SAE ®
Sociedad de Activos Especiales S.A.S.

El emprendimiento es de todos

Minhacienda

MEMORANDO No CI2022-003850

Bogotá, 17 de marzo de 2022

PARA:
Giovanny Alejandro Lopez Insuasti
Jefe Oficina de Gestión de la información.

DE: María del Pilar Mayor Varela

ASUNTO: **Informe Final De Ley de Derechos de Autor**

Respetados Doctores:

Conforme al Plan Anual de Auditoría vigencia 2022 aprobado por Comité Institucional de Coordinación de Control Interno, la Oficina de Control Interno realizó informe de ley de derechos de autor.

Adjunto se remite informe final que contiene los resultados de la auditoría, los cuales fueron comunicados previamente mediante correo electrónico del 10 de marzo de 2022 y en reunión de cierre el 17 de marzo de 2022.

En cumplimiento de lo establecido en el procedimiento P-EC2-109- *Para la elaboración y seguimiento de planes de mejoramiento*, para las oportunidades de mejora, las áreas auditadas deben realizar un plan de mejoramiento en el formato F-EC1-177 y remitirlo a la Oficina de Control Interno dentro de los diez (10) hábiles siguientes a la recepción del presente documento.

Cordialmente,

María del Pilar Mayor Varela
Jefe Oficina de Control Interno

Copias: Andrés Alberto Avila Avila-Presidente SAE
Anexo: Informe final en Word

APROBÓ: María del Pilar Mayor Varela
ELABORÓ: Equipo auditor.

SOCIEDAD DE ACTIVOS ESPECIALES SAE S.A.S

OFICINA DE CONTROL INTERNO

INFORME CUMPLIMIENTO AL USO DE SOFTWARE LEGAL - DERECHOS DE AUTOR

VIGENCIA 2021

Bogotá, D.C. marzo de 2022

TABLA DE CONTENIDO

O1. OBJETIVO. (Norma desempeño 2210)..... 5
2. ALCANCE. (Norma desempeño 2220) 5
3. CRITERIOS Y FUENTES DE REVISIÓN. (Norma desempeño 2040)..... 5
4. METODOLOGÍA. (Norma desempeño 2310)..... 6
5. FORTALEZA. (Atributo desempeño 2300)..... 7
6. DEBILIDADES. (Atributo desempeño 2300) 7
7. LIMITACIONES EN EL DESARROLLO DE LA AUDITORIA. (Norma atributo 1130) ..... 8~~7~~
8. DECLARACION DEL AUDITOR. (Norma atributo 1100-1120-1220)..... 8
9. COMPROMISO DEL AUDITADO. (Norma desempeño 2420)..... 8
10. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN. (Norma atributo 1220) 8
11. DESARROLLO DE LA AUDITORIA. (Norma desempeño 2300) 8
12. RESULTADOS OBTENIDOS. (Norma desempeño 2300)..... 10
13. EVALUACIÓN DE CONTROLES Y RIESGOS. (Norma desempeño 2320) 18
14. CONCLUSIONES Y RECOMENDACIONES GENERALES. (Atributo desempeño 2400) 31

INTRODUCCIÓN

La Oficina de Control Interno en desarrollo de su función constitucional, lo descrito en el Plan Anual de Auditoria de la vigencia 2022 se practicó auditoría interna de gestión orientada a verificar la eficacia del Sistema de Control Interno institucional en las actividades de cumplimiento regulatorio en materia de la ley de derechos de autor.

Este ejercicio se realizó con base en las Normas Internacionales en materia de Auditoría Interna del Instituto Internacional de Auditores, Guía de auditoría para entidades públicas de la Función Pública las cuales incluyen planeación de la auditoría, ejecución del trabajo y generación del informe.

El proceso auditor incluyó la solicitud, análisis y verificación de información, documentación, evaluación de controles y riesgos asociados a los procedimientos evaluados. Con los resultados obtenidos del ejercicio se pretende contribuir al mejoramiento continuo de SAE.

INFORME VERIFICACIÓN AL CUMPLIMIENTO DEL USO DE SOFTWARE LEGAL PARA REPORTE ANUAL A LA DIRECCIÓN NACIONAL DE DERECHOS DE AUTOR

1. OBJETIVO. (Norma desempeño 2210)

Dar cumplimiento al reporte de información a la Dirección Nacional de Derechos de Autor, el cual requiere que los Representantes Legales y Jefes de Control Interno de las entidades de orden nacional y Territorial, remitan la información relacionada con la verificación, recomendaciones y resultados sobre el cumplimiento de las normas en materia de Derechos de Autor sobre software, en cumplimiento de la Directiva Presidencial No. 002 de 2002 y conforme con el procedimiento determinado en la Circular 17 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, ley 1915 de del 12 de Julio de 2018.

2. ALCANCE. (Norma desempeño 2220)

Verificación del software instalado, controles, riesgos existentes, y conocimiento de la Política de Seguridad de la Información de SAE, con base al inventario e información recibida por la Oficina de Gestión de la información, con corte a 31 de diciembre de 2021. Se realizó verificación a una muestra aleatoria de 33 NUC auditados mediante vía remota distribuidos entre Dirección Central, Regional Centro Oriente, Regional Suroccidente, Regional Norte y Regional Occidente.

Sede	Cantidad de Equipos
Calle 93	18
Calle 96	4
Regional Suroccidente	5
Regional Occidente	3
Regional Norte	1
Total	**33**

3. CRITERIOS Y FUENTES DE REVISIÓN. (Norma desempeño 2040)

- Directiva Presidencial No. 001 de 1999
- Directiva Presidencial No. 002 de 2002
- Ley 87 de 1993, por la cual "*se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones*".
- Constitución política de Colombia, artículo 209 en armonía con el artículo 269 establece la existencia de un control interno en todos los ámbitos de la administración pública.
- Ley 1474 de 2011. Normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y efectividad del control de la gestión pública, y se aplica específicamente frente a las medidas administrativas para la lucha contra la corrupción y el fortalecimiento del control interno en las entidades.
- Circular 17 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor.
- Política de Seguridad de SAE
- Procedimientos: P-TE4-163 Procedimiento control de Software, PE-TE4-094 Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica y PE-TE1-164 Procedimiento seguridad para dispositivos tecnológicos.

- Información remitida por el dueño del proceso, como por las áreas intervinientes dentro de la prueba de recorrido, las cuales cumplen con lo establecido en el Articulo 2.2.21.4.8 del Decreto 648 de 2018 Instrumentos para la actividad de la Auditoría Interna.
- Ley 1915 del 12 de Julio de 2018.
- Demás normas externas y políticas establecidas por la Organización frente a los temas evaluados.

4. METODOLOGÍA. (Norma desempeño 2310)

- La Metodología que se aplicó son las técnicas de auditoria tales como: solicitud y recopilación de información, revisión de los documentos fuente y entrevistas a los colaboradores del área respectiva.
- Se solicitó a la Oficina de Gestión de la información, el inventario de los equipos instalados en la entidad de acuerdo con el alcance de la auditoría. Listado de usuarios desde el directorio activo y programas instalados en cada uno de ellos, así como la documentación de las licencias que soportan su debida adquisición y uso.
- Se solicitó a la Gerencia de Talento Humano la relación de los colaboradores activos (planta y temporales).
- Debido al cambio de estructura actual de la SAE (de equipos de escritorio a terminales de trabajo) se realiza la verificación de programas instalados debido a que se maneja de manera centralizada en vez de una instalación individual por cada uno de los equipos. Así que se procede a realizar la verificación en cada uno de los ambientes preestablecidos en los equipos al conectarse con el servidor y su aplicación de licencias.
- Se indaga sobre la capacitación realizada sobre las políticas de seguridad de la información impartida a toda la organización mediante la plataforma de TEAMS.
- Se realizó cruce de la información de la planta de personal suministrada por la Gerencia de Talento Humano vs los usuarios suministrados por la OGI.
- Se realizó cruce entre los inventarios de software suministrados por la OGI.
- En revisión de las distintas sedes que cuenta la SAE (Calle 93, Calle 96, Medellín, Barranquilla y Cali) se realizaron mediante videollamada con diferentes colaboradores pertenecientes a la mesa de ayuda y soporte de la OGI. En esta videollamada se realizaba un paneo de la oficina y el auditor indicaba de manera aleatoria (sin conocer área donde se encontraba el equipo) cual terminal se revisaría.
- Para la revisión de software y su licenciamiento, se solicitó al administrador de la plataforma Citrix su apoyo para el ingreso
- La evaluación fue efectuada con base en las Normas de Auditoría Generalmente Aceptadas en razón a que contemplan los principios fundamentales en los que se deben enmarcar todas las actividades y el desempeño de los auditores durante el proceso de la auditoria ya que así se espera garantizar la calidad en la gestión realizada acerca del fortalecimiento del Sistema de Control Interno Institucional, a partir de la identificación de oportunidades de mejora y la formulación de recomendaciones con el fin de coadyuvar a la superación de las debilidades observadas, actividad que la Oficina de Control Interno desarrolla en cumplimiento a lo reglamentado por la Ley 87 de 1993, MECI, y de conformidad con lo proyectado en el Plan Anual de Auditoría vigencia 2022 de la Oficina de Control Interna de la Entidad, aprobado por el Comité Institucional de Coordinación de Control Interno, en el cual, establece las funciones de la Auditoría Interna como la de planear, dirigir y organizar la verificación y la evaluación del Sistema de Control Interno de la entidad
- La Oficina de Control Interno utilizará para el presente informe, los términos y definiciones establecidos en el procedimiento de Ejecución de Auditorías internas y Manual de Auditoría Interna, los cuales deben ser tenidos en cuenta para su entendimiento y posterior formulación de los planes de mejoramiento, a saber:

- **Oportunidad de Mejora:** Incumplimiento de un requisito técnico legal o funcional. Se constituye cuando existe evidencia objetiva del incumplimiento.

- **Observación**: Hecho o situación que podría generar el incumplimiento de un requisito.

- **Recomendación:** Se constituye como una oportunidad de mejora.

- **Acción de Mejora:** Acción emprendida para incrementar la eficacia, eficiencia y efectividad de los procesos y la satisfacción de los usuarios y otras partes interesadas.

5. FORTALEZA. (Atributo desempeño 2300)

- ✓ De la muestra realizada a treinta y dos (33) usuarios, en los cuales, no se evidenciaron fotos, documentos, archivos de música o correos de carácter personal en las terminales de manera local debido a la nueva estructura de ingreso a sesión.
- ✓ Se pudo evidenciar que la entidad prosigue con las políticas y procedimientos donde se establecen mecanismos de seguridad y almacenamiento de la información mediante el uso de carpetas públicas, con las respectivas medidas (backup en tiempos continuos diarios).
- ✓ Se verificó que los permisos aplicados a los usuarios desde la consola de administración de Citrix permiten únicamente con acceso a los recursos tanto de red como aplicativos específicos según su rol y perfil en la organización.
- ✓ De acuerdo con la información suministrada por la OGI se evidencia que la documentación se encuentra actualizada y vigente respecto a las licencias adquiridas para el uso de aplicaciones y sistemas operativos.
- ✓ El riesgo de una instalación de software o aplicativos no permitidos se ha mitigado debido a que por la centralización en la conexión de las sesiones no permite que los usuarios tengan aplicaciones o programas instalados dentro de sus respectivos perfiles.

6. DEBILIDADES. (Atributo desempeño 2300)

- ✓ En un porcentaje alto de la muestra revisada, se evidencio que en las terminales se pueden descargar archivos de cualquier tipo, incluidos ejecutables ".exe".
- ✓ Se encontraron procedimientos que no son aplicables y se encuentran desactualizados, publicados en la arquitectura empresarial.[1]
- ✓ Se evidencia deficiencia en la información suministrada por la OGI en cuanto al listado de usuarios, reportado por el área..
- ✓ Se observan funcionarios en el listado adjunto por parte de talento humano, los cuales no tienen usuario asignado por parte de la OGI.
- ✓ A pesar de la gestión por parte de la OGI, se observa ausencia de actualización y publicación de política de definición de usuarios.
- ✓ Se evidencia un error de activación de usuarios windows en Azure a la fecha de la auditoria.
- ✓ No se evidencia documentado dentro de la arquitectura empresarial el procedimiento que haga referencia al perfil y cantidad de usuarios que tengan autorización para el uso de office 365 por fuera del citrix.

[1] 12.2 DOCUMENTACIÓN PROCEDIMIENTOS

7. LIMITACIONES EN EL DESARROLLO DE LA AUDITORIA. (Norma atributo 1130)

No se presentaron limitaciones que impidieran el desarrollo de la auditoria.

8. DECLARACION DEL AUDITOR. (Norma atributo 1100-1120-1220)

La auditoría se realiza con base en el análisis de la información presentada y de la comunicación recibida en mesas de trabajo a través de la plataforma Teams, de acuerdo con lo estipulado en el Decreto 648 de 2017 Artículo 2.2.21.4.8, la Oficina de Control Interno incorpora los siguientes instrumentos para la Actividad de la Auditoría Interna:

i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, confianza, objetividad, confidencialidad, competencia profesional, responsabilidad y debido cuidado profesional e interés público y valor agregado.

ii. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

9. COMPROMISO DEL AUDITADO. (Norma desempeño 2420)

Dentro del aviso de la auditoría realizada a través de memorando interno No CI2021-014519 del 19 de octubre de 2021, se les manifestó a los líderes de los procesos auditados que en el marco de la auditoría interna de gestión y en cumplimiento del artículo 2.2.21.4.8 del Decreto 648 de 2017 "*Instrumentos de la actividad de la Auditoría Interna -Carta de representación",* toda la información suministrada a la Oficina de Control Interno debe cumplir con los criterios de veracidad, calidad y oportunidad.

10. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN. (Norma atributo 1220)

Este documento contiene información de interés exclusivo del auditor y el auditado para surtir los trámites establecidos en la Guía de Auditoria de la función pública acogida por la oficina de control interna de la SAE

En ese sentido, hasta tanto no se constituya como informe final y sea publicado en la página Web de la Sociedad de Activos Especiales SAE SAS, no podrá ser distribuido ni utilizado por terceros, ni se podrá hacer referencia a él en ningún otro asunto, sin el consentimiento previo y por escrito del Jefe de Control Interno.

11. DESARROLLO DE LA AUDITORIA. (Norma desempeño 2300)

Mediante citación por correo electrónico del 1 de febrero de 2022 dirigido al Jefe Oficina Gestión de la Información, se solicitó información referente al cumplimiento de la ley de derechos de autor.

La OCI adjunto un listado con un total de 360 equipos, al realizar el muestreo se obtuvo un total de 33 equipos para dicha revisión (considerando que actualmente se está trabajando en modo virtual debido a la emergencia sanitaria se realizó la revisión aleatoriamente de dichos usuarios), resultado que fue realizado a través de la caja de herramientas de la función pública adoptada por la OCI en la SAE.

La Sociedad de Activos Especiales SAE SAS ha venido operando desde el mes de junio del 2020 bajo la modalidad de alternancia, dentro de la nueva normalidad y autorizado por el Gobierno Nacional, la Oficina de Control Interno

llevó a cabo el ejercicio de auditoria mediante la modalidad presencial y el mecanismo de trabajo en casa, realizando la etapa de entrevistas con los auditados a través de la herramienta tecnológica Teams.

11.1 Riesgos evaluados. (Norma desempeño 2110)

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.	Operativo	Alto
Se podría presentar que la persona en el momento del retiro no haga la debida entrega del puesto de trabajo	Operativo	Alto
Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.	Operativo	Moderado
Podría ocurrir que se incumpla con la normatividad vigente	Operativo	Alto
Inconsistencias o Pérdida de la Información	Seguridad de la información	Extremo
Puede ocurrir que se presente fuga o pérdida de información.	Seguridad de la información	Alto
Se podría presentar secuestro de datos “Ransomware”	Seguridad de la información	Extremo

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Se podría presentar inventario y/o etiquetado desactualizado de equipos de cómputo y comunicaciones	Operativo	Este riesgo no está contemplado dentro del mapa riesgos de SAE

12. RESULTADOS OBTENIDOS. (Norma desempeño 2300)

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

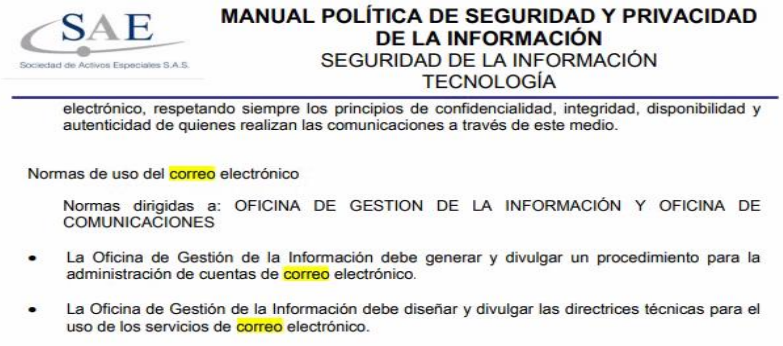
12.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en la Política de Seguridad de la Información en el cual establecen la creación por parte de la OGI de un procedimiento para la administración de cuentas de correo electrónico, a la fecha del informe se evidencia la ausencia del mismo.

La Política de seguridad de la Información es un compendio de documentos y estrategias donde se establecen las directrices para implementar desde un punto de vista lógico y físico, todos los aspectos relacionados con la seguridad y el control sobre la información, los cuales deben ser cumplidos por los directivos, funcionarios, colaboradores, contratistas y terceros en el adecuado cumplimiento de sus funciones, se logra evidenciar la 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.

Observación de la OGI: Solicito aclaración de este párrafo a que hace referencia la falta de estrategias dentro de la política de seguridad?

Análisis de la OCI:
Como se evidencia anteriormente no hay cumplimiento en la creación de un procedimiento para administración de correo electrónico enunciado en el manual política de seguridad y privacidad de la información, por lo anterior no se conoce la estructura definida para que existan demasiados usuarios con acceso por fuera de la arquitectura empresarial autorizados incluso por las mismas áreas y pueden constituir un alto riesgo de fuga o pérdida de información confidencial. Por lo anterior se mantiene la observación inicial dejada por la oficina de control interno.


MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
SEGURIDAD DE LA INFORMACIÓN
TECNOLOGÍA

electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

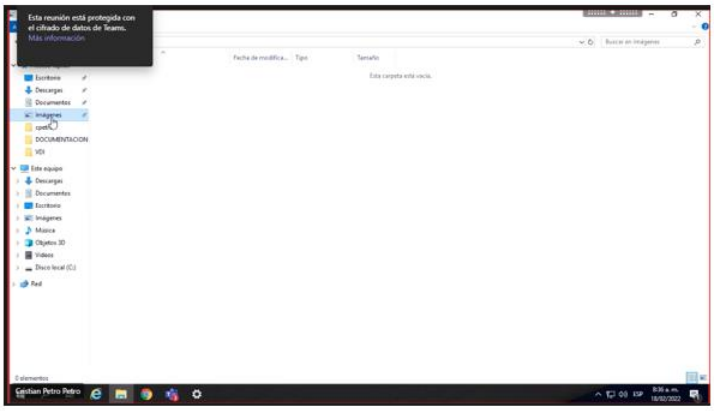
Normas de uso del correo electrónico

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN Y OFICINA DE COMUNICACIONES

- La Oficina de Gestión de la Información debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Oficina de Gestión de la Información debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

Fuente: Manual política de seguridad y privacidad de la información

Dentro de la muestra tomada para la realización de la presente auditoria, a diferencia de los resultados de la auditoría previa, en la revisión actual arrojo como resultados que no se encuentran existencia de archivos personales o no permitidos como lo son archivos de música, videos, imágenes o fotos, correos no corporativos o documentos personales. De la misma manera en la revisión de los posibles archivos guardados en escritorio se encontró que en las maquinas "terminales" no poseían archivos o iconos de programas no autorizados.



Carpetas personales de usuarios – **Fuente**: toma de pantalla equipo de auditoría Control Interno

Sin embargo, en la revisión se determina que si es posible realizar descargas de archivos y documentos dentro de la navegación local que permite la terminal, esto se observa en la carpeta "descargas" donde se pueden alojar archivos de diferente índole (incluyendo ejecutables). Es importante que este tipo de descargas sean restrictivas para así evitar un posible ataque mediante malware. De esta forma es necesario evaluar herramientas que permitan realizar el bloqueo de archivos ejecutables

Se realizó una capacitación en el año 2021 (como parte de las estrategias de divulgación y sensibilización de la OCI) donde se introdujo a los nuevos colaboradores y se reforzó a las políticas de seguridad de la información mediante la plataforma TEAMS y con alcance a toda la entidad. Para realizar la calificación de los conceptos explicados se realizó al finalizar la sesión un cuestionario con preguntas.

12.2. DOCUMENTACIÓN PROCEDIMIENTOS

Se procedió a revisar la documentación de los procedimientos que se encuentran publicados en la arquitectura empresarial en la intranet, respectivo a este tema se encontraron documentos y procedimientos desactualizados sobre esta nueva infraestructura. A continuación, se refieren los códigos.

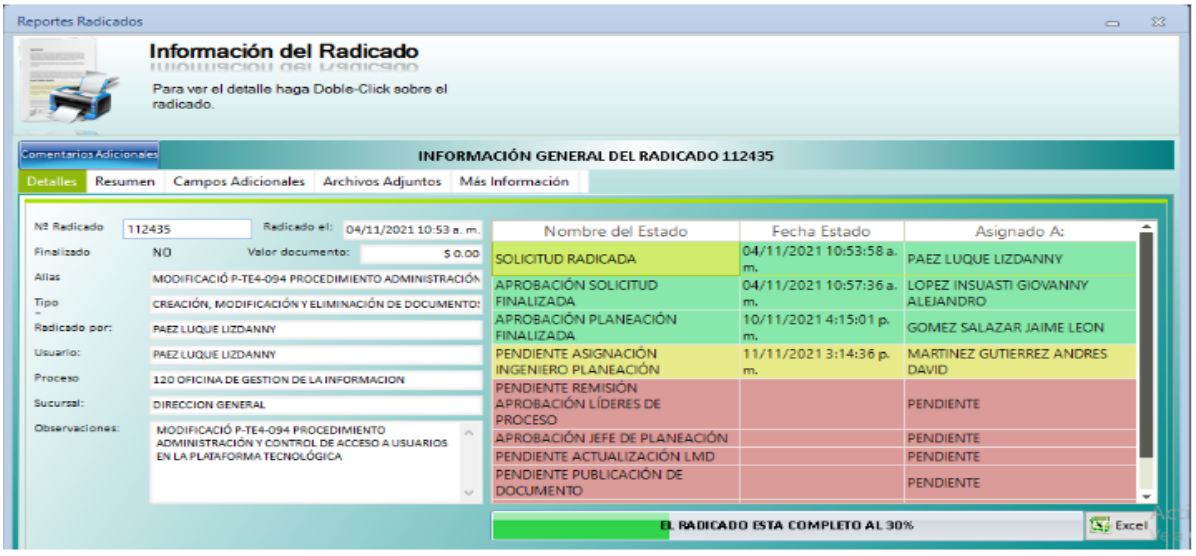
- P-TE1-203 - PROCEDIMIENTO DE MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA - Versión 1 - 19/08/2020: En concordancia con el punto anterior, el monitoreo debe cambiar debido que la organización cuenta con la plataforma CITRIX donde las máquinas de usuarios se monitorearían por la consola. Es importante que este aparte se explique dentro del procedimiento. Sigue sin actualización a febrero de 2022.
- N-TE1-017 - INSTRUCTIVO DE BORRADO SEGURO - Versión 3 – 19/02/2018: Debido al cambio de infraestructura tecnológica el instructivo ya no es aplicable, debido que el formateo de maquina en el momento de retiro de usuario ya no se practicable debido al nuevo esquema. A la fecha del informe (10 marzo de 2022) sigue sin actualización.
- P-TE1-164 - PROCESO DE GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA - Versión 2 – 16/10/2018. A la fecha del informe (10 marzo de 2022) sigue sin actualización.

12.3. CREACIÓN DE USUARIOS

A pesar de que el área de la OGI ha trabajado arduamente en la actualización de los procedimientos, siguen procedimientos sin actualizar.

En específico a pesar de que el procedimiento fue actualizado, mas no publicado según soportes del área de la OGI "P-TE4-094 Procedimiento Administración y Control de Acceso a usuarios" en la Plataforma Tecnológica establece: *"el usuario se creará con la siguiente estructura: primera inicial del nombre y el primer apellido, en caso de repetirse el usuario se tomará la primera y segunda letra del nombre y el primer apellido. En su defecto, en caso de repetirse con alguna de las dos opciones anteriores, se tomará la primera letra del primer y segundo nombre y el primer apellido",* se logró evidenciar en campo la no concordancia entre lo documental vs lo practico así:

- dcorreas (DANIELA CORREA SOTO)
- aquiroga (CINDY ALEJANDRA QUIROGA CATAÑO)
- lauhernandez (LAURA MATILDE HERNANDEZ CONSUEGR
- ehernandezb (HERNANDEZ BENAVIDEZ ESTEFANY)
- lhvizcaino (HERNANDEZ VIZCAINO LILIANA)
- mcardenasm (CARDENAS MUÑOZ MARISOL)
- mmoralesr (MORALES ROJAS MARLEN)
- ahernandeza (ADRIANA HERNANDEZ ALDANA)
- arodriguezr (ALEJANDRA RODRIGUEZ RODRIGUEZ)
- jvillamizal (JUAN CARLOS VILLAMIL PIZA)
- lsilva (JEIMMY LORENA SILVA FIGA)
- mrodriguezb (MILGUEL ANGEL RODRÍGUEZ BERNAL)



Fuente: Soporte entregado por el área de la actualización del procedimiento, pero sin ser publicado a la fecha de la revisión 16 Feb2021

Igualmente se encuentran usuarios que tienen errores en su nombre en relación con sus nombres y apellidos:

- apvanegas (Angelica Paola Vanegas Rojas – apellido según talento humano es Venegas)

- jvaldez (July Carolina Valdez Santofimio – apellido según talento humano es Valdés)

12.4. INVENTARIOS

Basados en el procedimiento "**P-TE1-164 Procedimiento seguridad para dispositivos tecnológicos**" en el cual se establece: "…*Mensualmente se realiza el inventario de Hardware y Software, los archivos soportes de esta información se almacena en la carpeta compartida…*". Al efectuar la verificación de la información correspondiente al inventario de software y hardware realizado por la OGI el cual se actualiza mensualmente, a Corte de 28 febrero de 2022 y no al corte de 30 de Diciembre de 2021, el inventario por ubicación fue el siguiente:

Ubicación	Mini PC	Notebook	QEMU	Total general
Archivo Central	28	1		29
Barranquilla	19			19
Cali	25	1		26
Calle 93	121	18		139
Calle 96	45	2		47
Medellin	22			22
OGI	24	3	51	78
Total general	**284**	**25**	**51**	**360**

Por la pandemia y las medidas de control adoptadas por la entidad, se realizó la revisión de manera remota de los diferentes equipos y sedes. Donde se revisó los programas instalados de manera local en cada una de las terminales. Debido a estas medidas de bioseguridad, en las sedes no están todos los puestos disponibles con equipos, por lo que el número que se encuentran instalados es más reducido que en una operación normal.

12.5. LICENCIAMIENTO DE SOFTWARE

Basados en el procedimiento "**P-TE1-164 Procedimiento seguridad para dispositivos tecnológicos**" en el cual se establece: "…*Mensualmente se realiza el inventario de Hardware y Software, los archivos soportes de esta información se almacena en la carpeta compartida…*". Al efectuar la verificación de la información correspondiente al inventario de software, hardware y usuario realizado por la OGI el cual fue remitido a la OCI tras solicitud formal, se evidencia lo siguiente:

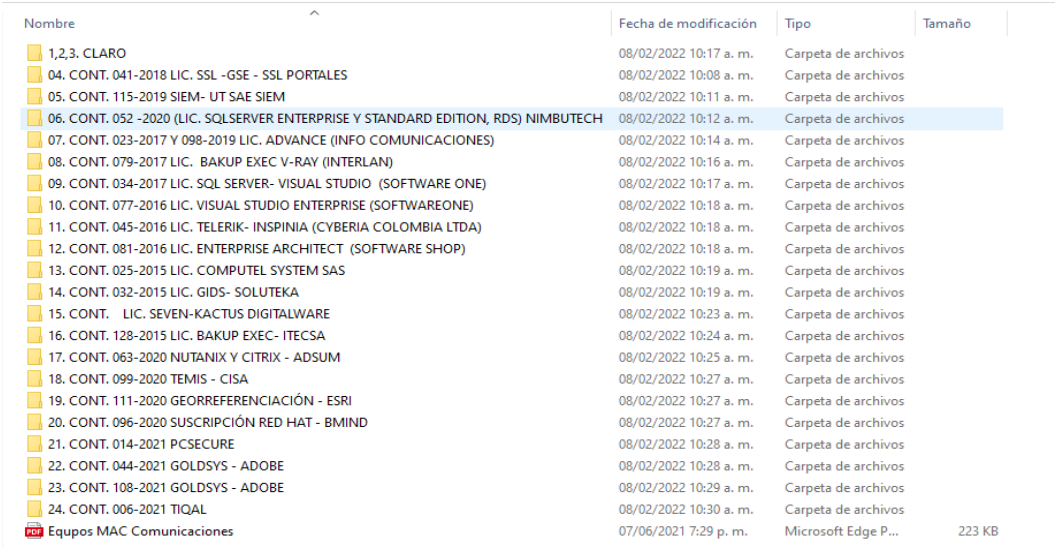
Item	Software	INSTALADAS SEGUN LISTADO	TIPO DE LICENCIA	CANTIDAD
1	7Zip	Libre	Libre	
2	Acrobat Pro	Sin evidencia en listado	Asignada	16
3	Acrobat Reader	libre	Libre	
4	Agentes Antivirus Kaspersky	Sin evidencia en listado	Por suscripción	332
5	Autodesk DWG TrueView	Sin evidencia en listado	Libre	
6	Azure Information Protector	Sin evidencia en listado	Por suscripción	Estan integradas con Office 365
7	Backup exec	Sin evidencia en listado	Asignada	5
8	Beyond Compare	Libre	Libre	
9	Centos 6	Libre	Libre	
10	Centos 7	Libre	Libre	
11	Centos 8	Libre	Libre	
12	Chrome, IE, Mozilla	Libre	Libre	
13	Citrix	Sin evidencia en listado	Por suscripción	400
14	Concisa	Sin evidencia en listado	Por suscripción	Ilimitada por derecho de uso
15	doPDF10	Libre	Libre	
16	Enterprise Archictect	Sin evidencia en listado	Recurrente	7
17	FileZila	Libre	Libre	
18	FirmayaDriver	Sin evidencia en listado	Asignada	El software es libre pero la asignación para uso es la firma digital que son 13
19	FortiClient VPN	Libre	Libre	
20	Fortinet DC agent	Sin evidencia en listado	Por suscripción	Estan integradas con la licencia de Fortigate
21	Fortinet FSSO	Sin evidencia en listado	Por suscripción	Estan integradas con la licencia de Fortigate
22	Fortinet TS agent	Sin evidencia en listado	Por suscripción	Estan integradas con la licencia de Fortigate
23	FusionInventory Agent	Libre	Libre	
24	GLPI	Libre	Libre	
25	Google Earth	Libre	Libre	
26	GoToMeeting	Libre	Libre	
27	Grass GIS	Libre	Libre	
28	IMC	Sin evidencia en listado	Por suscripción	Ilimitada por derecho de uso
29	IMS	Sin evidencia en listado	Por suscripción	ilimitada software propio
30	IPScanner 2.5	Libre	Libre	
31	Issabel	Libre	Libre	
32	Kactus	ASIGNADA	Por suscripción	600

Fuente: Reporte suministrado por la OGI

Item	Software	INSTALADAS SEGUN LISTADO	TIPO DE LICENCIA	CANTIDAD
33	KawaK	ASIGNADA	Por suscripción	
34	KeyStore Explorer	Libre	Libre	
35	Microsoft SQL Management Studio	Libre	Libre	
36	Microsoft SQL Report Builder	Libre	Libre	
37	MySQL	Libre	Libre	
38	MySqlWorkben 8	Libre	Libre	
39	Notepad++	Libre	Libre	
40	Npcap	Libre	Libre	
41	Nutanix	Sin evidencia en listado	Por suscripción	9
42	Office 365 E3	205	Asignada	401
43	Ms 365 E3	507	Asignada	561
44	Ms 365 E5	0	Asignada	1
45	Olympus	0	Por suscripción	Ilimitado software propio
46	Pcsecure	0	Por suscripción	Ilimitada
47	Pencil	Libre	Libre	
48	PGAdmin	Libre	Libre	
49	Postgres	Libre	Libre	
50	Postman	Libre	Libre	
51	Power BI Desktop	Libre	Libre	
52	Power BI	78	Asignada	106
53	Project Professional 2019	3	Asignada	4
54	Putty	Libre	Libre	
55	Remote Desktop Connection Manage	Libre	Libre	
56	SCHIP	Libre	Libre	
57	Seven	ASIGNADA	Por suscripción	10000
58	SIEM	Sin evidencia en listado	Por suscripción	1750 EPS
59	SoapUI	Libre	Libre	
60	SQL Server 2016 Enterprise	ASIGNADA	Asignada	2
61	SQL Server 2016 Estándar	ASIGNADA	Asignada	2
62	STORMUser	Libre	Libre	
63	Teams	ASIGNADA	Asignada	Hace parte integral de las licencias de O
64	Telerik	Libre	Libre	
65	Temis	Sin evidencia en listado	Por suscripción	Ilimitada por derecho de uso
66	Teracopy	Libre	Libre	
67	Ubuntu Server 1804	Libre	Libre	
68	Visio Professional 2019	Sin evidencia en listado	Asignada	17

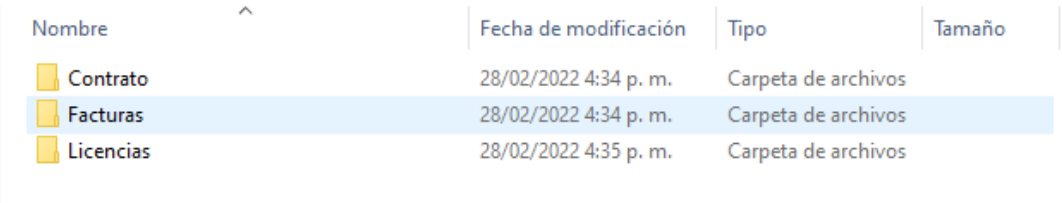
Fuente: Reporte suministrado por la OGI

La entidad tras el requerimiento de la OCI, suministro la copia digitalizada de cada uno de los contratos que soportan la información relacionada en la tabla anterior para las licencias adquiridas así:



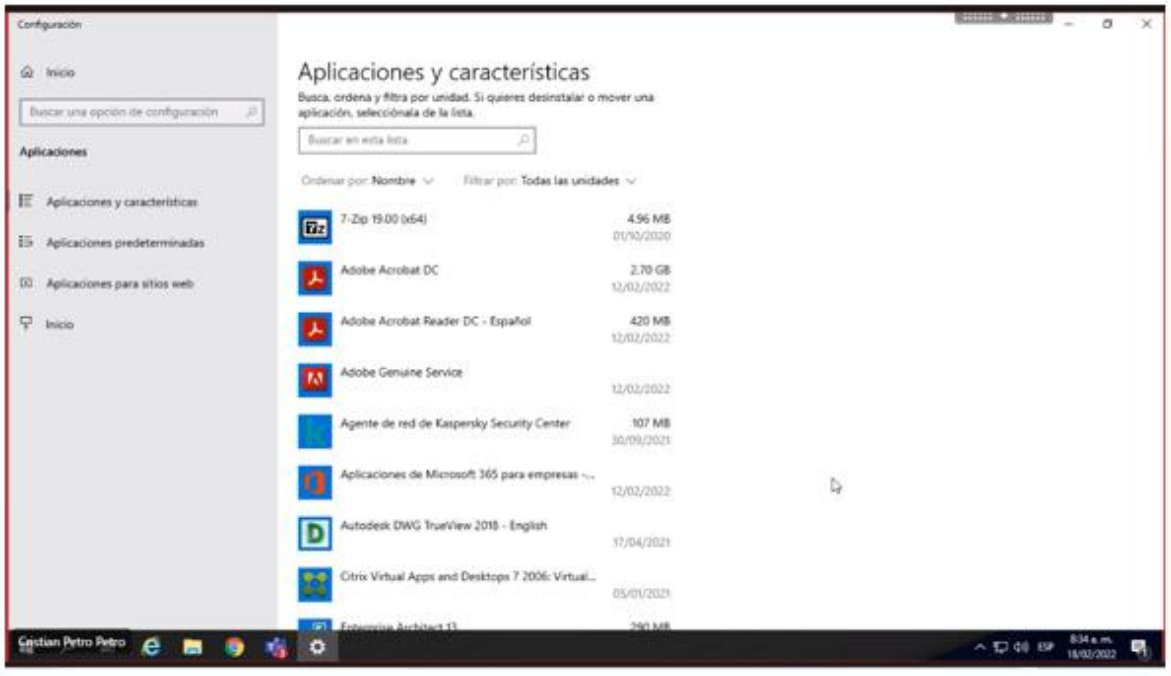
Fuente: Lista de contratos suministrado por la OCI.

Dentro de cada una de las carpetas entregadas por la OGI, se encuentra el contrato, factura y Licencia vigente así:

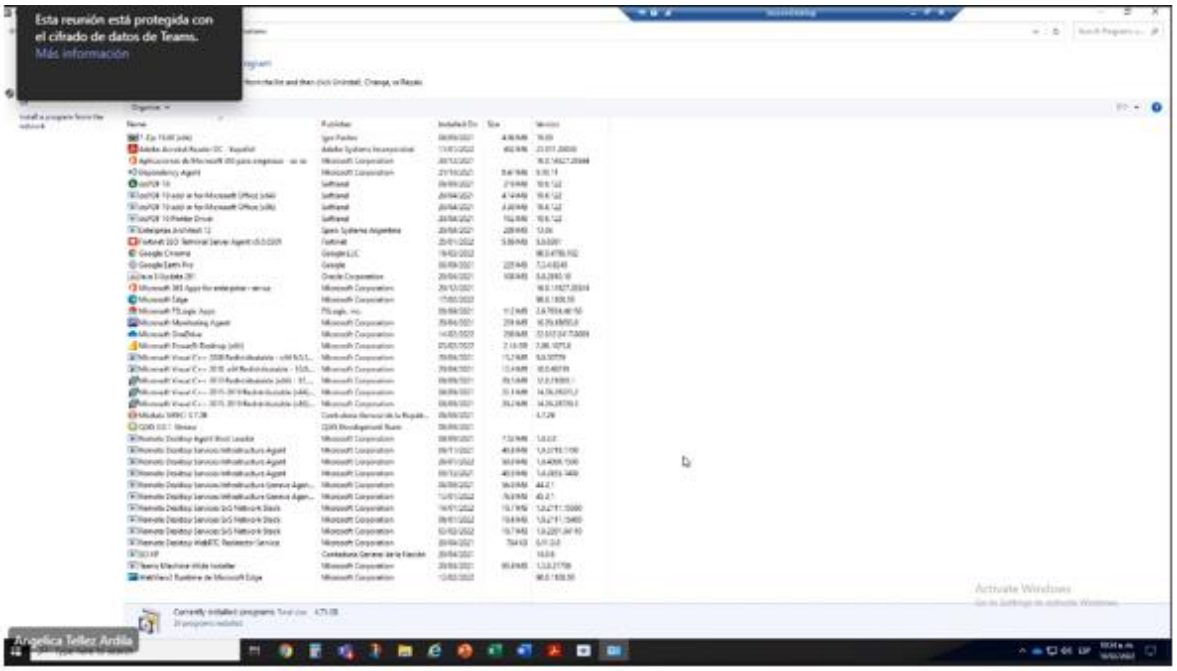


Fuente: Lista de contratos suministrado por la OCI.

Los soportes aportados por la Oficina de Gestión de la Información permite determinar un cumplimiento de la entidad respecto a los términos y condiciones establecidas dentro de cada una de las cláusulas que están acordes con solicitado y demostrado por el área responsable, lo que blinda a la entidad en lo relacionado con revisiones de adquisición de licencias para ser utilizadas dentro de la SAE; igualmente el conjunto de permisos que permitirá desarrollar y que el fabricante dentro de las estatutos legales otorga su funcionamiento.



Fuente: Software instalado en semilla – Captura de pantalla



Fuente: Pantalla de advertencia activación licencia windows –captura de pantalla

- **Software de Código Abierto Instalado en Equipos**

Se encontró software de código abierto en los ambientes de SAE (producción para usuarios estándar) y para los usuarios especializados Analista y Desarrollador (usuarios con perfil técnico de manejo exclusivo por la OGI), indicando así que en la totalidad de los usuarios se encuentran estas aplicaciones disponibles, pero permitiendo su control por parte de la Oficina de Gestión de la Información y no permitir que exista una actualización no permitida por parte de algún usuario.

13. EVALUACIÓN DE CONTROLES Y RIESGOS. (Norma desempeño 2320)

De conformidad con los resultados obtenidos, en el siguiente cuadro se presenta la metodología de evaluación de controles con sus respectivos comentarios para la adecuada comprensión y correcta implementación del plan de mejoramiento, de acuerdo con la siguiente clasificación:

	**DESEMPEÑO ALTO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que existe un alto grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además los controles y actividades se están ejecutando con efectividad.
	**DESEMPEÑO ADECUADO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que existe un grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además los controles y actividades se están ejecutando, pero presentan oportunidades de mejora para elevar la ganancia de valor en la Entidad.
	**DESEMPEÑO BAJO** En los procedimientos y pruebas de gestión y cumplimiento auditoría, se evidencia que existe un bajo grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además solo algunos controles y actividades se están ejecutando; pero son muy vulnerables y deben ser objeto de evaluación y rediseño para generar valor en la Entidad.
	**SIN DESEMPEÑO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que no se documentan y no se llevan a cabo actividades de control que garantizan el cumplimiento de los lineamientos de la alta dirección para mitigar los riesgos con impacto potencial en los objetivos institucionales.

Del análisis de controles realizado a actividades de los procedimientos, se evidenció que no existen los siguientes controles, por lo tanto, se identifican las oportunidades de mejora relacionadas a continuación.

En el capítulo 2.2.21.4.8, numeral b, el cual enuncia lo siguiente: *"Carta de representación en la que se establece la veracidad, calidad y oportunidad de la entrega de la información presentada a las oficinas de control interno"*

Esto basado en la política de seguridad digital y gobierno digital enmarcada por el Mictic en la cual recomienda como base como muestra la figura a continuación:

- No descargar archivos sospechosos.
- Actualizar el software del sistema periodicamente.
- Usar antivirus y aplicaciones anti-malware.
- Crear mejores contrase ñas y cambiarlas cada seis meses.
- Acostumbrar a cerrar las sesiones al terminar.
- Evitar operaciones privadas en redes abiertas y publicas.
- Desconectarse de internet cuando no se necesite.
- Realizar copias de seguridad.
- Navegar por páginas web seguras y de confianza.
- Comprobar la seguridad de la red WIFI.
- No hacer clic en enlaces raros.
- No dar datos personales a desconocidos.

Fuente: Política de seguridad digital enmarcada por el Mictic

13.1. Oportunidad de Mejora #1 - Actualización de Documentación de Procedimientos (desempeño bajo):

Con lo observado y comparado tanto en esta auditoría como en las revisiones de años anteriores (vigencia 2021, 2019 y 2018) se encuentran que algunos procedimientos aún se encuentran desactualizados, tomando en cuenta que estas observaciones fueron realizadas cuando la infraestructura del parque computacional se manejaba mediante la asignación de equipo por usuario especifico. Ahora con el cambio a terminales donde la sesión se maneja de manera virtualizada y se puede iniciar en cualquier equipo conectado a la red, es importante la revisión de los procedimientos en su totalidad para adaptarlos a la actualidad que maneja la entidad. En esta revisión se pudo identificar estos ejemplos de procedimientos que son necesarios actualizarlos.

P-TE1-203 - PROCEDIMIENTO DE MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA - Versión 1 - 19/08/2020: En concordancia con el punto anterior, el monitoreo debe cambiar debido que la organización cuenta con la plataforma CITRIX donde las máquinas de usuarios se monitorearían por la consola. Es importante que este aparte se explique dentro del procedimiento. Sigue sin actualización a febrero de 2022.
N-TE1-017 - INSTRUCTIVO DE BORRADO SEGURO - Versión 3 – 19/02/2018: Debido al cambio de infraestructura tecnológica el instructivo ya no es aplicable, debido que el formateo de maquina en el momento de retiro de usuario ya no se practicable debido al nuevo esquema.
P-TE1-164 - PROCESO DE GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA - Versión 2 – 16/10/2018.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.

Recomendaciones

Generar esquemas de trabajo que permitan realizar la actualización de los procedimientos en mención, con el fin de estar vigentes con la infraestructura manejada en la entidad.

Generar esquemas de trabajo no solo en la OGI, sino en la oficina de planeación con el fin de cerrar brechas en estos temas.

13.2. Oportunidad de Mejora #2 – Inventario (desempeño bajo):

Debido a la implementación de las terminales y los protocolos de bioseguridad actualmente ejecutados, actualmente se está trabajando bajo virtualización de equipos para los diferentes usuarios, sin embargo no fue presentado a la auditoría un desglose de las licencias instaladas o en uso por cada uno de los diferentes usuarios con corte a 31 de Diciembre de 2021.

Esto basado en el capítulo 2.2.21.4.8, numeral b, el cual enuncia lo siguiente: *"Carta de representación en la que se establece la veracidad, calidad y oportunidad de la entrega de la información presentada a las oficinas de control interno"*

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Se podría presentar inventario y/o etiquetado desactualizado de equipos de cómputo y comunicaciones.

Recomendaciones

Generar un inventario de equipos y software, al igual que de usuarios bajo la nueva tecnología, con el fin de mantenerlo debidamente organizado y actualizado.

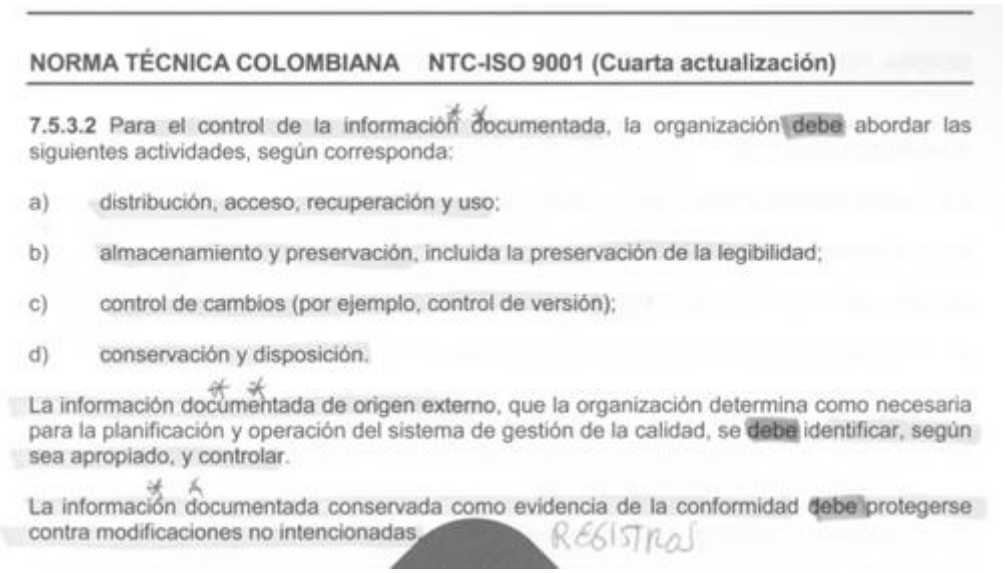
Mantener copias de respaldo con cortes mensuales en caso de requerirlo algún ente de control externo.

Observaciones de la OGI:

- No entiendo esta oportunidad de mejora, toda vez que no instalamos por usuario, sino en la semilla, me gustaría un poco mas de claridad en la observación.
- A los usuarios se les asigna una Semilla que contiene el software.
- Estoy de acuerdo con la observación de Giovanny.
- Además, el inventario de las semillas fue entregado en el desarrollo de la auditoria como parte de las evidencias y se esta dando cumplimiento a la instalación de software, además se remitió el listado de usuarios con licencias de Office, Power BI PRO, Adobe PRO, Cloud Creative y las licencias por concurrencia de Enterprise Architect, son 10 y no tienen dueño, por ser utilizadas a demanda.

Análisis Equipo Auditor: La Oficina de Control Interno realiza unas recomendaciones orientadas a la mejora continua de la entidad, es cierto que hay semilla pero todos los usuarios no tienen acceso a las misma características como por ejemplo power BI, entre otros por tal razón es necesario mantener un listado actualizado por usuario del acceso a licencia por cada uno de ellos.

A pesar de no tener dueño es necesario asignarlas con el fin de evitar conflicto en caso de concurrencia de las mismas en la entidad y con miras al retorno a la presencialidad de los funcionarios de la entidad.
De acuerdo a la ISO 9001:2015 la información debe mantenerse actualizada y documentada en sus numerales a al d en el punto 7.5.3.2.



NORMA TÉCNICA COLOMBIANA NTC-ISO 9001 (Cuarta actualización)

7.5.3.2 Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

a) distribución, acceso, recuperación y uso;

b) almacenamiento y preservación, incluida la preservación de la legibilidad;

c) control de cambios (por ejemplo, control de versión);

d) conservación y disposición.

La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de la calidad, se debe identificar, según sea apropiado, y controlar.

La información documentada conservada como evidencia de la conformidad debe protegerse contra modificaciones no intencionadas.

Fuente: Norma ISO 9001:2015

De igual forma el procedimiento P-TE4-163, establece en sì mismo el mantener actualizado el inventario tal como se muestra en la siguiente figura:

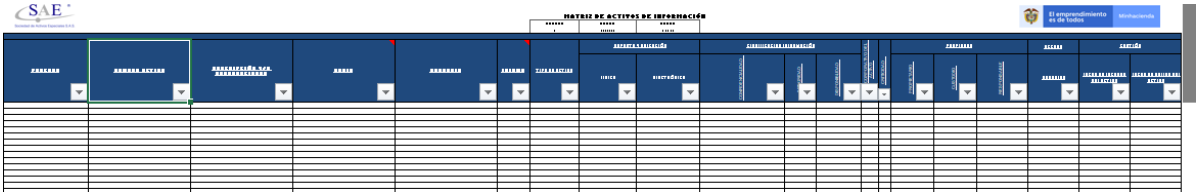


PROCEDIMIENTO PARA EL CONTROL DE SOFTWARE

RESPONSABLES					DESCRIPCIÓN DE ACTIVIDADES	CONTROL	DURACIÓN ESTIMADA	ÁREA	REGISTRO
DIRECTIVO	ASESOR	PROFESIONAL	TÉCNICO	ASISTENCIAL					
		1			**5. Asignación de escritorio virtual o preparación e equipo portátil.** El profesional asignado procede a hacer la asignación del escritorio virtual. Para la asignación de portátiles el profesional de la Oficina de Gestión de la Información prepara el equipo e instala las aplicaciones.	**Mecanismo:** Escritorio virtual y/ o portátil **Parámetro:** Asignación y/o instalación	30 min.	Oficina de Gestión de la Información	Mesa de Ayuda Consola administración escritorios virtuales
					6. Actualizar inventario. Se actualiza inventario de software y Hardware. Fin del procedimiento.	**Mecanismo:** Inventario de software y Hardware **Parámetro:** Actualización	5 min.	Oficina de Gestión de la Información	Mesa de ayuda

Fuente: Procedimiento para el control de software P-TE4-163

De igual forma se hace necesario utilizar para dicho fin como base una matriz de activos de información enunciada en la arquitectura de la SAE o en su defecto una específica elaborada para dicho fin, a criterio de la OGI:



Fuente:F-TE4-246 Matriz de activos de información

Por lo anteriormente sustentado la OCI mantiene la oportunidad de mejora.

13.3. Oportunidad de Mejora #3 - Licencias de Software. (desempeño adecuado):

Al igual que los archivos personales que podrían existir dentro de los equipos, la nueva arquitectura de sesión virtualizada y administrada de manera centralizada mediante la plataforma de Citrix, también permite llevar un control mucho más efectivo en la instalación y uso de las licencias, ya que este control evita instalaciones no autorizadas a usuarios que no aplique dicha herramienta o que por reasignación de equipos permita duplicar instalaciones con una sola licencia, resultando así diferencias entre las licencias adquiridas y compradas versus las licencias reales instaladas y utilizadas.

Sin embargo, es necesario tener un inventario actualizado de funcionarios, caso que se evidencio al revisar vía remota la instalación de software a los diferentes usuarios, según inventario suministrado por la OGI. Caso específico al llamar al funcionario Morales Gonzales Geraldine, retirado el 30 de diciembre de 2021, según lo evidenciado en reunión del 18 de febrero de 2021.

De igual forma cabe anotar insistir en la solución al error de activación de las licencias de Windows al realizar la conexión remota con ayuda del proveedor.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Inconsistencias o Pérdida de la Información.

Recomendaciones

Generar y mantener inventarios con cortes mensuales, con el fin de evitar inconsistencias y en caso de requerirlo un ente de control externo.

Dar solución a los errores de activación al realizar la conexión remota.

Observaciones de la OGI:

- No me es claro este párrafo a que diferencias se refiere
- Agradezco indicar a qué tipo de inventarios se refieren, toda vez que contamos con el inventario HW y SW y en cuanto a usuario llevamos la relación de los tickets de ingresos retiros y novedades

Análisis Equipo Auditor: La OGI entrego un inventario con corte a la fecha de la auditoria, pero al realizar el cruce se solicito a corte de Diciembre 30 de 2021, pero la razón dada por el área es que no se tenía un backup a esa fecha, por eso se mantiene la oportunidad de mejora.

Software PC				
Item	Software	INSTALADAS SEGUN LISTADO	TIPO DE LICENCIA	CANTIDAD
1	7Zip	Libre	Libre	
2	Acrobat Pro	Sin evidencia en listado	Asignada	16
3	Acrobat Reader	libre	Libre	
4	Agentes Antivirus Kaspersky	Sin evidencia en listado	Por suscripción	332
5	Autodesk DWG TrueView	Sin evidencia en listado	Libre	
6	Azure Information Protector	Sin evidencia en listado	Por suscripción	Estan integradas con Office 365
7	Backup exec	Sin evidencia en listado	Asignada	5
8	Beyond Compare	Libre	Libre	
9	Centos 6	Libre	Libre	
10	Centos 7	Libre	Libre	
11	Centos 8	Libre	Libre	
12	Chrome, IE, Mozilla	Libre	Libre	
13	Citrix	Sin evidencia en listado	Por suscripción	400
14	Concisa	Sin evidencia en listado	Por suscripción	Ilimitada por derecho de uso
15	doPDF10	Libre	Libre	
16	Enterprise Archictect	Sin evidencia en listado	Recurrente	7
17	FileZila	Libre	Libre	
18	FirmayaDriver	Sin evidencia en listado	Asignada	El software es libre pero la asignación para uso es la firma digital que son 13
19	FortiClient VPN	Libre	Libre	
20	Fortinet DC agent	Sin evidencia en listado	Por suscripción	Estan integradas con la licencia de Fortigate

Fuente:Reporte suministrado por la OGI sin asignación por usuarios

Por lo anteriormente sustentado la OCI mantiene la oportunidad de mejora.

13.4. Oportunidad de Mejora #4 - Inventario de Personal y de usuarios. (desempeño bajo):

Al realizar el cruce de funcionarios suministrados por el área de talento humano Vs el inventario soportado por la OGI y viceversa se puede evidenciar ausencia de registros de parte y parte cuando se intentan ubicar en los registros suministrados.

Listado funcionarios suministrados por Talento humano y no evidenciados como usuarios de la OGI.

CONTRATISTA : NOMBRE COMPLETO	ENCONTRADO	CONTRATISTA : NATURALEZA	CONTRATISTA : TIPO IDENTIFICACIÓN	CONTRATISTA : NÚMERO DE CÉDULA o RUT	CONTRATISTA : NÚMERO DEL NIT	OBJETO DEL CONTRATO (390)
ADRIANA FINLAY PRADA	sin evidencia	NATURAL	CEDULA		67003754	Prestación de servicios profesionales para ejercer la representación extrajudicial y/o judicial en los procesos de normalización jurídica y/o administrativa de los bienes que administra la Sociedad de Activos Especiales S.A.S dentro del marco del Código de Extinción de Dominio
LINA PAOLA VALDES SUAREZ	sin evidencia	NATURAL	CEDULA		53165955	Prestar servicios profesionales para ejercer la representación extrajudicial y/o judicial de los procesos asignados de naturaleza laboral de la SAE en representación del Fondo para la Rehabilitación, Inversión Social y Lucha contra el Crimen Organizado (FRISCO)
YESIKA CAROLINA CARRILLO CASTILLO	sin evidencia	NATURAL	CEDULA		1052387748	Prestar servicios profesionales para ejercer la representación prejudicial y/o judicial de los procesos asignados de naturaleza contencioso administrativo de la SAE en representación del Fondo para la Rehabilitación, Inversión Social y Lucha contra el Crimen Organizado (FRISCO)
SONIA PACHON ROZO	sin evidencia	NATURAL	CEDULA		52152968	Prestar servicios profesionales para ejercer la representación prejudicial y/o judicial de los procesos asignados de naturaleza contencioso administrativo de la SAE en representación del Fondo para la Rehabilitación, Inversión Social y Lucha contra el Crimen Organizado (FRISCO)
SERGIO ANDRES GONZALEZ RODRIGUEZ	sin evidencia	NATURAL	CEDULA		1014179736	Prestar servicios profesionales para ejercer la representación prejudicial y/o judicial de los procesos asignados de naturaleza contencioso administrativo de la SAE en representación del Fondo para la Rehabilitación, Inversión Social y Lucha contra el Crimen Organizado (FRISCO)
AMANDA ROCIO SABOGAL CUBILLOS	sin evidencia	NATURAL	CEDULA		52202465	Prestar los servicios profesionales al Grupo Interno de Trabajo de Servicios Administrativo de la SAE efectuando un acompañamiento al plan de choque Administrativo y operativo dirigido a apoyar las actividades asociadas al desarrollo, ejecución y elaboración del Procedimiento en los diferentes temas asociados a la administración de bienes devolutivos de Propiedad Planta y Equipo de la Sociedad de Activos Especiales S.A.S.
DIANA CAROLINA MARTINEZ AVILA	sin evidencia	NATURAL	CEDULA		53080273	Prestar los servicios profesionales a la Gerencia de Bienes Muebles de la SAE efectuando un acompañamiento Administrativo y operativo dirigido al análisis y monitoreo a las sustancias químicas y material mineral administrados por la Sociedad de Activos Especiales SAE – S.A.S.

Fuente: Listado empleados suministrado por Talento Humano

Listado de funcionarios suministrado por la OGI y no evidenciados en talento humano.

Usuario	en planta	en mision	Cruce a RH
Romero Figueroa Sergio Fernando	#N/D	#N/D	SIN EVIDENCIA
Alvarez Zuñiga Jeferso	#N/D	#N/D	SIN EVIDENCIA
Pulido Pena Lina Maria	#N/D	#N/D	SIN EVIDENCIA
Alvarez Zuñiga Jeferso	#N/D	#N/D	SIN EVIDENCIA
Marin Posada Carlos Hernan	#N/D	#N/D	SIN EVIDENCIA
Quiroga Maldonado Deisy Dayana	#N/D	#N/D	SIN EVIDENCIA
Diaz Barranco Saida Melisa	#N/D	#N/D	SIN EVIDENCIA
Ortega Meza Leslie Julieth	#N/D	#N/D	SIN EVIDENCIA
Garrido Martinez Angelica Stephanie	#N/D	#N/D	SIN EVIDENCIA
Diaz Barranco Saida Melisa	#N/D	#N/D	SIN EVIDENCIA
Acevedo Anabel Julio	#N/D	#N/D	SIN EVIDENCIA
De Alba Mercado Tatiana Paola	#N/D	#N/D	SIN EVIDENCIA
Cardona Hoguin Claudia Jimena	#N/D	#N/D	SIN EVIDENCIA
Gomez Sanchez Nataly	#N/D	#N/D	SIN EVIDENCIA
Pulido Pena Lina Maria	#N/D	#N/D	SIN EVIDENCIA
Rubiano Castellanos Jhon Edward	#N/D	#N/D	SIN EVIDENCIA
Arevalo Gonzalez Johana Andrea	#N/D	#N/D	SIN EVIDENCIA
Rubiano Castellanos Jhon Edward	#N/D	#N/D	SIN EVIDENCIA
Barajas Contreras Gloria Patricia	#N/D	#N/D	SIN EVIDENCIA
Quiroga Maldonado Deisy Dayana	#N/D	#N/D	SIN EVIDENCIA
Quiroga Maldonado Deisy Dayana	#N/D	#N/D	SIN EVIDENCIA
Villamarin Jimenez Rosalba	#N/D	#N/D	SIN EVIDENCIA
Valdez Santofimio July Carolina	#N/D	#N/D	SIN EVIDENCIA
Correa Diego Edinson	#N/D	#N/D	SIN EVIDENCIA
Tellez Ardila Angelica	#N/D	#N/D	SIN EVIDENCIA
Tellez Ardila Angelica	#N/D	#N/D	SIN EVIDENCIA
Paez Ramirez Monica Sofia	#N/D	#N/D	SIN EVIDENCIA

Fuente: Listado empleados suministrado por OGI

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Inconsistencias o Pérdida de la Información.

Recomendaciones

Generar y mantener inventarios con cortes mensuales, con el fin de evitar inconsistencias y en caso de requerirlo un ente de control externo.

Observaciones de la OGI:

- Es importante validar esta oportunidad de mejora y la información relacionada dado que existen diferente tipo de usuarios según la contratación directa por la entidad y los contratistas que dependen de los supervisores.

1. Proveedor Adsum – Soporte Técnico Mde
2. Ticket 69927 del 28 de diciembre
3. Lina Pulido esta activa en OGI y TH
4. Ticket 69927 del 28 de diciembre
5. Carlos Marin Desvinculado según tkt 70335 reportado de manera automática desde el aplicativo de TH el 11 de enero de 2022
6. Deysi Quiroga Maldonado paso a planta según tkt 69927 de fecha 28 de diciembre de 2021.
7. Saida Melissa Diaz TKT 21094 de fecha 16/01/2018 – Regional Norte.
8. Leslie Ortega tkt 70062 de fecha de 03/01/2022 TH reporta el retiro y se documenta en tkt 70074 del mismo 03/01/2022.
Posteriormente ingreso según correo de notificación automática de Talento Humano desde el 13 de enero de 2022
9. Angelica Garrido – Tkt 67000 desvinculación 27/09/2021 e ingreso según correo de notificación automática de Talento Humano desde el 13 de enero de 2022
10. Saida Melissa Diaz TKT 21094 de fecha 16/01/2018 – Regional Norte
11. Julio Acevedo - Tkt 69864 desvinculación reporatda el 24/12/2021 e ingreso según correo de notificación automática de Talento Humano desde el 13 de enero de 2022 y por listado de talento humano fue reportado para ingreso el 03 de enero de 2022
12. Tatiana de Alba, actualmente está activa, se inactivo en el mes de enero por periodo de vacaciones. Para la OGI el estado del usuario es activo en el listado e inactivo en el dominio.
13. Claudia Jimena Cardona: ingreso con tkt 65888 radicad del 01/09/2021por Susan Ahiquel.
14. Nataly Gómez Sanchez: Ingreso como practicante de con tkt 21089 16/01/2018 - y tkt 26400 18/07/2018 de Susan Ahiquel ingreso como planta SAE.
15. Lina Pulido esta activa en OGI y TH
16. Jhon Edward Rubiano esta activo en OGI y TH
17. Gloria Barajas esta activo en OGI y TH
18. Deysi Quiroga Maldonado paso a planta según tkt 69927 de fecha 28 de diciembre de 2021.
19. Deysi Quiroga Maldonado paso a planta según tkt 69927 de fecha 28 de diciembre de 2021.
20. Rosalba Villamarin – esta activo en OGI y TH
21. July Carolina Valdez. Esta activo en OGI
22. Diego Edinson Correa – Esta activo en OGI
23. Angelica Tellez - Esta activo en OGI 21/01/2021 ingreso tkt 56408
24. Angelica Tellez - Esta activo en OGI 21/01/2021 ingreso tkt 56408
25. Monica Paez Ramirez – desvinculación con tkt 64708 del 10(08/2021) radico automático de Talento Humano

- Agradezco indicar porque están referenciando estos riesgos

Análisis Equipo Auditor: Las diferencias están dadas por las fechas de corte del reporte suministrado por talento humano el cual está dado a Diciembre 30 de 2021 y la OGI dado a la fecha de la realización de la auditoría con corte a febrero de 2022 y, por tal razón al realizar el cruce de usuarios contra funcionarios se encontraban diferencias.

Esto basado en el capítulo 2.2.21.4.8, numeral b, el cual enuncia lo siguiente: *"Carta de representación en la que se establece la veracidad, calidad y oportunidad de la entrega de la información presentada a las oficinas de control interno"*

Por lo anteriormente sustentado la OCI mantiene la oportunidad de mejora.

13.5. Oportunidad de Mejora #5 - Inventario desactualizado de usuarios en Azure (desempeño bajo):

Al preguntar por los usuarios suministrados por recursos humanos y los suministrados por el área de la OGI, se preguntó por la conexión de los mismos y lo comunicado por el área fue a través de azure, sin embargo, no se encuentran diferenciados ni listados por el área a la fecha de la auditoria. Esto se da por razones de actualización del reporte y la imposibilidad de bajar el reporte solicitado a corte del 31 de diciembre de 2021.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Inconsistencias o Pérdida de la Información.

Recomendaciones

Generar y mantener inventarios con cortes mensuales, con el fin de evitar inconsistencias y en caso de requerirlo un ente de control externo.

Observaciones de la OGI:

- Según revisión interna no se realizó en el desarrollo de la auditoria una pregunta relacionada con el tema mencionado y no tiene relación con el objetivo de la auditoria.
- Agradecemos puntualizar esta oportunidad de mejora

Análisis Equipo Auditor:

El inventario de usuarios en Azure se solicitó después de revisar que no habían suficientes licencias dada la cantidad de funcionarios de la entidad y se respondió por parte de los funcionarios de la OGI que se conectaban no por citrix el cual tiene asignada 400 licencias y la cantidad de funcionarios exceden los 600, sino por Azure.

RV: Listado de Software

Por parte de OCI nos solicitan completar esta tabla, lo mas pronto posible

De: Javier Mauricio Peralta Cubillos <jperalta@saesas.gov.co>
Enviado el: lunes, 28 de febrero de 2022 9:05 a. m.
Para: Giovanny Alejandro Lopez Insuasti <glopez@saesas.gov.co>
Asunto: Listado de Software

Hola Giovanny:

Te adjunto listado de Software, en el cual queda pendiente la cantidad de licencias por cada uno.

Te agradezco complementarlo.

Muchas gracias.

Javier Mauricio Peralta Cubillos
Auditor Interno
Oficina de Control Interno SAE
jperalta@saesas.gov.co
Calle 93b # 13 - 47 – Bogotá

Fuente: Correo electrónico solicitud OCI.

13	Citrix	Por suscripción	400

Fuente: Correo electrónico solicitud OCI.

La Oficina de Control Interno realiza unas recomendaciones orientadas a la mejora continua de la entidad, en las diferentes reuniones se preguntó por la cantidad de empleados vs la cantidad de licencias disponibles por tal razón se argumentó que los usuarios no cubiertos por Citrix utilizaban la plataforma alterna. Por está razón se argumenta la necesidad de tener un listado de dichos usuarios que usan esta plataforma de acceso al corte de 30 Diciembre 2021.

La OGI no presento evidencias de las observaciones remitidas a la OCI, por lo anteriormente sustentado la OCI mantiene la oportunidad de mejora.

13.6. Oportunidad de Mejora #6 – Ausencia de un procedimiento para la creación de cuentas de correo electrónico (desempeño adecuado):

Teniendo en la Política de Seguridad de la Información en el cual establecen la creación por parte de la OGI de un procedimiento para la administración de cuentas de correo electrónico, a la fecha del informe se evidencia la ausencia del mismo.

La Política de seguridad de la Información es un compendio de documentos y estrategias donde se establecen las directrices para implementar desde un punto de vista lógico y físico, todos los aspectos relacionados con la seguridad y el control sobre la información, los cuales deben ser cumplidos por los directivos, funcionarios, colaboradores, contratistas y terceros en el adecuado cumplimiento de sus funciones, se logra evidenciar la 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.

Al preguntar en mesa de trabajo por los usuarios autorizados por fuera de citrix, se adjuntó un listado con un total de 192 usuarios autorizados en la entidad, lo cual a pesar de estar autorizado constituye un alto riesgo de fuga de información confidencial de la entidad en cuanto a la confidencialidad de la información consignado en las políticas de seguridad de la información en la SAE. Esto en cuanto la OGI debe proveer un ambiente seguro y controlado para el funcionamiento del correo electrónico, la cual puede ser descargada en diversos dispositivos de almacenamiento no controlados por la SAE.

Riesgos asociados

- Puede ocurrir que se presente fuga o pérdida de información.
- Inconsistencias o Pérdida de la Información.

Recomendaciones

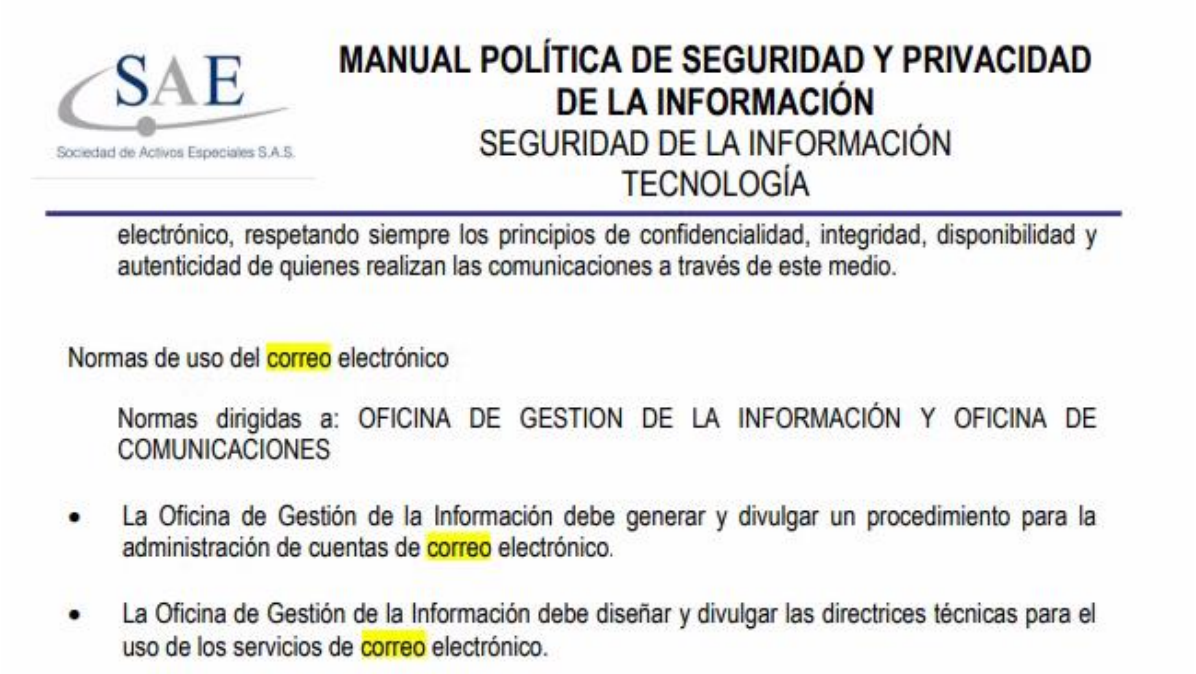
Evaluar los permisos de los diferentes usuarios con el fin de evitar pérdidas o fugas de información confidencial.

Observaciones de la OGI:

Esta política y permisos es autorización por los directivos y lideres de proceso por necesidades del servicio por parte de los usuarios y queda documentado a través de ticket solicitado y/o aprobado, único soporte de la OGI para crear estas excepciones.

Cabe anotar que existen mecanismos para controlar y el uso las herramientas de Office en dispositivos personales, que serán documentadas para presentar a aprobación del comité directivo.

Análisis Equipo Auditor: Si bien es cierto esto se debería dejar por explícito en la política de manejo de correo electrónico, con el fin de establecer un límite de cupos y límite por oficina con el fin de minimizar el riesgo.



SAE
Sociedad de Activos Especiales S.A.S.

MANUAL POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
SEGURIDAD DE LA INFORMACIÓN
TECNOLOGÍA

electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Normas de uso del correo electrónico

Normas dirigidas a: OFICINA DE GESTION DE LA INFORMACIÓN Y OFICINA DE COMUNICACIONES

- La Oficina de Gestión de la Información debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Oficina de Gestión de la Información debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

Fuente: Manual política de seguridad y privacidad de la información.

De acuerdo a las observaciones de la OGI, la Oficina de Control Interno realiza unas recomendaciones orientadas a la mejora continua de la entidad, en el cual se busca propender por la mejora continua de los procesos y evaluar y concientizar al personal de la brecha de seguridad al autorizar este tipo de permisos a los funcionarios de la entidad y prever una materialización de riegos.

A continuación, se presenta lo que se encuentra descrito en el manual de la política de seguridad de la información.

La OGI no presento evidencias de las observaciones remitidas a la OCI, por lo anteriormente sustentado la OCI mantiene la oportunidad de mejora.

13.7. Observación #1 - Políticas de Seguridad de la Información (desempeño adecuado):

En la revisión, se encontró que en observaciones anteriores se había anunciado la gran cantidad de usuarios que contenían dentro de sus equipos asignados archivos de carácter personal, como música o fotos. Sin embargo, en esta revisión en la nueva infraestructura de terminales, esta auditoría encontró que los archivos de esta categoría no fueron hallados de manera local, por lo tanto, se puede concluir que esta nueva arquitectura evita que los usuarios utilicen de manera no autorizada el almacenamiento de los equipos. Sin embargo, es posible descargar software en las terminales.

Riesgos asociados

- Inconsistencias o Pérdida de la Información

Recomendaciones

Evaluar el bloqueo en la descarga de archivos ejecutables en las sesiones de los usuarios del dominio de la SAE.

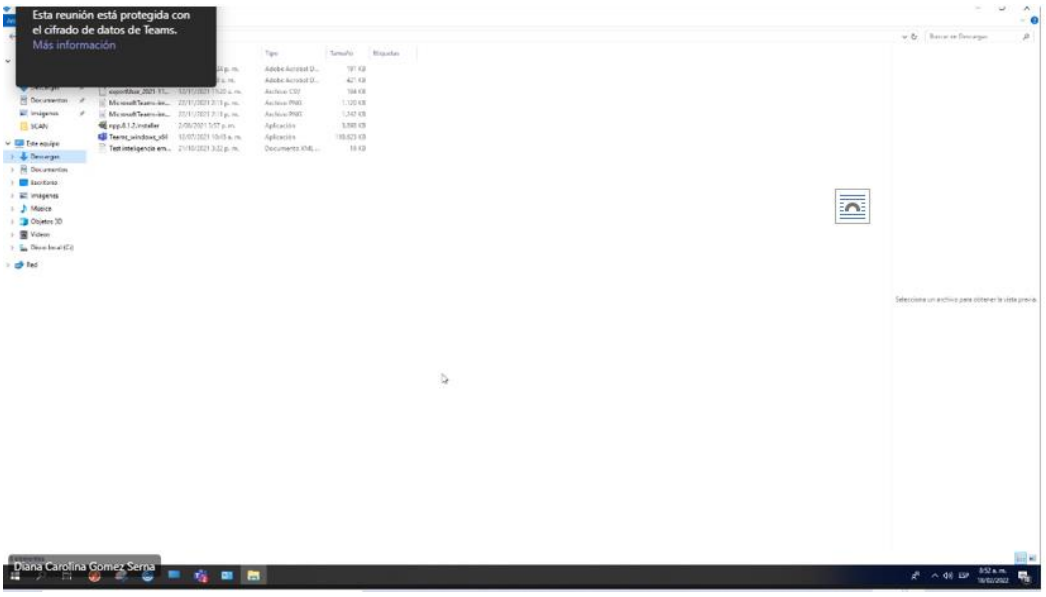
Observaciones de la OGI:

- Solicito indicar puntualmente si esta situación se presentó en toda la muestra, lo anterior, a que contamos con un software llamado pcsecure que si bien permite la descarga no permite la ejecución de ningún ejecutable que se trate de instalar en los portátiles o NUC.
  Es de aclarar que la descarga está autorizada, el bloqueo hace referencia específicamente a la ejecución.
  No es posible evitar la descarga de cualquier tipo de archivo porque hace parte de las necesidades de los usuarios, solamente se debe controlar la ejecución de archivos que puedan generar alguna amenaza para nuestra infraestructura

- EL control esta aplicado con la instalación de PCSeCUre localmente, además contamos con múltiples herramientas para prevenir este tipo de amenazas, como son antivirus, firewall, correlacionador de eventos, WAF (estás últimas no fueron auditadas ni verificadas como parte de la auditoria de derechos autor)
- Ya esta controlado en la ejecución no se puede bloquear la descarga.

Análisis Equipo Auditor: La Oficina de Control Interno observó la descarga de archivos a las diferentes terminales, tal como se muestra en la figura anexa y lo que se busca con la recomendación es minimizar los riesgos y sugerir recomendaciones con el fin de ayudar o dar un punto de vista objetivo sin ser parte del proceso y el dueño del proceso evaluar las mismas. Ejemplo en Windows defender se puede iniciar la descarga, pero al mismo tiempo el antivirus elimina los archivos .exe.

De igual forma la política de seguridad digital enmarcada por el Minctic ya referenciada en el informe hace especial enfásis en la descarga de información con especial cuidado.



Fuente: Tomado de la muestra realizada a la revisión de licenciamiento.

La Oficina de Gestión de la Información debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Sociedad.

Fuente: Procedimiento para control de software P-TE4-163

Al evaluar las observaciones de la OGI, se deja como una observación dicho punto.

14. CONCLUSIONES Y RECOMENDACIONES GENERALES. (Atributo desempeño 2400)

Al evaluar la eficiencia, eficacia, efectividad frente a la evaluación de derechos de autor se puede concluir que de acuerdo con las oportunidades de mejora registradas en el contenido del presente informe, los procedimientos ejecutados por OGI, son objeto de mejora.

Efectuar la implementación de la plataforma de Citrix da un valor agregado tanto a la administración de programas como a la gestión de la seguridad que pueda ejercer el área responsable, por lo que se mitigan riesgos como la instalación no autorizada de programas prohibidos, el almacenamiento de archivos de carácter personal no permitidos como lo son fotos, música, videos, documentos o correos, o las descargas de archivos que pueden comprometer la seguridad de la información.

Es importante verificar la creación de usuarios y que el líder del proceso vele por la aprobación, publicación y socialización del procedimiento en dicha materia, con el fin de mitigar dicha observación manifestada no solo en está auditoria, sino en auditorias anteriores, de igual forma en la política de seguridad de la información se menciona la necesidad de la creación de un procedimiento para manejo del correo electrónico que la fecha no se ha realizado.

Nuevamente y como se realizó en anteriores informes, mantener actualizados los procedimientos de acuerdo con lo que la entidad posee en materia de recursos e infraestructura, existen procedimientos que no poseen los documentos establecidos para ser congruentes con las acciones actuales que deben realizar la Oficina de Gestión de la Información. En las revisiones realizadas semestralmente y anualmente por la oficina de control interno, se observan ampliaciones continuas a las actividades propuestas a los planes de mejoramiento de los entes externos e internos, como se evidencio en la auditoría realizada en continuidad del negocio en el mes de diciembre de 2021.

Diseñar y ejecutar planes de mejoramiento, teniendo en cuenta la necesidad que tiene la OGI con el fin de 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. Dado esto para que no se materialicen los posibles riesgos.

Es importante anotar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de nuestros procedimientos de auditoría, evaluación o seguimiento, previamente planeados. La entidad y las áreas que la componen, son responsables de establecer y mantener un adecuado sistema de control interno y de prevenir posibles irregularidades, de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG. Así mismo, es responsabilidad del dueño del proceso por la información suministrada, por cualquier medio, para la realización de esta actividad de manera oportuna, completa, integra y actualizada y la de informar en su momento las posibles situaciones relevantes y/o errores que pudieran haber afectado el resultado final de la actividad.

Por lo anteriormente expuesto y en cumplimiento del procedimiento “Elaboración y seguimiento planes mejoramiento” se solicita suscribir por parte de la Oficina de gestión de la Información OGI un Plan de Mejoramiento para las oportunidades de mejora y observaciones identificadas en términos de oportunidad, calidad y efectividad de acuerdo con las posibles materializaciones de riesgos identificados y/o evaluados en la auditoria y el impacto que trae consigo para la Entidad.

Dicho plan, además de servir de base para la detección de mejoras, debe permitir el control y seguimiento de las diferentes acciones a desarrollar, así como la incorporación de acciones correctivas ante posibles contingencias no previstas, en la efectividad, en la mitigación de riesgos, reducción en la probabilidad y en el impacto hacia la SAE.

Finalmente es importante recordar que la toma de acciones correctivas y preventivas se constituye en un objetivo del proceso de mejora continua, y por tanto, integra la decisión estratégica sobre cuáles son los cambios que deben incorporarse a los diferentes procesos de la Sociedad de Activos Especiales - SAE, para que sean traducidos en mejoras en los servicios prestados y en las operaciones internas.

Agradecemos la atención prestada y esperamos contar con su disposición y la de los líderes de los procesos para adelantar las acciones de mejora a que haya lugar para corregir las situaciones presentadas en el informe y prevenir posibles desviaciones y materialización de riesgos. De igual forma la entidad cumple en materia de derechos de autor y las oportunidades de mejora relacionadas están con miras como su nombre lo indica a mejorar y siempre a estar a la vanguardia de las mejores prácticas como se ha venido realizando y cumpliendo en la entidad.

Cordialmente,

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

C.C. :Ing Jaime Leon – Jefe Oficina de Planeacion

Aprobó: María del Pilar Mayor Varela.
Elaboró: Javier Mauricio Peralta Cubillos