GOBERNACIÓN DE ANTIOQUIA República de Colombia	**INFORME DE SEGUIMIENTO A LA CONTRATACIÓN ESTATAL**	Código: FO-M7-P6-016
		Versión: 03
		Fecha de aprobación: 22/04/2024

NÚMERO DE INFORME	**1**					
SUPERVISIÓN	X					
INTERVENTORÍA	☐					
TIPO DE INFORME	**PARCIAL**	X	**PARA PAGO**	☐	**FINAL**	☐
PERIODO DE INFORME	Desde:	26/05/2026		Hasta:	25/07/2026	
PERIODO PARA PAGO	Desde:	26/05/2026		Hasta:	25/07/2026	

1. INFORMACIÓN GENERAL E HISTORIAL DEL CONTRATO / CONVENIO

CONTRATO	☐	**NÚMERO:**	4600019125	
CONVENIO	☐	**FECHA DE SUSCRIPCION:**	26/05/2026	
MODALIDAD DE SELECCIÓN:			SELECCIÓN ABREVIADA	
IDENTIFICACIÓN DEL PROCESO EN SECOP:			17065	
FECHA DE INICIO DEL CONTRATO/CONVENIO:			26/05/2026	
Renovación y suscripción de plataforma de protección Endpoints y herramientas en informática digital.				
ORGANISMO CONTRATANTE /CONVENIANTE:			**DEPARTAMENTO DE ANTIOQUIA – SECRETARÍA DE TALENTO HUMANO Y SERVICIOS ADMINISTRATIVOS**	
CONTRATISTA / CONVENIANTE	NOMBRE:		GRUPO MICROSISTEMAS COLOMBIA S.A.S	
	NIT		900.418.656-1	
VALOR [$]:	INICIAL:		OCHOCIENTOS VEINTISÉIS MILLONES NOVENTA Y OCHO MIL NOVECIENTOS OCHENTA MIL PESOS MLC ($826.098.980) TRIBUTOS INCLUIDOS	
	ADICIONES	**No.**	**VALOR ADICIONADO**	**% DE ADICION**
			N/A	N/A
	VALOR TOTAL:		OCHOCIENTOS VEINTISÉIS MILLONES NOVENTA Y OCHO MIL NOVECIENTOS OCHENTA MIL PESOS MLC ($826.098.980) TRIBUTOS INCLUIDOS	
	RPC NUMERO:		4200012041	
	FECHA DE LIBERACION (IMPRESIÓN):		22/05/2026	
	RPC NUMERO:		4500067018	
	FECHA DE LIBERACION (IMPRESIÓN):		25/05/2026	
REGISTRO PRESUPUESTAL	RPC NUMERO:		4500067017	
	FECHA DE LIBERACION (IMPRESIÓN):		26/05/2026	
VALOR Y PORCENTAJE DE ANTICIPO:			N/A	
PLAZO:	INICIAL		Doce (12) meses, contados a partir de la suscripción	

		del acta de inicio			
		FECHA DE INICIO		**FECHA DE TERMINACION**	
		03/06/2026		03/06/2027	
	PRÓRROGAS	**No.**	**TIEMPO PRORROGADO**	**NUEVA FECHA DE TERMINACIÓN**	
		N/A	N/A	N/A	
HISTORICO DE SUSPENSIONES:		**No.**	**FECHA INICIO SUSPENSIÓN**	**FECHA REANUDACIÓN**	**FECHA DE TERMINACION**
		N/A	N/A	N/A	N/A
FECHA DE TERMINACIÓN ACTUAL		03/06/2027			
TIENE GARANTÍAS VIGENTES, ACTUALIZADAS Y APROBADAS				SI	
SUPERVISOR(ES)/ INTERVENTOR	NOMBRE(S)/ RAZON SOCIAL:	JHON FREDY BORJA CARVAJAL CC. 98.580.313			
	NUMERO CONTRATO INTERVENTOR:	N/A			
% DE EJECUCIÓN FÍSICA		14%			
% DE EJECUCIÓN DE RECURSOS		100%			

2. CUMPLIMIENTO DE LAS OBLIGACIONES, ACTIVIDADES O COMPROMISOS DE LAS PARTES

2.1. CUMPLIMIENTO DE LAS OBLIGACIONES, ACTIVIDADES O COMPROMISOS DEL CONTRATISTA/CONVENIANTE EJECUTOR.

2.1.1. EJECUCIÓN FÍSICA Y FINANCIERA DE LOS CONVENIOS/CONTRATOS DERIVADOS DE CONFORMIDAD CON LO INFORMADO POR EL CONVENIANTE O CONTRATISTA EJECUTOR

% DE EJECUCIÓN FÍSICA CONSOLIDADA DE LOS CONTRATOS/CONVENIOS DERIVADOS	N/A
% DE EJECUCIÓN FINANCIERA CONSOLIDADA DE LOS CONTRATOS/CONVENIOS DERIVADOS	N/A

2.1.2. SEGUIMIENTO TÉCNICO DEL CONTRATO/CONVENIO:

Renovación y suscripción de plataforma de protección Endpoints y herramientas en seguridad digital.

OBLIGACIONES/COMPROMISOS PACTADOS DEL COMPONENTE TÉCNICO	% DEJECUCIÓN DEL PERIODO INFORMADO	% EJECUCIÓN ACUMULADO	MEDIO DE VERIFICACIÓN
Servicio de soporte técnico de 3400 suscripciones de EndPoint basadas en la nube con la solución “Sophos XDR User” o equivalente de fabricante y que despliegue actualizaciones. Por un periodo de 12 meses.	100%	14%	Se recibió a satisfacción
Servicio de soporte técnico de 300 suscripciones de EndPoint basadas en la nube con la solución “Sophos XDR User” o equivalente de fabricante y que despliegue actualizaciones. Por un periodo de 12 meses.	100%	14%	Se recibió a satisfacción
El CONTRATISTA debe suministrar libre de costo para La Gobernación de Antioquia, el acceso a los manuales requeridos para la operación y solución de problemas durante el licenciamiento de las plataformas de EndPoint.	100%	100%	Se recibió a satisfacción.
El PROPONENTE deberá anexar las certificaciones del fabricante de la plataforma de Endpoint (EPP), donde garantice la idoneidad y lo respalde para distribuir e implementar la solución.	100%	100%	Se recibió a satisfacción.
El CONTRATISTA debe contar como mínimo con un responsable certificado en la solución de Plataforma de Protección Endpoint (EPP) para realizar las tareas de la solución.	100%	14%	Se recibió a satisfacción.
El CONTRATISTA deberá brindar soporte de plataforma de protección Endpoint (EPP) por 12 meses por parte del fabricante, la atención telefónica debe ser en idioma español por personal experto en la solución.	100%	14%	Se recibió a satisfacción.
El CONTRATISTA entregará al supervisor del contrato, los documentos que acrediten el licenciamiento de la solución de Protección de Endpoint a nombre de la Gobernación de Antioquia.	100%	14%	Se recibió a satisfacción
La solución de la plataforma de protección Endpoint debe contar con soporte por un periodo de 12 meses por parte del fabricante, que comenzará a partir del día en que se activen las licencias de acuerdo con el acta de inicio, EL CONTRATISTA debe entregar un documento del fabricante donde certifique el licenciamiento y el cubrimiento de soporte por este periodo de tiempo.	100%	14%	Se recibió a satisfacción.

El CONTRATISTA debe incluir un procedimiento para el reporte y escalamiento de los incidentes y/o problemas, que incluya línea de atención telefónica en español, plataforma para el seguimiento y control y correo electrónico, 7 días a la semana, las 24 horas del día, los 365 días del año.	100%	14%	Se recibió a satisfacción.
La atención se podrá hacer por medio de la conexión de VPN que se le asigne al CONTRATISTA a los equipos de cómputo y servidores, en caso de que el acceso remoto no sea efectivo, se debe desplazar un ingeniero certificado al sitio en donde se reporta el problema, para agilizar en el diagnóstico y la solución.	100%	14%	Se recibió a satisfacción.
El PROPONENTE debe anexar a su propuesta, la(s) URL(s) para descargar las fichas técnicas en la página oficial del fabricante, del producto de Endpoint Protection ofrecido donde pueda validarse el cumplimiento técnico de todo lo solicitado. No se aceptarán documentos privados firmados por el comercializador o el fabricante avalando las especificaciones técnicas solicitadas.	100%	100%	Se recibió a satisfacción.
El CONTRATISTA deberá realizar transferencias de conocimiento teórico-práctico al grupo de seguridad de la información de la Gobernación de Antioquia y de la FLA o a quien consideren, que está conformado a los funcionarios públicos y contratistas del equipo de Seguridad, con una duración de 15 horas, los contenidos a tratar se acordarán con el supervisor del contrato.	0%	0%	Se programará las sesiones de transferencia de conocimiento
La transferencia de conocimiento deberá incluir mínimo los siguientes temas: gestión, administración y configuración de la herramienta de antimalware Endpoint y herramientas de auditoría de directorio activo y file servers, contraseñas del directorio activo, identificación de Vulnerabilidades y solución de inteligencia artificial de antimalware sobre aspectos de configuración, administración, monitoreo y reportes avanzados.	0%	0%	Se programará las sesiones de transferencia de conocimiento
El CONTRATISTA debe realizar un (1) estado de salud de todas las plataformas tecnológicas del contrato, entregando un informe donde se especifique el estado actual y las acciones de mejora que consideran importantes en realizar.	0%	0%	Se programará las sesiones de para realizar el estado de salud
Servicio de soporte en la nube de la herramienta Tenable One, de análisis de riesgos guiados por el contexto, que permite a los equipos de seguridad pasar de un abordaje reactivo tipo "apaga fuegos" a un abordaje de prevención. Los equipos de ciberseguridad pueden anticipar y bloquear las amenazas antes de que puedan causar daño. La plataforma basada en la nube identifica y evalúa los activos	100%	14%	Se recibió a satisfacción

a lo largo de la superficie de ataque para obtener una vista unificada del riesgo cibernético. Activos: 500. Por un periodo de 12 meses de suscripción.			
Servicio de soporte de una herramienta profesional en seguridad para realizar auditoría del Directorio Activo con alcance de 4 controladores de Dominio. La aplicación debe generar reportes de los cambios en los usuarios, grupos, ordenadores, GPO (Objeto de directiva de grupo) y OU (Consola de administración de Usuarios y Computadoras). Por un periodo de 12 meses de suscripción	100%	14%	Se recibió a satisfacción.
Servicio de soporte en software de auditoría y análisis en tiempo real de 3 File Servers Windows. Creación, modificación y eliminación de archivos desde accesos autorizados / no autorizados, con análisis forenses detallados de la seguridad y los cambios de permisos a los documentos en sus estructuras de archivos / carpetas y recursos compartidos. Por un periodo de 12 meses de suscripción	100%	14%	Se recibió a satisfacción.
Servicio de soporte en la nube de 250 suscripciones de una solución de IA (Cortex) que permita identificar ataques sofisticados, sino que también adapten sus defensas para favorecer la mejora constante y prevenir ciberataques futuros. Al correlacionar de forma nativa los datos de redes de alta capacidad, los EndPoints y la nube, que utilice el aprendizaje automático y el análisis para mejorar todas las fases de las operaciones de seguridad, correlacionando de manera automática con la protección perimetral PA. Por un periodo de 12 meses de suscripción	100%	14%	Se recibió a satisfacción.
Servicio de soporte en la nube del sistema de protección Web Application Firewall (WAF) tienen como función la de proteger sitios Web que tienen transacciones y están expuestos a la Internet, su objetivo es prevenir y anticipar diferentes tipos de ataque a los que pudiésemos ser vulnerables debido a las múltiples amenazas que permanentemente están buscando objetivos para atacar, especialmente entidades financieras y gubernamentales son el objetivo de múltiples actores delincuenciales cibernéticos. La renovación consta de los siguientes componentes tecnológicos del Web Application Firewall: • Renovar 21 licencias para ambientes web. • Renovar ancho de Banda de Enterprise 50Mbps. La solución de seguridad WAF, nos ayuda a mitigar los siguientes riesgos que está expuesta La Gobernación de Antioquia: Acceso a bases de datos y robo o corrupción de datos personales o confidenciales, modificar el código de un sitio web con el fin de cambiar lo que los usuarios ven o visualizar, interceptar datos personales y confidenciales,	100%	14%	Se recibió a satisfacción la solución del WAF

ataques de Denegación de Servicio (DoS) que deshabilitan la disponibilidad de los servicios, ataques de bots maliciosos que se definen como software malicioso. Por un periodo de 12 meses de suscripción			
Suscripción de una solución de gestión de contraseñas, los usuarios de las organizaciones por generar, producir, gestionar y actualizar innumerables credenciales. Esto provoca el olvido de sus claves, la sobrecarga de la mesa de ayuda y la creación de contraseñas vulnerables. Suscripción para 3500 Dominios para la Gobernación de Antioquia. Por un periodo de 12 meses de suscripción	100%	14%	Se recibió a satisfacción.
El PROPONENTE deberá informar en la propuesta, el fabricante y nombre exacto de la solución ofertada para las herramientas de seguridad Informática.	100%	100%	Se recibió a satisfacción.
Servicio de suscripción anual para la ampliación de capacidad de ingesta de datos en la plataforma Cortex XDR Pro de Palo Alto Networks, correspondiente a 100 GB. Este servicio permite la recolección, almacenamiento y análisis avanzado de eventos y telemetría provenientes de diferentes fuentes (endpoints, firewalls, servidores, servicios en la nube y otros dispositivos de seguridad), con el fin de fortalecer las capacidades de detección, correlación y respuesta ante amenazas cibernéticas. Por un periodo de 12 meses de suscripción.	100%	14%	Se recibió a satisfacción las Url's

Método de cálculo del % de ejecución del periodo informado: El contrato tiene una duración de 365 días (equivalente a 1 año). A la fecha actual, se registra una ejecución del 14%, considerando que el contrato inició el 03 de junio de 2026 y al 25 de julio de 2026 acumula 52 días de ejecución.

2.1.2.1 SEGUIMIENTO COMPONENTE SOCIAL DEL CONTRATO/CONVENIO:
N/A.

2.1.2.2 SEGUIMIENTO COMPONENTE AMBIENTAL DEL CONTRATO/CONVENIO:
N/A.

2.1.2.3 SEGUIMIENTO AL COMPONENTE DE SEGURIDAD Y SALUD EN EL TRABAJO DEL CONTRATO/CONVENIO:
N/A.

2.1.3. SEGUIMIENTO ADMINISTRATIVO Y LEGAL DEL CONTRATO/CONVENIO:

OBLIGACIONES/COMPROMISOS PACTADOS DEL COMPONENTE ADMINISTRATIVO Y LEGAL	CUMPLE/NO CUMPLE	MEDIO DE VERIFICACIÓN	OBSERVACIÓN
Presentar mensualmente un informe que dé cuenta del avance físico, administrativo, financiero y ambiental de la ejecución del contrato.	CUMPLE	El contratista ha cumplido con esta obligación	
Suministrar todos los equipos y herramientas, personal e instrumentos de trabajo que requiera para la ejecución adecuada de las labores contratadas dentro del plazo contractualmente establecido.	CUMPLE	Informe de supervisión	
Mantener en el sitio de los trabajos el personal requerido para cumplir el objeto del contrato.	CUMPLE	Informe de supervisión	
Disponer de los medios necesarios para la ejecución del contrato, conforme a lo estipulado en los pliegos.	CUMPLE	Informe de supervisión	
Allegar la Garantía con la cual se amparen los riesgos previstos del proyecto para el inicio del plazo contractual, así como las requeridas de acuerdo al inicio del contrato, las prórrogas, las adiciones, modificaciones o restablecimiento de las mismas de conformidad con el plazo establecido;	CUMPLE	Informe de supervisión	
Presentar de manera oportuna los documentos necesarios para el pago de conformidad con la forma de pago establecida en el presente documento.	CUMPLE	Informe de supervisión	
Previo a la suscripción del Acta de Inicio, y durante el plazo contractual, estará a cargo del contratista el pago mensual de salarios, prestaciones sociales, parafiscales, riesgos laborales, y cumplir con sus obligaciones frente al sistema de seguridad social integral, parafiscales (Cajas de Compensación Familiar, SENA e ICBF). Para el efecto el Contratista debe presentar al supervisor del contrato, dentro del término establecido, la documentación que acredite el cumplimiento del pago de estas obligaciones.	CUMPLE	Informe de supervisión	

Facilitar la labor de la supervisión dando respuesta oportuna a las observaciones y/o requerimientos que se realicen, de la cual se dejará constancia escrita.	CUMPLE	Informe de supervisión	
Informar a la Interventoría/supervisión oportunamente sobre cualquier anomalía, inconveniente o dificultad durante la ejecución de las actividades objeto del contrato, y las posibles soluciones para la resolución de los mismos**.**	CUMPLE	N/A	
Los informes, recolección de información, resultado y demás actividades asociadas a la ejecución del presente contrato, son de uso exclusivo y propiedad al 100% del Departamento de Antioquia, razón por la cual el contratista debe facilitar todos los documentos, estudios, bases de datos, resultados y demás relacionados al objeto del presente contrato o bien para reportes y análisis propios del Departamento o bien para patente de registro a nombre del Departamento, en los formatos solicitados y sin perjuicio de los derechos de autor que para el caso correspondan.	CUMPLE	Informe de supervisión	
Presentar los informes de cumplimiento ambiental con la periodicidad mensual, de seguridad y salud en el trabajo del proyecto.	CUMPLE	Informe de supervisión	
Garantizar la implementación de las medidas necesarias para prevenir la ocurrencia de posibles accidentes no solo para trabajadores sino para la comunidad en general.	CUMPLE	Informe de supervisión	
Cumplir con los requisitos para la prevención de accidentes y enfermedades laborales del personal propio y/o el de los proveedores de acuerdo con lo establecido en el Código Sustantivo del Trabajo y demás normas que rijan la materia, dando aplicación en lo que corresponda al Manual de Seguridad y Salud en el Trabajo dirigido a Contratistas del Departamento de Antioquia.	CUMPLE	Informe de supervisión	

La información entregada durante la ejecución del contrato, goza de confidencialidad. El contratista manifiesta que es jurídicamente capaz de salvaguardar la información recolectada y suministrada, obligándose a: 1: Guardar confidencialidad sobre los mecanismos y sistemas de información que se le brinda. 2. Reconocer y dar manejo adecuado a la información recolectada en desarrollo del objeto contractual; 3. Responsabilizarse por la información suministrada; 4. Suministrar información veraz, completa y correcta, en desarrollo de las diferentes actuaciones.	CUMPLE	Informe de supervisión	
Presentar en debida forma la factura correspondiente a la prestación del bien, obra o servicio. Si el contratista está obligado a facturar electrónicamente, deberá presentar al Departamento la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, de acuerdo con las instrucciones y directrices de la DIAN.	CUMPLE	Informe de supervisión	
Estarán a cargo del Contratista y de acuerdo al régimen tributario los IMPUESTOS, TASAS Y CONTRIBUCIONES, establecidos por las diferentes autoridades nacionales, departamentales o municipales.	CUMPLE	Informe de supervisión	
El Contratista, bajo la gravedad de juramento, manifiesta que ni él ni sus representantes legales, apoderados, revisor fiscal o quien haga sus veces: i). Están incluidos en la lista ONU emitida por el Consejo de Seguridad de las Naciones Unidas o la lista emitida por la oficina de control de activos extranjeros de las Naciones Unidas (OFAC) también conocida como lista Clinton, ni en ninguna otra lista restrictiva emitida por organismos nacionales o internacionales,	CUMPLE	Informe de supervisión	

policiales, judiciales o de investigación con igual fin; ii). Han participado en actividades de lavado de activos o financiación del terrorismo; iii). Declaración bajo la gravedad de juramento declaración de inasistencia alimentaria.			
Asumir el pago de salarios, prestaciones e indemnizaciones de carácter laboral del personal que contrate para la ejecución del contrato, lo mismo que el pago de honorarios, los impuestos, gravámenes, aportes y servicios de cualquier género que establezcan las leyes colombianas y demás erogaciones necesarias para la ejecución del contrato.	CUMPLE	Informe de supervisión	
Los precios de los bienes y servicios referenciados por el contratista en la propuesta de precio se entenderán fijos durante la vigencia del contrato.	CUMPLE	Informe de supervisión	
Suministrar al Departamento y/o al supervisor del contrato toda la información que se requiera con el fin de que estos puedan verificar tanto el cumplimiento de los requisitos y compromisos contractuales como los legales a que haya lugar en razón del contrato.	CUMPLE	Informe de supervisión	

Las obligaciones/compromisos N° 1 establecidos en la CLÁUSULA OCTAVA – FORMA DE PAGO del contrato que no se relacionaron en el cuadro anterior, fueron verificados en su totalidad, en los informes de seguimiento anteriores # 1.

2.2. CUMPLIMIENTO DE LAS OBLIGACIONES, ACTIVIDADES O COMPROMISOS DEL DEPARTAMENTO DE ANTIOQUIA.

OBLIGACIONES/COMPROMISOS PACTADOS	CUMPLE/NO CUMPLE	MEDIO DE VERIFICACIÓN	OBSERVACIÓN
Realizar el pago del contrato según la forma establecida para ello.	CUMPLE	Informe de supervisión	**En proceso**
Poner a disposición del contratista la información necesaria que se requiera para el desarrollo de las actividades a ejecutar.	CUMPLE	N/A	
Asignar un supervisor por parte de la entidad contratante Departamento de Antioquia, para que ejerza las respectivas funciones de seguimiento y control.	CUMPLE	La supervisión ha cumplido con esta obligación	Designación Supervisión

Verificar la efectiva prestación del servicio y el cumplimiento de todos los compromisos adquiridos por parte del Contratista, entre otras.	CUMPLE	Informe de supervisión	
Efectuar por escrito todas las comunicaciones que se refieran a solicitud de servicios, quejas o reclamos al contratista.	CUMPLE	Informe de supervisión	
Velar porque el contratista cumpla con los requisitos normativos de Seguridad y Salud en el Trabajo.	CUMPLE	Informe de supervisión	
Verificar el cumplimiento del pago de salarios / honorarios y demás obligaciones laborales, así como los aportes al Sistema de Seguridad Social Integral, conforme a lo señalado en el Artículo 50 de la Ley 789 de 2002 y normas reglamentarias.	CUMPLE	Informe de supervisión	
Elaborar informes mensuales que dé cuenta del seguimiento del contrato y el cumplimiento del mismo, evidenciándolo según cada necesidad.	CUMPLE	Informe de supervisión	
Mantener al día el SECOP II con el fin de cumplir con la normatividad vigente.	CUMPLE	N/A	SecopII
Informar por escrito, de manera oportuna e inmediata al CONTRATISTA las posibles irregularidades encontradas durante el desarrollo del contrato.	CUMPLE	N/A	
Otras que sean necesarias para coadyuvar a la supervisión del Contrato y para la correcta ejecución contractual.	CUMPLE	Informe de supervisión	

2.3. SEGUIMIENTO FINANCIERO Y CONTABLE DEL CONTRATO / CONVENIO:

RESUMEN DE LA EJECUCIÓN FINANCIERA				
ENTIDAD	**DEPARTAMENTO**	**ASOCIADO(S) si aplica**	**OTROS**	**TOTAL**
1. Recursos iniciales comprometidos	$826.098.980 Incluido IVA	$0	$0	$826.098.980 Incluido IVA
2. Adiciones	$0	$0	$0	$0
3. TOTAL RECURSOS COMPROMETIDOS	$826.098.980 Incluido IVA	$0	$0	$826.098.980 Incluido IVA
4. Anticipos	$0	$0	$0	$0
5. Recursos pagados / desembolsados	$0	$0	$0	$0
6. TOTAL RECURSOS ENTREGADOS	$0	$0	$0	$0
7. Recursos ejecutados	$0	$0	$0	$0
8. Recursos no ejecutados	$0	$0	$0	$0

2.4. INFORMACIÓN COMPLEMENTARIA:

N/A

3. REUNIONES Y/O VISITAS REALIZADAS EN EL PERIODO DE SEGUIMIENTO

FECHA	TIPO DE REUNIÓN Y/O VISITA	CONCLUSIONES/OBSERVACIONES
1/06/2026	Instalación y configuración de la solución de EndPoint Sophos XDR (3400 suscripciones) en la Gobernación de Antioquia	Instalación de la solución XDR
11/06/2026	Instalación y configuración de la solución de EndPoint Sophos XDR (300 suscripciones) en la Fábrica de Licores de Antioquia	Configuración del Sophos Central para gestionar la configuración y supervisión de los dispositivos.

4. CONTROL DE PAGOS O DESEMBOLSOS

N/A

5. VERIFICACIÓN DE PAGOS DE SEGURIDAD SOCIAL Y APORTES DE PARAFISCALES

N/A

6. CONTROL Y MITIGACIÓN DE RIESGOS

De conformidad con lo establecido en la normatividad vigente y el Manual de identificación y cobertura del riesgo expedido por Colombia Compra Eficiente, la Entidad deberá realizar el control y mitigación de los riesgos identificados y clasificados para el proceso de contratación en la matriz de riesgos del estudio y documentos previos, razón por la cual esta supervisión ha realizado las siguientes acciones de control y seguimiento a los riesgos previsibles que se han presentado durante la ejecución y liquidación del presente contrato/convenio.

Así mismo, si durante la ejecución del contrato se presentan riesgos imprevisibles, que por su misma naturaleza no fueron contemplados en la matriz de riesgos, también se deberá diligenciar la tabla con los controles y tratamientos respectivos a que hubiere lugar.

RIESGO	DESCRIPCIÓN DEL RIESGO/ RIESGO	QUIEN TIENE ASIGNADO EL RIESGO	TRATAMIENTO/ MITIGACIÓN	CUANDO Y COMO SE REALIZÓ EL MONITOREO	EVIDENCIA
N/A	N/A	N/A	N/A	N/A	N/A

7. CONTROL Y MITIGACIÓN DE INCUMPLIMIENTOS

N/A.

8. ANOTACIONES ADICIONALES

N/A.

9. ANEXOS

El licenciamiento de las suscripciones de las herramientas de Seguridad Informática, se describen a continuación:

Suscripción de la Solución Antimalware Avanzado Cortex Palo Alto XDR. Generan una suscripción inicial hasta diciembre de 2026.



Cortex XDR - Palo Alto Networks es una plataforma de ciberseguridad basada en la nube que ofrece protección integral contra amenazas avanzadas.

Cortex XDR es la primera aplicación de detección y respuesta del mundo que integra de forma nativa los datos de la red, del endpoint y de la nube para detener los ataques sofisticados.

Distribución del inventario por tipo de servidor y estado de protección reportado en Cortex XDR.

Tipo de activo	Inventario total	Conectados	Desconectado	Sin comunicación
Windows	154	133	2	19
Linux	76	68	0	8
BD	25	21	0	4

Integración Multifuente de Datos. Conecta los datos de endpoints, la nube, la red y los orígenes de identidades y aplica la IA a fin de detectar y priorizar los ciberataques Descubra Cortex XDR para la detección y respuesta. Consolida información de múltiples vectores de ataque en una sola plataforma

Tecnología de Inteligencia Artificial.

- Aplica el machine learning para perfilar el comportamiento y detección de anomalías indicativas de potenciales ataques Palo Alto Cortex XDR para empresas.

- Utiliza análisis de comportamiento para identificar amenazas sofisticadas
- Detecta adversarios camuflados entre usuarios legítimos

Capacidades de Protección:

- Funciona como herramienta de Endpoint Protection, compitiendo con antivirus de nueva generación

- Permite que su equipo de seguridad elimine al instante las amenazas a la red, el endpoint y la nube desde una única consola

- Detecta y detiene ataques dirigidos e internos

Suscripción de Diagnóstico de Brechas de Ciberseguridad Tenable ONE Standard (Diagnóstico de Vulnerabilidades).

Order Fulfillment

Order Date	5/28/2026
Sales Order #	439364
Delivery Date	5/29/2026
Delivery Method	Electronically Downloaded
Customer	50924
PO #	CO167449
Reference Information	Q-1602572
Registered Contact Email	sergio.cadavid@antioquia.gov.co
Start Date	5/29/2026
End Date	5/28/2027

Registered Contact Phone
Sergio Andrés Cadavid Echeverry
Registered Contact Email
sergio.cadavid@antioquia.gov.co

Se vienen realizando actividades continuas de análisis y monitoreo de seguridad informática sobre la plataforma tecnológica de la Entidad, incluyendo infraestructura de servidores, ambientes web y dispositivos tecnológicos, con el propósito de identificar vulnerabilidades, evaluar la exposición al riesgo y definir los respectivos planes de mitigación y fortalecimiento de la postura de ciberseguridad institucional.

Los resultados, diagnósticos y reportes de brechas de seguridad informáticos generados en el marco de estas actividades tienen carácter confidencial, en atención a la criticidad de la información y a las políticas de seguridad de la información de la Entidad.

Durante los meses de junio y julio se realizaron análisis de brechas de seguridad informática en los siguientes portales web institucionales. En dichos análisis se identificaron brechas de nivel Crítico, Alto, Medio y Bajo. Los hallazgos fueron reportados oportunamente a cada uno de los administradores responsables de los ambientes web. Los portales evaluados fueron:

- Portal de Certificados de Scripts
- Portal Web de Sede Electrónica (pasaporte)
- SISECMONITOR
- ESALES
- Aplicación Web de VIVA
- Portal Web Simeva
- Portales Web del Dagran
- Portal Web de la Primera Dama

AD_Audit Plus, Data_Security Plus, Gina (ADSelfService Plus)

1. Objetivo del informe

Presentar el estado actual de implementación, operación y evolución de las herramientas de auditoría y seguridad de la información (AD Audit Plus, DataSecurity Plus y Gina / ADSelfService Plus), con el fin de evaluar su aporte al fortalecimiento de los controles de seguridad, la trazabilidad de eventos, la gestión de accesos y la mejora continua de la postura de ciberseguridad de la entidad.

2. Resumen Ejecutivo

las herramientas de auditoría AD Audit Plus y DataSecurity Plus se encuentran completamente implementadas y operando de manera estable, permitiendo el monitoreo continuo de eventos críticos, la trazabilidad de accesos y la detección de comportamientos anómalos en el Directorio Activo y en los sistemas de archivos institucionales.

Durante el período evaluado, se realizaron actividades de actualización tecnológica, configuración de alertas, optimización de servidores, generación de reportes automáticos y atención de incidentes, lo que ha contribuido a fortalecer los mecanismos de control y vigilancia de la información.

Por su parte, la herramienta Gina / ADSelfService Plus presenta un alto nivel de avance en su implementación, destacándose las actividades de actualización de versión, integración con otras plataformas de identidad, configuración de reportes y ejecución de campañas de sensibilización dirigidas a los usuarios finales. No obstante, se identifica como principal reto la finalización del despliegue masivo del agente y la inscripción total de usuarios, especialmente en contextos de alto ingreso de contratistas.

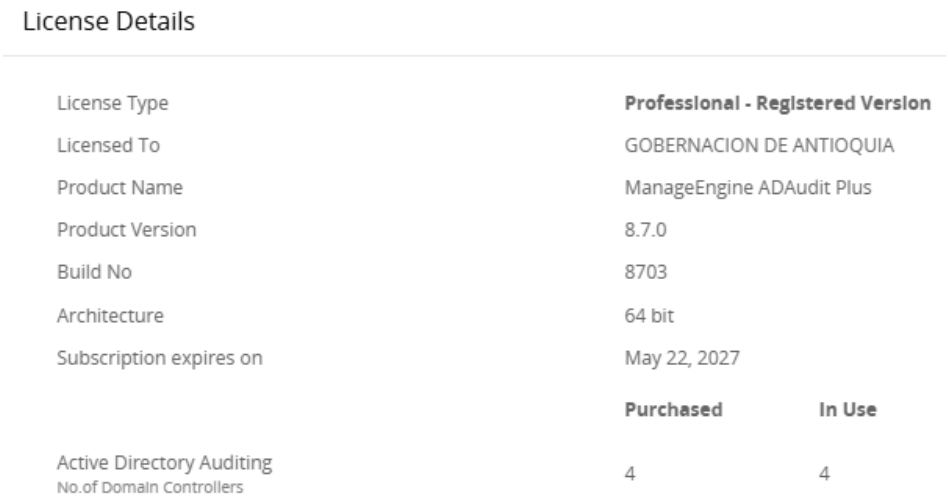
En términos generales, se evidencia un fortalecimiento progresivo de la postura de seguridad de la entidad, soportado en el uso estratégico de estas herramientas, la articulación con la mesa de servicios y la ejecución de iniciativas de cultura y concienciación en seguridad de la información.

ESTADO GENERAL DE LAS HERRAMINETAS

1. AD Audit Plus – Auditoría de Directorio Activo

Solución orientada a la auditoría en tiempo real del Directorio Activo (D.A)

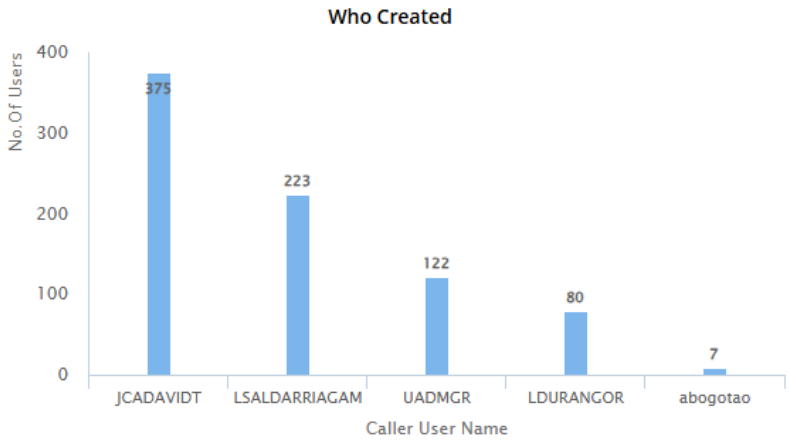
La herramienta se encuentra actualizada en la última versión 8.7.0 y con uso de 4 controladores de dominio, el 5 se omitirá para la renovación del contrato ya que no está en uso. Se extendió el licenciamiento de la herramienta por 1 año más dado los tiempos de contratación.



License Details

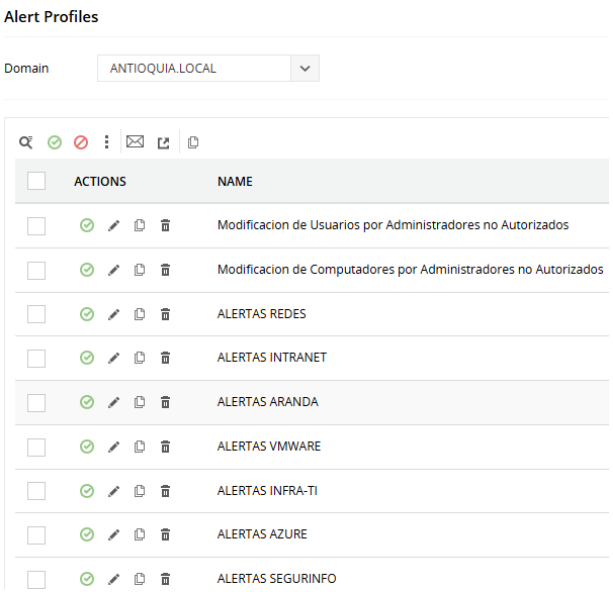
License Type	**Professional - Registered Version**	
Licensed To	GOBERNACION DE ANTIOQUIA	
Product Name	ManageEngine ADAudit Plus	
Product Version	8.7.0	
Build No	8703	
Architecture	64 bit	
Subscription expires on	May 22, 2027	
	Purchased	**In Use**
Active Directory Auditing No.of Domain Controllers	4	4

Durante el primer semestre del año se crearon alrededor 807 usuarios por parte de los administradores de DA y personal autorizado.



Se configuraron varios perfiles de alertas diferentes como:

- Modificación de usuarios o cambios de contraseña en Directorio Activo por parte de personal no Autorizado.
- Inclusión de equipos al dominio.
- Detección de intentos de fuerza bruta.



Actividades recientes

- Extracción y análisis de reportes de usuarios con múltiples sesiones activas y fallos de autenticación.
- Generación y envío de reportes automáticos sobre creación de usuarios, cambios en grupos y GPO.
- Seguimiento técnico mediante sesiones con proveedor (TIConsults) para fortalecimiento de la solución.
- Atención de requerimientos específicos a través de la mesa de servicios (MEGANT).

Estado

- **Nivel de implementación:** 100 %
- **Nivel de funcionamiento:** 100 %

2. DataSecurity Plus – Auditoría de Archivos

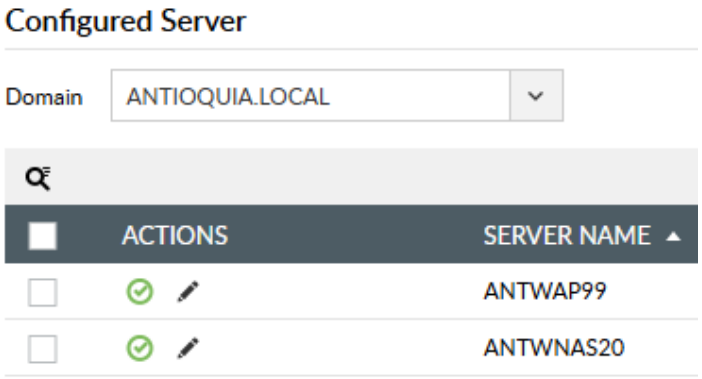
Herramienta especializada en la auditoría de archivos y protección de información sensible, que permite garantizar la integridad, disponibilidad y trazabilidad de los datos institucionales.

La herramienta se encuentra actualizada en la última versión 6.2.0 Se extendió el licenciamiento de la herramienta por 1 año más dado los tiempos de contratación.

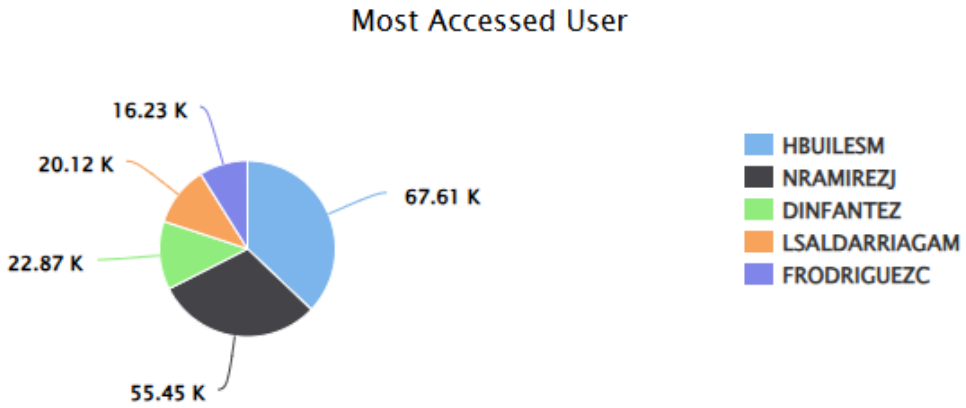
License Details

License Type	Registered - Professional Edition		
License To	GOBERNACION DE ANTIOQUIA		
Product Name	ManageEngine DataSecurity Plus		
Product Version	6.2.0		
Build Number	6290		
Valid Till	22/05/2027		
Support Type	Classic		
	Purchased	**Complimentary**	**In Use**
Number of File Servers - File Server Auditing	3	0	3

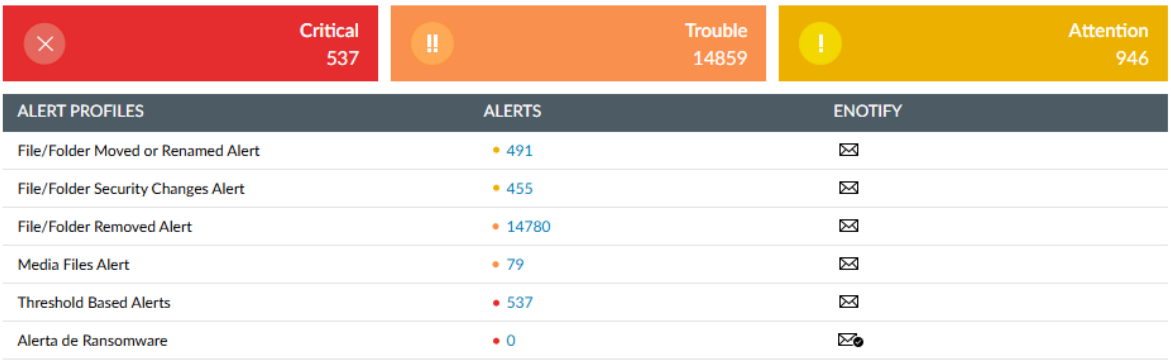
Actualmente se cuenta con las ANTWAP99 y ANTWNAS20 en uso de la herramienta.



Top 5 de los usuarios que más realizan cambios en los fileservers como modificación, edición, eliminación de archivos.



- Generaciones alertas de modificaciones y reportes para análisis forense y cumplimiento.



Actividades recientes

- Actualización de la solución para mejorar desempeño y control de accesos.
- Atención de incidentes asociados a pérdida de archivos con trazabilidad desde la herramienta.
- Reconfiguración del servidor asociado para optimizar la recolección de eventos y visualización de información.
- Ampliación de capacidades de almacenamiento para mejorar la retención de logs.
- Ejecución de actividades de transferencia de conocimiento sobre la herramienta.

Estado

- **Nivel de implementación:** 100 %
- **Nivel de funcionamiento:** 100 %

3. Gina / ADSelfService Plus – Gestión de Contraseñas

Solución de ADSelfService para la gestión de contraseñas de ManageEngine GINA (5000 users y 500 users de la Fábrica de Licores de Antioquia).

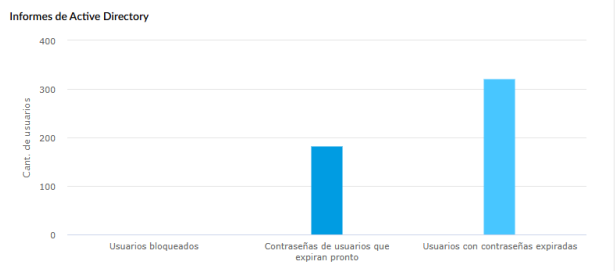
Autenticación Multifactor (MFA) Adaptativa ADSelfService Plus permite aumentar la complejidad de la autenticación multifactor para acceder a los recursos en función de la ubicación del usuario, el dispositivo, la dirección IP y la hora de acceso. Esta funcionalidad de acceso condicional es fundamental para implementar el modelo Zero Trust.

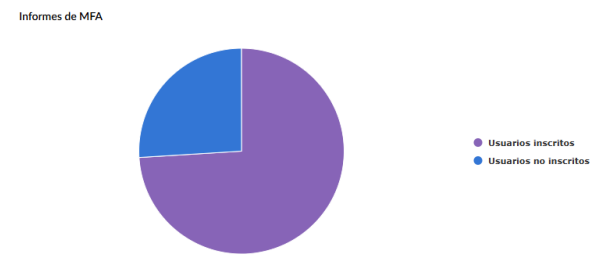
La herramienta se encuentra actualizada en la versión 7.0 y con una extensión de licencia por 1 año más, esta cuenta con 2651 agentes instalados.

Detalles de la licencia

Tipo de licencia	**Professional - Edición registrada**	
Autorizado a	GOBERNACION DE ANTIOQUIA	
Nombre del producto	ADSelfService Plus	
Versión del producto	7.0	
Arquitectura del producto	64 bit	
Compilación nro.	7000	
Período de validez de licencia	May 21, 2027	
Tipo de asistencia	Soporte Clásico	
	Comprado	**Consumido**
Number of Users	3500	2412
Licencias de Endpoint MFA	10	0
Complemento de servicios de tolerancia a fallas y puerta de enlace segura	Si	-

Herramienta de autoservicio orientada a la gestión de contraseñas, que mejora la experiencia del usuario, reduce la carga operativa del equipo de soporte y fortalece la seguridad en la gestión de identidades.

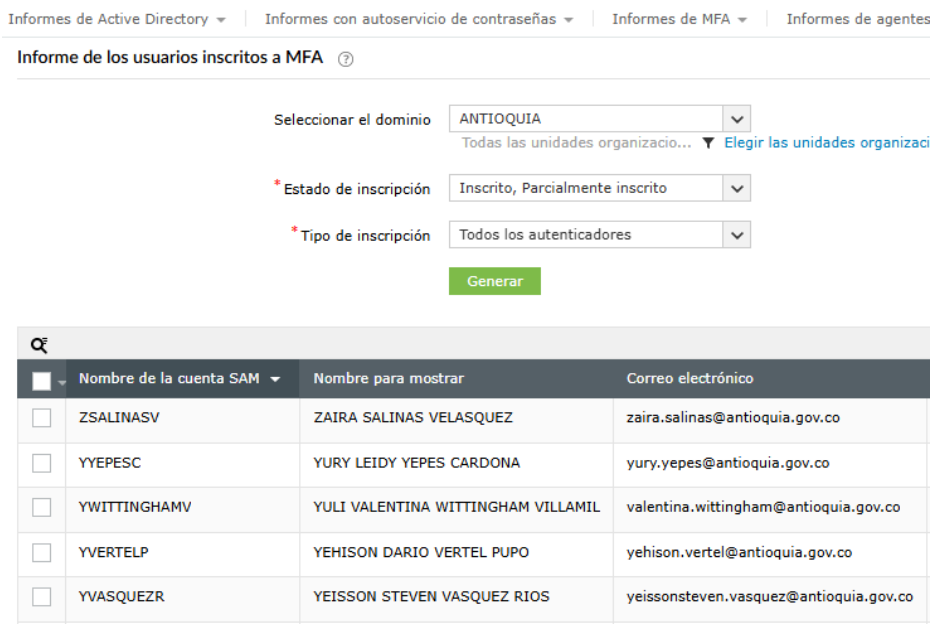




El Dashboard muestra un total de usuarios 2376 usuarios Inscritos y 835 faltantes de los cuales 372 son usuarios de servicio.

Configuración de Reportes

- Usuarios con cuentas próximas a expirar.
- Usuarios con cuentas expiradas.
- Instalación del agente en equipos (seguimiento diario).



Nombre de la cuenta SAM	Nombre para mostrar	Correo electrónico
ZSALINASV	ZAIRA SALINAS VELASQUEZ	zaira.salinas@antioquia.gov.co
YYEPESC	YURY LEIDY YEPES CARDONA	yury.yepes@antioquia.gov.co
YWITTINGHAMV	YULI VALENTINA WITTINGHAM VILLAMIL	valentina.wittingham@antioquia.gov.co
YVERTELP	YEHISON DARIO VERTEL PUPO	yehison.vertel@antioquia.gov.co
YVASQUEZR	YEISSON STEVEN VASQUEZ RIOS	yeissonsteven.vasquez@antioquia.gov.co

Estrategia de adopción y cultura

- Ejecución de campañas institucionales de sensibilización (boletines, infografías, cápsulas y publicaciones).
- Envío de comunicaciones a usuarios no registrados para fomentar la inscripción.
- Apoyo al Plan de Cultura de Seguridad mediante contenidos educativos continuos.





Actividades técnicas

Se da inicio al proceso de integración de ADSelfService (GINA) con Cisco ISE, con el propósito de fortalecer el control de acceso y mejorar los niveles de seguridad de la entidad y minimizar el porcentaje de Usuarios no inscritos en la herramienta

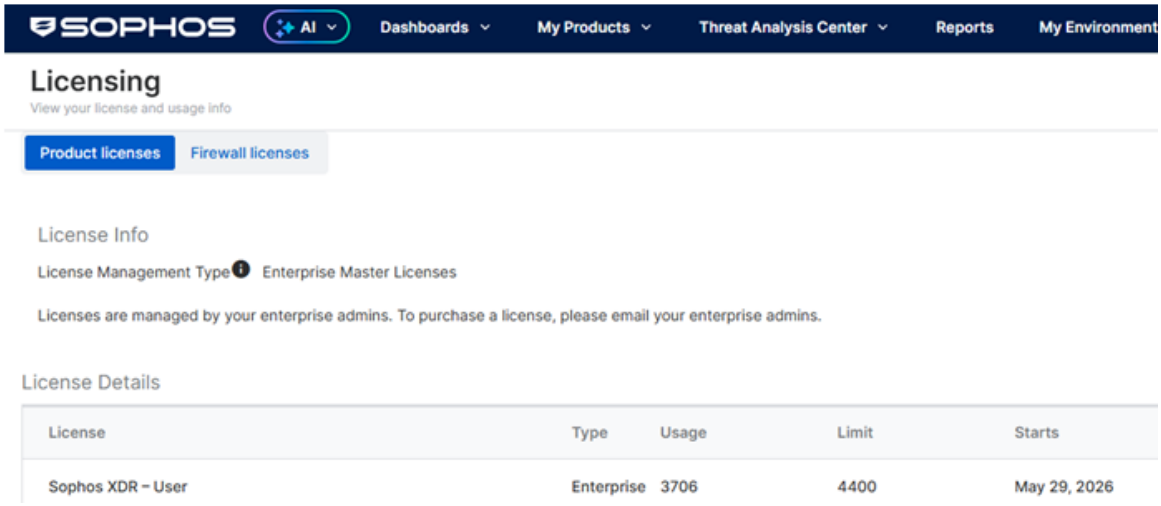
Estado

- **Nivel de implementación:** 95%
- **Nivel de funcionamiento:** 95 %
- **Pendiente:** despliegue de la integración Gina vs ISE.

Conclusiones Generales

- Las herramientas de auditoría (AD Audit Plus y DataSecurity Plus) se encuentran **totalmente implementadas y operando de manera estable**, brindando capacidades de monitoreo, trazabilidad y detección de eventos de seguridad.
- La herramienta Gina presenta un **alto nivel de avance**, con mejoras en adopción mediante campañas de sensibilización, aunque aún requiere completar el despliegue masivo de la postura ISE y la inscripción total de usuarios.
- Se evidencia un fortalecimiento continuo en la **postura de seguridad institucional**, soportado en actividades de actualización tecnológica, monitoreo activo, capacitación y cultura de seguridad.

ESTADO DE LA SOLUCIÓN SOPHOS XDR



1. Objetivo

Presentar el estado actual de la plataforma Sophos XDR implementada en la Gobernación de Antioquia, evaluando la cobertura de protección de endpoints, el nivel de exposición a amenazas, la operación de los controles de seguridad y las actividades de administración registradas en la consola de gestión.

Inventario de endpoints protegidos

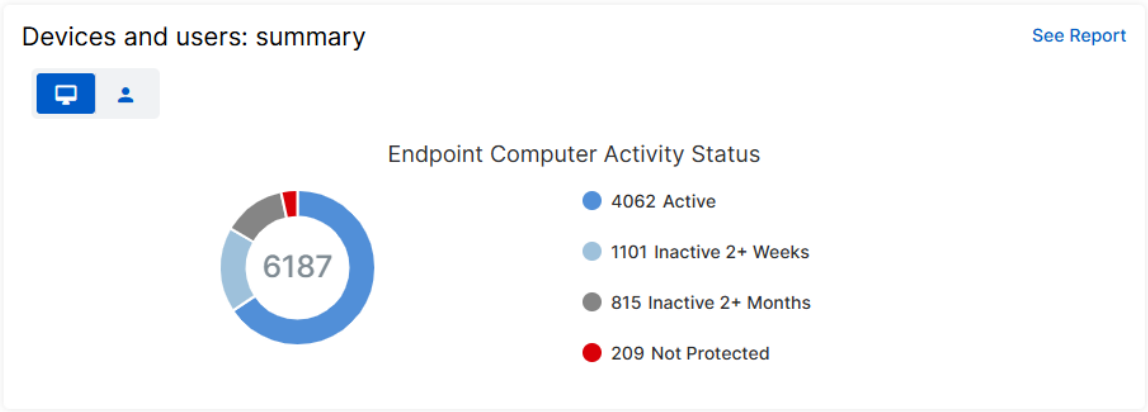
La plataforma registra 6.187 endpoints administrados. De estos, 4.062 se encuentran activos, 1.101 aparecen inactivos por más de dos semanas y 815 permanecen inactivos por más de dos meses. Asimismo, se identifican 209 equipos sin protección activa, los cuales requieren validación y seguimiento.

Equipos sin protección o con agente deshabilitado

Se identifican 209 dispositivos reportados como no protegidos. Se recomienda validar su estado operativo y ejecutar acciones de instalación o recuperación del agente donde corresponda.

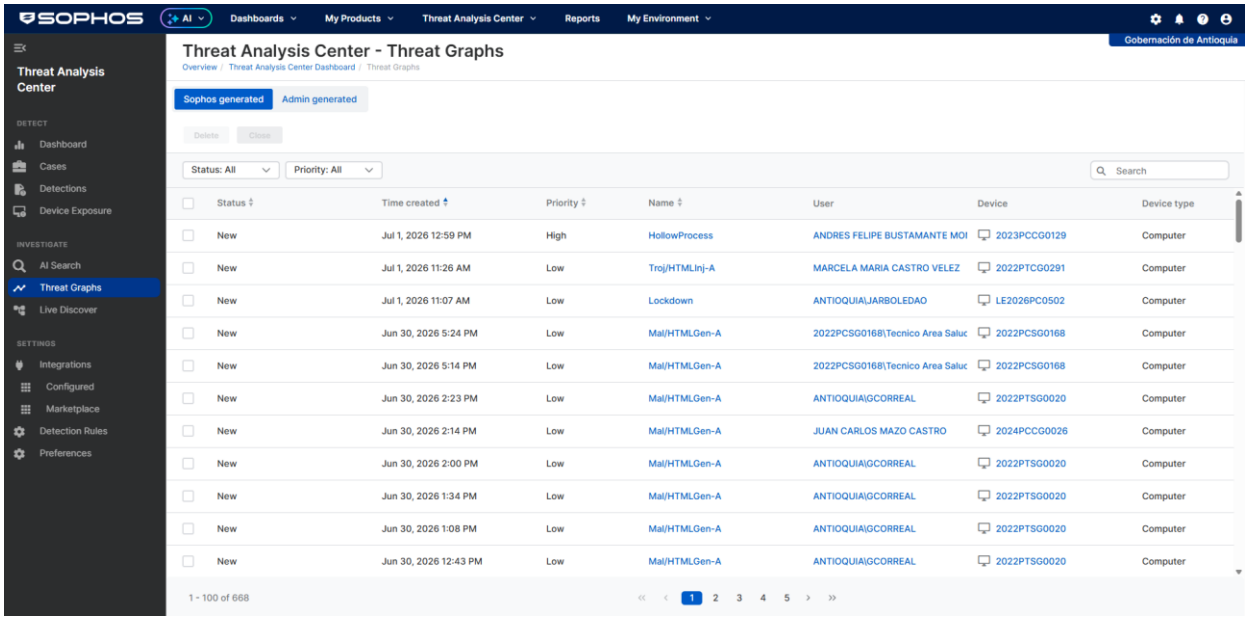
Equipos offline o sin comunicación

La existencia de equipos inactivos durante más de dos semanas y más de dos meses evidencia la necesidad de depurar inventario, verificar retiros de servicio o restablecer la comunicación de los activos aún vigentes.



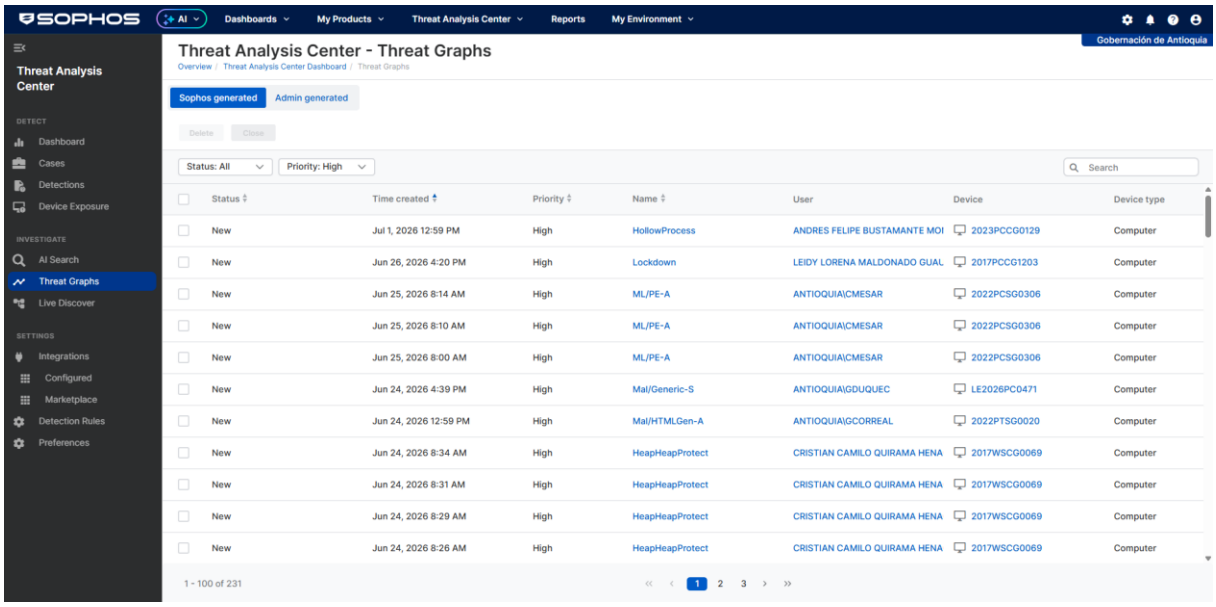
Amenazas detectadas y estado de remediación

La consola evidencia 668 detecciones registradas, incluyendo eventos tales como HollowProcess, Troj/HTMLInj-A, Mal/HTMLGen-A y Lockdown. Las capacidades de Sophos XDR permiten la identificación, investigación y remediación de estos eventos.



Equipos con vulnerabilidades críticas

La solución identifica equipos con exposiciones e incidentes que requieren atención prioritaria. Se recomienda mantener la gestión de vulnerabilidades y la aplicación oportuna de actualizaciones de seguridad.



Incidentes XDR clasificados por severidad

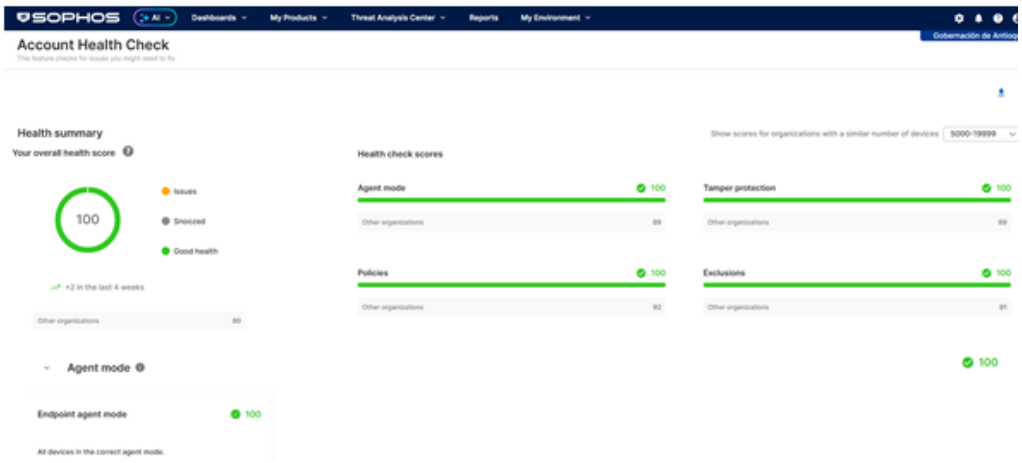
Se observan casos clasificados en niveles Critical, High, Medium y Low, con estados Investigating y Resolved. Esto evidencia el funcionamiento del proceso de monitoreo y respuesta ante incidentes.

Estado de Tamper Protection

La plataforma reporta un puntaje de salud de 100/100 para Tamper Protection. La protección contra manipulación se encuentra habilitada a nivel global y en los dispositivos administrados.

Equipos con protección en tiempo real deshabilitada

No se observan alertas relevantes asociadas a desactivación masiva de protección en tiempo real. Los indicadores de salud de la consola reflejan condiciones operativas adecuadas.

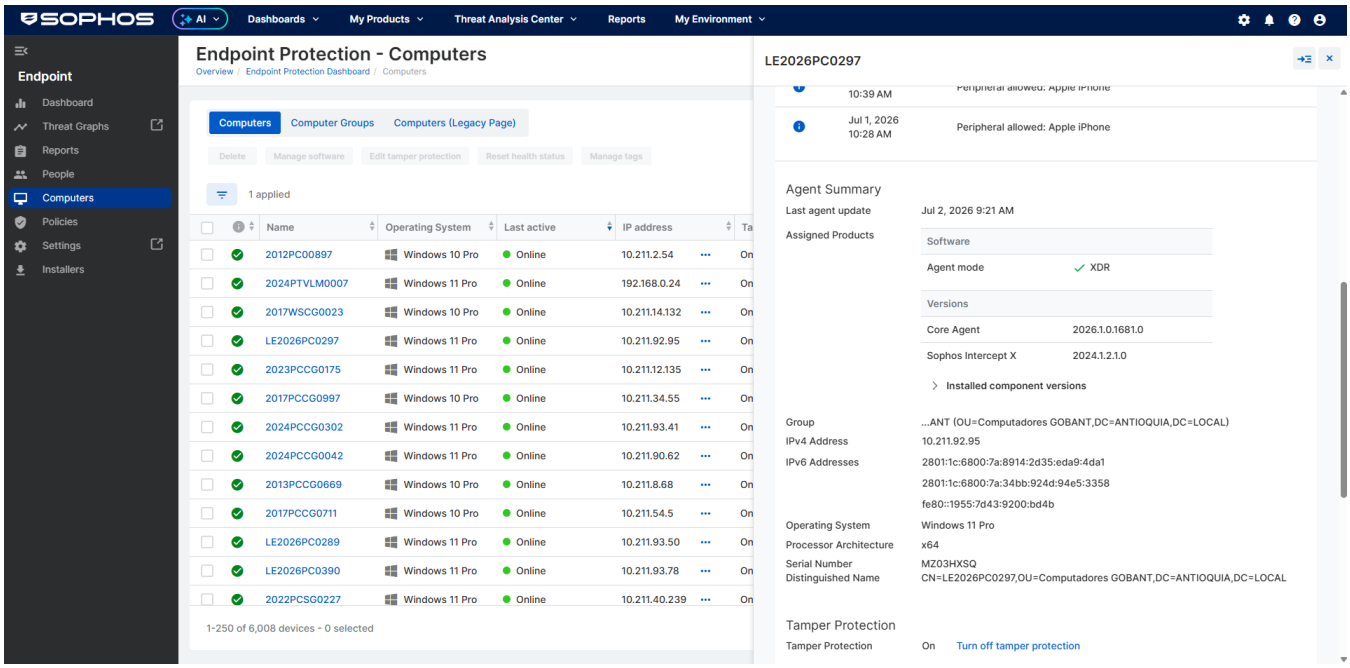


Cambios de políticas y actividad de administradores

La auditoría registra actividades relacionadas con autenticaciones administrativas, gestión de casos XDR, sincronización de Active Directory, administración de equipos y operaciones autorizadas ejecutadas por administradores del entorno.

audit_90_days.xlsx

Estado de actualización del agente y de las firmas



Resumen Ejecutivo

La solución Sophos XDR presenta un estado general favorable, con adecuados niveles de salud operacional, Tamper Protection habilitado y capacidades activas de detección y respuesta. La plataforma proporciona cobertura sobre más de seis mil endpoints administrados y mantiene monitoreo permanente de amenazas e incidentes de seguridad. No obstante, se recomienda realizar seguimiento a los equipos sin protección y a aquellos que presentan largos periodos de inactividad para reducir la superficie de riesgo institucional.

Solución de Web Application Firewall de Incapsula

imperva
a Thales company

Support Certificate

End User: Gobernacion de Antioquia

Part Number	Part Description	Quantity	Support From Date	Support Until Date
FLEX-APPTS2-TS21-BASE-50-1Y-R-SRV1	App Protect Professional, 50Mbps Base Plan, Annual Enhanced Subscription	1	05/08/2026	05/07/2027
A-FLEX-APP1-PRO-20APP-R-SRV1	Add 20 to 49 applications to App Protect Core/Essentials/Professional/ Enterprise, Annual Enhanced Subscription (per app)	20	05/08/2026	05/07/2027

Esta solución es una plataforma integral de seguridad web que combina protección avanzada, facilidad de gestión y capacidades empresariales para proteger aplicaciones web contra las amenazas cibernéticas más sofisticadas.

"**WAF IMPERVA.** El Web Application Firewall (WAF) de Imperva desempeña un papel fundamental en la protección de los sitios web institucionales, mediante la identificación, análisis y mitigación automática de múltiples tipos de ataques cibernéticos dirigidos a las aplicaciones web y servicios publicados en Internet.

Durante el periodo evaluado, el WAF bloqueó y mitigó eventos asociados a ataques de inyección SQL (SQL Injection), Cross-Site Scripting (XSS), intentos de acceso indebido a recursos, ataques de denegación de servicio distribuido (DDoS) y cargas maliciosas de archivos, evitando afectaciones sobre la confidencialidad, integridad y disponibilidad de la información institucional.

La solución analiza continuamente el tráfico HTTP/HTTPS, aplicando reglas avanzadas de seguridad, reputación IP, validación de firmas y mecanismos de comportamiento para detectar actividades sospechosas en tiempo real. Gracias a estas capacidades, el WAF permite reducir la exposición de los portales web frente a vulnerabilidades conocidas y ataques automatizados provenientes de Internet, fortaleciendo así la postura de ciberseguridad de la Entidad.

MES		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
Total Eventos WAF	**SQL Injection**	85	294	49	105	95	215
	Cross Site Scripting	109	78	59	282	120	568
	Ilegal Resource Access	4886	23360	18585	20568	20388	33807
	DDoS	4	9	108	321	12	12
	Remote File Inclusion	0	0	0	2	15	21
	Total	5084	23741	18801	21278	20630	34623

Características Técnicas Principales

- Reglas Gestionadas Proactivas. Los expertos del Imperva Threat Research identifican continuamente nuevas amenazas de vectores de ataque comunes como inyección SQL y XSS, crean y prueban nuevas reglas en producción y las envían proactivamente, con actualizaciones diarias regulares y actualizaciones en tiempo real para amenazas críticas.
- Análisis Inteligente de Incidentes. Attack Analytics de Imperva correlaciona automáticamente miles de alertas de seguridad en narrativas fácilmente digeribles. Mediante aprendizaje automático avanzado, proporciona visibilidad unificada e información contextual sobre cada incidente, incluyendo origen del ataque, métodos y severidad.

Capacidades de Despliegue y Gestión

- Despliegue Rápido y Flexible. Con reglas listas para usar que han sido probadas en entornos de producción, Imperva puede desplegarse en modo de bloqueo desde el inicio. Más del 90% de los clientes se despliegan en modo de bloqueo. Como solución SaaS es fácil de desplegar y gestionar todos sus sitios detrás de una solución y un panel de control.

Funciones Empresariales Avanzadas

- Gestión SSL Empresarial. La gestión completa de conexiones SSL proporciona continuidad del negocio, gobernanza de seguridad, renovación automatizada de certificados y validación de dominio, y observabilidad centralizada.
- Cumplimiento Normativo. Las organizaciones deben cumplir estándares regulatorios estrictos (GDPR, PII, PCI DSS) para proteger datos sensibles. Las características de cumplimiento como logging, auditoría y controles de acceso aseguran la adherencia a estos requisitos.

Ventajas de Ciberseguridad

- Gestión centralizada: Facilita la administración de múltiples subdominios desde un único punto, reduciendo errores de configuración que podrían comprometer la seguridad.
- Costos reducidos: Más económico que adquirir certificados individuales para cada subdominio, permitiendo mejor asignación de recursos de seguridad.
- Automatización: Simplifica la renovación y despliegue automatizado de certificados en infraestructuras complejas.

Para constancia, se firma la presente acta el 25/07/2026



JHON FREDY BORJA CARVAJAL
SUPERVISOR