acuerdos de nivel de servicio (ANS), la disponibilidad de las plataformas, la gestión de incidentes y la verificación del cumplimiento de las obligaciones contractuales por parte de los proveedores.

Por lo anterior, se recomienda continuar fortaleciendo los mecanismos de seguimiento y control asociados a la operación de los servicios tecnológicos provistos bajo modelos de nube, particularmente en lo relacionado con la verificación periódica del cumplimiento de los acuerdos de nivel de servicio (ANS), la gestión de incidentes reportados por los proveedores, la disponibilidad de las plataformas y la trazabilidad de las actividades de soporte y mantenimiento realizadas por terceros, con el fin de fortalecer la gobernanza y control institucional sobre la infraestructura y los sistemas de información que soportan la operación de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

5.6. Herramientas tecnológicas para monitoreo e inventario de software – Vigencia 2025

En atención al requerimiento relacionado con la identificación de las herramientas tecnológicas utilizadas para el monitoreo, inventario y control del software instalado en los equipos de cómputo institucionales, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) remitió la relación de las soluciones tecnológicas implementadas para tal fin, indicando su fecha de implementación, área responsable de administración y las funcionalidades asociadas al control de licenciamiento.

De acuerdo con la información analizada, la entidad dispone de diversas herramientas orientadas a fortalecer la gestión y control del software instalado en los equipos de usuario final, entre las cuales se destacan GLPI con agente de inventario, Microsoft Intune, las políticas de seguridad configuradas en Microsoft 365 y la plataforma Microsoft Defender, todas administradas por la OTIC.

En particular, la herramienta GLPI, implementada durante la vigencia 2025, permite realizar el inventario automatizado de los activos tecnológicos mediante la instalación de un agente en los equipos institucionales. A través de este mecanismo se recopila información relacionada con el software instalado en los dispositivos, incluyendo aplicaciones detectadas, versiones y otros datos asociados, lo cual facilita la generación de reportes por equipo y reportes consolidados utilizados como insumo para la verificación del cumplimiento de las políticas institucionales de licenciamiento.

Adicionalmente, la entidad utiliza Microsoft Intune como plataforma para la gestión y administración de dispositivos institucionales. Esta herramienta permite supervisar el estado de los equipos, verificar las aplicaciones instaladas y aplicar políticas orientadas al control de instalación y uso de software en los dispositivos administrados, generando reportes asociados al estado de cumplimiento de los equipos frente a las configuraciones definidas.

Así mismo, se evidenció la aplicación de políticas de seguridad gestionadas desde el entorno Microsoft 365, orientadas al fortalecimiento de los controles sobre los equipos y cuentas de usuario institucionales. Estas configuraciones incluyen medidas relacionadas con la gestión de privilegios, control de instalación de aplicaciones y otras configuraciones de seguridad que contribuyen a reducir el riesgo asociado al uso de software no autorizado.

De manera complementaria, la entidad emplea Microsoft Defender como herramienta de seguridad para la detección y prevención de amenazas, la cual permite aplicar reglas de seguridad y generar alertas relacionadas con la ejecución de aplicaciones potencialmente riesgosas o no autorizadas en los dispositivos institucionales.

En conjunto, las herramientas implementadas permiten contar con mecanismos tecnológicos orientados al inventario, monitoreo y control del software instalado en los equipos institucionales, lo cual contribuye a la identificación de aplicaciones instaladas, al seguimiento del cumplimiento de las políticas institucionales de seguridad de la información y al control del uso de software dentro de la entidad.

No obstante, se recomienda continuar fortaleciendo los mecanismos de seguimiento y análisis de la información generada por estas herramientas, particularmente en lo relacionado con la consolidación periódica de reportes de inventario de software, la verificación de posibles instalaciones no autorizadas y la documentación de las actividades de control realizadas por el área responsable, con el fin de mantener

actualizado y confiable el inventario institucional de software.

5.7. Procedimientos para la gestión del ciclo de vida del software

En atención al requerimiento relacionado con los procedimientos o lineamientos definidos para la gestión del ciclo de vida del software en la entidad, la Oficina de Tecnologías de la Información y las Comunicaciones informó que actualmente no se cuenta con un procedimiento institucional formal que integre de manera específica las etapas del ciclo de vida del software.

El proceso indicó que, en coordinación con la Oficina Asesora de Planeación Institucional, durante la vigencia 2026 se tiene proyectada la estructuración de un procedimiento que contemple las fases relacionadas con el desarrollo, pruebas, validación y despliegue de soluciones tecnológicas, con el fin de fortalecer la gestión de cambios y el control institucional sobre el software implementado en la entidad.

No obstante, se evidenció que la entidad cuenta con lineamientos operativos asociados al proceso de Gestión de las Tecnologías de la Información y las Comunicaciones, a través de los cuales se gestionan las solicitudes de software mediante requerimientos registrados en la plataforma institucional, incluyendo actividades de evaluación técnica, verificación de licenciamiento, instalación controlada por el área TIC, actualización y desinstalación cuando corresponde.

En este sentido, se recomienda continuar avanzando en la formalización del procedimiento institucional para la gestión del ciclo de vida del software, con el fin de consolidar en un único instrumento los lineamientos asociados a la solicitud, evaluación, instalación, control de licencias, actualización y retiro de aplicaciones utilizadas en la Región Metropolitana Bogotá-Cundinamarca (RMBC).

5.8. Controles técnicos para restringir la instalación de software no autorizado

En atención al requerimiento relacionado con las evidencias o configuración general de los controles técnicos implementados para restringir la instalación de software no autorizado en los equipos de usuario final, la OTIC informó que la entidad ha implementado controles preventivos basados en Microsoft Intune y configuraciones de seguridad en Microsoft 365, orientados a operar con perfiles de usuario estándar y a limitar el uso de privilegios de administrador local únicamente a personal autorizado. En consecuencia, la instalación de software en los equipos administrados queda restringida y sujeta a validación previa por parte del área responsable.

De acuerdo con la evidencia remitida, se observó la segmentación de equipos mediante grupos dinámicos en Intune (asociados a criterios de nomenclatura de dispositivo), sobre los cuales se despliegan directivas de configuración; entre estas, la política “WIN – Local Admins”, que permite administrar los usuarios y grupos locales del equipo y controlar quién cuenta con permisos elevados. Así mismo, se evidenció la asignación de la política a los grupos definidos y la parametrización para que los privilegios administrativos se otorguen únicamente a cuentas o grupos previamente autorizados, manteniendo el resto de los usuarios como estándar, lo cual reduce el riesgo de instalación o ejecución de software no autorizado en los dispositivos institucionales.

En este sentido, se recomienda mantener documentada la configuración de estos controles (alcance, criterios de aplicación, grupos objetivo y cuentas autorizadas), así como realizar revisiones periódicas de los miembros con privilegios elevados y conservar evidencias de los cambios efectuados, con el fin de fortalecer la trazabilidad y el control institucional sobre la restricción de instalación de software en los equipos de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

5.9. Reporte de incidentes relacionados con software no autorizado – Vigencia 2025

En atención al requerimiento relacionado con el reporte de incidentes, hallazgos o eventos detectados durante la vigencia 2025 asociados a la instalación de software no autorizado o incumplimiento de condiciones de licenciamiento, la Oficina de Tecnologías de la Información y las Comunicaciones informó que, durante el periodo evaluado, no se registraron incidentes ni alertas relacionadas con este tipo de situaciones en los equipos institucionales.

De acuerdo con lo manifestado por el proceso, el monitoreo de eventos de seguridad se realiza a través de las herramientas institucionales de protección y análisis de seguridad, particularmente Microsoft Defender for Endpoint, integrado con la plataforma Microsoft Sentinel, las cuales permiten realizar seguimiento a comportamientos de dispositivos, ejecución de aplicaciones y generación de alertas de seguridad. Según la información suministrada y la evidencia revisada, durante la vigencia 2025 no se generaron notificaciones ni eventos asociados a la instalación de software no autorizado o incumplimientos de licenciamiento en la infraestructura tecnológica de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

5.10. Identificación de riesgos asociados al manejo de software licenciado

Frente al requerimiento relacionado con la identificación de riesgos asociados al manejo

de software licenciado, la Oficina de Tecnologías de la Información y las Comunicaciones informó que, en el marco de la reestructuración de los procesos y procedimientos a cargo de dicha dependencia, durante la vigencia 2026 se tiene proyectado adelantar el levantamiento formal de riesgos y la definición de sus respectivos tratamientos, actividad que se realizará en coordinación con la Oficina Asesora de Planeación Institucional.

No obstante, el proceso indicó que actualmente se desarrollan diversas actividades orientadas a mitigar riesgos asociados al uso y administración de software licenciado en la entidad. Entre estas se encuentran la administración centralizada de licencias y suscripciones, la restricción de privilegios de instalación en los equipos institucionales, el monitoreo del software instalado mediante herramientas corporativas como Microsoft 365 Admin Center, Intune y Defender, así como el seguimiento periódico al cumplimiento del licenciamiento y el control del inventario de software a través del agente GLPI instalado en los equipos.

Estas actividades constituyen controles operativos que contribuyen a mitigar riesgos asociados al uso de software no autorizado o al incumplimiento de condiciones de licenciamiento en los equipos institucionales de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

En este sentido, se recomienda avanzar en la formalización de la identificación y gestión de riesgos asociados al manejo de software licenciado dentro del proceso de Gestión de Tecnologías de la Información y de las Comunicaciones, con el fin de incorporarlos en la matriz institucional de riesgos y definir controles, responsables y mecanismos de seguimiento que fortalezcan la gestión preventiva frente a posibles incumplimientos en materia de derechos de autor de software.

5.11. Plan de continuidad de negocio asociado a la operación del software institucional

En atención al requerimiento relacionado con la existencia de un plan de continuidad de negocio que permita mantener la operación de los sistemas y servicios tecnológicos ante incidentes o fallas en el funcionamiento del software institucional, la Oficina de Tecnologías de la Información y las Comunicaciones informó que durante la vigencia 2026 se inició la construcción y estructuración del Plan de Continuidad de Negocio, como parte de las actividades de fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) y del proceso de mejora continua en la gestión de riesgos tecnológicos de la entidad.

De acuerdo con lo manifestado por el proceso, dicho plan contempla la definición de escenarios de interrupción de servicios, mecanismos de recuperación operativa y la asignación de roles y responsabilidades para la gestión de incidentes que puedan

afectar la disponibilidad o funcionamiento de los sistemas y servicios tecnológicos institucionales.

Adicionalmente, se indicó que, para las soluciones tecnológicas adquiridas mediante procesos contractuales, los proveedores de licenciamiento y servicios tecnológicos asumen compromisos asociados al cumplimiento de Acuerdos de Niveles de Servicio (ANS), los cuales incluyen aspectos como disponibilidad del servicio, soporte técnico especializado, tiempos de respuesta y recuperación ante fallas, así como el restablecimiento de servicios o licencias en caso de incidentes operativos.

En este sentido, se recomienda continuar avanzando en la estructuración, formalización y adopción del Plan de Continuidad de Negocio institucional, con el fin de consolidar un marco integral que permita gestionar de manera estructurada la continuidad de los servicios tecnológicos y del software que soporta la operación de la Región Metropolitana Bogotá-Cundinamarca (RMBC).

6. Respuesta a requerimientos de la Dirección Nacional de Derecho de Autor – DNDA y aspectos relacionados

De conformidad con los lineamientos emitidos por la Dirección Nacional de Derecho de Autor (DNDA) en relación con la verificación del uso legal de software en las entidades públicas, y con base en la información suministrada por la Oficina de Tecnologías de la Información y las Comunicaciones, se presentan a continuación las respuestas a los requerimientos formulados, así como otros aspectos relevantes asociados al cumplimiento de la normativa sobre derechos de autor de software en la Región Metropolitana Bogotá-Cundinamarca (RMBC).

Pregunta	Respuesta OTIC
1. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?	La entidad ha implementado mecanismos de control preventivos y restrictivos para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva. Entre estos mecanismos se encuentra la gestión centralizada de dispositivos y usuarios, la restricción de privilegios de instalación y el uso de herramientas de seguridad de endpoint como Microsoft Defender, mediante la configuración de reglas de reducción de superficie de ataque y el bloqueo de ejecutables no autorizados. Estos mecanismos permiten disminuir el riesgo de instalación y ejecución de software no licenciado en los equipos institucionales.

<table>
<tr><th>Pregunta</th><th>Respuesta OTIC</th></tr>
<tr><td></td><td>
<table>
<tr><th colspan="6">Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas</th></tr>
<tr><th>Mecanismo de control</th><th>Herramienta / Plataforma</th><th>Descripción técnica del control implementado</th><th>Tipo de control</th><th>Alcance</th><th>Evidencia asociada</th></tr>
<tr><td>Restricción de privilegios de instalación</td><td>Microsoft Intune</td><td>Asignación de perfiles de usuario estándar sin privilegios de administrador local. Solo personal autorizado cuenta con permisos elevados para instalación de software.</td><td>Preventivo / Restrictivo</td><td>Equipos de usuario final administrados</td><td>Políticas de Intune, grupos dinámicos y documento de control de privilegios</td></tr>
<tr><td>Control de instalación de aplicaciones</td><td>Microsoft Intune</td><td>Aplicación de políticas que restringen la instalación de aplicaciones fuera de los canales autorizados y controlan el cumplimiento del dispositivo.</td><td>Preventivo</td><td>Equipos administrados por MDM</td><td>Perfiles de configuración y reportes de cumplimiento</td></tr>
<tr><td>Gestión de identidades y roles</td><td>Microsoft 365</td><td>Gestión centralizada de cuentas, limitando la creación y uso de usuarios administradores y separando roles entre usuarios finales y personal de soporte.</td><td>Restrictivo</td><td>Usuarios institucionales activos</td><td>Configuración de roles y políticas de seguridad</td></tr>
<tr><td>Bloqueo de ejecutables no autorizados</td><td>Microsoft Defender</td><td>Configuración de reglas de reducción de superficie de ataque (ASR) para bloquear la ejecución de instaladores y ejecutables no autorizados.</td><td>Preventivo / Detectivo</td><td>Equipos con protección de endpoint</td><td>Alertas de bloqueo y reportes de eventos de seguridad</td></tr>
<tr><td>Inventario y detección de software</td><td>GLPI + Agente</td><td>Inventario automático del software instalado que permite identificar aplicaciones sin licenciamiento y soportar acciones de desinstalación o regularización.</td><td>Detectivo / Correctivo</td><td>Equipos con agente instalado</td><td>Reportes de inventario y registros en GLPI</td></tr>
</table>
</td></tr>
<tr><td>2. ¿Cuál es el destino final que se le da al software dado de baja en la entidad?</td><td>Mediante memorando No. 202601600004403 la OTIC solicitó a la dependencia responsable el envío de la información. La Subdirección de Gestión Corporativa remite respuesta mediante memorando 202604000004963 así: “Durante la vigencia 2025 no se realizó la baja de ningún software, por lo tanto, no existe inventario de software dado de baja correspondiente a dicho período.”

Observación OCI: Frente a esta respuesta, se evidenció que durante la vigencia 2025 no se registraron procesos de baja de software en la entidad; no obstante, se recomienda documentar formalmente el procedimiento institucional para la gestión y disposición final de software dado de baja, con el fin de establecer lineamientos claros para su desinstalación, control de licencias y registro en los inventarios tecnológicos cuando esta situación se presente.</td></tr>
<tr><td>3. ¿Cómo se verifica que el software instalado en todos los equipos que utilizan los funcionarios y contratistas de la entidad se encuentre debidamente licenciado?</td><td>La verificación de que el software instalado en los equipos utilizados por funcionarios y contratistas se encuentre debidamente licenciado se realiza a la través de un proceso de control continuo. Este proceso se soporta en el inventario automático generado por GLPI, el cual permite identificar las aplicaciones instaladas en cada equipo, y en los reportes de cumplimiento y estado generados por Microsoft Intune. La información obtenida es contrastada con el software autorizado y las licencias disponibles, permitiendo identificar desviaciones y</td></tr>
</table>

Pregunta	Respuesta OTIC
	soportar acciones de regularización o desinstalación cuando aplica. El proceso de verificación del software instalado se realiza de manera periódica y continua mediante el uso de GLPI con agente, el cual permite el levantamiento automático del inventario de aplicaciones por equipo (nombre, versión, editor y dispositivo asociado); complementariamente, a través de Microsoft Intune se valida el estado de cumplimiento de los dispositivos administrados, asegurando la correcta aplicación de políticas institucionales y la restricción de privilegios de instalación a los usuarios; de forma paralela, Microsoft Defender permite la detección, bloqueo y registro de intentos de ejecución de software no autorizado mediante el monitoreo continuo de alertas y eventos de seguridad; la información obtenida es contrastada por OTIC / Gestión de TI frente a las licencias adquiridas y autorizadas por la entidad, permitiendo identificar software licenciado y no licenciado, y, cuando aplica, ejecutar acciones correctivas como la desinstalación o regularización del licenciamiento, dejando trazabilidad completa mediante reportes de inventario, reportes de cumplimiento, alertas de seguridad, matriz de licenciamiento, registros de intervención y tickets asociados, garantizando que los equipos se mantengan en estado conforme.
4.¿ Qué actividades concretas se desarrollaron en la vigencia 2025 para sensibilizar a los funcionarios y contratistas de la RMBC sobre la no instalación de software no licenciado?	Durante la vigencia 2025, la Región Metropolitana Bogotá – Cundinamarca (RMBC), a través de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC), desarrolló actividades de sensibilización dirigidas a funcionarios y contratistas, orientadas a prevenir la instalación y uso de software no licenciado, en el marco del fortalecimiento de la seguridad digital institucional. • Capacitación – Socialización de la Política de Seguridad Digital, Privacidad de la Información y Datos Personales • Capacitación en hábitos de seguridad digital (Oficina TIC – ColCERT)
5. ¿ Cuál es la documentación aplicable (políticas, procedimientos, manuales, guías, instructivos, etc.) que tiene definido la entidad con relación a Derechos de autor de software??	En atención a la solicitud relacionada con la documentación aplicable definida por la entidad en materia de Derechos de Autor de Software, se informa que la Región Metropolitana Bogotá – Cundinamarca cuenta con lineamientos establecidos dentro de su marco institucional de seguridad de la información, principalmente a través de los siguientes documentos:

Pregunta	Respuesta OTIC
	1. Política de Seguridad Digital, Privacidad de la Información y Datos Personales, la cual se puede visualizar en el siguiente link https://regionmetropolitana.gov.co/temas/politicas-lineamientos-manuales/politica-seguridad-digital-privacidad-informacion-datos. 2. Proceso Gestión de las Tecnologías de la Información y las Comunicaciones en el cual se encuentra identificado Mesa de Escalonamiento y Gestión Informática/8.3 Administración de Usuarios y Accesos.
6. Indicar cómo se gestionan los equipos asociados a personal retirado.	Mediante memorando No. 202601600004403 la OTIC solicitó a la dependencia responsable el envío de la información. La Subdirección de Gestión Corporativa remite respuesta mediante memorando 202604000004963 así: “Los equipos asociados a personal retirado se gestionan mediante la suscripción del Acta de Devolución de Bienes, en la cual se formaliza la entrega de los equipos asignados a la Entidad. Dicha acta es requisito obligatorio para la expedición de paz y salvo, garantizando la correcta devolución, verificación y control de los bienes institucionales.”

7. Cumplimiento de las Normas Internacionales de Auditoría, limitaciones, conflictos de interés y fortalezas evidenciadas.

Para la realización de este seguimiento, se aplicaron las Normas de Auditoría Generalmente Aceptadas en Colombia, teniendo en cuenta que las pruebas realizadas se efectuaron mediante muestreo selectivo, por consiguiente, no se cubrió la verificación de la efectividad de todas las medidas de control del proceso.

Aunado a lo anterior, se precisa que, durante el desarrollo, no se presentaron limitaciones, así como tampoco, se dio lugar a la presentación de conflicto de intereses que pudieran afectar o impedir su desarrollo y resultado.

Se precisa además que, debido a las limitaciones de cualquier estructura de Control Interno, pueden ocurrir errores e irregularidades que no hayan sido detectadas bajo la planeación y realización de la presente auditoría, es así como la Región Metropolitana Bogotá – Cundinamarca y las dependencias que la integran, son las responsables de establecer y mantener un adecuado Sistema de Control Interno y prevenir posibles irregularidades, de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión -MIPG//MECI-.

A la fecha del seguimiento la Región Metropolitana Bogotá -Cundinamarca, no cuenta con planes de mejoramiento resultantes de auditorías internas – Plan de Mejoramiento por Procesos- PMP y/o externas- Plan de Mejoramiento Institucional- PMI, sobre la materia de la presente auditoría.

8. Conclusiones: Hallazgos, Observaciones y/o Recomendaciones

En el desarrollo de la auditoría se identificaron situaciones y aspectos susceptibles de fortalecimiento, frente a los cuales se formularon recomendaciones que tienen como único fin generar oportunidades de mejora.

En este sentido, es pertinente precisar que:

I. *Las recomendaciones,* no están llamadas a establecer Plan de Mejoramiento, pero se invita a que sean evaluadas por el Líder del Proceso con el fin de ser tenidas en cuenta en la Entidad para generar oportunidades de mejora al proceso.

CONCLUSIONES

Como resultado del seguimiento realizado al cumplimiento de las disposiciones relacionadas con los Derechos de Autor de Software en la Región Metropolitana Bogotá-Cundinamarca (RMBC), se concluye lo siguiente:

1. Se evidenció que la entidad cuenta con inventario institucional de equipos de cómputo, el cual permite identificar la asignación de los activos tecnológicos a funcionarios y contratistas, facilitando el control administrativo sobre los equipos utilizados en la operación institucional.
2. Se verificó la existencia de contratos asociados al licenciamiento y servicios tecnológicos, los cuales respaldan el uso legal de herramientas tecnológicas implementadas por la entidad, incluyendo soluciones Microsoft, herramientas especializadas, licenciamiento de software y servicios asociados a la operación tecnológica.
3. Se evidenció la implementación de herramientas tecnológicas para el inventario, monitoreo y control del software instalado, tales como GLPI con agente de inventario, Microsoft Intune, Microsoft Defender y configuraciones de seguridad en Microsoft 365, las cuales permiten identificar aplicaciones instaladas en los equipos institucionales y fortalecer el control sobre el uso de software autorizado.
4. Se identificó la aplicación de controles técnicos orientados a restringir la

instalación de software no autorizado, mediante la gestión de perfiles de usuario estándar y la restricción de privilegios de administrador en los dispositivos institucionales, lo cual constituye un control preventivo frente a posibles riesgos asociados al uso de software sin licenciamiento.

5. Durante la vigencia 2025 no se registraron incidentes relacionados con instalación de software no autorizado o incumplimiento de condiciones de licenciamiento, de acuerdo con la información reportada por la Oficina de Tecnologías de la Información y las Comunicaciones y el monitoreo efectuado a través de herramientas de seguridad como Microsoft Defender y Microsoft Sentinel.
6. Se evidenció que la entidad adelanta acciones orientadas al fortalecimiento de la gestión tecnológica y la seguridad de la información, incluyendo actividades de sensibilización dirigidas a funcionarios y contratistas sobre el uso responsable del software institucional.
7. Se observó que algunos instrumentos de gestión asociados a la administración del software institucional, tales como el procedimiento formal para la gestión del ciclo de vida del software, la identificación de riesgos asociados al manejo de software licenciado y el Plan de Continuidad de Negocio, se encuentran en proceso de estructuración o fortalecimiento en el marco de la consolidación institucional y del desarrollo del Modelo de Seguridad y Privacidad de la Información (MSPI).

En términos generales, se evidencian avances en la implementación de controles tecnológicos y administrativos orientados al uso legal del software institucional; no obstante, se identifican oportunidades de fortalecimiento relacionadas con la formalización de procedimientos, la consolidación de mecanismos de control y la documentación de buenas prácticas en la gestión de activos tecnológicos.

RECOMENDACIONES

1. **Fortalecimiento documental del procedimiento asociado a la gestión del ciclo de vida del software institucional.** En atención a las observaciones presentadas por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC frente al informe preliminar, se evidenció que dicha dependencia se encuentra adelantando, en articulación con la Oficina Asesora de Planeación Institucional, la construcción del procedimiento asociado a la gestión del ciclo de vida del software institucional, el cual a la fecha del corte de la finalización de la etapa de socialización del informe preliminar se encontraba en proceso de revisión y validación.

   Así mismo, durante la auditoría se verificó que la entidad cuenta con controles tecnológicos y administrativos asociados a la gestión del software institucional,

tales como inventarios de software, herramientas de administración de dispositivos y restricciones para la instalación de software no autorizado.

En este contexto, se considera pertinente que el aspecto identificado se aborde como una recomendación orientada a continuar fortaleciendo la formalización, aprobación e integración documental del procedimiento dentro del sistema institucional de gestión, con el fin de asegurar la trazabilidad, estandarización y sostenibilidad del proceso y control institucional sobre la gestión del software y el cumplimiento de las disposiciones relacionadas con los derechos de autor de software.

2. **Fortalecimiento de la formalización del procedimiento institucional para la baja o desinstalación de software.** En el marco de la auditoría se identificó la conveniencia de fortalecer la formalización documental de los lineamientos relacionados con la baja, desinstalación o retiro de software instalado en los equipos institucionales, con el fin de asegurar la trazabilidad y adecuada articulación entre las dependencias responsables de los procesos de la gestión de las tecnologías de la información y las comunicaciones y el de gestión administrativa (Administración de Bienes).

   Frente al informe preliminar, en etapa de socialización, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC informó que cuenta con mecanismos operativos para la administración y control del software instalado, tales como inventarios de software, herramientas de gestión de dispositivos y registros de solicitudes tramitadas a través de la mesa de servicios institucional, lo cual permite realizar intervenciones controladas y mantener trazabilidad sobre los cambios efectuados en los equipos.

   Así mismo, la Subdirección de Gestión Corporativa indicó que, teniendo en cuenta que durante la vigencia evaluada no se presentaron procesos de baja asociados específicamente a software, y considerando que los procedimientos de baja de activos corresponden a procesos administrativos y contables bajo su competencia, analizará conjuntamente con la Oficina de Tecnologías de la Información y las Comunicaciones la pertinencia de estructurar y formalizar lineamientos institucionales que definan los parámetros para la baja y trazabilidad del retiro de software, en el marco de las responsabilidades atribuidas a cada dependencia.

   En este contexto, se formula la presente recomendación orientada a continuar fortaleciendo la documentación y formalización de los procedimientos institucionales relacionados con la gestión, retiro o sustitución de software, definiendo claramente responsabilidades, actividades y puntos de control, con el fin de garantizar uniformidad en su aplicación y fortalecer los mecanismos institucionales de control sobre los activos tecnológicos.

3. Continuar fortaleciendo las actividades de sensibilización dirigidas a funcionarios y contratistas sobre el uso legal del software y los riesgos asociados a la instalación de aplicaciones no autorizadas, con el fin de promover una cultura institucional orientada al cumplimiento de las disposiciones en materia de derechos de autor.
4. Consolidar en un instrumento de control centralizado la información relacionada con el inventario de software y licenciamiento institucional, incluyendo reportes periódicos generados por las herramientas tecnológicas implementadas por la entidad, con el fin de facilitar el seguimiento al cumplimiento de las condiciones de licenciamiento.
5. Se recomienda continuar consolidando en un punto único de control la información asociada a los contratos de licenciamiento y servicios tecnológicos, incorporando variables como objeto contractual detallado, valor, plazo de ejecución, fecha de inicio y terminación, supervisor designado y estado del contrato, con el fin de facilitar la trazabilidad, seguimiento y control integral del licenciamiento tecnológico institucional, lo cual permitirá tener mayor control del software instalado en los equipos de la Entidad y su vigencia.
6. Se recomienda mantener documentada los controles de configuraciones de las licencias de los equipos de cómputo, así como realizar revisiones periódicas de los miembros con privilegios elevados y conservar evidencias de los cambios efectuados, con el fin de fortalecer la trazabilidad y el control institucional sobre la restricción de instalación de software en los equipos de la Región Metropolitana Bogotá-Cundinamarca (RMBC).
7. Continuar fortaleciendo la identificación y gestión de riesgos asociados al manejo de software licenciado, incorporándolos en la matriz institucional de riesgos y definiendo controles y mecanismos de seguimiento que permitan prevenir posibles incumplimientos en materia de derechos de autor.
8. Continuar con el proceso de estructuración y adopción del Plan de Continuidad de Negocio institucional, con el fin de fortalecer la capacidad de la entidad para garantizar la continuidad de los servicios tecnológicos ante posibles incidentes o interrupciones operativas.

Elaboró el informe:

Crhistian Augusto Amador León
Auditor Líder

Revisó y aprobó:

Andrea Reyes Saavedra
Jefe Oficina de Control Interno