MEMORANDO CI2018-003478

Bogotá, marzo 23 de 2018

PARA: **Dra. María Virginia Torres Cristancho**
Presidente de SAE

DE: **María del Pilar Mayor Varela**

ASUNTO: **Informe Ejecutivo Cumplimiento al Uso de Software Legal – Derechos de Autor**

Doctor(a): Dra. María Virginia:

En cumplimiento a lo reglamentado por la Ley 87 de 1993, el Modelo Estándar de Control Interno del Departamento Administrativo de la Función Pública - MECI 2014, de conformidad con lo proyectado en el Plan de Auditoria para la vigencia 2018, en lo concerniente al Rol de Evaluación y seguimiento encomendado a la Oficina de Control Interno, Normas de Auditoria Generalmente aceptadas, Normas internacionales de Auditoria y demás normas aplicables, de manera atenta me permito presentar informe ejecutivo Cumplimiento al Uso de Software Legal – Derechos de Autor

Previamente se solicitó mediante correo electrónico la información documental la Oficina de Gestión de la Información el Inventario de los equipos, documentación de las licencias que soportan su debida adquisición y uso, así como a la Gerencia de Talento Humano la relación de los colaboradores activos (planta y temporales). para su análisis y con base en ella, se procedió a verificar el software instalado, controles, riesgos existentes, y conocimiento de la Política de Seguridad de la Información.

Se realizó revisión IN SITU en los puestos de trabajo para una muestra de 120 equipos en Dirección Central, Regional Centro Oriente y vía remoto con la Regional Norte, correspondiente al 23% del total informado por la OGI (527 equipos).

Resultado de la evaluación mencionada, le remitimos un informe de la auditoria al dueño del proceso que se encuentra en cabeza de la Oficina de Gestión de la Información que contiene las oportunidades de mejora identificadas, las cuales ya fueron previamente comunicadas en la reunión de cierre realizada el día 15 de marzo de 2018 y remitidas mediante memorando interno No. CI2018-003454.

Fortalezas

- ✓ La SAE cuenta con políticas documentadas sobre la seguridad y administración de la información.
- ✓ Actualmente la SAE cuenta con directivas a nivel directorio para evitar la instalación del software, los usuarios de los equipos no cuentan con permisos de administrador del equipo, este último solamente lo tienen asignado los administradores de infraestructura IT y el personal tercer izado que presta soporte técnico.
- ✓ En el 2017 la SAE adquirió la herramienta de seguridad PCSECURE la cual permite controlar la instalación de software no autorizado mitigando el riesgo de que los usuarios realicen la instalación de software no licenciado o no autorizado.
- ✓ En la vigencia 2017 la SAE implementó el *"P-TE4-163 Procedimiento Control de Software versión 1 del 09-09-2017"*
- ✓ Se realiza el respaldo de la información, mediante copias de seguridad y se tiene implementado el uso de carpetas públicas para garantizar el correcto uso de la información y el backup diario.
- ✓ Se encuentra identificado el control de realizar verificaciones y validaciones previas de la disponibilidad de licencias para la asignación de nuevos usuarios - PE-TE4-094 Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica (Actividad 6).
- ✓ La SAE en el documento PE-TE1-164 Procedimiento Seguridad para los Computadores Institucionales" tiene establecido: *"realizar mensualmente el inventario de Hardware y Software, los archivos soportes de esta información se almacena en la carpeta compartida".*

Debilidades

- ✓ Debilidades sobre el buen manejo de la información de uso de la SAE.
- ✓ Falta de instalación en algunos computadores de la herramienta de seguridad PCSECURE.
- ✓ Inventario de HW SW con falencias (fechas, PCSECURE solo relaciona equipos encendidos)
- ✓ Procedimiento control Software no contempla actividades para la disposición final del Software dado de baja ni para dar traslado a la Gerencia Financiera para el registro contable.
- ✓ Activos tecnológicos dados de baja sin registro contable de la baja.

- ✓ Debilidad en la identificación de Controles y Riesgos al Proceso

OPORTUNIDADES DE MEJORA

INSTALACIÓN HERRAMIENTA PCSECURE

Se identificó que no se ha instalado en todos los computadores institucionales asignados, la herramienta de seguridad PCSECURE, la cual permite controlar la instalación de software no autorizado.

Riesgo: 1. Instalación de software sin licencia
2. Acceso no autorizado

DIVULGACIÓN DE LA POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Pese a la divulgación de la política de seguridad de la información que realiza la OGI y documentación de procedimientos, se presentan debilidades sobre el buen manejo de la información de uso de la SAE, al encontrar en la revisión a los computadores de los funcionarios: fotos, música, información personal.

Riesgo: 1. Uso inadecuado de los servicios de IT

INVENTARIO DE HARDWARE Y SOFTWARE

Se evidencia que el inventario mensual presenta inconsistencias dadas las diferentes fechas que toma, las cuales no se identifican como cierre mensual y que no refleja la totalidad de los equipos con que cuenta la entidad, dado que la herramienta de seguridad PCSECURE solo relaciona y extracta los equipos encendidos.

Riesgo: 1. Pueden ocurrir falencias en el inventario de activos informáticos
2. No tener la identificación de los activos de S.W y H.W

BAJA CONTABLE DEL SOFTWARE Y DISPOSICIÓN FINAL DEL SOFTWARE DADO DE BAJA

El Procedimiento Control de Software no contempla actividades para la disposición final del Software dado de baja, tampoco contiene las actividades para dar traslado a la Gerencia Financiera para el registro contable y estableció que en 2017 se dieron de baja activos tecnológicos y no se realizó el registro contable.

Riesgo 1. Se podría reportar información financiera inexacta tanto de SAE como de los activos del FRISCO (Sobrevaloración de la cuenta contable).
2. Puede ocurrir que no tenga fiabilidad de la integridad de información operativa que afecte la información Financiera.

CREACIÓN DE USUARIOS

Se observan usuarios creados que no cumplen con las características establecidas en el Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica.

Riesgo: 1. Puede verse afectado el control y la administración de usuarios que no corresponde con los parámetros definidos por la entidad.

RIESGOS DEL MACROPROCESO GESTIÓN DE LA INFORMACIÓN

Los riesgos operativos del Macro proceso de Gestión de la Información publicados no guardan concordancia con los procesos y procedimientos ni con los riesgos identificados en el Mapa de Riesgos (Versión aprobada a mayo de 2017.)

Riesgo: 1. Puede ocurrir inadecuado tratamiento de los riesgos que afectan el proceso.

CONCLUSIONES Y RECOMENDACIONES

- ✓ Se recomienda instalar la herramienta PCSECURE a todos los equipos de la entidad con el fin de minimizar el riesgo de instalación de software no licenciado o no autorizado y establecer controles de monitoreo para asegurar que todos los equipos cuenten con él y realizar verificación periódica del software instalado en los equipos.
- ✓ Modificar el Procedimiento Control de Software e incluir las actividades a realizar sobre el destino final que se le debe dar al software y actividades necesarias para realizar la baja contable. Así mismo, revisar el software que la Oficina de Gestión de la Información ha dado de baja tecnológicamente y remitir a Contabilidad el producto de la baja como soporte para el registro contable.
- ✓ Realizar los inventarios tanto de software como hardware con el fin de asegurar que realmente corresponden a los equipos y licencias adquiridas por la entidad y que su realización corresponda a las fechas establecidas para los respectivos cortes de información.
- ✓ Revisar y analizar el 100% de los usuarios creados que no cumplen con lo que establece el Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica y hacer los ajustes respectivos al usuario o al procedimiento.
- ✓ Realizar actualización de la matriz de riesgos de acuerdo con el macroproceso y los procedimientos vigentes con el fin de obtener un adecuado tratamiento de éstos.

- ✓ Reforzar la capacitación sobre las políticas se seguridad de información, teniendo presente la existencia de nuevos funcionarios, con el fin de crear conciencia en los procesos de Gestión de Información y uso de datos personales en los computadores de la Entidad.

Conforme al resultado de la Auditoria adelantada por parte de esta Oficina y aceptada por el dueño del proceso, de manera atenta, se solicitó al dueño de proceso elaborar un Plan de Mejoramiento con las acciones correctivas encaminadas a subsanar las acciones de mejoramiento en torno al proceso auditado y sean remitidas a la Oficina de Control Interno en un tiempo de diez (10) días hábiles para seguimiento y evaluación.

Es importante informar que no se presentó limitación alguna para realizar la revisión y el equipo auditor tuvo acceso a la totalidad de la información que soporta nuestra labor, sin que se hubiese presentado evento alguno que afectare el resultado de nuestras recomendaciones.

Cordialmente,

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

APROBÓ: Maria del Pilar Mayor Varela.
ELABORÓ: Blanca Nelly Sierra M.