SOCIEDAD DE ACTIVOS ESPECIALES SAE S.A.S

OFICINA DE CONTROL INTERNO

INFORME CUMPLIMIENTO AL USO DE SOFTWARE LEGAL - DERECHOS DE AUTOR

VIGENCIA 2020

Bogotá, D.C. marzo de 2021

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

1. OBJETIVO.

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.

2. ALCANCE

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 2020. Se realizó verificación a una muestra aleatoria de 32 equipos mediante vía remota distribuidos entre Dirección Central, Regional Centro Oriente, Regional Suroccidente, Regional Norte y Regional Occidente.

Sede	Cantidad de Equipos
Calle 93	15
Calle 96	5
Regional Suroccidente	4
Regional Occidente	4
Regional Norte	4
Total	**32**

3. CRITERIOS Y FUENTES DE REVISIÓN

- Directiva Presidencial No. 001 de 1999
- Directiva Presidencial No. 002 de 2002
- 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.

4. METODOLOGÍA

- 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 a una entrega realizada previamente por cambio de proveedor del parque computacional, en el momento de realizarse esta auditoría no se puede tomar muestra de cantidad de equipos de manera física. Por lo tanto, se solicitó a la oficina de gestión de la información una relación de los equipos entregado a fecha del 31 de diciembre del 2020.
- Con respecto al punto anterior, se solicita certificación de borrado seguro de toda la información que pudo haber estado almacenado dentro del HW entregado mediante un formateo seguro.
- 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 2021 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

- ✓ De la muestra realizada a treinta y dos (32) equipos, los cuales contenían 45 perfiles de usuarios distintos, 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

- ✓ En la muestra se encontraron 11 equipos que no tenían usuarios registrados y se ingresaba mediante un usuario local y desde ese perfil, se ingresa al módulo de conexión a Citrix. En el caso de regional norte (Barranquilla) los equipos de la muestra (4 terminales) no estaban registrados en el dominio y solamente poseían el usuario local para ingreso.
- ✓ Aunque ya la infraestructura de terminales no permite instalaciones no autorizadas, si permite de manera local en los equipos descargar y almacenar archivos. Lo cuál puede acarrear un riesgo de seguridad ante software dañino (malware)
- ✓ En algunos equipos de Medellín se encontraron 4 terminales donde la licencia de Kapersky estaba vencida. Por lo que mantener todas las licencias actualizadas impide que en posibles revisiones de entes externos la entidad sea sometida a posibles multas o sanciones.
- ✓ Se encontraron procedimientos que no son aplicables y se encuentran desactualizados, en la revisión de esta auditoría se hallaron 4 de estos documentos.

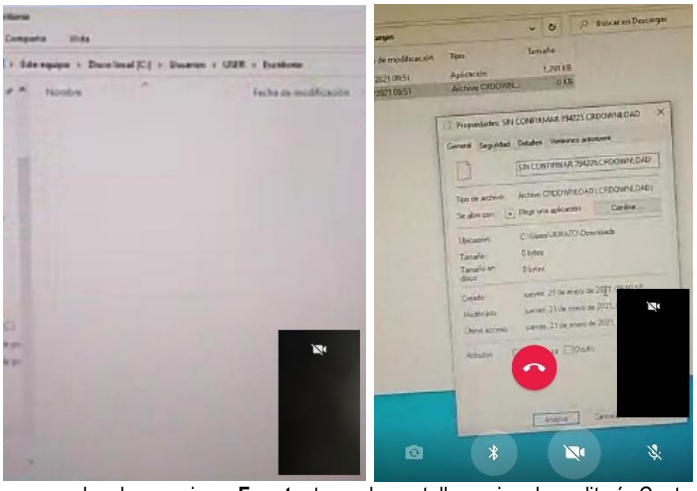
7. RESULTADOS OBTENIDOS

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

7.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que 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.

Dentro de la muestra tomada para la realización de la presente auditoria, a diferencia de los resultados de la auditoría previa (en la cual se pudo evidenciar que un 86.67% de los usuarios entrevistados, no tienen presente las políticas de seguridad de la información), 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 alojaban archivos de diferente índole (incluyendo ejecutables). Es importante que este tipo de descargas sean restrictivas para así evitar un posible ataque mediante malware.

Se realizó una capacitación en el año 2020 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

7.2. DOCUMENTACIÓN PROCEDIMIENTOS

De acuerdo con la nueva estructura la cual se estaba implementando desde noviembre del 2020 en las instalaciones, se procedió a revisar la documentación de los procedimientos que se encuentran publicados en la intranet, respectivo a este tema se encontraron documentos y procedimientos desactualizados sobre esta nueva infraestructura. A continuación, se refieren los códigos.

- 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-TE1-203 - PROCEDIMIENTO DE MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA - Versión 1 - 19/08/2018: 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.
- P-TE4-163 – PROCEDIMIENTO DE CONTROL DE SOFTWARE – Versión 1 – 19/09/2017: se encuentra desactualizado con respecto a la inclusión de políticas contables (observación realizada en auditoría anterior) además de la no actualización con respecto a la nueva infraestructura que necesitaría cambios en algunos pasos del procedimiento como se maneja la adquisición e instalación de nuevo software tomando en cuenta que ya la instalación no sería de manera individual por máquina sino ahora es por paquete de usuarios debido a la plataforma CITRIX.
- P-TE4-094 PROCEDIMIENTO ADMINISTRACIÓN Y CONTROL DE ACCESO A USUARIOS – Versión 6 – 14/07/2020: de acuerdo con el procedimiento se realizará asignación de usuarios a equipos de cómputo debe cambiar. (observación realizada en auditoría anterior). Con la arquitectura actual y que se implementó desde finales del año 2020, el procedimiento ya no es aplicable a las terminales y su respectiva asignación a los usuarios.

7.3. CREACIÓN DE USUARIOS

Teniendo en cuenta lo descrito en el procedimiento “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)
- robregozo (CARLOS EDUARDO RUIZ OBREGOZO)
- lauhernandez (LAURA MATILDE HERNANDEZ CONSUEGRA)
- ehernandezb (HERNANDEZ BENAVIDEZ ESTEFANY)
- lhvizcaino (HERNANDEZ VIZCAINO LILIANA)
- mcardenasm (CARDENAS MUÑOZ MARISOL)
- mmoralesr (MORALES ROJAS MARLEN)
- ahernandeza (ADRIANA HERNANDEZ ALDANA)
- drodriguezr (DANIEL RODRIGUEZ ROMERO)
- arodriguezr (ALEJANDRA RODRIGUEZ RODRIGUEZ)
- agomezm (ANDRES CAMILO GÓMEZ MERCHAN)
- jvillamizal (JUAN CARLOS VILLAMIL PIZA)
- lsilva (JEIMMY LORENA SILVA FIGA)

- mrodriguezb (MILGUEL ANGEL RODRÍGUEZ BERNAL)

Igualmente se encuentran usuarios que tienen errores en su nombre en relación con la tabla entregada por talento humano:

- ggonzales (Geraldine Gonzales Briceño – apellido según talento humano es González)
- apvanegas (Angelica Paola Vanegas Rojas – apellido según talento humano es Venegas)
- jvaldez (July Carolina Valdez Santofimio – apellido según talento humano es Valdés)
- hvillareal (Hollman Villareal Hernández – apellido según talento humano es Villarreal)

7.4. SOFTWARE DADO DE BAJA

La Sociedad de Activos Especiales creo la Resolución No 4354 del 2018 donde se creó el Comité Técnico de baja de bienes, en virtud de oportunidades de mejora dejas por la OCI, durante cada vigencia "*Esta observación se ha establecido como acción en el plan de mejoramiento interno del 2019 en su actividad numeral 8.6 "Oportunidad de Mejora – Baja contable del software y disposición final del software dado de baja" que a su vez en el seguimiento del 24 de agosto del 2020 no se había cumplido con la actividad*". Para el segundo semestre de 2019, la Oficina de Gestión de la Información identificó las licencias de software que por obsolescencia tecnológica ~~se~~ debían dar de baja, adicionalmente, se ha venido trabajando conjuntamente con la Vicepresidencia Administrativa y Financiera en la identificación del inventario del licenciamiento.

Actualmente el documento "P-TE4-163 Procedimiento control de Software", se encuentra con fecha de última actualización septiembre de 2017, por lo cual se mantiene igual a lo validado en las vigencias anteriores (2018, 2019, 2020) el cual no se evidencia las actividades a tener en cuenta para dar de baja contablemente el software, como tampoco hace referencia al destino final que se le debe dar al software dado de baja (requerimiento del cuestionario de la Dirección Nacional de Derechos de Autor). Evidenciando así no solo una inadecuada gestión sobre las observaciones realizadas por el equipo de Control Interno sobre este tema, sino también manteniendo un riesgo que la entidad en una revisión de un ente externo pueda ser sancionada o multada.

7.5. 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 fue remitido a la OCI tras solicitud formal, se evidencia lo siguiente:

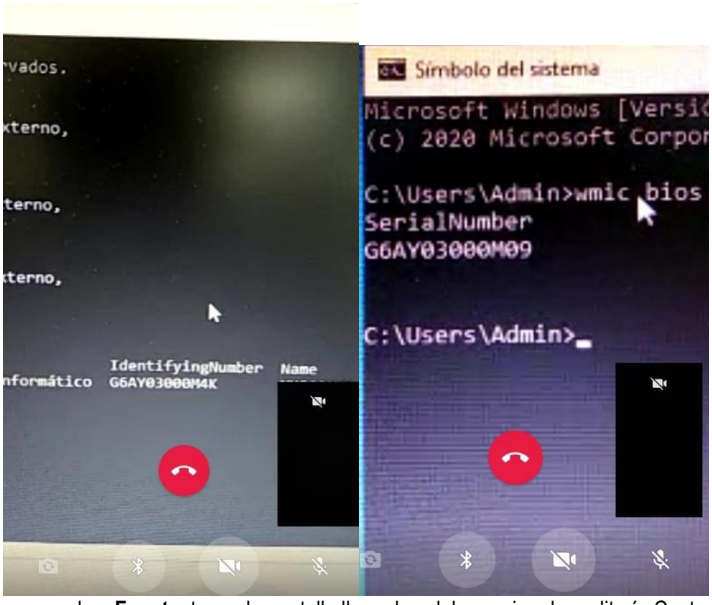
EQUIPOS POR DEPENDENCIA A DICIEMBRE DE 2020						
DEPENDENCIA	HARDWARE					TOTAL
	SERVIDORES FISICOS	SERVIDORES VIRT	PORTATILES	TABLETS	AIO/PC	
ENAJENACION TEMPRANA (EQUIPOS ASIGNADOS)			0	0	15	15
GERENCIA ADMINISTRATIVA Y FINANCIERA			0	0	10	10
GERENCIA COMERCIAL			6	0	3	9
GERENCIA DE ASUNTOS LEGALES			2	0	27	29
GERENCIA DE CONTRATOS			0	0	3	3
GERENCIA DE INMUEBLES			1	0	15	16
GERENCIA DE BIENES MUEBLES			4	2	19	25
GERENCIA REGIONAL SUR OCCIDENTE			8	2	41	51
GERENCIA DE SOCIEDADES ACTIVAS			2	0	19	21
GERENCIA DE SOCIEDADES EN LIQUIDACION			0	0	13	13
GERENCIA DE TALENTO HUMANO			1	0	15	16
GERENCIA FINANCIERA			2	0	22	24
GERENCIA PROYECTOS ESPECIALES - COLOMBIA EN PAZ			0	0	3	3
GERENCIA REGIONAL CENTRO ORIENTE			2	1	49	52
GERENCIA REGIONAL NORTE			8	0	18	26
GERENCIA REGIONAL OCCIDENTE			3	0	30	33
GERENCIA TÉCNICA			1	0	27	28
GIT ARCHIVO Y CORRESPONDENCIA			1	0	15	16
GIT DE ASEGURAMIENTO Y CONTROL DE LA INFORMACIÓN			1	0	9	10
GIT GESTION DEPOSITARIOS Y PROVISIONALES			1	0	3	4
OFICINA ASESORA DE PLANEACIÓN			5	0	2	7
OFICINA DE COMUNICACIONES Y ATENCION AL CIUDADANO			1	0	9	10
OFICINA DE CONTROL INTERNO			0	0	6	6
OFICINA DE GESTIÓN DE LA INFORMACIÓN	19	157	4	2	9	191
PRESIDENCIA			2	0	10	12
VICEPRESIDENCIA DE BIENES MUEBLES E INMUEBLES			0	0	4	4
VICEPRESIDENCIA DE SOCIEDADES			1	0	4	5
VICEPRESIDENCIA FINANCIERA Y ADMNISTRATIVA			1	0	3	4
VICEPRESIDENCIA JURÍDICA			0	0	2	2
PLAN VENTA MASIVA			0	0	4	4
Total general	19	157	57	7	409	649

Sin embargo, al momento de la revisión (febrero-marzo 2021) ya se habían realizado las respectivas entregas de los equipos que se encontraban en préstamo por parte del proveedor Microhard. Por lo tanto, no fue posible realizar la revisión física de los inventarios y su confrontación con los datos de inventario que proveyó la Oficina de Gestión de la Información. De acuerdo con esto, se solicitó al área responsable una certificación de la entrega de los equipos, para poder determinar si el control de inventario que poseía en su momento el área responsable (imagen adjunta) correspondía a la realidad de equipos en funcionamiento y en el área respectiva relacionada. Al no poder realizar esta verificación y sin documentos de soporte ante la entrega, no es posible determinar e incurrir en un posible riesgo de perdida de información o no poder cumplir con los compromisos establecidos en los contratos.

Igualmente, 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.



Distanciamiento de equipos instalados – **Fuente**: Foto de equipo de auditoría Control Interno



Toma de seriales por comando – **Fuente**: toma de pantalla llamada celular equipo de auditoría Control Interno

7.6. 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 y hardware realizado por la OGI el cual fue remitido a la OCI tras solicitud formal, se evidencia lo siguiente:

No.	SOFTWARE	LICENCIAS INSTALADAS	LICENCIAS ADQUIRIDAS
1	Licencias Officce 365 Enterprise E3	229	235
	Licencias MSOfficce 365 Enterprise E3	510	515
2	Licencias Power BI Pro	65	70
3	Licencias Project para Officce 365	5	5
4	GSE Globalsign extend ssl-vigencia 2 años / Global extend san adicional - vigencia 2 años, GSE- Contrato 041-2018	1	1
5	UNION TEMPORAL SISTEMA DE REDES DE DATOS (SIEM) Contrato 115-2019	1	1
6	Microsoft@windowsserverCAl 2016OLP 1License NoLevelDvcCAL, GOLD SYS Contrato 031-2018 Microsoft@WinwodsserverExternalConnector2016 GovemmentOLP1License Qualifield, GOLD SYS Contrato 031-2018	250	250
	Microsoft@WinwodsserverExternalConnector2016 GovemmentOLP1License Qualifield, GOLD SYS Contrato 031-2018	2	2
	Acrobat Pro DC GOLD SYS Contrato 031-2018	4	4
	Creative Cluod GOLD SYS Contrato 031-2018	2	2
7	(SQLSvrEntCore LicSAPkOLP, NIMBUTECH Contrato 052-2020	4	4
	Licencias Microsoft SqlServer Enterprise (SQLSvrEntCore LicSAPkOLP), NIMBUTECH, Contrato 052-2020	4	4
	Licencias de Visual Studio Profesional 2017a perpetuidad, NIMBUTECH Contrato 001-2018	2	2
	Licencias WinRmtDsktpSrvcsCAL 2019 OLP NL UsrCAL Contrato 052-2020	400	400
8	Kaspersky Endpoint Security for Business Advanced, Infocomunicaciones Contrato 023-2017 y 098-2020	753	753
9	Licencias ESSENTIAL 12 MONTHS RENEWAL FOR BACKUP EXEC V-RAY ED WIN 1 CPU ONPREMISE STANDARD PERPETUAL LICENSE GOV, Interlan Contrato 079-2017	12	12
	Licencias ESSENTIAL 12 MONTHS RENEWAL FOR BACKUP EXEC OPT LIBRARY EXPANSION WIN 1 DEVICE ONPREMISE STANDARD PERPETUAL LICENSE GOV, Interlan Contrato 079-2017	2	2
	Backup Exec Agent For Win 1 Server Onpremise standard perpetual Licencse	0	5
10	Renovación de licencias de SQL server Enterprise Edition con software assurance , Softwareone Colombia SAS Contrato 034-2017	0	2
	Licencias de Visual Studio Profesional with MSDN Qualified Government, Softwareone Colombia SAS Contrato 034-2017	3	3

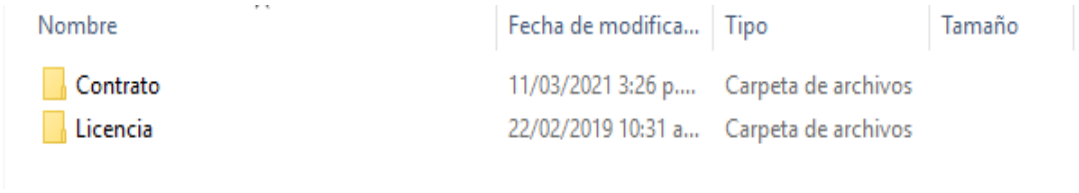
No.	SOFTWARE	LICENCIAS INSTALADAS	LICENCIAS ADQUIRIDAS
11	Licencias de Visual Studio Softwareone Colombia SAS Contrato 077-2015	1	1
12	Adquisición de licencia corporativa a perpetuidad del aplicativo PCSECURE – PC ADMIN, PCtechSoft contrato 006A-2017	596	596
13	Licencia Telerik Devcraft Ultimate, CYBERIA COLOMBIA LTDA - Contrato 045 - 2016	1	1
	Licencias Telerik Devcraft Complete, CYBERIA COLOMBIA LTDA - Contrato 045 - 2016	4	4
	Licencia de inspinia, CYBERIA COLOMBIA LTDA - Contrato 045 - 2016	1	1
14	Licencia Enterprise Architect Corporate Edition - Floating License, SOFTWARE SHOP DE COLOMBIA SAS - Contrato 081-2016	7	7
15	Licencias WinSvrDataCtr 2012R2 OLP NL Gov 2Pro Qlfd, COMPUTEL SYSTEM - Contrato 25-2015	3	8
	Licencias SQLSvrEntCore LicAPk OLP 2Lic Gov Core Lice Qldf, COMPUTEL SYSTEM - Contrato 25-2015	2	2
	Licencias SQLSvrEntCore 2014 OLP 2Lic Gov Core Lice Qldf, COMPUTEL SYSTEM - Contrato 25-2015	2	2
	WinSvrCAL 2012 OLP NL Gov DvcCAL DÓLAR	300	300
	PrjtProO365Open ShrdSvr SubsVL OLP NL Annual Gov Qlfd	2	10
	Visio Std LicSAPkOLP NL Gov	10	10
	SYMC BCKUP EXEC 15 AGENT FOR WINWODS WIN PERSERVER BNLD STD STD EXPREESS BND ESSENTI 12 MONTHD, COMPUTEL SYSTEM - Contrato 25-2015	0	4
16	Licencia suite especializada de diseño para creativos - ADOBE CREATIVE CLOUD (2015), GREEN FON GROUP SAS - Contrato 41-2015	1	1
17	Licencias Gids Cliente - Server xra carteleras Cliente 1 -Server 1,SOLUTEKA - Contrato 32-2015	0	2
18	GLPI, Free softwar distribited under GNU/GPL version 2 licence - http://www.gnu.org/licenses/old-licenses/gpl-2.0.html	1	1
19	Licencia SEVEN y KACTUS - Digitalware - CANTIDAD 1	0	1
20	Licencia BackupExec 2015 Server Onpremise Estándar Licencse para servidor- Itecsa 128	0	1

No.	SOFTWARE	LICENCIAS INSTALADAS	LICENCIAS ADQUIRIDAS
21	21. CONT. 063-2020 NUTANIX Y CITRIX - ADSUM	144	144
	21. CONT. 063-2020 NUTANIX Y CITRIX - ADSUM	42	42
	Citrix ADC Instance pool for VPX, CPX & BLX Softwa 2 re ADC 3-year Subscription (per instance)	2	2
	Citrix ADC Bandwidth pool for VPX, CPX & BLX Softw 3 are ADC 3-year Subscription Advanced Edition (per	3	3
26	Licenciamiento SEVEN y KACTUS- Actual - Digitalware	2	2
28	plataforma Issabel	1	1

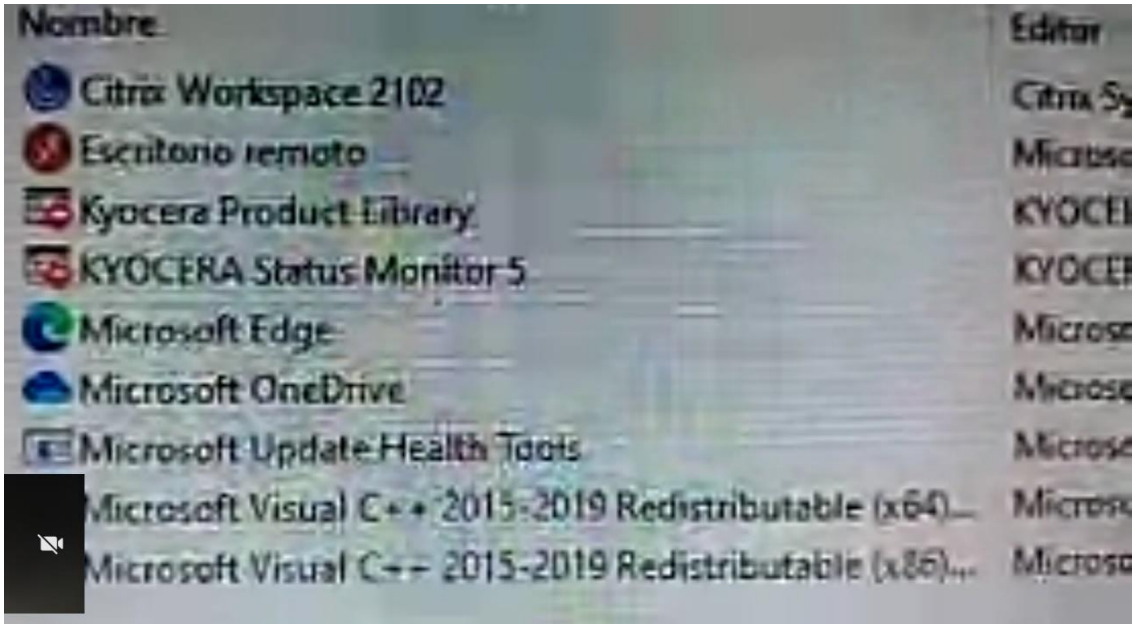
La entidad tras el requerimiento de la OCI, suministro la copia digitalizada de cada uno de los contratos que soportan la información relacionada en la tabla anterior así:



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



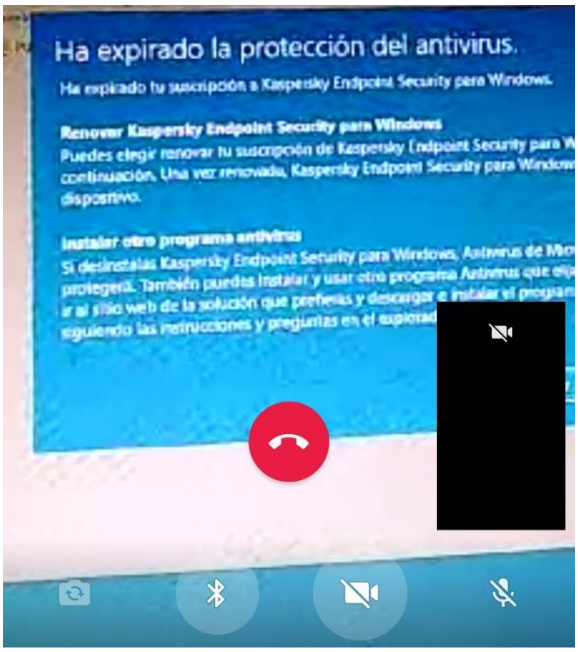
Los soportes aportados por la Oficina de Gestión de la Información permite determinar un cumplimiento de la entidad respecto a los términos y condiciones establecidas dentro de cada una de las cláusulas que están acordes con solicitado y demostrado por el área responsable, lo que blinda a la entidad 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.



Software instalado Localmente – **Fuente**: toma de pantalla llamada celular equipo de auditoría Control Interno

Sin embargo, con lo anteriormente enunciado sobre los inventarios físicos entregados que fue explicado en un punto previo. No fue posible determinar los equipos entregados al anterior contratista (Microhard) fueron entregados en su totalidad, si existe alguna observación de daño físico o faltante y como fue manejada la información residual que podría quedar dentro de los medios de almacenamiento dentro de los equipos (disco duros) Con respecto al PCSECURE (software para llevar el inventario de equipos) en las terminales de los nuevos equipos esta auditoría no tiene evidencia de esta instalación (revisado mediante panel de control).

En cuatro (4) equipos en la regional occidente (Medellín) se encontró que la licencia de Kaspersky (software de seguridad antivirus) había expirado la licencia, esto se identifica mediante un mensaje de alerta que genera el mismo aplicativo como se adjunta en la evidencia fotográfica.



Pantalla de advertencia expiración licencia – **Fuente**: toma de pantalla llamada celular equipo de auditoría Control Interno

En el alcance de esta auditoría no se realiza revisión de las terminales actuales, debido a que se terminó su instalación en los primeros meses del 2021, y el alcance determinado fue hasta finales del año 2020.

- **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.

8. EVALUACIÓN DE CONTROLES Y RIESGOS

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.

8.1. 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 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-TE1-164 - Proceso de Gestión de la Infraestructura Tecnológica:
P-TE4-163 - Procedimiento control de Software
PE-TE4-094 - Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica
N-TE1-017 - Instructivo de Borrado Seguro
P-TE1-203 - Procedimiento de Monitoreo de la Infraestructura Tecnológica

8.2. Oportunidad de Mejora #2 - 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, se encuentra en casos dentro de la regional del norte que los equipos aún no se encuentran dentro del dominio y los usuarios para poder utilizar el recurso informático tienen que ingresar mediante usuario local

genérico, permitiendo de esta manera si puedan guardar, descargar o administrar archivos y que no sea aplicado a estos la política de seguridad de la información. Además de permitir posibles instalaciones de programas no autorizados, los cuales a su vez se incrementaría la probabilidad de no tener licencias de software instalado.

8.3. Oportunidad de Mejora #3 – Inventario (desempeño bajo):

Debido a la implementación de las terminales y los protocolos de bioseguridad actualmente ejecutados, no se tiene todas las maquinas instaladas en las instalaciones de la entidad, por lo que no se puede realizar la revisión total del parque computacional. También existe la incidencia que el anterior proveedor (Microhard) no ha emitido ante la SAE un certificado donde se indique el estado, cantidad y fecha de entrega definitiva de estos elementos. Al igual que una verificación que la información que podría estar almacenada dentro de los dispositivos (discos duros) fue sometida a un borrado seguro y el resultado de dicho procedimiento. Igualmente poder determinar que no existen faltantes en las existencias entregadas que pueda incidir en reclamos a futuro por parte del proveedor donde la ubicación y respectiva entrega pueda dificultarse debido a la dificultad de volver a ubicar un recurso en el paso del tiempo.

Esto también podría tener incidencia en posibles licencias de programas o herramientas que hayan quedado instaladas, debido a que sería una incongruencia en los controles que se lleva de manera interna por parte de la SAE y de acuerdo con posibles usos no autorizados al dejarlos instalados por otras personas podría aplicar sanciones o multas por parte de algún ente rector o casa programadora dueña de la licencia.

Ante estos documentos faltantes es importante que la SAE cuente a la mayor brevedad posible con dichas certificaciones para así poder tener la seguridad o el soporte documental que se realizó la entrega de manera correcta con todas las garantías.

8.4. Oportunidad de Mejora #4 - 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.

De acuerdo con esto, para que la efectividad del control sea mayor, es necesario que todos los equipos se encuentren dentro del dominio corporativo y que a su vez solo sea posible el ingreso de usuarios mediante su usuario respectivo, esta situación evita que el usuario realice instalaciones sin autorización de la OGI y su mesa de ayuda de programas no autorizados.

9. CONCLUSIONES Y RECOMENDACIONES GENERALES

Efectuar la implementación de la plataforma de Citrix es una infraestructura que 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 puedan comprometer la seguridad de la información.

Es importante manejar de manera mas correcta la creación de usuarios que sean acordes con los lineamientos establecidos por la organización, debido a que se encontraron no solamente errores de nombres con respecto a la relación entregada por la gerencia de talento humano, sino nuevos casos que no están alineados con la métrica que se debe utilizar al crear nuevos perfiles de usuarios.

Nuevamente y como se realizó en anteriores auditorías, 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 procedimientos como el P-TE4-094 procedimiento administración y control de acceso a usuarios ya poseían observaciones sobre este tema.

Realizar la validación que todos los equipos disponibles para el uso de los usuarios en las diferentes sedes se encuentren dentro del dominio corporativo establecido; esto para asegurar que todas las directivas, políticas, normas y restricciones que se establezcan de manera centralizada en la red sean adoptadas por todos los equipos de cómputo que se conecten a la LAN de la entidad. Y así evitar posibles ataques o daños por software malicioso o por mala utilización de los recursos. En este punto es importante recordar que se encontraron en una regional que los equipos no poseían licencias actualizadas, por lo que también al tener estos equipos registrados en el dominio también se evitarían posibles desactualizaciones o mal funcionamientos de software.

Continuar con las estrategias de sensibilización a toda la planta de empleados de la entidad sobre los temas de políticas de seguridad de la información, para que se vuelva parte de una cultura empresarial generalizada permitiendo así un mayor desempeño de los recursos tecnológicos.

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.

Se solicitó de manera concurrente la certificación de entrega de los equipos del anterior proveedor y así poder confirmar que la totalidad de los equipos fueron entregados, que los inventarios entregados por la Oficina de la Gestión de la Información correspondían con la realidad, que no existió alguna reclamación por posible daño o perdida y que la información que podía estar aún almacenada sufrió un borrado seguro y que no exista una filtración posterior a entrega o un uso no autorizado de información perteneciente a la SAE. A fecha de entrega de este informe aún no se ha recibido dicha certificación o documento relacionado que permita garantizar que el proceso de entrega haya sido culminado a satisfacción de las partes o que la información que podrían poseer los equipos no sea extraída, comercializada y/o utilizada por terceros no autorizados. Al igual que existir un riesgo de incumplimiento en las cláusulas de contrato con sus respectivas acciones de acuerdo a lo estipulado en este.

Cordialmente,

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

Aprobó: María del Pilar Mayor Varela.

Elaboró: Jairo Andrés González Vaca