Radicado No: 202230001232
Fecha Radicación: 2022/03/16

COMUNICACIÓN INTERNA

PARA: **MÓNICA OSPINA LONDOÑO**
Directora General

SERGIO ANDRÉS SOLER ROSAS
Director de Tecnología e Información

WILLIAM ALFREDO SANDOVAL SANDOVAL
Subdirector de Información

HANS RONALD NIÑO GARCÍA
Subdirector de Abastecimiento y Servicios Generales

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: **Informe Derechos de Autor 2022**

Estimados líderes:

En desarrollo de las Directivas Presidenciales 01 de 1999 y 02 de 2002, el Consejo Asesor del Gobierno Nacional en materia de Control Interno de las Entidades del Orden Nacional y Territorial, expide la Circular 04 del 22 de diciembre de 2006, la cual solicita a los Representantes Legales y Jefes de las Oficinas de Control Interno de las entidades u organismos públicos del orden nacional y territorial, la información asociada con la "*verificación, recomendaciones y resultados sobre el cumplimiento de las normas en materia de derechos de autor sobre Software".*

Así mismo, la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor emitió la Circular 12 del 2 de febrero de 2007, modificada por la Circular 17 de 2011, en el cual se aclara el procedimiento, contenido y condiciones para el recibo de la información sobre el licenciamiento del software de la entidad del año inmediatamente anterior, a través del aplicativo disponible en la página: www.derechodeautor.gov.co.

En este orden de ideas, se presentan los resultados de la verificación de los soportes lógicos (software), efectuada a los equipos de cómputo que se encuentran a cargo de los funcionarios y contratistas del ICFES, así como, la verificación de las licencias de software a cargo de la Entidad.

OBJETIVOS

- Verificar el cumplimiento de la normativa tocante al Derecho de Autor, relativa al uso de soportes lógicos o software, por parte del ICFES en la vigencia 2022.
- Verificar la correspondencia del inventario de hardware del Instituto con el inventario reportado por la Dirección de Tecnología e Información, lo anterior, a través del análisis de una muestra representativa.
- Verificar que los soportes lógicos instalados en los equipos de computo del Instituto cuenten con las licencias correspondientes y vigentes.
- Validar los mecanismos y metodologías de control que se han implementado en la entidad, esto con el objetivo de evitar que los usuarios instalen programas que no cuenten con la licencia autorizadas.
- Consolidar la información que será reportada a la Dirección Nacional de Derechos de Autor (DNDA) en concordancia a lo dispuesto en las Circulares 12 de 2007 y 17 de 2011.

ALCANCE

La información objeto de análisis se tomó con los reportes suministrados el día 16 de febrero de 2022 y con la revisión muestral efectuada en sitio el 1 de marzo de 2022.

Ahora bien, con esta información se preparó el reporte del estado del hardware y software, el cual fue remitido a la Dirección Nacional de Derecho de Autor, de acuerdo a las directrices dadas por la Circular 12 de 2007 y Circular 17 de 2011 del DNDA.

NORMATIVIDAD

La normatividad vigente que se ha tenido en cuenta como criterios para el presente seguimiento son las siguientes:

- Directivas presidenciales 01 de 1999 y 02 de 2002.
- Circular 04 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en materia de Control Interno.
- Circular 12 de 2007 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor.
- Circular 17 de 2011 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor.
- Procedimiento Administración de Servicios Tecnológicos GTI PR001 - Versión 001.
- Procedimiento Gestión de Accesos GTI PR012 - Versión 003.
- Procedimiento Configuración de equipos de cómputo GTI PR019 – Versión 002.
- Procedimiento de Gestión de Bienes e Inventarios GAB-PR001 – Versión 001.
- Norma ISO 9001:2015.

METODOLOGÍA

Para el presente informe, se seleccionaron equipos de la base de datos denominada, "*1. RELACIÓN EQUIPOS COMPUTO - V. 16022022"* suministrada por la Dirección de Tecnología e Información:

ESTADO	CANTIDAD
ACTIVO	430
BODEGA-DISPONIBLE	21
BODEGA-DAÑADO	51
EN CAMBIO	2
TOTAL	504

FUENTE: Archivo DTI, Relación Equipos Cómputo

Una vez verificada la información contenida en los equipos de cómputo, estos se encuentran clasificados según su tipo, de la siguiente manera:

TIPO DE EQUIPO	CANTIDAD
ESCRITORIO	374
PORTÁTIL	98
WORKSTATION	32
TOTAL	504

FUENTE: Archivo DTI, Relación Equipos Cómputo

Sobre la población se aplicó la fórmula estadística de selección de muestras, cumpliendo con los siguientes criterios:

ESTADO	CANTIDAD	ERROR	P	CONFIANZA	MUESTRA
ACTIVO	430	5	5	95	62
BODEGA-DISPONIBLE	21	5	5	90	15
BODEGA-DAÑADO	51	5	5	90	26
EN CAMBIO	2				0
TOTAL	**504**				**103**

El tamaño de la muestra se determinó en 103 equipos de cómputo, que corresponden al 20% del total de los equipos.

La Dirección de Tecnología e Información suministró la base de datos de licencia denominada: "*2. RELACIÓN SOFTWARE Y LICENCIAS - V. 16022022*", en esta base de datos se relaciona un total de 804 licencias instaladas, que corresponde a 33 tipos de licencias; de este total, 4 tipos son "desarrollo propio" y 29 adquiridas. Es decir, se tomó como población los 29 tipos de licencias con los siguientes criterios: error muestral: 5%, proporción de éxito (p): 5%, y nivel de confianza del 90%, para una muestra de 19 licencias.

La Oficina de Control Interno realizó inspección de verificación el día 1 de marzo de 2022, con el objeto de verificar y contrastar la información remitida por la Subdirección de Información. En la cual se discriminó la información de cada uno de los equipos de la muestra, incluyendo el usuario asignado a cada equipo y los soportes lógicos (software) instalados en éstos. Igualmente, se realizó verificación sobre el licenciamiento y mecanismos de control informados por la DTI.

RESULTADOS DEL SEGUIMIENTO

1. Verificación del inventario de equipos de cómputo del Instituto.

De acuerdo con la base de datos suministrada, se procedió a verificar: (i) La muestra de 62 equipos "*ACTIVOS*", (ii) La existencia de los 15 equipos con estado "*BODEGA DISPONIBLE*", y (iii) La muestra de 26 reportados como "*BODEGA DAÑADO*", con los siguientes resultados:

↓ No fue posible verificar la existencia física de los siguientes dos (2) equipos:

RESPONSABLE	DESCRIPCIÓN	PLACA CPU
Yamile Ariza Luque	Escritorio	000678
Jackeline Gómez Giraldo	Escritorio	119933

↓ Un (1) equipo de cómputo se registra asignado a un usuario. No obstante, **NO** corresponde al equipo que utiliza:

RESPONSABLE	DESCRIPCIÓN	PLACA CPU
Jackeline Gómez Giraldo	Escritorio	119933

- No fue posible verificar el software instalado en los siguientes tres (3) equipos, toda vez que se encontraban en la casa de las personas responsables. No obstante, se solicitó mediante correo electrónico a la SAYSG las actas de entrega firmadas de los mencionados equipos. Las cuales fueron verificadas por la OCI, cumpliendo lo establecido en el procedimiento GAB -PR001 Asignación Física de los Bienes e Inventarios.

ESTADO	RESPONSABLE	DESCRIPCIÓN	PLACA CPU
ACTIVO	John Manuel Hernández Garzón	Portátil	120555
ACTIVO	Manuel Amado	Portátil	120784
ACTIVO	Carlos Andrés Bayona Becerra	Portátil	120935

- La Oficina de Control Interno verificó en la bodega de almacenamiento ubicada en el piso 18, los equipos de cómputos registrados como dañados y disponibles que se establecieron en la muestra. En esta visita se logró constatar que los equipos almacenados se encuentran identificados por sus características y su categoría, lo cual facilita su ubicación.

2. Verificación del software instalado en los equipos de cómputo seleccionados en la muestra:

Una vez contrastada la base de datos que contiene la relación del software instalado en los computadores, obtenida de Aranda y suministrada por la Subdirección de Información, con la verificación física realizada, se evidencia que:

↓ El reporte Aranda (control de software instalado en cada equipo) se encuentra desactualizado, toda vez que, relaciona software o aplicaciones instaladas en los computadores, que, al verificarlos por parte de esta Oficina, no se encontraron instalados:

SOFTWARE INSTALADO	EQUIPO
ZOOM	DGE-P-05
	OAJ-P-03
	OAJ-P-05
	OCI-E-02
	SAI-E-03
CISCO WEBEX MEETINGS	DGE-P-05
	OAJ-P-03
	SAI-E-03
	SES-E-10
	SPI-P-01

FUENTE: Muestra Solicitud ARANDA

↓ En los equipos relacionados a continuación se encontró el uso de software gratuito no autorizado, así como, software licenciado que no está autorizado para todos los computadores:

SOFTWARE	PLACA CPU
CHROME REMOTE DESKTOP HOST	6284
	120165
	120193
	120735
(HP CLIENT SECURITY MANAGER, HP CONNECTION OPTIMIZER, HP DEVICE ACCES MANAGER, HP DOCUMENTATION, HP EPRINT SW, HP ESU FOR MICROSOFT WINDOWS, HP HOTKEY SUPPORT, HP JUMPSTART BRIDGE, HP JUMPSTART LAUNCH, HP NOTIFICATIONS, HP SUPPORT ASSISTANT, HP SUPPORT SOLUTIONS FRAMEWORK, HP VELOCITY)	120221
	119649
	120261
	120405
	120512
	65
	119633
	119941
	119677
	119953
	120165
	120073
	120981
	120193
	120523
	120885
	120501
	120705
	120173
	119669
	120668

	119797
	120185
	120289
HP SUPPORT INFORMATION	162
HP 3D DRIVEGUARD	120705
	120668
HP MAC ADDRESS	120705
	120668
ARCHI 3.3.1	120512
FREEMIN	120512
ARIS EXPRESS	120512
GOOGLE WORKSPACE SYNC	120221
	120902
	119649
	120193
	119797
	120185
	120735
VLC MEDIA PLAYER	120776
OCR SOFTWARE BY I.R.I.S	162
Dropbox	120193
Google Drive	120221
	120902
	120193
	119797
	120735
Pandoc	120193
TeXstudio	120193
Vim	120221
	120193
	120185
	120735
OFFLINEOST TO PST CONVERTER	120705
SBO 14000	229
ImpresionEn Linea	229
SEAGATE REPORT ACTIVEX VIEWER	229
SUN ODF PLUGIN	229
CMAKE	120735
Backup and Sync from Google	120902

PSQLODBC	120512
WBS SXHEDULE PRO	120512
Synaptics pointing Device Driver	120512
	120776
PGJDBC	120512
Postgre sql	120512
ControlImpresión BOE	162
MICROSOFT VISUAL STUDIO No está autorizado para todos los computadores	120221
	120930
	120523
R FOR WINDOWS No está autorizado para todos los computadores	6284
	120221
	120902
	120165
	120133
	831
	120101
	120185
	120735
RSTUDIO No está autorizado para todos los computadores	6284
	120221
	603
	120133
	120193
	120101
	120185
	120735

↓ En los equipos relacionados a continuación, se encontró el uso de software sin licencia:

SOFTWARE	PLACA CPU
PDF COMPLETE CORPORATE EDITION	65
SOPHOS ENDPOINT	119649
	120193
	120649
WINRAR	120668
TeamViewer	120261

Sobre este software se precisa que, en desarrollo del seguimiento, la Oficina de Control Interno comunicó esta situación a la Dirección de Tecnología, quienes procedieron a desinstalar de manera inmediata estas aplicaciones de los equipos relacionados.

3. Verificación de las licencias de software instaladas en los equipos de cómputo de la entidad

Al verificar la muestra de 19 licencias, se evidencia que éstas se encuentran debidamente organizadas e inventariadas; así mismo, se tiene identificado en qué equipo está instalada cada una de ellas. Sin embargo, se recomienda eliminar el siguiente software del listado, toda vez que no requiere estar licenciado para su uso:

Placa Licencia	PC	Marca	Modelo	Serial	Usuario logueado	Software instalado	Cantidad
16942	UAC-E-08	HP	HP ELITEDESK 705 G4 SFF	MXL90118J6	NZRODRIGUEZV	CMS SUPERVISOR R17	7

4. Validación de los mecanismos de control que se han implementado para evitar que los usuarios instalen programas que no cuenten con la licencia respectiva

La Dirección de Tecnología e Información mediante correo electrónico del día 16 de febrero comunicó a la Oficina de Control Interno, los mecanismos de control implementados para evitar que los usuarios instalen y/o ejecuten software no licenciado ni permitido por la entidad, los cuales se relacionan a continuación:

"1. Implementación de directivas de seguridad local, las cuales contienen una serie de opciones de seguridad que son aplicadas a los equipos de cómputo de la entidad y que hacen parte del controlador de dominio icfes.gov.co.

Esta directiva permite administrar las sesiones y la seguridad de los usuarios, las cuales pueden ser aplicadas por usuarios o unidades organizacionales y es la encargada de que no se puedan realizar instalaciones, ni cambios en el sistema de la máquina sin solicitar permiso del administrador de dominio. A continuación, la evidencia correspondiente:

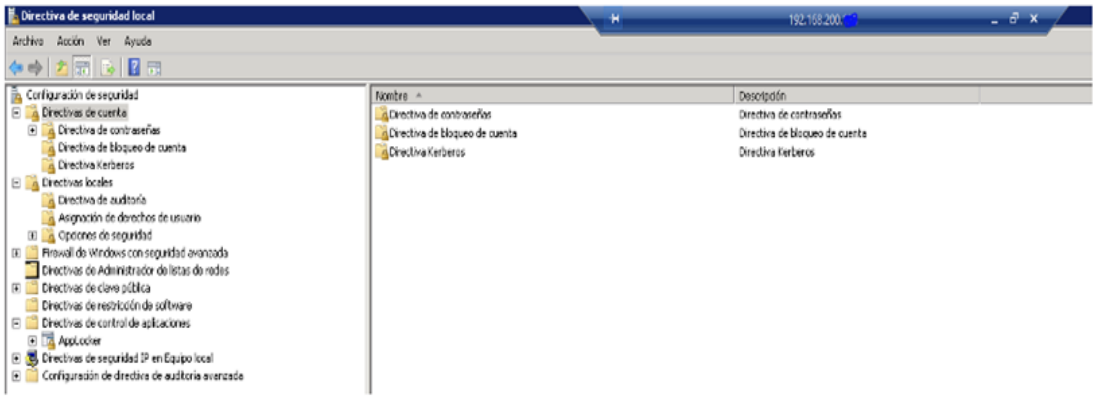


Fig-1 – Directiva de Seguridad local

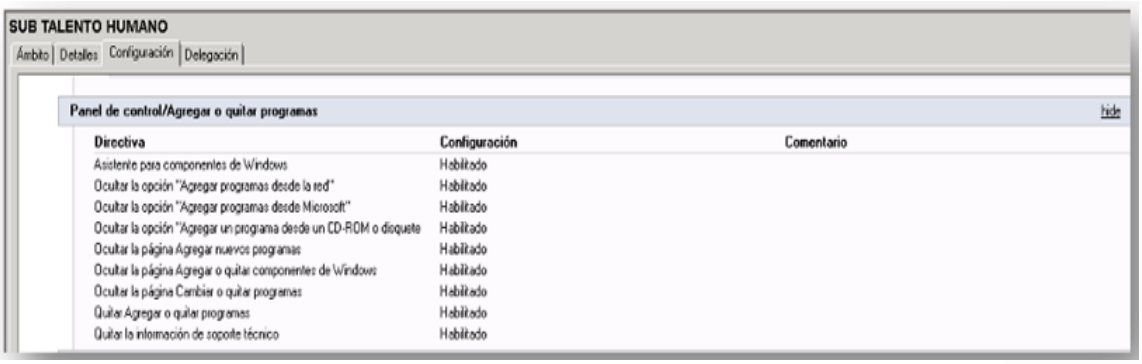


Fig-2. Directiva de bloque de instalación de software

2. De acuerdo con lo anterior, se realizó la depuración de los usuarios con permisos y privilegios de tipo administrador, lo que permite tener el control de los usuarios con permisos para realizar la instalación de software. A continuación, la evidencia correspondiente:

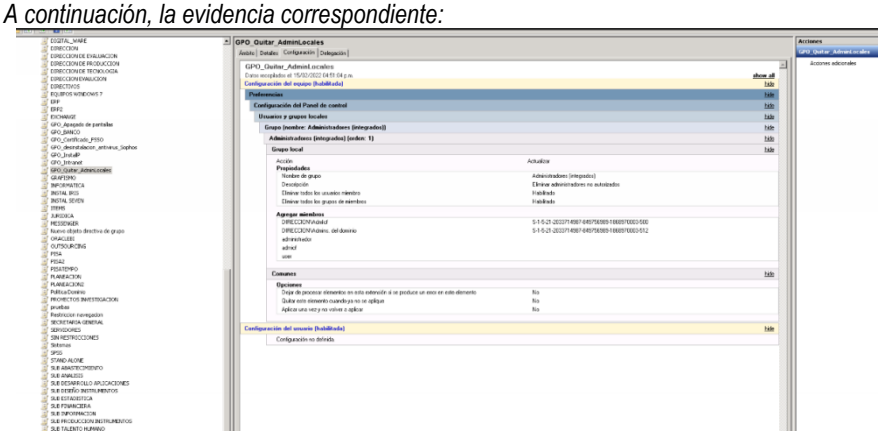


Fig-3. Usuarios con Perfil de Administrador

3. En el caso de la seguridad perimetral - firewall, este se encuentra actualizado y se tienen implementadas en el módulo de Security Profiles las siguientes políticas de Web Filtrer y Application Control, las cuales bloquean la descarga de aplicaciones en sitios web no autorizados. A continuación, la evidencia correspondiente:

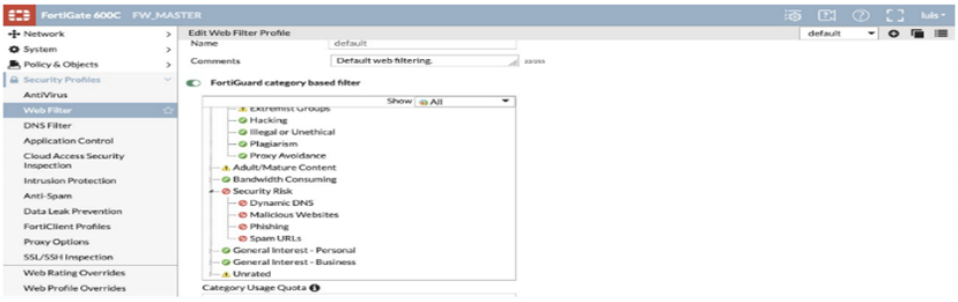


Fig-4. Políticas de Web Filtrer

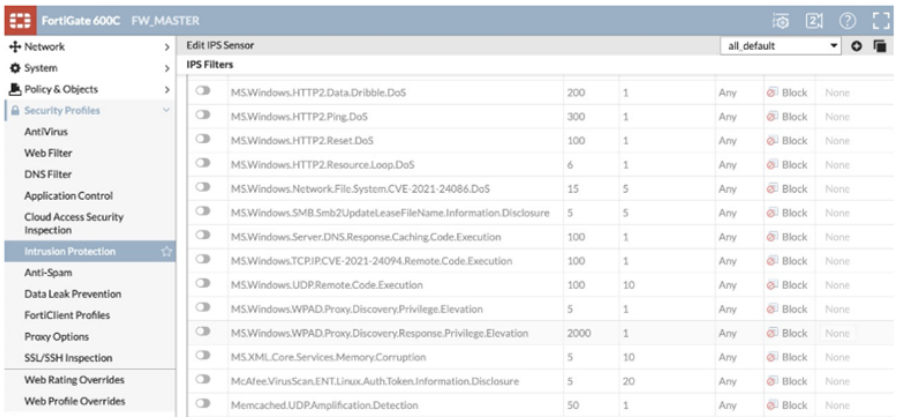


Fig-5. Políticas configuradas en Intrusion Protection

4. Se definió, socializó y publicó el listado de software permitido y no permitido por la entidad, este fue determinado teniendo en cuenta el licenciamiento y suscripciones vigentes y los requerimientos de las diferentes áreas con su correspondiente justificación en caso de que aplique. Este listado fue divulgado a través de una campaña de socialización con los Super I, como se puede evidenciar a continuación:

Y publicado en el Intranet institucional en el sitio de la Dirección de Tecnología a Información: https://icfesgovco.sharepoint.com/sites/FamiliaIcfes/SitePages/Servicios-Tecnol%C3%B3gicos.aspx, la última versión es la 3 con corte a octubre de 2021.

5. Luego de definido el listado de software permitido y no permitido la mesa de servicios realizó la desinstalación del software, que no estaba permitido o que no se encontrará en los permitidos.

6. Se realizó la actualización del procedimiento GTI –PR009 Configuración de Equipos de Cómputo, en el cual se establecieron las generalidades para el licenciamiento de software como la adquisición, instalación, gestión, solicitud y desinstalación de software.

GENERALIDADES PARA EL LICENCIAMIENTO DE SOFTWARE

- La Dirección de Tecnología e Información es la única dependencia autorizada para la adquisición y administración del licenciamiento.
- El personal de mesa de servicios es el único en la operación autorizado para la instalación, soporte y/o desinstalación del licenciamiento en los equipos de cómputo del Icfes. En el caso de los usuarios administradores, para realizar instalación de sofware deberán pedir previa autorización al responsable del CI Licenciamiento.
- En caso de que un usuario no haga uso del software por un espacio de cuatro (4) meses, se procederá con la desinstalación para garantizar el uso eficiente del licenciamiento.
- Las áreas, dependencias y/o colaboradores que requieran la instalación de un nuevo software deberán radicar un caso a la mesa de servicios indicando la descripción y justificación de la necesidad. En este caso, el responsable de licenciamiento será el encargo de validar la pertinencia y condiciones de uso a nivel institucional.
- El responsable del CI Licenciamiento debe:

  - Establecer, publicar y mantener actualizado el listado de software permitido, autorizado y no permitido en la entidad de acuerdo con derechos de autor, licencias y usos.

  - Controlar la gestión de licenciamiento y las actividades que la mesa de servicios desempeña en función de este componente, generando las acciones de mejora que correspondan.

  - Cuando se evidencie la instalación de software no autorizado o no permitido, debe notificar al jefe inmediato del colaborador que tenía instalado el software la situación.

  - Mantener prueba y evidencia de la propiedad de las licencias de software y los medios de instalación.

  - Gestionar que las licencias adquiridas sean instaladas en su totalidad a los colaboradores que lo requieran con el fin de garantizar el uso eficiente de las adquisiciones.

- La mesa de servicios debe establecer los mecanismos para:

  - Controlar que las licencias instaladas no excedan la cantidad de licencias adquiridas.

  - Cuando se requiera la instalación de una licencia de software, validar previamente en los listados de software adquiridos y autorizados la disponibilidad o no de este licenciamiento.

  - Controlar que no se realice la instalación de software no permitido y, en caso de encontrase instalado, tomar las acciones necesarias para su desinstalación y generación de la alerta al responsable del CI Licenciamiento.

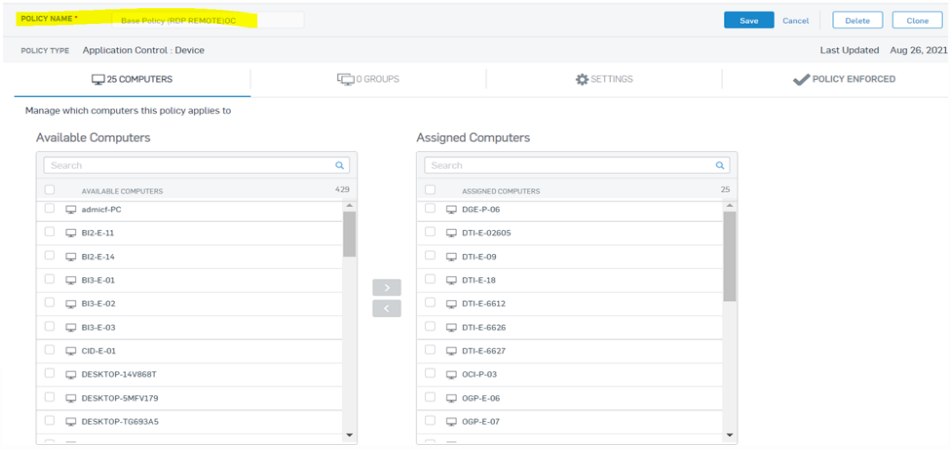
  - Estandarizar las versiones del licenciamiento instalado.

De acuerdo con el procedimiento el personal de mesa de servicios es el único autorizado para realizar la instalar software.

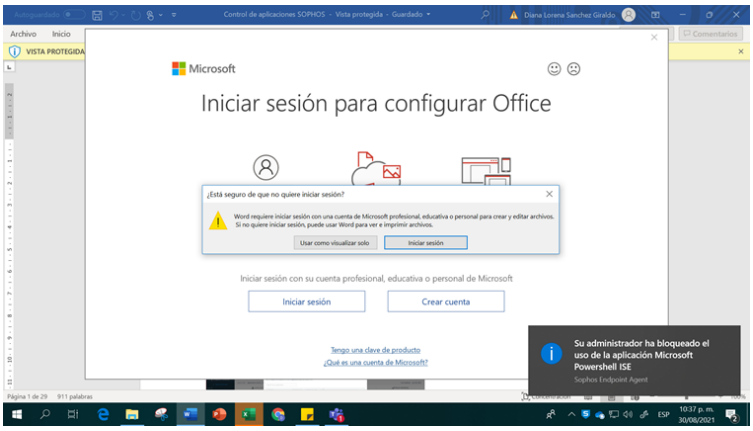
7. De igual manera, para la vigencia 2021 se establecieron controles en la herramienta Sophos (Antimalware), mediante los cuales se bloquea la ejecución, descarga e instalación de software, el listado de este software fue tomado del listado propuesto por la herramienta y del cual se fueron depurando políticas. Así mismo, se definió una política general llamada Base Policy – Application Control, que bloquea todos los software para todos los equipos del Instituto:

CONTROLLED APPLICATIONS	SELECTED / TOTAL	CONTROL NEW APPS
Application vulnerabilities	2 / 2	
Archive tool	7 / 9	
Asset Management tool	13 / 14	
Browser plug-in	34 / 39	
Desktop search tool	7 / 9	
Distributed computing	8 / 8	
Download manager	59 / 62	
Email sync tool	1 / 2	
Encryption / Steganography tool	27 / 31	
File sharing application	95 / 98	
FTP Client	15 / 16	
Game	353 / 357	
Instant messaging	124 / 139	
Jailbreak Software	3 / 3	
Mapping application	1 / 6	
Media conversion tool	15 / 15	
Media player	133 / 142	
Mobile Synchronization	32 / 39	
Network monitoring / Vulnerability tool	60 / 60	

De acuerdo con esta política general y las excepciones solicitadas por los usuarios se establecieron las demás políticas por grupos de usuarios, por ejemplo, la política RDP Remote; se configuro para permitir la ejecución de acceso remoto y en esta política se excluyeron 25 usuarios:



Cuando un usuario intenta ejecutar alguna aplicación no permitida por Sophos, se muestra un mensaje como el siguiente:



Estas políticas y controles implementados fueron suspendidos a partir del mes de septiembre de 2021, dado que la entidad cambió de herramientas de Antimalware y debió establecer un nuevo plan de implementación y afinamiento de la nueva herramienta Windows Defender.

8. Por último, se cuenta con políticas de seguridad y privacidad de la información dentro del Sistema de Gestión de Seguridad de la Información - SGSI, las cuales son divulgadas de manera efectiva y continua a todos los colaboradores del Icfes".

No obstante, se continúan identificando debilidades en la aplicación de políticas relacionadas con la instalación de software no permitido por la entidad, sustentado en las situaciones planteadas en el numeral 2 del presente informe.

5. Destino final que se le da al Software dado de baja en la entidad

La Dirección de Tecnología e Información mediante correo electrónico del día 16 de febrero comunicó a la Oficina de Control Interno que durante la vigencia 2021 emitió el "*Concepto Técnico para proceso de baja de activos fijos intangibles*" (radicado 202130002060 de noviembre de 2021), con el fin de que se adelantaran los procesos de baja por parte de la Subdirección de Abastecimiento y Servicios Generales. Teniendo en cuenta que en diciembre de 2021 no se celebró el comité de bajas, la SAySG incluyó dicha solicitud en el Plan de acción de Inventarios 2022, programando el comité para el primer trimestre del año; en el cual, se darán de baja bienes intangibles, equipos obsoletos, dañados y fuera de servicio.

NO CONFORMIDADES

↓ **No Conformidad 01: Instalación de aplicaciones o software no autorizado:** Se continúan identificando debilidades en la aplicación de los lineamientos sobre las condiciones de licenciamiento de software, programas autorizados y las condiciones de seguridad de equipos descritos en las Políticas de Seguridad y Privacidad de la Información GTI-MN001; lo anterior, teniendo en cuenta las situaciones planteadas en el numeral 2 del presente informe relacionadas con la evidencia sobre software gratuito o sin licencia que se encontró instalado en algunos de los equipos de la muestra evaluada.

Adicionalmente, se incumple lo establecido en el Procedimiento Gestión de Accesos que establece:

- "*El líder de servicios tecnológicos debe definir y mantener los recursos y herramientas validados y aprobados por el Director de Tecnología e Información.*
- *El líder de servicios tecnológicos y su equipo de trabajo deberán mantener, restringir y monitorear frecuentemente las herramientas informáticas del Icfes.*
- *El monitoreo a los diferentes sistemas de información y servicios tecnológicos del instituto deberá realizarse con periodicidad mensual con el fin de garantizar que se desactiven del directorio activo a funcionarios que no tengan vinculación laboral o contractual vigente*".

Si bien es cierto que, en desarrollo del seguimiento la Dirección de Tecnología saneó la situación presentada con relación a los equipos evaluados en la muestra con software no licenciado; la No Conformidad se mantiene, toda vez que se debe realizar el mismo ejercicio con el software libre no autorizado; además, se reitera le necesidad de realizar una revisión integral sobre la totalidad del inventario de equipos del Instituto.

OPORTUNIDADES DE MEJORA

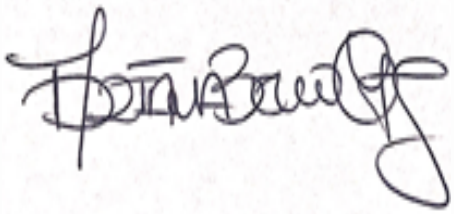
- Se corroboró que durante la vigencia 2021 se implementaron mejoras en el control de inventarios de activos del Instituto; no obstante, se recomienda a la Subdirección de Abastecimiento y Servicios Generales realizar la actualización del inventario en la vigencia 2022, toda vez que no fue posible la revisión de dos equipos de cómputo, debido a que no se encontraba actualizado el responsable del activo, como fue expuesto en el numeral 1 del presente informe.

- Se reitera la importancia de realizar una validación sobre el efectivo funcionamiento de la herramienta Aranda, así como efectuar una actualización de las bases de datos que maneja la Subdirección de Información sobre el estado de cada uno los equipos de cómputo de la entidad.

RECOMENDACIONES

- Es urgente fortalecer la implementación de mecanismos de control efectivos que permiten mitigar los riesgos derivados de la utilización de programas no autorizados, controlar el uso de software y vigilar que se cumplan con las disposiciones en materia de Seguridad de la Información y derechos de autor.

Cordialmente,



ADRIANA BELLO CORTÉS
Jefe Oficina de Control Interno

Equipo Auditor:
María del Pilar González Henao.
Oscar David Posada Daza.