Gobierno de Colombia

Bogotá D.C, 13 de marzo de 2026

PARA: *Amelia Pérez Parra*
Presidenta

DE: *Oficina de Control Interno*

ASUNTO: **Informe anual de seguimiento, verificación y recomendaciones independientes en materia de derechos de autor y uso de software legal para la vigencia de 2025.**

Respetada Doctor(a) Amelia,

En el marco de las funciones asignadas a la Oficina de Control Interno (OCI) y en cumplimiento del Plan Anual de Auditoría aprobado para la vigencia 2026, se adelantó la Evaluación Independiente del cumplimiento de la normativa en materia de derechos de autor, con especial énfasis en el uso de legal de software, correspondiente a la vigencia 2025.

El ejercicio evaluativo tuvo como propósito verificar el cumplimiento de la Sociedad de Activos Especiales S.A.S. respecto de las obligaciones relacionadas con la legalidad del software instalado en los equipos institucionales, la existencia de inventarios actualizados, los soportes de licenciamiento, así como los controles implementados para la instalación, uso y baja de software.

Para tal fin, la Oficina de Control Interno evaluó lo establecido en los procedimientos de la Entidad, tomando como insumo la información suministrada por las áreas responsables, de conformidad con la herramienta oficial definida por la DNDA para el reporte del Informe de Derechos de Autor, y en armonía con los principios del Sistema de Control Interno de la entidad.

Cordialmente,

Beisner E. Arboleda P.
Beisner Elipson Arboleda Palacios
Oficina de Control Interno

Elaboró:
Carolina Aguilera Martínez - *PII*
Sandra Jazmín Durán Sierra - *PIII*

Revisó: *Beisner Elipson Arboleda Palacios* - *PEIII – Encargado de la OCI.*
Aprobó: *Beisner Elipson Arboleda Palacios* - *PEIII – Encargado de la OCI.* Beisner E. Arboleda P.

ARCHIVO: *164.01*

INFORME ANUAL DE SEGUIMIENTO, VERIFICACIÓN Y RECOMENDACIONES INDEPENDIENTES EN MATERIA DE DERECHOS DE AUTOR Y USO DE SOFTWARE LEGAL PARA LA VIGENCIA 2025

VIGENCIA 2025

MARZO DE 2026

1. INTRODUCCIÓN

En cumplimiento del Plan Anual de Auditoria 2025, basado en riesgos, la Oficina de Control Interno realizó una evaluación independiente del Sistema de Control Interno Institucional, enfocada en verificar el cumplimiento de la normativa vigente en materia de derechos de autor sobre software.

Esta verificación se desarrolló en el marco de la Directiva Presidencial No. 02, la Circular No. 017 de 2011 y la Circular Externa No. 027 de 2023, emitidas por la Dirección Nacional de Derecho de Autor, que establecen la obligación de las entidades públicas de verificar el uso legal de software y publicar el informe correspondiente en el micrositio dispuesto para tal fin.

En cumplimiento de este marco normativo, la Oficina de Control Interno llevó a cabo las actividades necesarias para: (i) verificar la cantidad de equipos tecnológicos con los que cuenta la Sociedad de Activos Especiales; (ii) constatar el número de licencias de software adquiridas, así como el software libre o gratuito instalado; (iii) evaluar la aplicación de controles orientados a garantizar el cumplimiento de las disposiciones en materia de derechos de autor, previniendo la instalación de software no licenciado; y (iv) revisar las políticas y procedimientos aplicables para la baja de software. Lo anterior con el propósito de fortalecer el cumplimiento normativo, mitigar riesgos legales y contribuir al mejoramiento continuo del Sistema de Control Interno Institucional.

2. OBJETIVO GENERAL

Verificar el cumplimiento de la normativa vigente en materia de derechos de autor sobre software en los equipos de cómputo de la Sociedad de Activos Especiales S.A.S., de conformidad con la Directiva Presidencial N. 002 y la circular N. 017 de 2011 de la Dirección Nacional de Derecho de Autor, mediante la revisión del inventario de software, los controles de instalación y los procedimientos de baja, en atención a las responsabilidades asignadas a las Oficinas de Control Interno.

2.1. Objetivos especificos

- *Evaluar y verificar el seguimiento a los mecanismos de control implementados para prevenir la instalación de programas o aplicativos que no cuenten con la respectiva licencia en los equipos de cómputo de la entidad.*
- *Evidenciar la aplicación de los lineamientos y mecanismos de control definidos para la instalación y uso de software estándar libre en los equipos de cómputo de la Sociedad de Activos Especiales S.A.S.*
- *Revisar el nivel de implementación de las recomendaciones formuladas por la Oficina de Control Interno en el informe de derechos de autor correspondiente a la vigencia 2024, ejecutadas durante la vigencia 2025.*
- *Evaluar la gestión del riesgo asociada al licenciamiento de software, incluyendo la identificación, tratamiento y controles establecidos para mitigar posibles incumplimientos en materia de derechos de autor.*

3. ALCANCE

Para la presentación del informe ante la Dirección Nacional de Derecho de Autor - DNDA, la Oficina de Control Interno realizó una evaluación independiente, dando cumplimiento a las normas y técnicas de auditoría generalmente aceptadas, orientada a verificar el inventario de hardware (equipos de cómputo), el software instalado, los controles implementados, los riesgos identificados, y el nivel de conocimiento y aplicación de la Política de Seguridad de la Información de la Sociedad de Activos Especiales S.A.S.

La verificación se efectuó con base en el inventario y la información suministrada por la Oficina de Tecnologías y Sistemas de la Información - OTI, con corte al 31 de diciembre de 2025.

3.1. Limitación al alcance



En el desarrollo del presente informe, la Oficina de Control Interno ejecutó las actividades de evaluación conforme con las funciones establecidas en la Ley y a los procedimientos internos vigentes. No obstante, el alcance del trabajo se vio limitado por la siguiente situación:

- *Ausencia de soportes/registros/respuesta para verificar las evidencias de la Dirección Territorial Sur, dado que la Dirección Territorial sur no remitió respuesta a esta Oficina sobre la confirmación de acompañamiento para el levantamiento de esta información.*

En consecuencia, los resultados, conclusiones y recomendaciones aquí consignados se fundamentan exclusivamente en la información efectivamente suministrada y disponible al momento de la evaluación.

4. METODOLOGÍA

En cumplimiento del Plan Anual de Auditoría – vigencia 2026 y del rol de la Oficina de Control Interno como actividad independiente y objetiva de evaluación y seguimiento que contribuye al mejoramiento continuo de los procesos de gestión, control y administración del riesgo de la Entidad, en ese sentido, se solicitaron las evidencias relacionadas con el cumplimiento de la normativa en materia de derechos de autor de software para el informe de seguimiento correspondiente a la vigencia 2025.

Lo anterior tuvo como finalidad revisar la consistencia de los datos, verificar las evidencias aportadas, analizar los archivos remitidos y evaluar la documentación aplicada. Adicionalmente, con el acompañamiento de un designado de la mesa de servicio de la OTI, se realizó una verificación en sitio mediante muestra aleatoria, con un total de 176 puntos físicos distribuidos en la Sede Nivel Central, Archivo y Correspondencia, Direcciones Territoriales y Agencias, en la cual se revisaron los equipos de cómputo asignados a los trabajadores y trabajadores de la SAE S.A.S., verificando el hardware y el software instalado, mediante la captura de evidencias de cada equipo de la muestra revisando el escritorio, carpetas de documentos y descargas e información del sistema con las especificaciones del dispositivo, así como el listado de programas y características con el fin de validar la legalidad del software. En sitio se realizó la prueba de recorrido a equipos aleatorios de la muestra, intentando descargar e instalar software libre con usuario sin privilegios de instalación en el equipo.

En ese contexto, para la elaboración del Informe de Derechos de Autor sobre Software vigencia 2025, la Oficina de Control Interno adelantó la evaluación conforme con sus funciones, solicitando la información a las áreas responsables, la suscripción de la carta de representación y evaluación integral de las evidencias suministradas.

5. CRITERIOS APLICABLES

El desarrollo de este informe se fundamentó en el siguiente marco normativo y documental vigente, aplicable a la gestión del control interno de la Entidad, el cumplimiento de los derechos de autor y el uso legal de Software en la SAE S.A.S.:

5.1. Normativa externa

- *Ley 87 de 1993, "por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado", en especial lo dispuesto en el artículo 2°, literales a), e) y f), relacionados con la protección de los recursos de la entidad, la confiabilidad de la información y la evaluación independiente del Sistema de Control Interno.*

- *Directiva Presidencial No. 002 del 12 de febrero de 2002, numeral 2, mediante la cual se imparten instrucciones a las entidades públicas para garantizar el uso legal de software debidamente licenciado.*

- *Circular No. 04 del 22 de diciembre de 2006, expedida por la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor (DNDA), mediante la cual se establecen lineamientos para la verificación, seguimiento y reporte del uso legal de software en las entidades públicas.*
- *Circular No. 17 del 1.° de junio de 2011, expedida por la Dirección Nacional de Derecho de Autor, que asigna a las Oficinas de Control Interno la responsabilidad de verificar el cumplimiento de la normativa en materia de derechos de autor sobre software y remitir la información correspondiente a esta entidad.*
- *Circular Externa No. 027 del 29 de diciembre de 2023, de la Dirección Nacional de Derecho de Autor, que define los lineamientos y plazos para la presentación del informe anual de derechos de autor por parte de las entidades públicas.*

5.2. Normativa interna

- *PG-TI-001 Política de Seguridad y Privacidad de la Información - V03, fecha 06/05/2025*
- *PR-TI-008 Procedimiento para control de Software - V04, fecha 07/03/2025*
- *PR-TI-006 Procedimiento de seguridad para los dispositivos tecnológicos institucionales – V04, fecha 04/04/2025*
- *PR-TI-007 Procedimiento monitoreo de la Infraestructura Tecnológica - V03, fecha 09/06/2025*
- *PR-MS-001 Procedimiento requerimientos e incidentes de Tecnología – V04, fecha 13/03/2025*
- *PR-TI-002 Procedimiento de gestión de usuarios plataforma tecnológica – V10, fecha 16/06/2025*
- *PR-TI-003 Procedimiento incidentes de seguridad de la información – V03, fecha 18/112/2025*
- *PR-GA-006 Procedimiento para la baja de bienes devolutivos propiedad de la SAE S.A.S. – V05, fecha 05/12/2024*

6. RESULTADOS

En atención al cuestionario emitido por la Dirección Nacional de Derechos de Autor, la Oficina de Control Interno (OCI) realizó pruebas de recorrido orientadas a verificar el cumplimiento de las políticas internas relacionadas con la gestión, el control y la instalación de software en la entidad.

Para el desarrollo de estas pruebas se seleccionó una muestra de ciento setenta y seis (176) computadores portátiles, tomada de los 1.122 equipos reportados por la OTI para la vigencia 2025. Esta muestra corresponde aproximadamente al 15,7% del total, garantizando una cobertura representativa de las diferentes áreas de la Sociedad de Activos Especiales (SAE). El ejercicio contó con el acompañamiento de un funcionario designado por la mesa de servicio de la Oficina de Tecnologías y Sistemas de la Información (OTI), quien brindó el soporte técnico necesario para la validación.

La muestra incluyó equipos asignados a distintos procesos y áreas, con el fin de garantizar representatividad institucional y cubrir diferentes perfiles de usuario, lo que permitió obtener una visión transversal del cumplimiento de las políticas internas relacionadas con la instalación y gestión de software. Esta distribución favorece la representatividad del ejercicio, al abarcar perfiles de usuario y dinámicas operativas.

A continuación, se relacionan los equipos y usuarios incluidos en las pruebas realizadas:

Tabla 1. Muestra

Equipo	Usuario	Equipo	Usuario	Equipo	Usuario	Equipo	Usuario
P34ARCHIVO52	jborda	P35DIRCON04	jarodriguez	PDTCAR133	pgutierrez	P38OTI70	pestepa
P34DALM01	wahernandez	P35DIRCON07	magalvisp	PDTCAR136	caibanez	P38OTI71	mparra
P34DALM07	diklopez	P35DIRCON09	jmantique	PDTCAR147	ldealba	P38OTIPRESTA01	kpenuela
P34DALM12	dbadillo	P35DIRFINAN18	pesanchez	PDTCAR156	dapadilla	P33DIRDAIR14	legonzalez
P34DALM15	mgaitan	P35DIRFINAN22	csierra	PDTCO54	magomezs	P33GEDEP26	alicona
P34DALM40	mamontero	P35DIRFINAN24	analvarez	PDTOCC05	lcastro	P36DIRDAIR46	shgomez
P34DALM41	mrodriguez	P35DIRFINAN29	oalvarado	PDTOCC23	abello	P36DIRDAIR57	anmolina
P34DALM51	damartinezd	P35DIRFINAN35	josorio	PDTOCC32	hbetancur	P36DIRDAIR59	ecaicedo
P34DALM80	jhhernandez	P35DIRFINAN51	ajflores	PDTOCC36	mherrera	p36dirdaiu19	juocampo
P34DALM89	lprodriguez	P35DIRFINAN78	aguerra	PDTOCC41	macastano	P36DIRDAIU38	spenalozs
P34DAM05	lreyes	P35DIRTH02	joprieto	PDTOCC53	mobregon	P36DIRDAIU45	ncalderon
P34DIRADMIN04	esanabria	P35DIRTH08	aidiaz	PDTOCC55	ardaza	P36DIRDAM03	cagarzon
P34DIRADMIN11	gmoreno	P35DIRTH19	lculma	PDTOCC60	mramos	P36DIRDAM09	bcastro
P34DIRADMIN13	yzabala	P35DIRTH20	agranados	PDTOCC61	jmacias	P36DIRDAM27	agonzalez
P34DIRADMIN15	pagarcia	P35DIRTH37	hediaz	PDTOCC62	daflorez	P36DIRDAM38	jpoveda
P34DIRADMIN22	yapineda	P35DIRTH64	lumuñoz	P06DALM10	ncastilla	P36DIRDAM60	sevargas
P34DIRADMIN38	rbenguera	P35VICECOR25	lguzman	P06DTC015	jbonza	P36DIRDAM70	ealayon
P34DIRPROY05	mmoscoso	P35VICECOR26	kreascos	P06DTCO01	mamodriguez	P38DIRDAIR06	jsfernandez
P34DIRPROY07	kariza	P7DIRGCDS80	lcrtiz	P06DTCO02	lcastaneda	P107OPC04	mdelgado
P34DIRPROY25	jdcortes	P32PRESI26	jupulido	P06DTCO03	ovalenzuela	P32DIRCOM07	ksuarez
P34OCI02	fburbano	P37DIRGCDS09	jjmartinez	P06DTCO06	achaves	P32DIRCOM11	yroa
P06DTCO81	apascuas	P37DIRGCDS13	macorrea	P06DTCO08	lguerrero	P32DIRCOM15	amois
P33DDIP04	rospina	P37DIRGCDS16	mlinares	P06DTCO44	lzamora	P32DIRCOM31	sarias
P33DDIP11	sgallo	P37DIRGCDS38	wpedroza	P06DTCO68	lpatino	P32DIRCOM51	mfranco
P33DDIP15	mpardo	P37DIRGCDS80	mgarzon	P06DTCO92	hfigueroa	P32DIRCOM58	maacosta
P33DDIP40	djamaica	P37DIRGCDS82	vcandamil	P06DTCO99	mmendez	P32DPP15	sburgos
P33DIRAAV03	joruiz	P37DIRGCDS127	ksalamanca	P06DTCO108	ccastano	P32DPP38	ptacha
P33DIRAAV28	mpmeciado	P37DIRSCL09	ecurcio	P06DTCO118	acarbono	P32OIAC06	nmarin
P33DIRAAV31	szamudio	P37DIRSCL13	dcaro	P06DTCO121	kbastidas	P32OIAC11	vhuertas
P33DIRAAV36	lirodriguez	P37DIRSCL35	ufajardo	P06DTCO131	lposada	P32OIAC13	lamejia
P33DIRAAV37	jcastellanos	P37DIRSCL45	dardila	P06DTCO132	jquinones	P32OPC01	lguevara
P33DIRAAV41	alfranco	P37DIRSCL99	amartinezm	P38GERAS10	dnunez	P32OPC22	lpenuela
P33DIRAAV53	joorozco	P37OCI02	cavila	P38GERAS12	jperdomo	P32PRESI77	hbautista
P33DIRAAV77	nbrito	P37VICESOC77	damaya	P38GERAS19	vgalindo	P32PRESI122	dpalomino
P33DIRAAV79	wpadilla	P37VISESOC15	dmunito	P38GERAS20	lcuadros	DIRPER07	sunibe
P33GEDEP004	epaez	P38OCI25	wramirez	P38OTI05	yguaiteros	PBMANGA01	eyhernandez
P33GEDEP11	ktorres	PDTCAR09	ddelacruz	P38OTI06	sramirez	PMONTERIA01	iojeda
P33GEDEP21	fbautista	PDTCAR11	ymontoya	P38OTI14	carodriguez	PARCHIVO33	mmorales

Equipo	Usuario	Equipo	Usuario	Equipo	Usuario	Equipo	Usuario
P33GEDEP45	mvillanueva	PDTCAR31	jbohorquez	P38OTI20	ljrodriguez	PARCHIVO41	jforozco
P33VICEOP03	jcardozo	PDTCAR48	mcjimenez	P38OTI22	jzamudio	PARCHIVO43P	jpinzon
P33VICEOP06	cvgonzalez	PDTCAR57	scabrera	P38OTI24	edpena	PARCHIVO70	squinones
P35DIRADMIN22	cgranados	PDTCAR60	anmorales	P38OTI45	jesalinas	PARCHIVO82	lgil
P38DIRDAIR04	kgiraldo	PDTCAR62	casoto	P38OTI50	mcamargo	PARCHIVO83	jmonroy
P35DIFINAN52	osolano	PDTCAR106	alovar	P38OTI69	jpereira	PARCHIVO85	dpintor

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

La Oficina de Control Interno (OCI) dio respuesta a los requerimientos establecidos en el cuestionario de la Dirección Nacional de Derecho de Autor y publicó en la sede electrónica de la SAE el informe de seguimiento correspondiente. Asimismo, atendió lo dispuesto en la Circular 04 del 22 de diciembre de 2006, remitiendo a través de la página web de la Dirección Nacional de Derecho de Autor el Informe de Software de la Sociedad de Activos Especiales S.A.S., para la vigencia 2025.

6.1. Equipos de Cómputo

De acuerdo con la información suministrada por la Oficina de Tecnologías y Sistemas de la Información (OTI), la Sociedad de Activos Especiales, contaba para la vigencia 2025, con un total de 1.122 equipos de cómputo.

En el marco del requerimiento efectuado por la Dirección Nacional de Derecho de Autor, la Oficina de Control Interno (OCI) reportó la distribución de estos equipos por tipología, clasificándolos en MiniPC, Notebook y Desktop, tal como se presenta en la Tabla 1.

Tabla 2. Computadores Vigencia 2025

Ubicación	Mini PC	Notebook	Desktop	Total General	Ubicación	Mini PC	Notebook	Desktop	Total General
Archivo Central	0	40	2	42	San Martin Piso 32	0	88	0	88
Barranquilla	0	73	0	73	San Martin Piso 33	0	121	0	121
Cali	0	89	0	89	San Martin Piso 34	0	124	0	124
Medellín	0	67	0	67	San Martin Piso 35	0	111	2	113
Bucaramanga	0	4	0	4	San Martin Piso 36	0	84	0	84
Montería	0	3	0	3	San Martin Piso 37	1	102	0	103
Pereira	0	6	0	6	San Martin Piso 38	1	93	0	94
San Martin Piso 1 (Atención al Ciudadano)	0	8	0	8	San Martin Piso 39	0	0	2	2
San Martin Piso 6	0	92	0	92	Solución Copy	0	0	9	9
					Total General	2	1105	15	1122

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

En desarrollo de las pruebas efectuadas, se revisó el archivo de soporte denominado "Software y Hardware equipos rentados v3", el cual contiene el inventario detallado de los equipos de cómputo rentados por la Sociedad de Activos Especiales S.A.S. El archivo incluye información relacionada con: ciudad, piso, área, nombre del equipo, número de serie, tipo de equipo, sistema operativo (versión, ID del producto y número de serie), modelo, componentes (procesador, número de núcleos, memoria, tipo y tamaño de disco duro), redes (IP), usuario asignado, última

actualización, antivirus, volúmenes (tamaño global y espacio libre), software instalado, entre otros datos técnicos relevantes.

De acuerdo con la muestra seleccionada de 176 equipos de cómputo, y con base en la validación física realizada en sitio, se evidenció que 8 equipos (equivalentes al 5 % de la muestra) no cumplen con la estructura actualizada de nombramiento, específicamente en lo relacionado con el piso donde se encuentran ubicados.

Lo anterior incumple lo dispuesto en el Procedimiento PR-TI-002 PROCEDIMIENTO DE GESTIÓN USUARIOS PLATAFORMA TECNOLOGICA Versión No.10 V 16/06/2025..." El nombramiento de computadores portátiles asignados tendrá la siguiente estructura: La P corresponde a portátil, la N corresponde a NUC, piso, iniciales del área, consecutivo ejemplo: Un portátil, que se encuentra en el Piso 32, en la dependencia de Despacho de Presidencia, sería nombrado: P32PRESI01"

A continuación, se relacionan los ocho (8) equipos en los cuales se evidenció diferencia entre el nombramiento registrado y la ubicación física verificada:

Tabla 3. Nombramiento de Computadores portátiles asignados vs ubicación física

Fecha Muestra	Piso	Equipo	Usuario	Dependencia
10/02/2026	33	P06DTCO81	apascuas	Vicepresidencia Operativa
10/02/2026	33	P35DIRADMIN22	cgranados	Dirección de Control del Inventario
10/02/2026	33	P38DIRDAIR04	kgiraldo	Dirección para la Democratización de Activos Inmuebles Rurales
11/02/2026	37	P7DIRGCDS80	lortiz	Dirección de Gobierno, Control y Democratización de Sociedades
11/02/2026	37	P32PRESI26	jupulido	Dirección de Seguimiento y Control de Liquidaciones
11/02/2026	37	P38OCI25	wramirez	Oficina de Control Interno
17/02/2026	36	P33DIRDAIR14	legonzalez	Dirección para la Democratización de Activos Inmuebles Rurales
17/02/2026	36	P33GEDEP26	alicona	Dirección para la Democratización de Activos Inmuebles Rurales

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

La inconsistencia identificada, evidencia debilidades en la actualización y control del inventario tecnológico, particularmente en lo relacionado con la actualización del nombramiento de los equipos.

6.2. Licenciamiento Software Instalado en los Equipos de Cómputo

De acuerdo con los soportes suministrados por la Oficina de Tecnologías y Sistema de Información (OTI), se puede evidenciar que, el software instalado en los equipos de cómputo (portátiles y servidores) está debidamente licenciado y activado. Mediante consulta a portales como el centro de administración de Microsoft 365, sobre licenciamiento (SQL Server Standard LSA OLV, Visual Studio Pro-MSDN OLV, SQL Sever Enterprise Core LSA OLV), se evidencia que las licencias se encuentran vigentes para el período evaluado 2025.

Ilustración 1. Soporte de Licenciamiento Vigente



Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI)

En la Tabla 4 se relaciona el detalle del licenciamiento vigente para la vigencia 2025, incluyendo licencias de seguridad informática, herramientas de productividad, plataformas empresariales, infraestructura tecnológica, bases de datos, soluciones de respaldo, certificados digitales y sistemas misionales, indicando fechas de inicio y vencimiento o su carácter vitalicio, según corresponda:

Tabla 4. Licenciamiento para la Vigencia 2025

Nombre de la licencia	Fecha Inicio	Fecha Fin	Nombre de la licencia	Fecha Inicio	Fecha Fin
Trend Vision One Attack Surface Risk Management	10/10/2025	09/04/2026	Licencia FortiGate 600F 2 Year FortiCare Premium and FortiGuard	23/10/2025	31/12/2026
Trend Micro Cloud One - Conformity - Per Cloud Account	29/08/2025	28/04/2026	Unified Threat Protection (UTP)		
Trend Micro Cloud One - Workload Security with XDR	29/07/2025	28/04/2026	Licencia FortiSwitch-124F-POE 2 Year FortiCare Premium Support	22/10/2025	31/12/2026
Trend Vision One Credits	10/10/2025	09/04/2026	Licencia FortiSwitch-124F-POE 2 Year FortiCare Premium Support	22/10/2025	31/12/2026
Trend Micro Smart Protection Complete (Endpoints)	29/07/2025	28/04/2026	Licencia FortiAP-231F 2 Year FortiCare Premium Support	29/10/2025	31/12/2026
Trend Micro Smart Protection Complete (Endpoints)	10/10/2025	09/04/2026	LICENCIAS FORTIAP 231F	04/07/2025	31/12/2026
ArcGIS Enterprise Professional (formerly Standard) User	30/08/2025	31/08/2026	LICENCIA FORTISWITCH 148F POE	04/07/2025	31/12/2026
Type Month Subscription 11.5			LICENCIA FORTIANALYZER 300G	04/07/2025	31/12/2026
ArcGIS Pro Download	30/08/2025	31/08/2026	LICENCIA FORTIGATE 600F	04/07/2025	31/12/2026

Nombre de la Licencia	Fecha de	Fecha fin	Nombre de la licencia	Fecha de	Fecha fin
ArcGIS CityEngine Download	30/08/2025	31/08/2026	LICENCIA FORTIGATE 60HE	04/07/2025	31/12/2026
Mobile Map Pkgs for Navigator Download	30/08/2025	31/08/2026	LICENCIA FORTIGATE 40F	04/07/2025	31/12/2026
TreeSize Professional - Single License - with 12 months	30/12/2025	29/12/2026	LICENCIAS FORTIGATE 60F	04/07/2025	31/12/2026
al Maintenance - (Subscripción) - Auto-Renewal active			LICENCIA FORTIMANAGER 200G	04/07/2025	31/12/2026
Red Hat MW2000-Red Hat Application Foundations, Premium, (2 Cores or 4 vCPUs) 1 Año	30/12/2025	31/12/2026	LICENCIA FORTIAP 231F	04/07/2025	31/12/2026
Visio Plan 2	MENSUAL	MENSUAL	Licencia FORTISIEM	04/07/2025	31/12/2026
Planner and Project Plan 3	MENSUAL	MENSUAL	Licencia FORTIWEB VM 8 CPU	04/07/2025	31/12/2026
Microsoft Teams Enterprise	MENSUAL	MENSUAL	Licencia FORTISWITCH 124F POE	04/07/2025	31/12/2026
Microsoft 365 F5 (no Teams)	MENSUAL	MENSUAL	Licencia FORTISWITCH 148F POE	04/07/2025	31/12/2026
Microsoft 365 Copilot	MENSUAL	MENSUAL	SQL Server Standard LSA OLV	19/11/2025	19/11/2027
Microsoft Teams Rooms Pro	MENSUAL	MENSUAL	Visual Studio Pro MSDN OLV	19/11/2025	19/11/2027
Licencias sistemas ERP Seven	Vitalicias	Vitalicias	SQL Server Enterprise Core LSA OLV	19/11/2025	19/11/2027
Licencias Sistemas Kactus	Vitalicias	Vitalicias	LIC-02494626	01/10/2024	31/05/2028
certificado SSL - Wildcard OV 1 año	19/11/2025	19/11/2026	LIC-02494627	01/10/2024	31/05/2028
Licencia FortiGate-90G 2 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	23/10/2025	31/12/2026	243W003376335, LIC-02495823	12/10/2024	31/05/2026
Licencia FORTISWITCH 1024D	04/07/2025	31/12/2026	243W003376560, LIC-02496131	15/10/2024	31/05/2026
Licencias Lic. Ref:S1024-7528-48Y-6CAC-F - Item#: 2,00 und CTC-2025-0391	19/11/2025	31/12/2026	243W003376561, LIC-02496132	15/10/2024	31/05/2026
Licencias Lic. Ref: 97004-5326-48H-8XE - Item#: 1,00 und CTC-2025-0391	19/11/2025	31/12/2026	Licencia de soporte de copias de respaldo Nakivo	13/12/2024	Vitalicias
Licencia de la plataforma LUMU que soporta el servicio por un(1) año	03/04/2025	03/04/2026			

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

6.2.1 Software Básico

La Oficina de Tecnologías y Sistemas de la Información (OTI), proporcionó el archivo de Excel denominado "Programes Equipos SAE" en Mesa de Trabajo realizada el 26 de febrero de 2026, se informó que dicho listado corresponde al software básico que el personal de la Mesa de Servicio instala durante el proceso de alistamiento y configuración inicial de los equipos de cómputo.

La Tabla 5 presenta la relación de programas básico-incluidos en la imagen estándar de los portátiles, los cuales comprenden sistema operativo actualizado, herramientas de seguridad, utilitarios, navegadores, herramientas de productividad, software misional y aplicaciones de soporte institucional.

Tabla 5. Programas Básicos de Instalación de las imágenes de los portátiles

N.º	Programas	N.º	Programas
1	WINDOWS 11 VESRION MAS RECIENTE ACTUALIZADO	12	FORTICLIENT VPN
2	ANTIVIRUS TREND MICRO	13	ZEUS
3	PC SECURE	14	OFFICE 365
4	LUMU	15	POWER BI DESKTOP
5	GLPI AGENT	16	SCHIP SAE Y FRISCO CONTADURIA GENERAL DE LA REPÚBLICA
6	K-Lite Codec Pack (CODECS AUDIO VIDEO)	17	PUBLICA REDISEÑO
7	visual c++ redistributable CODECS	18	OLYMPUS
8	7-ZIP (Compresor de Archivos)	19	CONFIGURACION SEVEN - ERP Y KACTUS T.H.
9	ACROBAT READER	20	FUENTE DE ORFEO
10	GOOGLE CHROME	21	TEAMS ACTUALIZADO
11	MICROSOFT EDGE	22	PDF 24

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

En la prueba de recorrido realizada a los equipos de la muestra seleccionada con la finalidad de verificar software instalado no permitido, ingresando al panel de control en los equipos de cómputo según la ruta: Panel de control \Programas\" Programas y características" listar y descargar la imagen de pantalla de cada equipo para revisar si se instaló algún software no permitido.

Ilustración 2. Evidencia Programas Instalados – Equipo P32DIRCOM31



Fuente: Elaboración propia OCI

La Oficina de Tecnologías y Sistemas de Información, proporcionó la relación de programas que pueden ser instalados bajo demanda, previa solicitud tramitada a través de la Mesa de Servicio:

Tabla 5. Programas para instalar bajo demanda

BAJO DEMANDA	QGIS	CAMERCLOUD DESKTOP
	GOOGLE EARTH	SIRECI CONTRALORIA
	DWG VIEWER	SIPOST 4-72

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

De acuerdo con la información suministrada, se realizó prueba especifica sobre la instalación del aplicativo QGIS en la muestra seleccionada, en cumplimiento del procedimiento "PR-TI-008 Procedimiento para control de software – Versión No.04 – V 07/03/2025" ..."Actividad 7. Reemplazar con herramientas libres, validación de herramientas Open Source, solicitud de instalación de aplicaciones recibida mediante la mesa de Servicio. (con la trazabilidad e información relaciona de asignación de recursos tecnológicos)"

Como resultado de la validación, se identificaron equipos con instalación del aplicativo QGIS. Al realizar el cruce con los registros de la Mesa de Servicio, se evidenció que algunos equipos cuentan con el tiquete correspondiente, mientras que en otros casos no se encontró registro asociado:

Tabla 6. Muestra Programa a instalar bajo demanda QGIS Vs Tiquete Mesa de Servicio

HOSTNAME	USUARIO	NOMBRE	Dependencia	TICKET
P33DOIP04	rospina	Raul Ospina Cruz	Dirección de Control de Inventarios	Sin tiket relacionado
P36DIRDAIR59	ecaicedo	Esteban Caicedo Fernandez	Dirección para la Democratización de Activos Inmuebles Rurales	114241
P33DOIP11	sgallo	Susana Gallo Sanchez	Dirección de Control de Inventarios	Sin tiket relacionado
P33DIRAAV28	mpreciado	Marcos Elberto Preciado Guerrero	Dirección de Analitica, Alistamiento y Valoración	117780
P36DIRDAIR04	kgiraldo	Kelly Johana Giraldo Bermudez	Dirección para la Democratización de Activos Inmuebles Rurales	108343
P36DIRDAIR46	shgomez	Shirly Tatiana Gomez Rondon	Dirección para la Democratización de Activos Inmuebles Rurales	Sin tiket relacionado
P36DIRDAIR06	jshernandez	Juan Sebastian Fernandez Avella	Dirección para la Democratización de Activos Inmuebles Rurales	108778
P32DIRCOM51	mfranco	Miguel Arturo Franco Avila	Dirección comercial	122046
P33DOIP40	djamaica	Danny Jamaica Delgado	Dirección de Control de Inventarios	114476
P33DIRAAV37	jcastellanos	Jany Vanessa Castellanos Jimenez	Dirección de Analitica, Alistamiento y Valoración	123210

Fuente: Oficina de Tecnologías y Sistemas de la Información (OTI) – Elaboración OCI

6.3. Mecanismos de Control para la instalación de Software

En la Sociedad de Activos Especiales S.A.S., la Oficina de Tecnologías y Sistemas de Información ha implementado controles técnicos y administrativos orientados a prevenir la instalación de software no autorizado s o sin licenciamiento en los equipos de cómputo de la entidad. En cuanto a los controles técnicos, se evidenció la adopción de diversos mecanismos diseñados para restringir, supervisar y asegurar el uso adecuado del software corporativo.

- *Herramienta PCSECURE: utilizada para el control de bloqueo de ejecución de archivos y la restricción de instalación de programas ejecutables en los equipos de los funcionarios, así como para limitar el acceso a configuraciones locales del sistema.*
- *Restricción de privilegios de administrador: los usuarios finales no cuentan con permisos de administrador local en sus equipos. Únicamente el personal autorizado de la Mesa de Servicio de la OTI dispone de credenciales con privilegios para realizar instalaciones o configuraciones.*
- *Políticas de Directorio Activo: mediante la asignación de roles y perfiles se restringe la instalación de software, exigiendo autenticación con credenciales administrativas cuando se intenta ejecutar un instalador.*

Estos controles se encuentran alineados con lo establecido en el procedimiento interno "PR-TI-008 Procedimiento para control de software Versión 4 – 07/03/2025, en el cual se definen actividades especificas relacionadas con: Recepción y verificación de solicitudes de instalación, la validación de requerimientos, evaluación de uso de herramientas libres, actualización de inventario de equipos, control y actualización del licenciamiento.

Asimismo, los controles observados guardan coherencia con la "PG-T001 Política de Seguridad y Privacidad de la Información Versión No.03 – 06 de mayo del 2025, particularmente en lo relacionado con: Políticas de control de acceso, Seguridad en equipos institucionales, Protección frente a software malicioso, Control del Software operativo, Uso adecuado de internet, Cumplimiento de requisitos legales y de propiedad intelectual.

Con el propósito de verificar la efectividad de los controles implementados, se realizó una prueba práctica consistente en:

- *Descargar un programa libre desde internet en equipos de usuario final*
- *Intentar ejecutar el instalador desde el perfil del usuario final sin privilegios administrativos*
- *Verificar la generación de alertas y/o bloqueos del sistema.*

A continuación, la relación de la prueba de recorrido a los equipos de la muestra intentando descargar e instalar software libre con usuario sin privilegios de instalación en los equipos:

Tabla 7. Equipos de muestra prueba de instalación de software libre

Piso	Equipo	Usuario	Área	Resultado de la Prueba
32	P32DPP15	sburgos	Dirección de Planeación y Prospectiva	Permitió instalar "Mozilla Firefox"
32	P32DIRCOM51	mfranco	Dirección Comercial	Se descargo "FoxitPDF Reader20253_L10N Setup_Front", Se evidencio la alerta del Evento de Seguridad Pcsecure "Este Ejecutable no ha sido verificado. Se ha bloqueado por seguridad. Al tratar de ejecutar el archivo reporta: "No se pudieron extraer los archivos al directorio temporal"
32	P32DIRCOM31	sarias	Gerencia de Comercialización de Activos No Sociales	Se descargo "mirc783" - Al tratar de ejecutar el archivo reporta: "Parece que no tiene permiso para instalar mIRC en la carpeta C:\Archivos de programa (x86)\mIRC. Seleccione otra carpeta"
32	P32OPC01	lguevara	Oficina de Prensa y Comunicaciones	Se descargo "BlueStacksInstaller_5.22.166.1003_native_b4b42ec8...", Se evidencio la alerta del Evento de Seguridad Pcsecure "Este Ejecutable no ha sido verificado. Se ha bloqueado por seguridad. Al tratar de ejecutar el archivo reporta: "No se pudieron extraer los archivos al directorio temporal"
32	P32OMC06	omorin	Oficina de Integridad, Anticorrupción y Cumplimiento	Se descargo "ulweb_installer" - Al tratar de ejecutar el archivo reporta: "Debe iniciar sesión como administrador al instalar este programa."
32	P32PRES177	hbautista	Oficina Jurídica	Se descargo "qbittorrent_5.1.4_x64_setup" - Al tratar de ejecutar el archivo reporta: Es posible que no tenga los permisos necesarios para usar todas las funciones del programa que va a ejecutar. Puede ejecutar este programa con un usuario diferente o continuar con el usuario actual. Ejecute el programa con el siguiente usuario: Nombre de usuario: administrador
32	P32PRES1122	dpalomino	Despacho de Presidencia	Permitió descargar de software portable "PuTTY", no relacionado en programas estándar de los equipos de la entidad
NA	PSMONTERIA01	lojeda	Dirección Territorial Caribe	Permitió descargar de software portable "PuTTY", no relacionado en programas estándar de los equipos de la entidad
NA	PSMANGA01	syhernandez	Dirección Territorial Centro Oriente	Se descargo "RPCS3 Play Station 3 Emulator" al ejecutarlo no se habilita el proceso para continuar el ejecutable.
NA	DIRPER07	suribe	Dirección Territorial Occidente	Se descargo "ulweb_installer" - Al tratar de ejecutar el archivo reporta: "Debe iniciar sesión como administrador al instalar este programa."

Fuente: Elaboración OCI

En el ejercicio de la revisión realizada en sitio por la Oficina de Control Interno, se evidenciaron diferentes situaciones que conciernen a la aplicación de las Políticas de Seguridad de la Entidad. Durante la verificación de los equipos y del comportamiento del sistema frente a la instalación y uso de software, se identificaron eventos relacionados tanto con la descarga de programas no institucionales como con la activación —o ausencia de activación— de los controles automáticos establecidos, así:

1. P32DPP15:

Las evidencias relacionadas presentan la descarga de un software libre que fue instalado en el equipo, frente al cual no se activó el bloqueo automático de la política institucional de control de software. Esta situación evidencia una brecha en los mecanismos de prevención, dado que aun tratándose de software libre. El hecho de que el sistema no haya impedido la instalación pone de manifiesto un posible fallo en la aplicación de las políticas de seguridad o una configuración insuficiente de los controles, lo que puede comprometer la integridad del inventario de software y la gestión institucional de cumplimiento normativo.

Ilustración 3. Evidencia Programa Instalado – Equipo P32DPP15



Fuente: Elaboración propia OCI

2. P32DIRCOM51:

Se observa el intento de instalación de un software no autorizado. La política de seguridad restringió la operación, en aplicación de los lineamientos institucionales que prohíben la instalación de programas que no se encuentren previamente validados, licenciados o incluidos dentro del catálogo oficial de software autorizado por la entidad. Este control automático tiene como propósito prevenir el uso de herramientas que puedan vulnerar derechos de autor, introducir riesgos de seguridad informática o generar incumplimientos normativos, garantizando que únicamente se utilicen programas que han sido evaluados técnica, jurídica y operativamente. La activación de la política "PCsecure" evidencia que el mecanismo funcionó correctamente.

Ilustración 4. Evidencia Programa Instalado – Equipo P32DIRCOM51

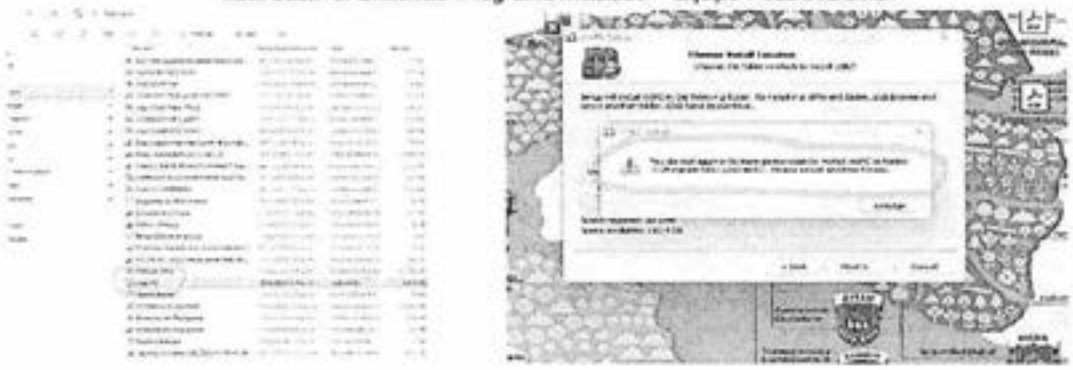


Fuente: Elaboración propia OCI

3. P32DIRCOM31:

Se evidencia actividad relacionada con la descarga de un software no institucional. Si bien la política de seguridad permitió la descarga del instalador, el sistema bloqueó la ejecución del programa, activando los controles establecidos para impedir el uso de aplicaciones no autorizadas que no cuentan con verificación de licenciamiento ni validación técnica previa. Esta situación demuestra un funcionamiento parcial de los mecanismos de seguridad: por un lado, se evita la ejecución del software no permitido; por otro, la descarga inicial constituye un riesgo, dado que expone el equipo a la posible incorporación de archivos no certificados y puede fomentar prácticas que se apartan de los lineamientos institucionales en materia de derechos de autor y gestión de software.

Ilustración 5. Evidencia Programa Instalado – Equipo P32DIRCOM31

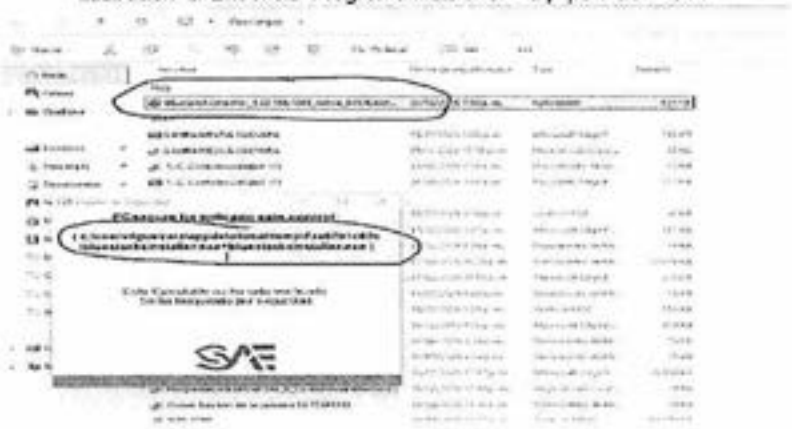


Fuente: Elaboración propia OCI

4. P32OPC01

Se intentó instalar el archivo "BlueStacksInstaller_5.22.166.1003_native_b4b42ec8...", frente a lo cual se evidenció la alerta del sistema de seguridad Pcsecure indicando: "Este ejecutable no ha sido verificado. Se ha bloqueado por seguridad". Adicionalmente, al intentar ejecutar el instalador, el sistema mostró el mensaje "No se pudieron extraer los archivos al directorio temporal", impidiendo su ejecución. En consecuencia, el ejecutable fue bloqueado de manera efectiva, demostrando que el control implementado opera adecuadamente y se encuentra alineado con la política institucional de prevención de software no autorizado.

Ilustración 6. Evidencia Programa Instalado – Equipo P32OPC01

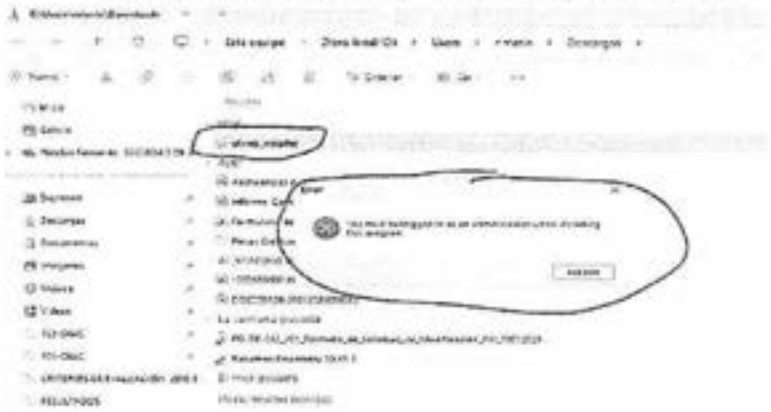


Fuente: Elaboración propia OCI

5. P32OIAC06

Se descargo "utweb_installer" - Al tratar de ejecutar el archivo reporta: "Debe iniciar sesión como administrador al instalar este programa.". Se evidencia el control de privilegios funcionó correctamente.

Ilustración 7. Evidencia Programa Instalado – Equipo P32OIAC06



Fuente: Elaboración propia OCI

6. P32PRESI77

Se descargo "qbittorrent_5.1.4_x64_setup" - Al tratar de ejecutar el archivo reporta: Es posible que no tenga los permisos necesarios para usar todas las funciones del programa que va a ejecutar. Puede ejecutar este programa con un usuario diferente o continuar con el usuario actual. Ejecute el programa con el siguiente usuario: Nombre de usuario: administrador. Se evidencio adecuada restricción de privilegios.

Ilustración 8. Evidencia Programa Instalado – Equipo P32PRESI77



Fuente: Elaboración propia OCI

7. P32PRESI122

Permitió descargar de software portable "PuTTY", no relacionado en programas estándar de los equipos de la entidad. El software portable no requiere instalación formal, lo que puede eludir parcialmente los controles de restricción de instalación.

Ilustración 9. Evidencia Programa Instalado – Equipo P32PRESI122

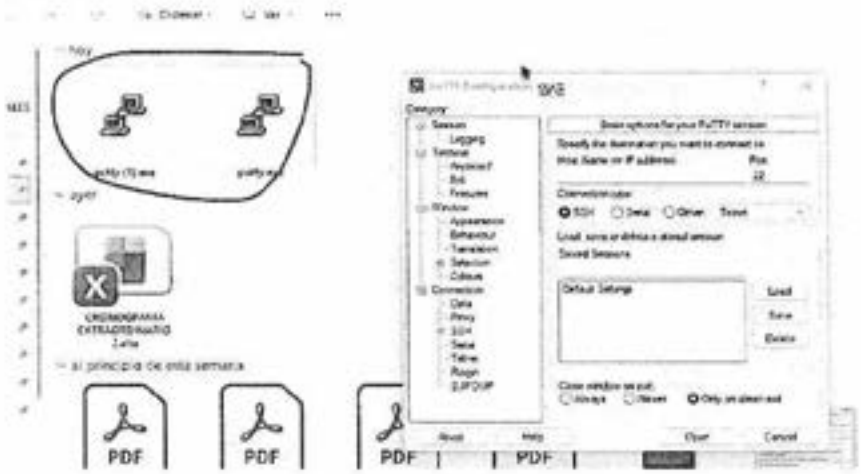


Fuente: Elaboración propia OCI

8. PMONTERIA01

Permitió descargar de software portable "PuTTY", no relacionado en programas estándar de los equipos de la entidad. El software portable no requiere instalación formal, lo que puede eludir parcialmente los controles de restricción de instalación.

Ilustración 10. Evidencia Programa Instalado – Equipo PMONTERIA01



Fuente: Elaboración propia OCI

9. PBMANGA01

Se descargo "RPCS3 Play Station 3 Emulator" al ejecutarlo no se habilita el proceso para continuar el ejecutable. El sistema restringió efectivamente la ejecución del programa.

Ilustración 11. Evidencia Programa Instalado – Equipo PBMANGA01



Fuente: Elaboración propia OCI

10. DIRPER07

Se descargo "utweb_installer" - Al tratar de ejecutar el archivo reporta: "Debe iniciar sesión como administrador al instalar este programa.". Control efectivo mediante restricción de privilegios.

Ilustración 12. Evidencia Programa Instalado – Equipo DIRPER07



Fuente: Elaboración propia OCI

De los diez equipos evaluados:

- *En siete (7) casos los controles técnicos funcionaron adecuadamente, bloqueando la instalación o requiriendo credenciales administrativas.*
- *En un (1) caso se permitió la instalación de software no estándar.*
- *En dos (2) casos se permitió la ejecución de software portable no autorizado.*

6.4 Disposición Final del Software dado de Baja

La Sociedad de Activos Especiales S.A.S. creó el Comité Técnico de Bajas mediante la Resolución No. 4354 del 22 de octubre de 2018, acto administrativo que estableció su conformación y funciones. Posteriormente, dicha resolución fue modificada por las Resoluciones No. 0026 del 14 de enero de 2022, No. 114 del 22 de febrero de 2024 y No. 300 del 23 de mayo de 2024, definiendo su integración actual.

La gestión de baja de bienes se encuentra regulada en el PR-GA-006 – Procedimiento para la Baja de Bienes Devolutivos Propiedad de la SAE S.A.S. – Versión 05 (vigente 05/12/2024), cuyo objetivo es establecer los lineamientos, parámetros y actividades necesarias para gestionar la baja de bienes muebles devolutivos que no son requeridos para el desarrollo de las actividades institucionales.

En lo relacionado con bienes intangibles (software y licencias), el procedimiento establece que su disposición debe realizarse conforme con las políticas definidas en el PR-TI-008 – Procedimiento para el Control de Software – Versión 04 (vigente 07/03/2025). El cual menciona criterios para dar de baja software en la SAE:

- *Cuando no cumple con las funcionalidades requeridas para los procesos del negocio.*
- *Cuando no existe soporte del fabricante o no es posible realizar actualizaciones.*
- *Cuando el fabricante modifica su esquema de licenciamiento.*
- *Cuando el software fue reemplazado por versiones actualizadas incompatibles con el licenciamiento inicial.*
- *Cuando no es compatible con el hardware institucional.*
- *Cuando presenta obsolescencia tecnológica o descontinuación en el mercado.*

La Oficina de Control Interno verificó la trazabilidad documental relacionada con la baja de software y activos tecnológicos autorizada mediante Resolución No. 750 del 31 de diciembre de 2025.

Se evidenció la siguiente secuencia:

1. *Acta de Inspección Ocular No. 02 (03/09/2025) emitida por la Oficina de Tecnologías y Sistemas de la Información (OTI), donde se identificaron elementos inservibles, vencidos, sin soporte o tecnológicamente obsoletos.*
2. *Diligenciamiento del Formato FO-GA-021, en el cual se consignó el concepto técnico que sustenta la baja.*
3. *Presentación ante el Comité Técnico de Bajas, el cual en sesión asincrónica del 15 de octubre de 2025 (Acta No. 01) emitió recomendación aprobatoria unánime.*
4. *Expedición de la Resolución No. 750 de SAE del 31 de diciembre 2025, autorizando formalmente la baja.*
5. *Actualización del inventario institucional, módulo de control de activos y registros contables.*

Los bienes dados de baja incluyen, entre otros:

Tabla 8. Relación Software y equipos dados de baja

PLACA	DESCRIPCIÓN DE BIENES REGISTRADOS EN LA BODEGA 103 - (ACTIVOS FIJOS)	FECHA DE COMPRA
108005	CONSOLA PARA DELL PARA MONTAR EN RACK CON MONITOR DE 18 CON 2 RACK	05/05/2015
108024	LICENCIA KASPERSKY ENDPOINT SECURITY	05/06/2018
108025	LICENCIA KASPERSKY ENDPOINT SECURITY	13/02/2018
108026	CONFIGURACIÓN DE CERTIFICADOS SSL 1	27/09/2018
108027	CONFIGURACIÓN DE CERTIFICADOS SSL 4 LICENCIA 2 AÑOS	27/09/2018
102191	TELEFONO IP BASICO	16/03/2015
102249	TELEFONO IP BASICO	16/03/2015
102253	TELEFONO IP BASICO	16/03/2015
102041	TELEFONO IP BASICO	16/03/2015
208303	AGENTE HYPER V	31/10/2014
208304	AGENTE HYPER V	31/10/2014
208298	AGENTE PARA CLIENTE - WINDOWS	31/10/2014
208299	AGENTE PARA CLIENTE - WINDOWS	31/10/2014
208300	AGENTE PARA CLIENTE - WINDOWS	31/10/2014
208305	AGENTE PARA CLIENTE - WINDOWS	31/10/2014
208301	AGENTE PARA DIRECTORIO ACTIVO - WINDOWS	31/10/2014
208302	AGENTE PARA EL SISTEMA LINUX	31/10/2014
208360	LICENCIA FIREWALL	27/12/2019
208001	LICENCIA SCRIPT CASE 6 ENTERPRISE EDITION	31/10/2014
208002	LICENCIA SCRIPT CASE 6 ENTERPRISE EDITION	31/10/2014
208003	LICENCIA SCRIPT CASE 6 ENTERPRISE EDITION	31/10/2014
208004	LICENCIA SCRIPT CASE 6 ENTERPRISE EDITION	31/10/2014
208005	LICENCIA SCRIPT CASE 6 ENTERPRISE EDITION	31/10/2014
201006	SERVIDORES DELL POWEREDGE R720 CON LICENCIA WINDOWS	31/10/2014
201007	SERVIDORES DELL POWEREDGE R720 CON LICENCIA WINDOWS	31/10/2014
201009	SERVIDORES DELL POWEREDGE R720 CON LICENCIA WINDOWS	31/10/2014
201005	SOLUCIÓN DE ALMACENAMIENTO	31/10/2014
201037	SWITCH 24 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201041	SWITCH 24 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201022	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201014	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201015	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201018	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201020	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201021	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201025	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201029	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014
201034	SWITCH 48 PUERTOS GIGABIT 10/100/100 ADMINISTRABLE / SOPORTE A VLAN	31/10/2014

Fuente: Resolución 750 de la SAE - Elaboración OCI

El concepto técnico común registrado en los formatos FO-GA-021 señala:

- *Falta de soporte del fabricante.*
- *Licencias vencidas.*
- *Descontinuación en el mercado.*
- *No uso.*
- *Obsolescencia tecnológica.*
- *Reemplazo por soluciones más actualizadas (ej. implementación de nueva solución de seguridad).*

De acuerdo con la documentación revisada, se evidencia que el proceso de baja de software y activos tecnológicos:

- *Cuenta con concepto técnico formal emitido por la OTI.*
- *Fue evaluado y aprobado por el Comité Técnico de Bajas.*
- *Está soportado mediante acto administrativo (Resolución No. 750 de 2025).*
- *Cumple con lo establecido en el PR-GA-006 y el PR-TI-008.*
- *Presenta trazabilidad documental suficiente.*

La baja de los bienes tecnológicos e intangibles relacionados en la Resolución No.750 de SAE del 31 de diciembre de 2025, se encuentra debidamente sustentada desde el punto de vista técnico, procedimental y administrativo, sin evidenciarse incumplimiento normativo en la muestra evaluada

7. Seguimiento a Recomendaciones del Informe Software de Derechos de Autor - Vigencia 2024

En el marco del seguimiento realizado a las actividades de cumplimiento adelantadas por la OTI respecto de las disposiciones sobre uso legal de software y derechos de autor, se revisaron las recomendaciones emitidas para la vigencia 2024 y las evidencias documentales disponibles. Asimismo, se formulan las observaciones correspondientes para la evaluación aplicable a la vigencia 2025.

La Oficina de Control Interno mediante correo electrónico del 30 de enero de 2026 solicito a la Oficina de Tecnologías y Sistemas de la Información, informar las acciones adelantadas y remitir evidencias frente a las actuaciones realizadas, de acuerdo con las recomendaciones generadas por la Oficina de Control Interno en el informe final de cumplimiento al uso de software legal – derechos de autor vigencia 2024, a continuación, se presentan las observaciones de acuerdo con la evidencia recibida:

Tabla 9. Seguimiento a Recomendaciones – OCI Vigencia 2024 Vs Observaciones OCI Evaluación seguimiento Vigencia 2025

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluacion Seguimiento vigencia 2025
1. Inclusión de lineamientos y validaciones que complementen las ya establecidas en la PG-TI-001 Política de Seguridad y Privacidad de la Información Versión No.01 – 20 de Noviembre del 2024 y en el P-TE4-094 Procedimiento Administración y Control de Acceso a Usuarios en la Plataforma Tecnológica Versión 8 – 21/02/2022, respecto a definir y enunciar un Catálogo de Software licenciado Estándar y un Catálogo de Software libre, gratuito, freeware, shareware, AGPL permitido para uso e instalación en los equipos de cómputo de la Sociedad de Activos Especiales SAE.	Se evidenció la actualización de la Política de Seguridad y Privacidad de la Información – PG-TI-001 Versión 03 del 06 de mayo de 2025, la cual incorpora lineamientos relacionados con: • Políticas de control de acceso. • Seguridad en equipos institucionales. • Protección frente a software malicioso. • Control del software operativo. • Uso adecuado de internet. • Cumplimiento de requisitos legales y de propiedad intelectual. En particular, la política establece que: "Los usuarios no pueden instalar o usar software en los equipos, aplicaciones móviles o portales web que no sean validados y autorizados por la Oficina de Tecnologías y Sistemas de Información, previa verificación de riesgos de seguridad de la información". No obstante, durante las pruebas de evaluación realizadas para la vigencia 2025, se evidenció que aún no se encuentra formalmente definido ni publicado un catálogo institucional de software libre o portable autorizado, lo cual dificulta la estandarización de los controles de instalación y uso de software en los equipos institucionales. Por lo anterior, se reitera la recomendación de establecer y estandarizar un catálogo institucional de software autorizado, que incluya software licenciado, software libre y software portable permitido.
2. Revisión, validación y consideración de desinstalar el software instalado denominado "Libre" y que se puede con el software licenciado que tiene adquirida la entidad ejecutar las labores o actividades que requieren las dependencias de la SAE, por ejemplo: zoom, cubierto por Teams Microsoft.	De acuerdo con la revisión de la evidencia suministrada por la OTI, se evidencian registros de solicitudes de instalación de software libre gestionadas mediante tickets, lo cual permite contar con un mecanismo básico de trazabilidad de las solicitudes realizadas por las dependencias. No obstante, durante la evaluación realizada para la vigencia 2025 y con base en la muestra de equipos analizados, se identificó la presencia de diversas herramientas de software libre o portable instaladas en equipos institucionales, entre ellas: • AnyDesk (PMONTERIA01) • TeamViewer (PBMANGA01)

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluación Seguimiento vigencia 2025
	• Mozilla Firefox (P33GEDEP11, P35DIRFINAN22, P38OTI05, P38OTI50, P36DIRDAIU45) • Picasa 3 (PBMANGA01) • PuTTY Release (P37DIRSCL35, P38OTI05, P38OTI14, P38OTI22, P38OTI50, P38OTI70) • WinRAR 7.01 (PBMANGA01) • Zoiper (P38OTI05, P38OTI70) • Zoom (P38OTI05) • Zoom Workplace (P35DIRFINAN51, P35DIRTH37, P37DIRGDCS80, PDTCAR136, PDTOCC36, P38OTI14, PBMANGA01) Si bien algunas de estas herramientas pueden corresponder a software libre o de uso gratuito, no se evidencia un catálogo institucional formal que establezca qué software libre o portable se encuentra autorizado para su instalación y uso en los equipos de la entidad. Adicionalmente, se observa que algunas herramientas identificadas podrían solaparse funcionalmente con software licenciado institucional, como es el caso de Zoom frente a Microsoft Teams, lo cual podría generar duplicidad de herramientas y debilidades en el control del software instalado. En este sentido, se reitera la necesidad de fortalecer los mecanismos de control relacionados con la autorización, instalación, seguimiento y eventual desinstalación de software libre o portable, garantizando su alineación con las herramientas licenciadas institucionales y con las políticas de seguridad de la información.
3. Se sugiere realizar revisiones periódicas a todos los computadores de la entidad por parte de la OTI, adelantando las acciones necesarias de actualización del nombre del equipo respecto a los traslados físicos, teniendo en cuenta el renombramiento con la estructura: Tipo_ubicacion_Area_consecutivo.	Durante el proceso de evaluación realizado para la vigencia 2025, y con base en la muestra de equipos verificados, se evidenció que la situación relacionada con inconsistencias entre el nombre asignado a los equipos y su ubicación física continúa presentándose, situación que ha sido identificada de manera reiterada en los ejercicios de evaluación y seguimiento correspondientes a las vigencias 2023 y 2024. En la muestra analizada se identificaron diferencias entre el nombre registrado del equipo y la ubicación física verificada, en los siguientes casos: Piso 33 • P06DTCO81 • P35DIRADMIN22 Piso 37 • P38DIRDAIR04

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluación Seguimiento vigencia 2025
	• P37DIRGDCS80 • P32PRESI26 • P38OCI25 Piso 36 • P33DIRDAIR14 • P33GEDEP26 La inconsistencia identificada, aunque corresponde aproximadamente al 5 % de la muestra evaluada, evidencia debilidades en la actualización y control del inventario tecnológico, particularmente en lo relacionado con la actualización del nombramiento de los equipos frente a su ubicación física real. Esta situación puede generar dificultades en la trazabilidad de los equipos, en la gestión del soporte técnico y en la administración eficiente de los activos tecnológicos de la entidad.
4. Se recomienda el uso de una herramienta en la que se pueda consultar y realizar el listado completo del software que tiene instalado un equipo, en razón a que en la revisión realizada en sitio se evidencio software instalado que no se observó en el inventario suministrado por la OTI.	De acuerdo con la mesa de trabajo realizada el 25 de febrero de 2026, se evidenció el uso de la herramienta GLPI para realizar consultas relacionadas con los equipos registrados en el inventario tecnológico, incluyendo la visualización del software instalado en algunos equipos de manera individual. No obstante, durante la verificación realizada se identificó que la herramienta actualmente no genera un reporte consolidado que permita obtener de manera automática el listado completo del software instalado en los equipos institucionales, lo cual limita la capacidad de realizar análisis globales y controles periódicos sobre el inventario de software. Esta situación puede dificultar el seguimiento integral del software instalado, la identificación de herramientas no autorizadas y la verificación del cumplimiento de las políticas institucionales relacionadas con licenciamiento y uso de software.
5. Seguir implementando las recomendaciones dadas en el informe de la vigencia 2023, para garantizar la revisión de la actividad de la implementación en los perfiles de PCSECURE política para evitar que los usuarios dejen documentos en las carpetas de descargar, escritorio y documentos de los equipos locales. Y más campañas de sensibilización de "PG-TI-001	De acuerdo con la muestra aleatoria realizada sobre 176 equipos institucionales, se evidenciaron los siguientes resultados respecto al cumplimiento de la política de escritorio limpio: • 84 equipos, equivalentes al 48 % de la muestra, cumplen con la política, evidenciando que no presentan elementos almacenados en el escritorio. • 92 equipos, equivalentes al 52 % de la muestra, presentan elementos almacenados en el escritorio, con cantidades que oscilan entre 1 y 97 elementos.

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluación Seguimiento vigencia 2025
POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Versión No.01- 20 DE NOVIEMBRE DEL 2024.	*Los resultados obtenidos evidencian un nivel de cumplimiento inferior al esperado para la política de escritorio limpio, lo cual podría indicar debilidades en la aplicación efectiva de los controles configurados en la herramienta PCSecure o en la apropiación de la política por parte de los usuarios.* *Adicionalmente, durante la verificación se identificó el caso particular del equipo P38GERAS12, el cual presenta una cantidad considerable de elementos almacenados en el escritorio, situación que sugiere la necesidad de validar la correcta configuración y funcionamiento de la política en la herramienta PCSecure, particularmente en lo relacionado con la opción de activación de la política de escritorio limpio o control del escritorio del usuario.*
6. Se recomienda gestión y seguimiento a las actividades de la implementación de controles de acuerdo con el cumplimiento del plan de tratamiento en el Monitoreo de la Matriz de Riesgos de Seguridad de la Información, ejemplo: la verificación en línea de la actualización del Tablero de Control en Power BI "Usuarios Perfiles por Sistema".	*Durante la verificación realizada por la Oficina de Control Interno al tablero de Power BI denominado "Equipos – Inventario SAE", se evidenció que la información registrada no se encuentra completamente actualizada.* *En particular, se observaron las siguientes situaciones:* *• Al realizar la consulta por área organizacional, la información correspondiente a la Oficina de Control Interno no refleja el total de funcionarios vinculados a la vigencia 31 de diciembre de 2025.* *• Algunos nombres o identificadores de equipos registrados en el tablero no se encuentran actualizados, lo cual podría generar inconsistencias en la información utilizada para la gestión y seguimiento de los activos tecnológicos.* *Estas inconsistencias evidencian debilidades en la actualización o sincronización de la información presentada en el tablero, lo cual podría afectar la confiabilidad de los datos utilizados para el monitoreo de la Matriz de Riesgos de Seguridad de la Información y la toma de decisiones asociadas a la gestión de activos tecnológicos.*
7. Se sugiere revisar la matriz de riesgos de operación , para identificar riesgos que no se identificaron definidos a los relativos al uso de software sin licencia, ilegal o que expira, tales como los sugeridos e informados en el seguimiento realizado por la OCI (ver Tabla 16) de tal manera que se sugiere evaluar la eventualidad de incluir en la Matriz de Riesgos Operacionales, definir y aplicar controles necesarios para evitar una materialización y/o posible sanción por una probabilidad de incumplimiento sobre Derechos de Autor.	*De acuerdo con la información suministrada por la OTI, se evidenció la inclusión del Control No. 5 en la Matriz de Riesgos Operacionales, el cual establece que:* *El profesional delegado de la OTI, en caso de identificar un software instalado que no haya sido autorizado o que no cuente con licencia, procede a radicar un ticket en la mesa de servicios solicitando la desinstalación del software, quedando como evidencia el registro del ticket en la herramienta de gestión de servicios.* *Durante la verificación realizada, se evidenció en la herramienta GLPI el registro de algunos tickets asociados a revisiones de seguridad y control de software en los equipos institucionales, entre los cuales se destacan:* *• Ticket No. 113734 – 16/06/2025* *Revisión del agente antivirus y actualizaciones críticas en el equipo DIRPER05.* *• Ticket No. 110973 – 04/04/2025*

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluación Seguimiento vigencia 2025
	Instalación de antivirus Trend Micro, revisión de seguridad y aplicación de actualizaciones en el equipo PDTCAR22. *No obstante, durante la revisión de la muestra de equipos analizados en el seguimiento realizado por la Oficina de Control Interno, se evidenció la presencia de software libre o aplicaciones no contempladas dentro de un catálogo institucional de software autorizado, lo cual podría generar riesgos asociados a seguridad de la información, gestión de licencias y cumplimiento de derechos de autor.* *Entre los softwares identificados se encuentran:* *• AnyDesk: PMONTERIA01* *• TeamViewer: PBMANGA01* *• Mozilla Firefox: P33GEDEP11, P35DIRFINAN22, P38OTI05, P38OTI50, P35DIRDAIU45* *• Picasa 3: PBMANGA01* *• PuTTY Release: P37DIRSCL35, P38OTI05, P38OTI14, P38OTI22, P38OTI50, P38OTI70* *• WinRAR 7.01: PBMANGA01* *• Zoiper: P38OTI05, P38OTI70* *• Zoom: P38OTI05* *• Zoom Workplace:* *P35DIRFINAN51, P35DIRTH37, P37DIRGDCS80, PDTCAR136, PDTOCC36, P38OTI14, PBMANGA01* *La presencia de estas aplicaciones evidencia la necesidad de fortalecer los controles asociados a la instalación de software en los equipos institucionales, así como de definir un catálogo institucional de software autorizado, especialmente en lo relacionado con software libre o de uso corporativo permitido.*
8. Se recomienda el seguimiento y control de los tiquetes Registrados en la Mesa de Ayuda para la validación e instalación de Software libre, de acuerdo con la inactivación de usuarios por retiro, y la necesidad del uso de software libre para nuevo usuario el respectivo registro de tiquete en la Mesa de Servicio.	*De acuerdo con la revisión realizada y la evidencia proporcionada:* *1. Se confirma la existencia del Control No. 5 en la Matriz de Riesgos, el cual establece que el profesional delegado de la OTI radica un ticket a la Mesa de Servicios cuando se identifica software no autorizado o sin licencia, quedando registrada la evidencia en GLPI.* *2. Si bien se mantienen registros de tickets relacionados con software libre, la herramienta GLPI no permite generar reportes consolidados. La consulta se realiza mediante parámetros como número de ticket o descripción, lo que dificulta:* *- La trazabilidad centralizada de todas las solicitudes de instalación de software libre.*

Seguimiento Recomendaciones - OCI Vigencia 2024	Observaciones OCI Evaluacion Seguimiento vigencia 2025
	- El control actualizado de qué software está instalado en cada equipo. *- La generación de reportes periódicos para monitoreo y auditoría.* *3. Esta situación evidencia una oportunidad de mejora en la gestión y seguimiento del registro de software libre, especialmente en cuanto a mantener una base de control actualizada y consolidada que permita monitorear, clasificar y auditar todas las solicitudes de instalación de software libre.*

Fuente: Elaboración OCI

8. CONCLUSIONES Y RECOMENDACIONES

8.1. Conclusiones

- *La Entidad ha adelantado acciones orientadas al fortalecimiento del control del uso de software institucional, mediante la actualización de la Política de Seguridad y Privacidad de la Información (PG-TI-001) y del procedimiento de gestión de usuarios, los cuales incorporan lineamientos que prohiben la instalación de software no autorizado y promueven el cumplimiento de las disposiciones relacionadas con propiedad intelectual y licenciamiento de software.*

- *Se evidencian avances en la implementación de mecanismos de control para la gestión del software institucional, tales como el registro de tickets en la mesa de servicios para la instalación de software, el uso de la herramienta GLPI para la administración del inventario tecnológico, la configuración de controles de seguridad mediante PCSecure y la utilización de tableros de control en Power BI para consulta de información institucional.*

- *Asimismo, la entidad atendió la recomendación relacionada con la gestión del riesgo asociado al uso de software no autorizado, mediante la inclusión del riesgo RO-TI-4 en la Matriz de Riesgos Operacionales de Tecnologías de la Información para la vigencia 2025, así como la definición de controles orientados a la identificación y gestión de software sin licencia o no autorizado.*

- *No obstante, durante la verificación realizada para la vigencia 2025 se identificaron oportunidades de mejora en la estandarización y fortalecimiento de los controles asociados a la gestión de software, particularmente en lo relacionado con la ausencia de un catálogo institucional formal de software autorizado, el cual permita definir de manera clara las herramientas licenciadas, libres o portables permitidas para su instalación y uso en los equipos institucionales.*

- *La ausencia de este catálogo puede generar debilidades en los procesos de control, seguimiento y estandarización del software utilizado en la entidad, así como posibles duplicidades funcionales entre herramientas licenciadas y software libre, afectando la optimización del uso de las licencias institucionales y generando riesgos asociados al cumplimiento normativo, seguridad de la información y gestión de activos de software.*

- *Aunque la Oficina de Tecnologías y Sistemas de la Información mantiene registros de solicitudes de instalación de software mediante la mesa de servicios, se evidencian limitaciones en la consolidación y generación de reportes globales, debido a que la herramienta GLPI no permite generar de forma directa reportes consolidados del software instalado en todos los equipos, lo cual dificulta la trazabilidad integral y el seguimiento sistemático del inventario de software institucional.*

- *De igual manera, durante la evaluación se identificaron algunas inconsistencias entre la nomenclatura registrada de ciertos equipos y su ubicación física real, situación que ha sido observada en evaluaciones de vigencias anteriores. Aunque el porcentaje identificado es bajo en relación con la muestra analizada, evidencia oportunidades de mejora en los procesos de verificación y actualización del inventario tecnológico.*

- *En relación con los controles de seguridad implementados en los equipos institucionales, se evidenció que la entidad cuenta con la herramienta PCSecure para la aplicación de políticas de seguridad, incluyendo la Política de Escritorio Limpio; sin embargo, los resultados de la muestra evaluada muestran niveles de cumplimiento parciales, lo cual sugiere la necesidad de fortalecer los mecanismos de monitoreo y sensibilización a los usuarios.*

- *De igual manera, si bien la entidad cuenta con tableros de control en Power BI para la consulta de información del inventario tecnológico, se evidenció que la información registrada en algunos casos no se encuentra completamente actualizada, lo cual limita su efectividad como herramienta de monitoreo y apoyo para la gestión de riesgos de seguridad de la información.*

- *En términos generales, las acciones adelantadas por la entidad evidencian avances en la implementación de controles relacionados con la gestión de software y la seguridad de la información; no obstante, la mayoría de las recomendaciones evaluadas se consideran parcialmente implementadas o en proceso de fortalecimiento, debido a la necesidad de consolidar mecanismos institucionales más robustos de estandarización, control, monitoreo y reporte del software utilizado en los equipos institucionales.*

7.2 Recomendaciones

- *Formalizar e implementar un Catálogo Institucional de Software Autorizado, que incluya el software licenciado institucional, el software libre aprobado y las herramientas freeware o portables permitidas, estableciendo para cada uno aspectos como nombre del software, tipo de licencia, versión autorizada, dependencia responsable y condiciones de instalación y uso.*

- *Incorporar el catálogo de software autorizado como referencia dentro de la Política de Seguridad de la Información o de los procedimientos de gestión tecnológica, con el fin de garantizar su aplicación institucional y facilitar su consulta por parte de las dependencias y usuarios.*

- *Establecer un mecanismo de actualización periódica del catálogo, administrado por la Oficina de Tecnologías y Sistemas de la Información, que contemple la evaluación técnica, análisis de riesgos de seguridad de la información y validación de cumplimiento legal previo a la autorización de nuevas herramientas.*

- *Realizar un análisis funcional del software libre actualmente instalado en los equipos institucionales, con el fin de identificar posibles duplicidades con herramientas licenciadas institucionalmente y optimizar el uso de las licencias adquiridas por la entidad.*

- *Implementar revisiones periódicas del software instalado en los equipos institucionales, que permitan identificar aplicaciones no autorizadas o herramientas que deban ser desinstaladas por no encontrarse dentro del catálogo institucional aprobado.*

- *Fortalecer los controles de seguimiento sobre la instalación y desinstalación de software, mediante el registro de solicitudes en la mesa de servicios, incorporando campos adicionales que permitan identificar el tipo de licencia, la justificación técnica de la instalación, la validación de seguridad de la información y la fecha de revisión o permanencia del software.*

- *Consolidar una base de control actualizada de software libre instalado, integrando la información de los tickets registrados en la herramienta GLPI, con el fin de garantizar trazabilidad, control y seguimiento centralizado de las solicitudes.*

- *Evaluar la posibilidad de generar reportes consolidados del inventario de software, ya sea mediante mejoras en la herramienta GLPI o a través de soluciones complementarias como Microsoft Intune u otras herramientas de gestión.*

- *Fortalecer las revisiones periódicas del inventario tecnológico, con el fin de verificar la correspondencia entre el nombre asignado a los equipos y su ubicación física real, incorporando esta validación dentro de los procesos de traslado o cambio de ubicación de funcionarios.*
- *Mantener actualizado el inventario tecnológico institucional, garantizando la consistencia entre la información registrada en las herramientas de gestión tecnológica y la realidad operativa de los equipos instalados en las diferentes dependencias.*
- *Validar la correcta configuración y aplicación de la Política de Escritorio Limpio en la herramienta PCSecure, realizando verificaciones periódicas del cumplimiento en los equipos institucionales y aplicando acciones correctivas cuando se identifiquen incumplimientos.*
- *Fortalecer las campañas de sensibilización dirigidas a los trabajadores y contratistas, relacionadas con el adecuado manejo de la información institucional, el uso de repositorios corporativos de almacenamiento y el cumplimiento de la Política de Seguridad y Privacidad de la Información.*
- *Promover el uso de herramientas institucionales de almacenamiento y colaboración, evitando el almacenamiento de información en los discos locales de los equipos y reduciendo riesgos de pérdida o exposición de información.*
- *Realizar la revisión y actualización periódica de la información registrada en los tableros de control en Power BI, garantizando la consistencia de los datos con el inventario real de equipos y la información institucional vigente.*
- *Definir responsables y periodicidad para la actualización de la información en los tableros de control, con el fin de fortalecer su uso como herramienta de monitoreo en la gestión de activos tecnológicos y riesgos de seguridad de la información.*
- *Fortalecer la aplicación de los controles definidos en la Matriz de Riesgos Operacionales de Tecnologías de la Información, particularmente aquellos asociados al riesgo de instalación o uso de software no autorizado, mediante verificaciones periódicas y registro de evidencias en la mesa de servicios.*

Lo anterior, de conformidad con la Circular No.017 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derechos de Autor, en donde se ordena a las Oficinas de Control Interno como responsables de la verificación del cumplimiento de las disposiciones en materia de derechos de autor sobre software, así como la remisión de la información relacionada al inventario, controles de instalación y dada de baja de software.

La Oficina de Control Interno (OCI), conforme con lo señalado en el Circular Externa No.027 del 2023 de la Unidad Administrativa Especial Dirección Nacional de Derechos informa "El alcance de la presente Circular es para informar a los Representantes Legales y Jefes de Oficina de Control Interno o quienes hagan sus veces, de la Entidades u Organismos Públicos del Orden Nacional y Territorial que a partir de la vigencia 2024 en la página web de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor www.derechodeautor.gov.co se habilitará un nuevo campo en le micrositio del Informe de Software, en el cual deberán subir el link que permita acceder al informe "Verificación, recomendaciones, seguimientos y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre software".

Conforme con lo anterior, se presenta informe de seguimiento y verificación sobre el cumplimiento de las normas en materia de derecho de autor sobre software correspondiente a la vigencia 2025, de acuerdo con el proceso que lidera la Oficina de Control Interno dentro de la Entidad, denominado Seguimiento y Evaluación.

Cordialmente,

Amelia Pérez Parra
Presidenta

Elaboró:
Carolina Aguilera Martínez - PII
Sandra Jazmin Durán Sierra - PIII

Revisó: Beisner Elipson Arboleda Palacios - PEIII – Encargado de la OCI.
Aprobó: Beisner Elipson Arboleda Palacios - PEIII – Encargado de la OCI. Beisner E. Arboleda P.