

Nº INFORME: OCI-2024-012

PROCESO O SUBPROCESO O ACTIVIDAD:

Informe de derechos de autor vigencia 2023

EQUIPO AUDITOR

Diana Elizabeth Patiño, Contratista – Contratista Oficina de Control Interno

LÍDER DEL PROCESO: Dirección Corporativa y Dirección de TIC

OBJETIVO (S)

1. Verificar el cumplimiento de la normativa legal vigente en materia de derechos de autor.
2. Revisar la correcta administración de los equipos de cómputo y licencias de software.
3. Validar el cumplimiento de los lineamientos establecidos por la entidad en relación con los mecanismos de protección utilizados para controlar de forma continua la instalación de software no autorizado.
4. Verificar la destinación final del software que se da de baja dentro de la entidad.

ALCANCE

Verificar que la entidad, para la vigencia 2023, haya realizado un inventario actualizado de los equipos de cómputo, tanto propios, como en alquiler. Asimismo, validar las acciones adelantadas para prevenir el uso no autorizado de software y el destino final del que se da de baja.

LIMITACIONES AL ALCANCE

Para el trabajo desarrollado no se presentaron limitaciones

CRITERIOS

- Circular externa No 027 de 2023 de la Unidad Administrativa Especial de Derechos de Autor mediante la cual se decreta «Modificación Circular 017 del 01 de junio de 2011, sobre recomendaciones, seguimientos y resultados sobre el cumplimiento de las

normas en materia de derechos de autor sobre programas de computador (software).»

- Directiva Presidencial No 002 de 2002. Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
- Manual de Políticas de Seguridad y Privacidad de la Información, M-DA-001 versión 6, diciembre de 2022.
- Protocolo para gestionar el uso de los medios removibles, T-DT-003, Versión 2, diciembre 2023.
- Instalación y desinstalación de software, P-DT-016, Versión 0, enero de 2019.
- Procedimiento Compra y Actualización de Software, P-DT-005, Versión 2, enero de 2019.

DESCRIPCIÓN DEL TRABAJO REALIZADO:

Para verificar el cumplimiento de la Directiva Presidencial 002 del 2002 y la Circular Externa 027 de 2023, respecto del uso legal de software, la Oficina de Control Interno solicitó el 19 de febrero tanto a la Dirección Corporativa, como a la Dirección de TIC, la siguiente información

1. Listado de los equipos de cómputo adquiridos por la entidad mediante compra como en arrendamiento, con información actualizada hasta el 31 de diciembre de 2023.
2. Confirmar a través de T-DOC (herramienta de gestión documental oficial de la entidad) si todo el software instalado en los equipos de cómputo asignados tanto al personal de planta como a los contratistas es legal.
3. Indicar los mecanismos de control que se han implementado en la entidad para evitar por parte del personal de planta y contratistas la instalación de software no autorizado.
4. Especificar cuál es el destino final del software que es eliminado en la entidad.

Con base en lo anterior, la Oficina de Control Interno llevó a cabo una verificación tanto en sitio, como documental de la información suministrada por las áreas el 24 de febrero y diligenció lo solicitado por la Dirección Nacional de Derechos de Autor.

RESULTADO DEL INFORME DE SOFTWARE:

De acuerdo con la información solicitada por la Dirección Nacional de Derechos de Autor, mediante cuatro preguntas que se encuentran publicadas en su plataforma, se verificó la siguiente información:

Pregunta No 1: ¿Con cuántos equipos cuenta la entidad?

En el año 2023, la entidad disponía de un total de 542 equipos, de los cuales 379 eran de propiedad de la entidad y 163 estaban arrendados bajo la orden de compra número CCE102971 con el contratista TECHNOLOGY WORLD GROUP SAS, según lo informado por la Dirección de TIC.

Así las cosas, se seleccionó una muestra de 41 equipos, incluyendo escritorios y portátiles, los cuales fueron verificados individualmente en términos de ubicación física, número de serie y el profesional responsable asociado, encontrando las siguientes situaciones:

- 5 equipos, equivalentes al 12% de la muestra seleccionada, están asignados a un funcionario distinto al registrado en el inventario de la Dirección Corporativa, pero sí coincidían con el inventario de la Dirección de TIC.
- 2 portátiles asignados al Técnico Administrativo de la Dirección de TIC no fueron ubicados.
- 1 portátil se encuentra registrado en el inventario entregado por la Dirección Corporativa señala que se encuentra asignado a un profesional que manifestó no tener ningún portátil a su cargo.
- Durante la pandemia de COVID-19, se entregó un portátil a un profesional de la Dirección Técnica de Buses. A pesar de que este profesional ya se ha incorporado nuevamente de manera presencial a la entidad, el equipo no ha sido devuelto, lo que impidió su verificación.

Teniendo en cuenta las situaciones observadas, queda claro que es necesario implementar un único inventario de activos tecnológicos por parte de la Dirección Corporativa y la Dirección de TIC. Esto permitirá identificar el estado de los equipos de cómputo, así como su asignación y ubicación física, facilitando su ubicación.

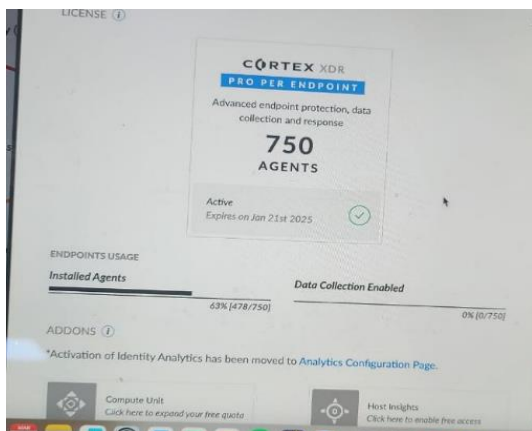
Pregunta No 2: ¿El software instalado en todos los equipos se encuentra debidamente licenciado?

Sea lo primero señalar que, de acuerdo con las funciones establecidas numeral 2, artículo 10 del Acuerdo No 4 de 2023¹, es función de la Dirección de Tecnologías de la Información y Comunicaciones la de «Liderar los procesos de desarrollo, mantenimiento y soporte de la plataforma de TIC's de la Empresa, velando por la funcionalidad, confiabilidad, oportunidad y seguridad de la operación del software, hardware y comunicaciones».

Así las cosas, mediante el memorando CI-30521-2024 la Dirección de TIC informó que todo el software de la entidad se encuentra legalmente instalado.

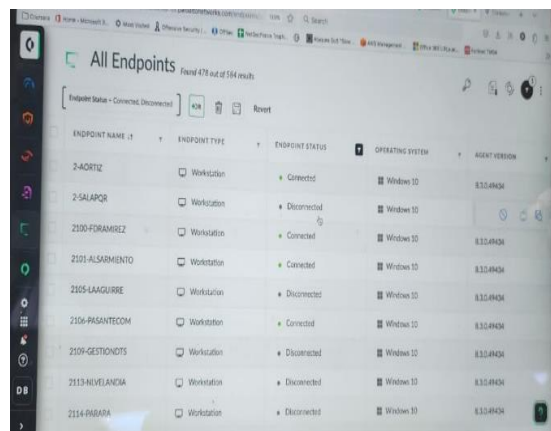
Por otra parte, la Dirección de TIC emplea la plataforma CORTEX, la cual está instalada en los equipos de cómputo proporcionados a los profesionales y contratistas de la entidad para monitorear la instalación de software no autorizado y detectar posibles amenazas mediante un análisis de comportamiento en los equipos. Asimismo, permite tomar medidas preventivas, como se ilustra en las siguientes imágenes:

Imagen Nro. 1



Cantidad de licencias instaladas de CORTEX

Imagen Nro. 2

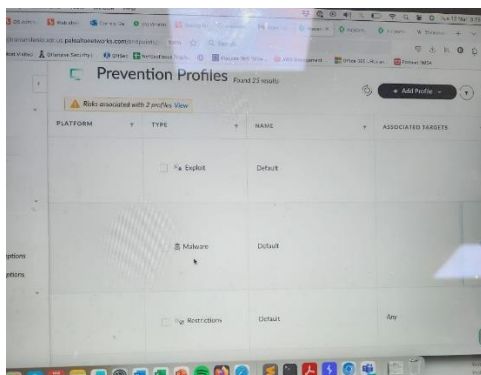


The screenshot shows the 'All Endpoints' dashboard in CORTEX. It displays a table with columns: ENDPOINT NAME, ENDPOINT TYPE, ENDPOINT STATUS, OPERATING SYSTEM, and AGENT VERSION. The table lists several endpoints, including 2-ACRIZ, 2-SALAPOR, 2100-FRANRREZ, 2101-ALSARMENTO, 2105-LAAGURRE, 2106-PASANTECOM, 2109-GESTIONOTS, 2113-ALVILANCIA, and 2114-PABARA. The status of each endpoint is indicated by a green dot for 'Connected' and a red dot for 'Disconnected'.

Usuarios parametrizados en la herramienta CORTEX

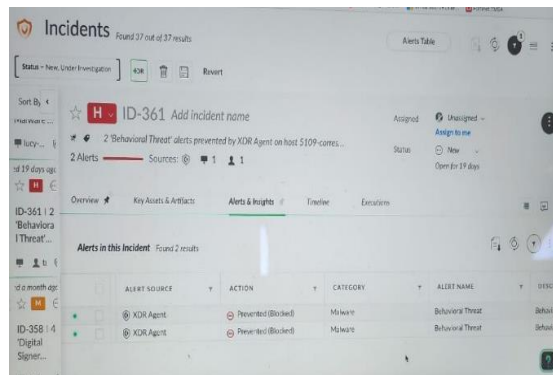
¹ «Por el cual se establece la estructura organizacional y las funciones de las dependencias de la Empresa de Transporte del Tercer Milenio – TRANSMILENIO S.A. y se dictan otras disposiciones»
Informe OCI-2024-012 Derechos de autor.

Imagen Nro. 3



Parametrización de la política de seguridad

Imagen Nro. 4



Monitoreo de incidentes detectados

Pregunta No 3: De forma concreta, por favor describa los mecanismos de control que se han implementado en su entidad para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva.

Conforme a la comunicación emitida por la Dirección de Tecnologías de la Información y Comunicación (TIC), la entidad ha consignado los siguientes documentos como instrumentos para supervisar la instalación de software por parte del personal de planta y contratistas a quienes se les ha asignado un equipo de cómputo.

- Manual M-DT-001 Políticas de Seguridad y Privacidad de la Información versión 6 de diciembre de 2022.
- P-DT-016 Procedimiento Instalación y desinstalación de Software V.0 de enero de 2019.
- Protocolo para gestionar el uso de medios removibles, T-DT-003, Versión 2 de diciembre de 2023.

Con base en esta información y el inventario de activos tecnológicos proporcionado por las áreas, se seleccionó una muestra de 21 equipos de cómputo. Cada uno de ellos se evaluó individualmente para verificar el cumplimiento de las políticas, protocolos y procedimientos mencionados anteriormente, donde se encontraron las siguientes situaciones:

- En el 33% de la muestra, equivalente a 7 equipos, fue posible conectar una memoria USB, desde la cual se accedió y extrajo información del equipo. Este acceso no estaba autorizado por el jefe inmediato o supervisor porque corresponde a equipos de cómputo que han sido reasignados a otros funcionarios y no fue configurado nuevamente en la herramienta de CORTEX con los nuevos permisos, lo que genera un incumplimiento al protocolo de medios removibles.
- En 2 equipos con número de placa 1670021017 y 1670021533 se instaló software sin la autorización de un usuario administrador, lo que incumple lo definido en el Procedimiento de «Instalación y desinstalación de Software».

De acuerdo con lo anterior, se observan debilidades en los controles establecidos por la Dirección de TIC para la instalación de software no autorizado.

Pregunta No 4: De forma concreta, describa por favor cuál es el destino final que se le da al software dado de baja en la entidad.

Para la vigencia 2023 la entidad adquirió licencias de tiempo limitado, las cuales una vez llega a su fecha final son desactivadas por el proveedor.

Por otra parte, toda vez que los softwares son bienes intangibles, la Dirección Corporativa los ingresa al inventario del almacén con una fecha de finalización de vida útil y posteriormente son llevadas a los libros contables con un valor de cero (\$0).

Para la vigencia 2023, no se realizó ninguna baja de licenciamiento.

CONCLUSIÓN Y RECOMENDACIÓN

Tras verificar la información proporcionada por las áreas respecto de la cantidad de equipos de cómputo que se encuentran en la entidad y a los funcionarios a quienes se encuentran asignados, la Oficina de Control Interno pudo establecer que, si bien se está llevando a cabo una actualización de dicho inventario por parte de la Dirección Corporativa, es necesario asegurar su alineación con los datos de la mesa de servicios bajo la supervisión de la Dirección de TIC. Esto es fundamental para garantizar el cumplimiento de los lineamientos establecidos en el manual de inventarios M-DA-002 de noviembre de 2020.



INFORME DE AUDITORÍA



ALCALDÍA MAYOR DE
BOGOTÁ

Por otra parte, se han identificado debilidades en la aplicación de los controles definidos en el Manual de Política de Seguridad y Privacidad de la Información, así como en el Manual de Instalación y Desinstalación de Software, y en el Protocolo para Gestionar el Uso de Medios Removibles. Lo que garantiza la seguridad e integridad de la información de la entidad.

Teniendo en cuenta lo anterior, se recomienda implementar un plan de mejoramiento donde se incluya la actualización del inventario de activos tecnológicos, así como la actualización de los procedimientos, manuales y protocolos establecidos por la entidad para proteger la seguridad de la información ante la instalación de software no autorizado.

Los resultados del presente seguimiento fueron socializados durante las pruebas de recorrido con los profesionales de la Dirección corporativa y la Dirección de TIC.

Este documento se expide el día 13 de marzo de 2024, por parte de TRANSMILENIO y es firmado por Sandra Jeannette Camargo Acosta, jefe de la Oficina de Control Interno.

Sandra Jeannette Camargo Acosta

Jefe Oficina de Control Interno

Elaboró: Diana Elizabeth Patiño Sabogal, Contratista - Oficina de Control Interno.

Revisó: Luz Nelly Castañeda, Contratista - Oficina de Control Interno.