

FECHA DE SEGUIMIENTO INFORME:

Marzo de 2025

DEPENDENCIAS:

Secretaría General, Oficina Asesora de Ciencia, Tecnología e Innovación,
Oficina de Recursos Físicos y Oficina de Control Interno.

LIDER DEL PROCESO DE SEGUIMIENTO:

José Cardozo Álvarez, Jefe de Control Interno

TEMA DE SEGUIMIENTO/INFORME:

Informe de Seguimiento Derechos de Autor Software

VIGENCIA EVALUADA:

2024.

1. INTRODUCCIÓN:

El presente informe tiene como finalidad verificar el cumplimiento de la Ley 603 de 2000, la cual modifica el artículo 47 de la Ley 222 de 1995, estableciendo la obligación de presentar un informe de gestión sobre las licencias de software utilizadas en los equipos de la entidad. Asimismo, se da cumplimiento a las circulares presidenciales 01 de 1999, 02 de 2002, 04 de 2006 y 017 de 2011, relacionadas con el uso legal del software en entidades públicas.

En este contexto, la Dirección Nacional de Derecho de Autor (DNDA) requiere a las entidades y organismos públicos, tanto del orden nacional como territorial, la verificación del uso legal del software, en concordancia con la Directiva Presidencial No. 002 de 2002. Dicha directiva recuerda a los representantes legales y jefes de Control Interno su obligación de remitir información sobre la verificación, recomendaciones y resultados en materia de derechos de autor respecto al software empleado en sus entidades, conforme a lo estipulado en la Circular 17 de 2011.

Adicionalmente, en cumplimiento de las Directivas Presidenciales 01 de 1991 y 02 de 2002, el Consejo Asesor del Gobierno Nacional en materia de Control Interno expidió la Circular 04 del 22 de diciembre de 2006, mediante la cual solicita a los representantes legales y jefes de las Oficinas de Control Interno de entidades y organismos públicos la entrega de información sobre la verificación, recomendaciones y resultados relacionados con el cumplimiento de la normativa sobre derechos de autor en el uso de software.

En este marco normativo, y con el propósito de garantizar el uso exclusivo de software autorizado, se elabora el *Informe de Seguimiento al Cumplimiento de la Ley de Software y Derechos de Autor – Vigencia 2024* en la Corporación Autónoma Regional del Atlántico (CRA). La DNDA ha establecido un procedimiento para la recepción, administración y custodia de esta información a través del aplicativo disponible en su portal oficial (www.derechodeautor.gov.co), con un plazo de presentación comprendido desde el primer día hábil de enero hasta el tercer viernes de marzo de cada año.

2. OBJETIVO:

Verificar y evaluar el cumplimiento de la normatividad vigente en materia de derechos de autor, así como el uso adecuado del software dentro de la Corporación Autónoma Regional del Atlántico (C.R.A), garantizando la legalidad y correcta gestión de los programas de cómputo utilizados en la entidad.

3. ALCANCE:

El presente seguimiento evalúa la aplicación de la normativa vigente sobre el uso de software en la Corporación Autónoma Regional del Atlántico (CRA), con corte al 31 de diciembre de 2024.

Asimismo, se verifica las acciones implementadas por la CRA para prevenir el uso no autorizado de programas sin licencia y se analiza la efectividad de los controles establecidos para garantizar el cumplimiento de la regulación en materia de derechos de autor y software.

4. MARCO INFORMATIVO:

- ✓ **Directiva Presidencial No. 001 del 25 de febrero de 1999**, Relacionada con el respeto al derecho de autor y los derechos conexos. A través de dicha circular se instruyó a los servidores públicos en la obligación de adoptar un comportamiento respetuoso del derecho de autor y la prohibición de utilizar o adquirir obras literarias o artísticas, fonogramas y señales de televisión que infrinjan tales derechos.
- ✓ **Directiva Presidencial No. 002 del 02 de febrero de 2002**, se reitera el interés del Gobierno en la protección del derecho del autor y los derechos conexos y se ordena a las oficinas de control interno, auditores u organismos de control de las respectivas entidades, verificar el cumplimiento de las disposiciones en materia de derechos de autor en la adquisición y uso de programas de computador en la entidad.

- ✓ **Circular 4 de 2006 del Consejo Asesor del Gobierno Nacional en Materia de Control Interno**, La Evaluación Institucional a que se refiere la presente circular siguiente vigencia, de manera tal que se entienda como parte integrante del informe Ejecutivo Anual de Evaluación del Sistema de Control Interno, que debe remitir el Jefe de la Oficina de Control Interno, Auditor Interno, Asesor o quién haga sus veces a los Representantes Legales y Jefes de las Entidades y Organismos del Estado a más tardar el 30 de Enero de cada año, conforme a los establecido en el literal e) del artículo 8 del Decreto 2145 de 1999, concordante con el artículo 2 del Decreto 2539 de 2000.
- ✓ **Circular 12 de 2007 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor**, La presente circular tiene por objeto definir la información que debe contener el reporte sobre “Verificación, recomendaciones, seguimiento y resultados sobre el cumplimiento de las normas en materia de derecho de autor sobre Software” a presentar por los Jefes de Control Interno en virtud de lo solicitado por la Circular 4 de 2006, expedida por el Consejo Asesor del Gobierno Nacional en materia de control interno de las Entidades del Orden Nacional y Territorial.
- ✓ **Circular 17 de 2001 de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor**, La presente Circular tiene por objeto modificar el numeral 2 del título III de nuestra Circular 4 del 22 de diciembre de 2006 del Consejo Asesor del Gobierno Nacional en materia de Control Interno de las Entidades del Orden Nacional y Territorial, por el responsable de cada entidad en el aplicativo que para efecto dispondrá la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor en la página www.derechodeautor.gov.co, desde el primer día hábil del mes de enero de cada año hasta el tercer viernes del mes de marzo, fecha en la cual se deshabilitara el aplicativo.
- ✓ **Ley 87 de 1993**, “Por el cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones”.

5. DESARROLLO DEL SEGUIMIENTO:

Este informe se elabora en cumplimiento del cronograma de actividades del *Informe de Seguimiento sobre Derechos de Autor y Software – Vigencia 2024*, enmarcado dentro de la normativa vigente en materia de Derecho de Autor y Derechos sobre Software, con el propósito de garantizar el uso exclusivo de software autorizado, en conformidad con la legislación aplicable.

CRONOGRAMA DE ACTIVIDADES

10
MARZO

ENVÍO DE MEMORANDO A LAS ÁREAS CORRESPONDIENTES

Oficina Secretaría General y Oficina de Ciencia, Tecnología e innovación (CTI).

Jose Lima, Juan Coha, Irina Blanco (Apoyo asignado).

14
MARZO

PLAZO PARA LA RECEPCIÓN DE INFORMACIÓN DE LAS ÁREAS INVOLUCRADAS

Oficina Secretaría General y Oficina de Ciencia, Tecnología e innovación (CTI).

Jose Lima, Juan Coha, Irina Blanco (Apoyo asignado).

17
MARZO

PROCESO DE VERIFICACIÓN Y REVISIÓN DE LA INFORMACIÓN RECIBIDA

Oficina de Control Interno

Kelly Barceló (Apoyo asignado).

19
MARZO

CONSOLIDACIÓN DE INFORMACIÓN PARA REVISIÓN Y APROBACIÓN DEL JEFE DE LA OCI

Oficina de Control Interno

Kelly Barceló (Apoyo asignado).

21
MARZO

DILIGENCIAMIENTO DEL CUESTIONARIO EN LA PÁGINA WEB DE LA DNDA Y ADJUNCIÓN DEL INFORME

Oficina de Control Interno

Jose Cardozó (Apoyo asignado).

La Oficina de Control Interno (OCI), mediante el Memorando No. 000424 del 10 de marzo de 2025, solicitó a la Secretaría General —específicamente a la Oficina de Recursos Físicos y la Oficina Asesora de Ciencia, Tecnología e Innovación — los soportes de información requeridos para el reporte de hardware (equipos) y software (programas) legales registrados ante la Unidad Administrativa Especial de Derechos de Autor (DNDA). En respuesta, la información fue remitida el 14 de marzo de 2025 a través de los correos electrónicos sistemas@crautonomia.gov.co y

almacen@crautonomia.gov.co, con las respuestas oficiales presentadas por la Corporación Autónoma Regional del Atlántico (CRA).

Con base en los documentos enviados por la Secretaría General y La Oficina Asesora de Ciencia, Tecnología e Innovación, la OCI llevó a cabo la verificación y análisis de la información con el propósito de evaluar el manejo e implementación de los programas, licencias y software utilizados por la CRA. Posteriormente, se procederá con la consolidación del informe requerido por la Dirección Nacional de Derecho de Autor, con corte al 31 de diciembre de 2024:

- Totalidad de Equipos de Cómputo Instalados al 31 de diciembre de 2024.

La Oficina Asesora de Ciencia, Tecnología e Innovación (CTel), tecnología e innovación de la Corporación Autónoma Regional del Atlántico (CRA) informa que, al corte del 31 de diciembre de 2024, la entidad cuenta con un total de ciento treinta y seis (136) equipos de cómputo tipo PC instalados.

Equipos Cómputo	Marca	Dependencia	Cantidad
Escritorio	HP	Dirección General	2
	HP	Oficina Asesora de Planeación	13
	HP	Oficina Asesora Jurídica	8
	HP	Oficina de Ciencia, Tecnologías e Innovación	6
	HP	Oficina de Control Interno	2
	HP	Oficina de Gestión Humana	1
	HP	Secretaría General	16
	HP	Subdirección de Gestión Ambiental	23
	HP	Subdirección Financiera	16
	LENOVO	Secretaría General	1
Total Escritorio			88
Portatil	Dynabook Inc.	Dirección General	1
	Dynabook Inc.	Oficina Asesora de Comunicaciones	1
	Dynabook Inc.	Oficina Asesora de Planeación	1
	Dynabook Inc.	Oficina de Ciencia, Tecnologías e Innovación	1
	Dynabook Inc.	Secretaría General	2
	Dynabook Inc.	Subdirección de Gestión Ambiental	9
	Dynabook Inc.	Subdirección Financiera	1
	HP	Dirección General	4
	HP	Oficina Asesora de Comunicaciones	1
	HP	Oficina Asesora de Planeación	4
	HP	Oficina Asesora Jurídica	4
	HP	Oficina de Ciencia, Tecnologías e Innovación	1
	HP	Oficina de Control Interno	1
	HP	Oficina de Gestión Humana	2
	HP	Secretaría General	4
	HP	Subdirección de Gestión Ambiental	10
HP	Subdirección Financiera	1	
Total Portatil			48
Total Equipos Cómputo			136

Se cuenta con un total de ciento treinta y seis (136) equipos en estado activo y veintiséis (26) equipos en bodega de almacén en estado pasivo, en proceso de baja.

¿El software instalado en estos equipos se encuentra debidamente licenciado? Indicar nombre de software.

La Oficina Asesora de Ciencia, Tecnología e Innovación (CTel), informa que todos los equipos de la Corporación Autónoma Regional del Atlántico C.R.A cuentan con los softwares correspondientes.

Software
Innova
Docunet
Kaspersky
Kaspersky Next EDR Optimun Kaspersky Security for Microsoft Office 365 (Incluidas en Kaspersky Next EDR Optimun)
Microsoft
Microsoft 365 Office 2019 Home and Business Office Profesional Plus 2021 Windows 10 Windows 11 Windows 11 Pro / Windows 11 Pro for Workstations - Windows 10/11 Pro - Windows 10/11 Pro for Workstations Windows Server 2012 R2 Standard - Windows Server 2012 R2 (Std and DataCtr) Windows Server 2016 Standard Windows Server 2019 Standard
Oracle
Oracle
PCT
PCT
Software libre
Orfeo
Vmware
Vcenter Vsphere

Asimismo, se indica que existen otros programas instalados en las estaciones de trabajo, como navegadores (Google Chrome, Mozilla Firefox, Microsoft Edge), Adobe Reader, Adobe Flash Player, 7-Zip, entre otros, los cuales son de uso libre y no requieren la adquisición de licencias pagas.

- ✚ ¿Cuáles son los mecanismos de control implementados para la instalación de software en los equipos de cómputo?

La Oficina Asesora de Ciencia, Tecnología e Innovación (CTel) de la Corporación Autónoma Regional del Atlántico (CRA) informa que es la única dependencia con credenciales de administrador para la instalación de software en los equipos de cómputo de la Corporación. Por lo tanto, es la única autorizada para realizar estas instalaciones, garantizando así que no se incorporen programas informáticos sin el debido licenciamiento.

Adicionalmente, se señala que la Corporación cuenta con una mesa de ayuda, a través de la cual los usuarios dentro del dominio y el directorio activo pueden crear un caso para solicitar la instalación de software. El personal de CTel, único con permisos de administrador, es el responsable de gestionar dichas solicitudes y llevar a cabo las instalaciones correspondientes, asegurando el control y cumplimiento de las políticas establecidas.

Por último, se destaca que la instalación de software está enmarcada dentro del Plan de Seguridad y Privacidad de la Información de la CRA y el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI) de la Corporación.

- ✚ ¿Qué licencia se encuentran vigentes y cuál es su fecha de finalización de licenciamiento?

Licencias vigentes:	Cant.
GPL	1
Software libre	1
Orfeo	1
MAK	23
Microsoft	23
Windows 11 Pro / Windows 11 Pro for Workstations - Windows 10/11 Pro - Windows 10/11 Pro for Workstations	10
Windows Server 2012 R2 Standard - Windows Server 2012 R2 (Std and DataCtr)	7
Windows Server 2016 Standard	3
Windows Server 2019 Standard	3
OEM	123
Microsoft	123
Windows 10	72
Windows 11	51
OEM - Perpetua	49
Microsoft	49
Office Profesional Plus 2021	49
Perpetua	5
Oracle	1
Oracle	1
PCT	1
PCT	1
Vmware	3
Vcenter	1
Vsphere	2
Perpetua - Electrónica	72
Microsoft	72
Office 2019 Home and Business	72
Perpetua (Sin soporte)	1
Innova	1
Docunet	1
Suscripción – SaaS	257
Microsoft	257
Microsoft 365	257
Suscripción – SaaS F. Final 08/12/2025	400
Kaspersky	400
Kaspersky Next EDR Optimun	160
Kaspersky Security for Microsoft Office 365 (Incluidas en Kaspersky Next EDR Optimun)	240
Total general	931

✚ ¿Qué mecanismo de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva?

El control que ha implementado la Oficina Asesora de Ciencia, Tecnología e Innovación (CTel) para evitar la instalación de programas o aplicativos no autorizados por la entidad se encuentra plasmado en la Política de Seguridad de la Información de la CRA. Según esta disposición, cada usuario cuenta con un perfil dentro del dominio que impide la instalación de programas por cualquier persona.

Solo el personal de soporte técnico de la Oficina Asesora de Ciencia, Tecnología e Innovación (CTel) está autorizado para realizar estas instalaciones, utilizando el perfil de administrador local presente en cada equipo de cómputo.

Del mismo modo, para instalar cualquier tipo de programa, el interesado debe realizar una solicitud de servicio a través de la mesa de ayuda, donde se evalúa si el software requiere algún tipo de serial o licenciamiento, con el fin de determinar la viabilidad o no de su instalación.

✚ ¿Cuál es el destino final que se da al software dado de baja en la entidad?

De acuerdo con la información suministrada por la Oficina Asesora de Ciencia, Tecnología e Innovación (CTel), el software dado de baja en la Corporación Autónoma Regional del Atlántico (CRA) se encuentra bajo custodia de dicha oficina. Esto se debe a que dichos programas y/o licencias tecnológicas pueden seguir utilizándose en los equipos de la entidad, siempre que sean compatibles y cuenten con el debido licenciamiento.

Las licencias de Windows adquiridas por la Corporación son electrónicas y están vinculadas a cada equipo de cómputo, lo que significa que solo son legales en su equipo original. Por su parte, las licencias de Office son de tipo perpetuo y cuentan con seriales de activación o claves digitales, por lo que su destino final está ligado al equipo en el que fueron instaladas. En el caso de los antivirus, estos son adquiridos mediante suscripción, lo que implica su renovación periódica según las necesidades institucionales.

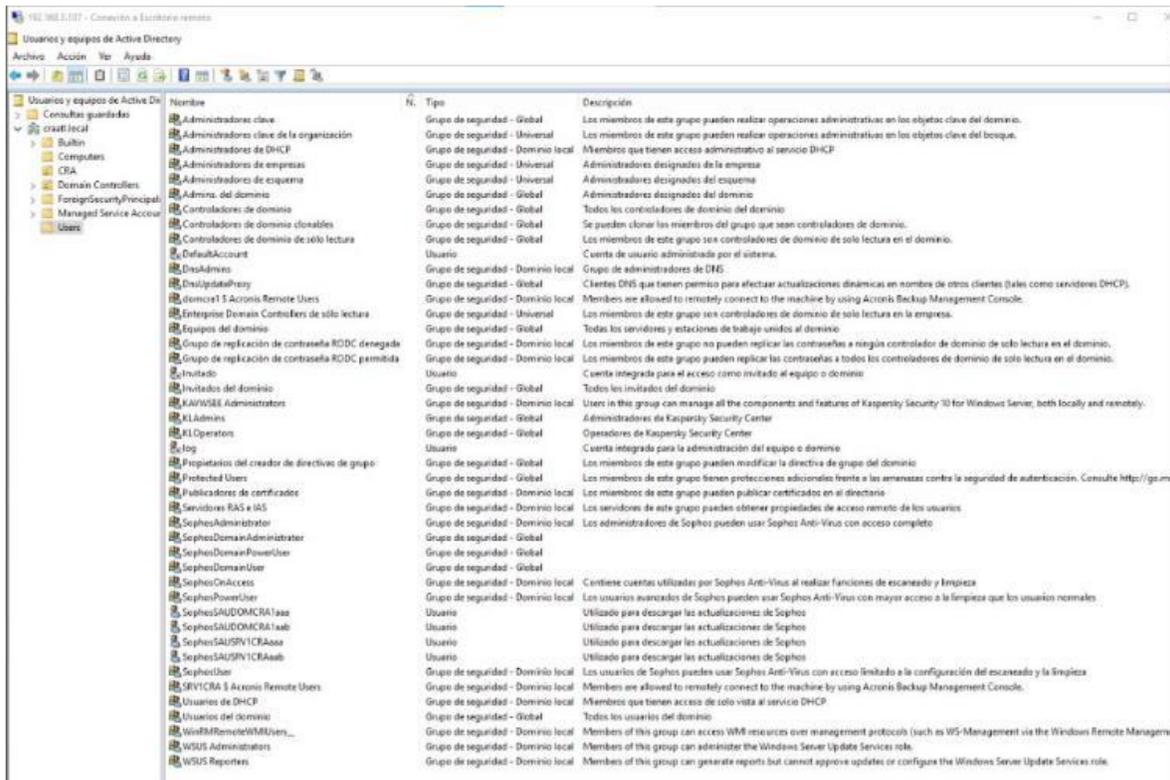
Con el fin de verificar la información relacionada con los equipos activos y los softwares dados de baja, se determinó que, al 31 de diciembre de 2024, la CRA cuenta con 136 equipos activos instalados. En cuanto al software dado de baja, se confirmó que permanece bajo custodia de la Oficina Asesora de Ciencia, Tecnología e Innovación (CTel), garantizando su adecuada gestión y posible reutilización en equipos que lo requieran.

Asimismo, la verificación realizada por la Oficina de Control Interno, en coordinación con la Oficina de Recursos Físicos, confirmó la exactitud del reporte de equipos de cómputo instalados y activos en la entidad. En cuanto al licenciamiento del software en estos equipos, se ha constatado su cumplimiento con la documentación disponible, evidenciando que la CRA mantiene una sólida política de seguridad de la información y control sobre la instalación de software autorizado.

Por otro lado, la Oficina Asesora de Ciencia, Tecnología e Innovación (CTel) reitera que es la única oficina con credenciales de administrador para la instalación de software en los equipos de la Corporación. Esta oficina lleva a cabo el seguimiento,

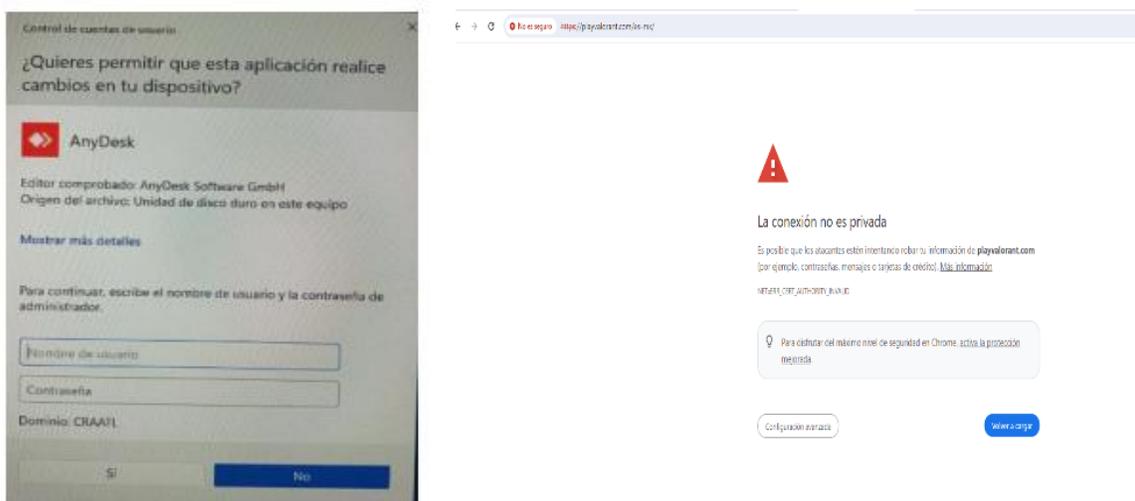
verificación y control de todas las instalaciones realizadas, asegurando que no se instalen programas sin el debido licenciamiento.

Como evidencia nos llega los siguientes pantallazos:



Nombre	N.º	Tipo	Descripción
Administradores clave		Grupo de seguridad - Global	Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del dominio.
Administradores clave de la organización		Grupo de seguridad - Universal	Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del bosque.
Administradores de DHCP		Grupo de seguridad - Dominio local	Miembros que tienen acceso administrativo al servicio DHCP.
Administradores de empresas		Grupo de seguridad - Universal	Administradores designados de la empresa.
Administradores de esquema		Grupo de seguridad - Universal	Administradores designados del esquema.
Admins. del dominio		Grupo de seguridad - Global	Administradores designados del dominio.
Controladores de dominio		Grupo de seguridad - Global	Todos los controladores de dominio del dominio.
Controladores de dominio eliminables		Grupo de seguridad - Global	Se pueden eliminar los miembros del grupo que sean controladores de dominio.
Controladores de dominio de sólo lectura		Grupo de seguridad - Global	Los miembros de este grupo son controladores de dominio de sólo lectura en el dominio.
DefaultAccount		Usuario	Cuenta de usuario administrada por el sistema.
DisAdmins		Grupo de seguridad - Dominio local	Grupo de administradores de DNS.
DnsUpdateProxy		Grupo de seguridad - Global	Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes (tales como servidores DHCP).
Enterprise15Acronis Remote Users		Grupo de seguridad - Dominio local	Members are allowed to remotely connect to the machine by using Acronis Backup Management Console.
Enterprise Domain Controllers de sólo lectura		Grupo de seguridad - Universal	Los miembros de este grupo son controladores de dominio de sólo lectura en la empresa.
Equipos del dominio		Grupo de seguridad - Global	Todos los servidores y estaciones de trabajo unidos al dominio.
Grupo de replicación de contraseña RODC denegada		Grupo de seguridad - Dominio local	Los miembros de este grupo no pueden replicar las contraseñas a ningún controlador de dominio de sólo lectura en el dominio.
Grupo de replicación de contraseña RODC permitida		Grupo de seguridad - Dominio local	Los miembros de este grupo pueden replicar las contraseñas a todos los controladores de dominio de sólo lectura en el dominio.
Invitado		Usuario	Cuenta integrada para el acceso como invitado al equipo o dominio.
Invitados del dominio		Grupo de seguridad - Global	Todos los invitados del dominio.
KASPERSKY Administrators		Grupo de seguridad - Dominio local	Users in this group can manage all the components and features of Kaspersky Security IT for Windows Server, both locally and remotely.
KIAdmins		Grupo de seguridad - Global	Administradores de Kaspersky Security Center.
KIOperators		Grupo de seguridad - Global	Operadores de Kaspersky Security Center.
Keylog		Usuario	Cuenta integrada para la administración del equipo o dominio.
Propietario del creador de directiva de grupo		Grupo de seguridad - Global	Los miembros de este grupo pueden modificar la directiva de grupo del dominio.
Protected Users		Grupo de seguridad - Dominio local	Los miembros de este grupo tienen protecciones adicionales frente a las amenazas contra la seguridad de autenticación. Consulte http://go.microsoft.com/fwlink/?linkid=854826 .
Servidores RAS e IAS		Grupo de seguridad - Dominio local	Los miembros de este grupo pueden publicar certificados en el directorio.
SophosAdmin		Grupo de seguridad - Dominio local	Los servidores de este grupo pueden obtener propiedades de acceso remoto de los usuarios.
SophosDomainAdministrator		Grupo de seguridad - Dominio local	Los administradores de Sophos pueden usar Sophos Anti-Virus con acceso completo.
SophosDomainPowerUser		Grupo de seguridad - Global	
SophosDomainUser		Grupo de seguridad - Global	
SophosOnAccess		Grupo de seguridad - Dominio local	Centrose cuentas utilizadas por Sophos Anti-Virus al realizar funciones de escaneo y limpieza.
SophosPowerUser		Grupo de seguridad - Dominio local	Los usuarios avanzados de Sophos pueden usar Sophos Anti-Virus con mayor acceso a la limpieza que los usuarios normales.
SophosAUDOMCRAaaa		Usuario	Utilizado para descargar las actualizaciones de Sophos.
SophosAUDOMCRA1aab		Usuario	Utilizado para descargar las actualizaciones de Sophos.
SophosSAUSP1CRAaaa		Usuario	Utilizado para descargar las actualizaciones de Sophos.
SophosSAUSP1CRAaab		Usuario	Utilizado para descargar las actualizaciones de Sophos.
SophosUser		Usuario	Los usuarios de Sophos pueden usar Sophos Anti-Virus con acceso limitado a la configuración del escaneo y la limpieza.
SVC15Acronis Remote Users		Grupo de seguridad - Dominio local	Members are allowed to remotely connect to the machine by using Acronis Backup Management Console.
Usuarios de DHCP		Grupo de seguridad - Dominio local	Miembros que tienen acceso de sólo vista al servicio DHCP.
Usuarios del dominio		Grupo de seguridad - Global	Todos los usuarios del dominio.
WinRMRemoteWMIUsers_		Grupo de seguridad - Dominio local	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management).
WSUS Administrators		Grupo de seguridad - Dominio local	Members of this group can administer the Windows Server Update Services role.
WSUS Reporters		Grupo de seguridad - Dominio local	Members of this group can generate reports but cannot approve updates or configure the Windows Server Update Services role.

Así mismo, en visita de campo se realizó verificación de los controles en cuanto a la restricción de ingreso a páginas no permitidas y la descarga de programas ejecutables desde un sitio de internet tal como se pudo apreciar con las siguientes imágenes



6. CONCLUSION:

El presente informe evidencia el cumplimiento de las normativas vigentes en materia de derechos de autor y software en la Corporación Autónoma Regional del Atlántico (CRA). Se ha verificado que los equipos de cómputo activos cuentan con software debidamente licenciado y que la entidad ha implementado mecanismos de control adecuados para evitar la instalación de programas no autorizados. Asimismo, se confirma que el software dado de baja es gestionado de manera adecuada para su posible reutilización dentro de la organización.

7. RECOMENDACIÓN:

Se recomienda continuar fortaleciendo los controles sobre la instalación y gestión de software, asegurando la actualización periódica de licencias y la evaluación constante de cumplimiento normativo. Adicionalmente, sería beneficioso implementar auditorías periódicas y capacitaciones para los usuarios, con el objetivo de reforzar la conciencia sobre la importancia del uso de software autorizado y la seguridad de la información en la entidad.

Atentamente,



JOSE CARDOZO ALVAREZ
Jefe Oficina de Control Interno

Elaborado por: Kelly Barceló.