ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA GENERAL

# INFORME EJECUTIVO
# AUDITORÍA DE EVALUACIÓN DE LA EFECTIVIDAD DE LOS CONTROLES ESTABLECIDOS PARA EL USO DE SOFTWARE

1. Objetivo General: Verificar la existencia y aplicación de las políticas y controles establecidos para el asegurar el uso de software legal y autorizado en la Entidad, apoyando el cumplimiento de la normativa vigente en materia de derechos de autor.

2. Alcance: Evaluación de la efectividad de los controles establecidos para asegurar el uso de software licenciado o autorizado, mediante la verificación de una muestra de registros para el período comprendido entre enero y diciembre de 2018. Seguimiento al cumplimiento de los planes de mejora derivados de revisiones anteriores y gestionados en 2018 con este mismo fin.

3. Principales criterios:
   - Modelo de privacidad y seguridad de la información del MINTIC vs. 3.0.2
   - Procedimiento de Seguridad de la Información vs. 1.0.0.
   - Manual del Sistema de Seguridad de la Información vs. 01
   - Proceso de Gestión de Recursos Físicos (vs. 08) y procedimientos (Egreso o salida definitiva de bienes (vs.06) e Ingreso o entrada de bienes (vs.13)).
   - Proceso Gestión, administración y soporte de infraestructura y recursos tecnológicos (vs.11), procedimiento de Gestión de incidentes y requerimientos tecnológicos vs.11 y Guía Sistema de Gestión de Servicios vs.5.
   - Circular 049 de 2007 de la Secretaría General, por la cual se establecen instrucciones sobre el uso adecuado de Internet y del correo electrónico de la entidad
   - Circular 04 de 2006 Consejo Asesor del Gobierno Nacional, Circular 07 de 2005 DAFP, Circular 12 de 2007 Dirección Nacional de Derechos de Autor y Circular 17 de 2011 Dirección Nacional de Derechos de Autor; dónde se establecen directrices relativas al reporte de cumplimiento de normas de uso de software y derechos de autor sobre programas de computador.
   - Decreto 1499 de 2017 – MIPG, dimensión 7. Control Interno.

4. Conclusión General: Resultado de las verificaciones realizadas se observó que al Entidad cuenta con controles para prevenir el uso de software no licenciado o autorizado, tales como el monitoreo de licencias instaladas (Microsoft, Antivirus, Adobe y Sistemas Operativos de los equipos conectados a la red), el uso de herramienta *Tenant* donde se registran las licencias de Microsoft adquiridas vs las asignadas y la configuración del perfil del usuario "estándar" sin permisos de "administrador".

   No obstante lo anterior, se observó que los controles evaluados tiene una efectividad limitada y/o débil, debido a las siguientes situaciones:

- En la matriz de riesgos del proceso de "Gestión, administración y soporte de infraestructura y recursos tecnológicos ", no se han identificado riesgos de uso de software no autorizado o licenciado, por lo cual, los controles implementados para prevenir este tipo de riesgos, no se monitorean y valoran periódicamente para determinar su efectividad.

- Aún cuando la Entidad cuenta con una herramienta (OCS Inventory) para la administración del software instalado, no se ha implementado una actividad de monitoreo regular (frecuencia, responsable, alcance) que permita confirmar que el software que se reporta instalado esta herramienta, se encuentre debidamente autorizado y licenciado según las licencias de software vigentes y/o adquiridas.

  Aunado a lo anterior, se encuentra que la herramienta OCS Inventory no ha sido parametrizada para gestionar el licenciamiento a través de la misma (al encontrarse en proceso de actualización el inventario de software y licencias la Entidad) y esta misma herramienta no registra todos los equipos de cómputo en servicio (servidores, PCs que no se conectan a la red y equipos dispuestos para servicios en otras Entidades como RTVC y la EAN).

- En ausencia de una política de control de accesos que contemple los parámetros y directrices bajo los cuales deben gestionarse los roles de "administradores", no se cuenta con una configuración en el Directorio Activo para controlar los equipos y usuarios que cuentan con este rol, lo que ha permitido la descarga o instalación de software libre no autorizado y posibilita, el uso de software no licenciado.

- La ausencia de gestión centralizada de todas las compras de recursos de software y/o TI, posibilita que algunos contratos suscritos con esta finalidad, puedan describir de forma imprecisa el alcance u obligaciones específicas de los mismos, dificultándose la confirmación de su cumplimiento en los términos descritos en el contrato, orden de compra y/o anexo.

- El inventario de software no se encuentra debidamente actualizado y conciliado (adquirido vs instalado).

- Se observaron inconsistencias no justificadas entre la relación de bajas de software aportada por la Subdirección de servicios administrativos y la disminución de software registrada al corte de 2017 y 2018.

Derivado de lo anterior, la principal recomendación es incorporar en el plan de gestión de la OTIC, un programa de trabajo de corto y mediano plazo (recursos, actividades, plazos y responsables) que oriente al mejoramiento de la gestión de recursos de software y TI en los aspectos observados, considerándose actividades de seguimiento cuando menos de forma mensual, de tal forma que su desarrollo apoye el cumplimiento de las políticas de seguridad de la información adoptadas en la Secretaría General. Entre las actividades claves para la prevención y mitigación de los riesgos advertidos en este informe, se encuentra relevante considerar las siguientes:

- Finalizar en el corto plazo de las actividades iniciadas en 2018 para identificar el software y las licencias vigentes y conciliar los equipos en servicio vs. el reporte de inventario de la

Entidad, de tal forma que se posibilite determinar con certeza el estado actual de este inventario y parametrizar la herramienta OCS Inventory para implementar un control centralizado de monitoreo y gestión de licenciamiento.

- Implementar un control de monitoreo automático desde la herramienta OCS Inventory, asegurando que a todos los equipos de cómputo (PC Escritorio y Portátiles, PC All in One, servidores y CPU) que se encuentren en servicio, se les verifique periódicamente la pertinencia (licenciamiento y autorización) del software instalado. Con este mismo fin, implementar controles complementarios para los equipos que no se conecten a la red.

- Convenir entre la Subdirección de servicios administrativos y la Oficina de tecnologías de la información y las comunicaciones una denominación común del software adquirido, de tal forma que se posibilite la gestión articulada de la administración funcional (instalación y monitoreo) y operativa (asignación, inventario y baja) de este tipo de bienes.

- Fortalecer e instrumentalizar las políticas de seguridad de la información adoptadas por la Entidad, considerando la definición de los criterios con arreglo a los cuales se debe realizar la configuración centralizada del Directorio Activo para la administración y control de los perfiles de "administrador" en los equipos de cómputo.

- Actualizar, con acompañamiento de la Oficina Asesora de Planeación, la matriz de riesgos del proceso de "Gestión, administración y soporte de infraestructura y recursos tecnológicos" para que ésta disponga de las "actividades de control" previstas para i) evitar el uso de software no licenciado o autorizado y ii) asegurar la pertinencia de los recursos y servicios de TI adquiridos, según las directrices establecidas en el numeral 7.2.3 del MIPG. Con este mismo fin, considerar la incorporación en el proceso de contratación, de actividad de control consistente en la emisión de un concepto técnico que, en la etapa precontractual, apoye la descripción precisa de las necesidades de recursos tecnológicos sujetas de contratación.