Bogotá D.C., marzo 22 de 2019

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**

Doctora 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 2019, 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 correspondiente a la vigencia 2019

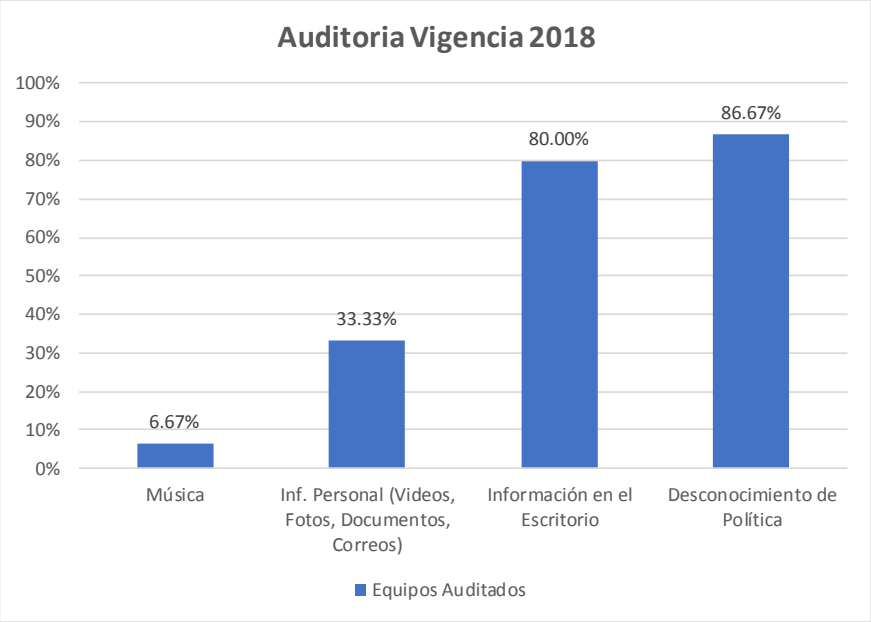
Previamente se solicitó mediante correo electrónico la información documental la Oficina de Gestión de la Información el Inventario de los equipos, documentación de las licencias que soportan su debida adquisición y uso, así como a la Gerencia de Talento Humano la relación de los colaboradores activos (planta y temporales). para su análisis y con base en ella, realizó la verificación de los programas instalados en cada uno de los equipos objeto de la muestra aleatoria frente a lo informado por la Oficina de Gestión de la Información, así mismo, se indagó a los usuarios de los equipos sobre el conocimiento y aplicación de las Políticas de Seguridad de la Información, el uso de los aplicativos que gestionan conforme a las funciones establecidas y el nivel de interiorización sobre el uso de la información de SAE.

Se realizó revisión IN SITU en los puestos de trabajo para una muestra de 60 equipos distribuidos entre Dirección Central, Regional Centro Oriente y vía remoto con la Regional Suroccidente, Regional Norte, Regional Occidente, que corresponde al 15% del número de equipos informados por la Oficina de Gestión de la Información según reporte extraído de la herramienta PCSECURITE (440 usuarios asociados a 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 2019 y remitidas mediante memorando interno No. CI2019-002945.

RESULTADOS OBTENIDOS:

Una vez realizada la revisión a la muestra seleccionada, las verificaciones y análisis de la información suministrada, se obtuvieron los siguientes resultados:



AÑO 2018	Música	Inf. Personal (Videos, Fotos, Documentos, Correos)	Información en el Escritorio	Desconocimiento de Política
Equipos Auditados	4	20	48	52
	7%	33%	80%	87%

Se logró evidenciar el desconocimiento o poco conocimiento del contenido, finalidad y ubicación del Manual Política de seguridad, por lo cual los usuarios a los cuales se les realizo la auditoria en campo de forma presencial o telefónica, manifestaron la falta de campañas, métodos o estrategias por parte de la entidad, para generar un sentido de recordación de las políticas establecidas para garantizar la seguridad de la información en todos los niveles de la organización.

Fortalezas

- ✓ Actualmente la SAE cuenta con directivas a nivel directorio activo para evitar la instalación del software estableciendo políticas locales en cada equipo que restringen a 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 contratista encargado de realizar las labores de Helpdesk en la entidad para brindar el soporte técnico. Sin embargo, se evaluará la eficacia de la herramienta PCSECURE.

- ✓ La SAE cuenta con políticas documentadas sobre la seguridad y administración de la información.

- ✓ La SAE cuenta con políticas y procedimientos establecidos para realizar 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.

- ✓ Los usuarios entrevistados en campo o remotamente cuentan únicamente con el acceso a los recursos tanto de red como aplicativos específicos según su rol y perfil en la organización.

- ✓ Los usuarios entrevistados informan que se da cumplimiento a la política establecida mensualmente respecto al cambio de contraseñas establecido para aplicativos y acceso al dominio del directorio activo.

- ✓ La SAE cuenta con la documentación actualizada y vigente respecto a las licencias adquiridas para el uso de aplicaciones y sistemas operativos con los que se soporta la operación.

Debilidades

- ✓ Falta de control de inventarios de Hardware y Software en razón a las diferencias encontradas una vez se compara la información reportada y extraída desde la herramienta PCSECURE contra el levantamiento de información realizado en conjunto entre la OGI y la entidad encargada de brindar el Helpdesk a la SAE.

- ✓ Se evidencia la no aplicabilidad a la política para la creación de usuarios de red respecto a la estructura definida en el procedimiento "*P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios*".

- ✓ Falta de estrategias de sensibilización para promover una cultura en seguridad de información la cual permita asegurar el correcto uso de los elementos dispuestos por la entidad para la consecución de los objetivos planteados.

- ✓ Debido a la existencia en los equipos de fotos, música, información personal, así como gran cantidad de información en el escritorio del computador, se presenta una debilidad en la aplicación de los lineamientos dados por la política de seguridad de la entidad los cuales se encuentra oficializados dentro del documento *"M-TE4-038_Manual Política de seguridad*" y "*P-TE4-163_Procedimiento para control de software*"

- ✓ Existencia de Software de código abierto en los equipos tomados como parte de la muestra.

- ✓ Uso indebido de los equipos y aplicaciones dispuestas a los funcionarios.

- ✓ Debido a la utilización del correo electrónico institucional para el uso personal, se podría maximizar el riesgo de divulgación de información de carácter confidencial a personas no autorizadas lo que afectaría directamente los costos reputacionales, la fuga o pérdida de información y el incumplimiento a la normatividad vigente establecida por la entidad.

- ✓ Desactualización del procedimiento "*P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios*" respecto a la inclusión de las políticas contables que incluyan hasta la disposición final de todo activo motivo de baja.

ADMINISTRACIÓN DE RIESGOS

Los riesgos analizados en la presente auditoría fueron tomados de la Matriz de Riesgos enero 2018 publicada en la página web de SAE y de la metodología interna de gestión del riesgo código G-DE2-001 versión 3 del 08/09/2016.

Adicionalmente, en el desarrollo del proceso auditor se identificaron unos posibles riesgos que podrían tener una probabilidad e impacto significativo en la Entidad, en la reunión de cierre fueron presentados a los auditados para su revisión, evaluación y si es del caso, inclusión en la matriz de riesgos interna.

	OPORTUNIDADES DE MEJORA	Riesgos	
1	Herramienta para Control de Inventarios	Pueden ocurrir falencias en el inventario de activos informáticos	Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.
		Falta de disponibilidades de los Servicios de IT	Riesgo: Moderado
2	Sensibilización de la Política Seguridad de la	Operación inadecuada de los sistemas de información	Riesgo: Moderado
		Filtro o utilización indebida de información privilegiada de los sistemas de información	Riesgo: Moderado
		Falta de conocimiento / capacitación en el uso de los servicios de IT	Riesgo: Alto
3	Creación de Usuarios de Red	Puede verse afectado el control y la administración de usuarios que no corresponde con los parámetros definidos por la entidad	Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.
		Falta de conocimiento / capacitación en el uso de los servicios de IT	Riesgo: Alto
4	Control y Seguimiento al Software en los Equipos de Usuarios	Operación inadecuada de los sistemas de información	Riesgo: Moderado
		Falta de conocimiento / capacitación en el uso de los servicios de IT	Riesgo: Alto
5	Control y Seguimiento al uso de los correos institucionales en los Equipos de Usuarios	Operación inadecuada de los sistemas de información.	Riesgo: Moderado
		Fuga o mal uso de datos personales	Riesgo: Moderado
		Perdida de información de datos personales	Riesgo: Moderado
		Falta de conocimiento / capacitación en el uso de los servicios de IT	Riesgo: Alto
6	Baja contable del software y disposición final del software dado de baja	Reportar información financiera inexacta tanto de SAE como de los activos del FRISCO (Sobrevaloración de la cuenta contable).	Riesgo: Alto
7	Control y Seguimiento a la instalación de Software en los Equipos de Usuarios	Instalación de Software sin Licencia	Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.
		Filtro o utilización indebida de información privilegiada de los sistemas de información	Riesgo: Alto

OPORTUNIDADES DE MEJORA

Con base en la información anteriormente descrita en el desarrollo del presente informe, se identificaron las siguientes observaciones y/o oportunidades de mejora y su respectiva calificación del riesgo:

Oportunidad de Mejora – Herramienta para control de Inventarios. Se identificó que la SAE no cuenta con una aplicación, herramienta o programa específico para el manejo y control de los inventarios de hardware y software en línea, ya que actualmente por medio de archivos en Excel se realiza control.

Riesgo: 1. Pueden ocurrir falencias en el inventario de activos informáticos *
2. Falta de disponibilidades de los Servicios de IT — Moderado

* *Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.*

Recomendación: Adquirir una herramienta que permita llevar el control de inventarios de hardware y software el cual tenga un módulo que se integre al sistema de información en desarrollo para la Gerencia Talento Humano con la finalidad de tener un engranaje actualizado en la información de cada empleado, junto con la información asociada al equipo, a los periodos de licencia, vacaciones, ausencias, inactividad entre otros, y así de esta manera se podría tener un mayor control sobre los activos físicos y lógicos.

Oportunidad de Mejora – Sensibilización de la Política Seguridad de la Información. Durante el 2018, la OGI realizo una jornada de capacitación sobre las políticas de seguridad de la información, sin embargo, los usuarios entrevistados durante el proceso de validación en campo o remoto, manifestaron en gran medida, el desconocimiento general de la información y de la ubicación del documento dentro de la intranet.

Riesgo: 1. Operación inadecuada de los sistemas de información — Moderado
2. Filtro o utilización indebida de información privilegiada de los sistemas de información. — Moderado
3. Falta de conocimiento / capacitación en el uso de los servicios de IT — Alto

Recomendación: Generar estrategias de sensibilización para promover una cultura en seguridad de información la cual permita asegurar el correcto uso de los elementos dispuestos por la entidad para la consecución de los objetivos planteados.

Oportunidad de Mejora – Creación de Usuarios de Red: Se observan usuarios creados que no cumplen con la estructura establecidas en el documento "*P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios.* "

Riesgo: 1. Puede verse afectado el control y la administración de usuarios que no corresponde con los parámetros definidos por la entidad. *
2. Falta de conocimiento / capacitación en el uso de los servicios de IT — Alto

* *Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.*

Recomendación: Revisar y analizar el 100% de los usuarios creados que no cumplen con lo que establece el *P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios* "y generar una jornada de corrección a los usuarios para dar cumplimiento a lo establecido en el procedimiento.

Oportunidad de Mejora – Control y Seguimiento al Software en los Equipos de Usuarios: Se observa la existencia de fotos, música, información personal, por lo que se evidencia una debilidad en la aplicación de los lineamientos dados

por la política de seguridad de la entidad los cuales se encuentra oficializados dentro de los documentos *"M-TE4-038_Manual Política de seguridad"* y "*P-TE4-163_Procedimiento para control de software*".

Riesgo: 1. Operación inadecuada de los sistemas de información. — Moderado
2. Falta de conocimiento / capacitación en el uso de los servicios de IT — Alto

Recomendación: Efectuar una revisión automatizada o manual de forma periódica por parte de la OGI para validar el cumplimiento de los lineamientos institucionales respecto al correcto uso y aprovechamiento de los equipos dispuestos por la entidad para el desarrollo de las tareas asociadas a cada usuario.

Oportunidad de Mejora – Control y Seguimiento al uso de los correos institucionales en los Equipos de Usuarios: Se observa el uso inadecuado del correo institucional para el envío y recepción de información personal de los funcionarios, lo cual está prohibido dentro de las políticas de seguridad de la entidad.

Riesgo: 1. Operación inadecuada de los sistemas de información. — Moderado
2. Fuga o mal uso de datos personales — Moderado
3. Perdida de información de datos personales. — Moderado
4. Falta de conocimiento / capacitación en el uso de los servicios de IT. — Alto

Recomendación: Establecer políticas de restricciones de dominios al momento de usar el correo institucional cuando los usuarios envíen correos a dominios no autorizados, informando mediante un correo a la cuenta origen un aviso sobre por qué no se efectuó el envío.

Oportunidad de Mejora – Baja contable del software y disposición final del software dado de baja: Durante la vigencia motivo de análisis y lo corrido del 2019, la entidad aún no ha puesto en marcha lo propuesto para el plan de acción referente al dar de baja contablemente el hardware y software junto con su disposición final, ni su articulación con la Gerencia Financiera. Así mismo está pendiente la actualización del procedimiento "*P-TE4-163_Procedimiento_para_control_de_software".*

Riesgo 1. Reportar información financiera inexacta tanto de SAE como de los activos del FRISCO (Sobrevaloración de la cuenta contable). — Alto

Recomendaciones:

1. Modificar "P-TE4-163_Procedimiento_para_control_de_software", con el fin de incluir las actividades que se deben realizar sobre el destino final que se le debe dar al software y para realizar la baja contablemente.
2. Revisar el software que se ha dado de baja tecnológicamente y remitir a Contabilidad el producto donde la OGI dio de baja el software como soporte para el registro contable.
3. Revisar la destinación final al software dado de baja anteriormente, para que se ajuste a lo que se establezca en la actualización del procedimiento.

Oportunidad de Mejora – Control y Seguimiento a la instalación de Software en los Equipos de Usuarios: Se observa la existencia software free en equipos motivo de análisis de la muestra aleatoria, por lo que pese a que existe la herramienta PCSECURE y a que por políticas del directorio se tiene restricción para instalar software en las máquinas, no deberían estar presentes las aplicaciones de libre distribución en las máquinas de la organización tal como lo establece el documento *"P-TE4-163_Procedimiento_para_control_de_software".*

Riesgo: 1. Instalación de Software sin Licencia *
2. Filtro o utilización indebida de información privilegiada de los sistemas de información — Alto

* *Este riesgo no se encuentra incluido dentro de la Matriz de Riesgos de la Entidad y se pone a consideración de los auditados para su revisión y evaluación.*

Recomendación: Efectuar un plan de acción para mitigar la presencia de software libre en los equipos de la entidad, así como la funcionalidad de la actual herramienta instalada en la entidad.

CONCLUSIONES Y RECOMENDACIONES

- ✓ Efectuar la implementación de un sistema de inventarios para evidenciar un impacto favorable en la OGI en razón al control en línea sobre la información de activos informáticos de la entidad. Así mismo con la implementación de una herramienta de control se podrá tener un registro actualizado de cada uno de los dispositivos que conforman la infraestructura tecnológica de la entidad.

- ✓ Contar con una integración entre el sistema de información usado por la Gerencia Talento Humano y la herramienta a implementar por parte de la OGI para el manejo de inventarios ya que de esta manera se podrá mantener actualizada la información de los empleados que tengan equipos tecnológicos asignados, sus periodos de inactividad, licencias, vacaciones, entre otros y de esa manera obtener un estado consolidado de la situación de cada trabajador y su máquina.

- ✓ Debido a la existencia en los equipos de fotos, música, información personal, así como gran cantidad de información en el escritorio del computador, generar planes de acción para mitigar la no aplicabilidad de los lineamientos dados por la política de seguridad de la entidad los cuales se encuentra oficializados dentro del documento *"M-TE4-038_Manual Política de seguridad*" y "*P-TE4-163_Procedimiento para control de software*"

- ✓ Establecer políticas de restricciones de dominios al momento de usar el correo institucional cuando los usuarios envíen correos a dominios no autorizados, informando mediante un correo a la cuenta origen un aviso sobre por qué no se efectuó el envío.

- ✓ Revisar y analizar el 100% de los usuarios creados que no cumplen con lo que establece el *P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios* "y generar una jornada de corrección a los usuarios para dar cumplimiento a lo establecido en el procedimiento.

- ✓ Generar estrategias de sensibilización para promover una cultura en seguridad de información la cual permita asegurar el correcto uso de los elementos dispuestos por la entidad para la consecución de los objetivos planteados.

- ✓ Efectuar una revisión automatizada o manual de forma periódica por parte de la OGI para validar el cumplimiento de los lineamientos institucionales respecto al correcto uso y aprovechamiento de los equipos dispuestos por la entidad para el desarrollo de las tareas asociadas a cada usuario.

- ✓ Realizar la actualización de los procedimientos pendientes por incluir la información requerida en la auditoria de la vigencia 2017 respecto a las actividades que se deben realizar sobre el destino final que se le debe dar al software y para realizar la baja contablemente.

- ✓ Efectuar un plan de acción para mitigar la presencia de software de código abierto en los equipos de la entidad, así como la funcionalidad de la actual herramienta instalada.

- ✓ Diseñar y ejecutar planes de mejoramiento a corto plazo, fundamentalmente para cerrar las oportunidades de mejora y observaciones de anteriores auditorias y dar cumplimiento a los procedimientos del proceso que

permitan el cierre efectivo de las mismas. Estos planes deben estar sujetos a una permanente evaluación, supervisión y monitoreo por parte del dueño del proceso.

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: María del Pilar Mayor Varela.
Elaboró: Guido Alexander Martínez Caceres