INFORME EJECUTIVO

AUDITORIA SOBRE USO DE SOFTWARE Y DERECHOS DE AUTOR

PERIODO DE EJECUCIÓN: Entre los días 17 de febrero y el 16 de marzo de 2020, se llevó a cabo evaluación sobre el uso de software y derechos de autor, de acuerdo con lo programado en el Plan Anual de Auditoría para el 2020.

OBJETIVO GENERAL: Verificar la existencia, aplicación de políticas y controles implementados para la prevención de instalación de software no autorizado, conforme a disposiciones normativas aplicables en materia de derechos de autor.

ALCANCE:

- Verificar la efectividad de los controles establecidos para asegurar la vigencia de licencias de software administradas por la entidad, según inventario de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC a 31 de diciembre de 2019.
- Revisar los controles aplicados frente al uso de software no licenciado y/o autorizado, relacionados con permisos para instalación de software, configuración de políticas en el directorio activo, monitoreo de software línea base, procedimientos para registro de licencias de software hecho en casa o a la medida, monitoreo y manejo de equipos no conectados a la red, entre otros.
- Verificar los controles establecidos por la entidad para asegurar la consistencia de información entre los diferentes sistemas de información que soportan el licenciamiento de software en la entidad (SAI/SAE vs OCS Inventory)
- Realizar seguimiento al cumplimiento de las acciones de mejora de los planes en gestión a 29 de febrero de 2020 para mitigar el riesgo de uso de software no autorizado.

EQUIPO AUDITOR: Jorge Eliecer Gómez Quintero - Jefe Oficina de Control Interno y Constanza Cárdenas Aguirre – Auditora de Sistemas.

METODOLOGIA APLICADA: Para el desarrollo de la auditoría sobre uso de software y derechos de autor, se aplicaron las técnicas de auditoria internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva.

PRINCIPALES REFERENTES NORMATIVOS

- Circular 17 de 2011 Dirección Nacional de Derechos de Autor
- Circular 12 de 2007 Dirección Nacional de Derechos de Autor
- Decreto 1499 de 2017 - MIPG
- Modelo de privacidad y seguridad de la información del MINTIC
- Circular 049 de 2007 Secretaría General alcaldía Mayor de Bogotá D.C.

CONCLUSIÓN

Como resultado del proceso de auditoría realizado al uso de software y derechos de autor, se pudo establecer que, en términos generales, la Entidad cumple con la normatividad y tiene mecanismos de control implementados para el control del software instalado, definición de la línea base de software no autorizado, trámite de bajas de software y seguimiento periódico al cumplimiento de las acciones establecidas planes de mejoramiento producto de auditorías.

En la evaluación se identificaron algunos aspectos de observación susceptibles de mejora, en cuanto a fortalecer continuamente los controles de monitoreo del software instalado en los equipos de cómputo que pudiese permitir no estar autorizado, de equipos que no se conectan a la red, conciliación periódica entre los sistemas de información SAI/SAE donde se administran los inventarios de equipos de la entidad vs OCS Inventory (herramienta que monitorea el software instalado en los equipos de cómputo conectados a la red), definición de fuentes de información para la administración de licencias, al igual que la actualización del mapa de riesgos operativo con sus respectivos controles para la gestión y administración de licenciamiento y uso autorizado de software.

Es de anotar que, como medidas de control, la Entidad tiene implementadas las siguientes:

- Configuración de políticas de seguridad desde el Directorio Activo para controlar la instalación de software en los equipos de cómputo.
- Definición de la línea base de software autorizado, identificado por la OTIC y con el cual se determinó la cantidad de software que requiere ser desinstalado de los equipos, actividad que se encuentra en proceso a un 51% de ejecución.
- Al momento de realizar la asignación de un equipo al usuario final se configura el perfil como usuario estándar sin permisos de administrador. Este perfil no puede cambiar configuraciones del equipo como tampoco realizar instalaciones de software.
- Los equipos asignados a desarrolladores o diseñadores que requieren perfil de Administrador localmente, realizan la solicitud por el correo electrónico a la OTIC con la justificación respectiva para que se les habilite el usuario con perfil de administrador.

A continuación, se relacionan aspectos observados y las recomendaciones formuladas como producto de la evaluación practicada:

- **Diferencias cantidad de equipos de cómputo entre el inventario registrado en SAI/SAE y los equipos de OCS Inventory (herramienta de gestión y administración del software)**

Observación No. 1:

Se evidenció que persiste la falta de integridad de la información almacenada en el sistema de inventarios SAI/SAE (fuente oficial de inventarios de la Secretaria General) y la herramienta técnica OCS Inventory (monitoreo de los equipos). Estableciendo que la Entidad no cuenta con un control efectivo conciliatorio que permita establecer la causa de brechas de información entre el Sistema de Administración de Inventarios (SAI/SAE) y la herramienta OCS Inventory que controla el software instalado en los equipos.

Existen 45 equipos de cómputo que estando ubicados en Bodega (fuente SAI) cuentan con registro de conexión a OCS Inventory y 819 equipos de cómputo que estando en Servicio (fuente SAI), no cuentan con registro en OCS Inventory, así:

ELEMENTO	SAI-BODEGA vs Registrado en OCS		SAI-SERVICIO vs Registrado en OCS		TOTAL
	NO en OCS	SI en OCS	NO en OCS	SI en OCS	
COMPUTADOR ESCRITORIO	15	14	51	36	116
COMPUTADOR PORTATIL	44	9	97	44	194
CPU	205	15	431	710	1361
PC ALL IN ONE	38	7	112	175	332
PC PARA GRABACION DE AUDIO	0	0	1	0	1
SERVIDOR *	14	0	127	0	141
UNIDAD CENTRAL DE PROCESAMIENTO	1	0	0	0	1
Total General	**317**	**45**	**819**	**965**	**2.146**

Recomendación:

Es necesario que la OTIC implemente un control de monitoreo periódico que permita contar con la conciliación de la información de equipos de cómputo y licencias de software (inventario SAI/SAE) con los equipos de cómputo y el software instalado que se monitorea a través de la herramienta OCS Inventory. Así como, definir controles complementarios para el monitoreo de equipos que no se conecten a la red, lo cual permitirá identificar oportunamente software no autorizado y tomar acciones a que hubiese lugar.

Asimismo, bajo el entendido que la Subdirección de Servicios Administrativos, tiene previsto realizar la toma y actualización de inventarios para ajustar la información en el sistema SAI/SAE se recomendó que a partir de dicha información se actualice la herramienta OCS Inventory y se asegure que todos los equipos de cómputo en servicio están siendo monitoreados y controlados por la herramienta.

- **Controles para la Instalación de Software en Equipos de Cómputo de la Entidad**

Se verificó la existencia de mecanismos de control para la instalación de software, entre otros, como: la configuración de políticas de seguridad en el Directorio Activo, validación en la OTIC de la existencia de licenciamiento y necesidad de uso para todo requerimiento de instalación de software, contratación del personal necesario en la OTIC para adelantar el proceso de desinstalación de software no autorizado en los equipos de la entidad y definición una única vez de la línea base de software autorizado para uso de la Entidad.

Observación No. 2:

Se encontraron algunas debilidades con respecto a la periodicidad en la ejecución y revisión de la línea base de software vs software instalado en los equipos, por medio de la herramienta OCS Inventory, monitoreo del software comercial instalado que no hace parte de la revisión periódica que se realiza con la herramienta OCS Inventory.

Recomendación:

Se considera importante definir una política sobre uso de software como parte integral de las ya existentes en el Manual del Sistema de Seguridad de Información vs.01, y fortalecer los procedimientos actuales, incluyendo actividades de control para la administración y gestión de las licencias de software, considerando entre otras, el monitoreo periódico del software vs la línea base definida, revisión del licenciamiento del software ofimática de Microsoft y conciliación de las diferentes fuentes de información existentes.

- **Fuentes de Información para la Administración de licencias adquiridas vs licencias instaladas en los equipos de cómputo**

Observación No. 3:

Se observó que la Entidad cuenta con diferentes sistemas, herramientas y/o archivos Excel para el registro, administración y control del software, tales como: Sistema de Inventarios SAI/SAE, Excel administrado por la OTIC, registro en GLPI de licencias existentes vs instaladas y por último la herramienta Tenant de Microsoft, que se considera fuente de control para la administración de las licencias adquiridas vs asignadas de Office 365 pero no es fuente de información de software en términos generales.

Observación No. 4:

Por otro lado, en una muestra de once (11) Sistemas de Información que están en funcionamiento, dos (2) de ellos no se encuentran relacionados en SAI/SAE y uno (1) aunque se encuentra registrado en el inventario no existe en la relación de licencias administrado por la OTIC (archivo Excel). Los Sistemas de Información son: Sistema Integrado de Gestión del Archivo y Correspondencia – SIGA, Sivic – Sistema de Información de Victimas del Distrito Capital, Biblioteca Jurídica Virtual – BJV (se encuentra en SAI y no en Excel de la OTIC debido a que es un software del área Jurídica).

Recomendación para las observaciones 3 y 4:

Es necesario fortalecer los controles en esta materia y llevar a cabo el proceso de conciliación de las diferentes fuentes de información existentes y desde la OTIC liderar de forma centralizada, la administración y actualización de las licencias de software de toda la Entidad.

- **Gestión de Riesgos y Controles sobre Licenciamiento de Software y Uso de Software Autorizado**

Observación No. 5:

El mapa de riesgos de los procesos Tecnológicos de la entidad, no se observó la identificación de riesgos y controles orientados a prevenir el uso de software no autorizado o licenciado.

Recomendación:

Se recomendó a la OTIC con acompañamiento de la Oficina Asesora de Planeación, actualizar lo más pronto posible el mapa de riesgos del proceso de esta dependencia, incluyendo la identificación de riesgos y controles asociados a la administración y gestión de las licencias de software, considerando los lineamientos de la norma ISO27001 numeral 6.1.

En atención a las observaciones identificadas y recomendaciones formuladas en el informe preliminar con radicado 3-2020-8502 del 27 de marzo de 2020, las dependencias objeto del proceso auditor establecieron las acciones de mejora dirigidas a subsanar las observaciones con el informe final, las cuales se registrarán en la herramienta Planes de Mejoramiento para el seguimiento periódico tanto por las dependencias responsables como por parte de esta Oficina.

Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborado por: Constanza Cárdenas Aguirre – Contratista, Auditora de Sistemas
Revisado y Aprobado por: Jorge Eliecer Gómez Quintero – Jefe Oficina de Control Interno