Bogotá D.C. FECHA: marzo de 2026

Señora Capitán de Fragata
CLAUDIA PATRIACIA PÉREZ RODRIGUEZ
Jefe Departamento Administrativo Y Ordenadora del Gasto
Escuela Superior de Guerra "General Rafael Reyes Prieto"

ASUNTO: INFORME DE SUPERVISIÓN No. 02 CONTRATO DE PRESTACIÓN DE SERVICIOS PROFESIONALES No. 052-MDN-COGFM-ESDEG-2026.

Respetuosamente, me dirijo a la señora Capitán de Fragata Jefe Departamento Administrativo y Ordenador del Gasto de la Escuela Superior de Guerra "General Rafael Reyes Prieto", con el fin de presentar el informe de supervisión del contrato del asunto, correspondiente al pago No. 2 según forma y condiciones de pago y actividades del plan de trabajo descritas en el contrato.

1. DATOS DEL CONTRATO SUPERVISADO

Contratista	YESSID ARAMIS CÁCERES VÁSQUEZ
C.C. No.	72.342.326
Dirección Del Contratista	Carrera 116ª No 15C-70
Correo Electrónico Del Contratista	yessid.caceres@esdeg.edu.co
Objeto	Prestación de Servicios Profesionales en la Categoría H, como ingeniero de sistemas con el fin de gestionar la infraestructura tecnológica y de seguridad para el departamento de tecnologías de la información y comunicaciones de la Escuela Superior de Guerra "General Rafael Reyes Prieto"
Fecha De Suscripción	20/01/2026
Fecha De Inicio	27/01/2026
Plazo de ejecución	El plazo de ejecución del contrato será de once (11) meses en el 2026, contado a partir del cumplimiento de los requisitos de ejecución (expedición del registro presupuestal, aprobación póliza de cumplimiento y afiliación a la ARL).
Valor Inicial (Incluido Iva)	El valor total del contrato asciende a la suma de CINCUENTA Y CINCO MILLONES DE PESOS CON CERO CENTAVOS (59.675.000) M/TCE, sin IVA por RÉGIMEN SIMPLIFICADO
CDP (Certificado De Disponibilidad Presupuestal) No.	El valor total del contrato se subordina a las apropiaciones presupuestales del año 2026 y se pagará con cargo a la Unidad Ejecutora 15-01-02-001, de acuerdo con el certificado de disponibilidad presupuestal No **6926** de fecha 16 de enero de 2026, rubro presupuestal A-02-02-02-008-003 SERVICIOS PROFESIONALES, CIENTIFICOS U TÉCNICOS REC 10, expedido por el responsable del área presupuestal de la ESDEG
Rp (Registro Presupuestal) No.	No. 7026 Y FECHA 20 de enero de 2026

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Recurso presupuestal	R10
Forma Y Condiciones De Pago	El valor total del contrato se cancelará en forma parcial al CONTRATISTA de la siguiente forma (menos los descuentos de ley): ONCE (11) pagos cada uno por valor de CINCO MILLONES CUATROCIENTOS VEINTICINCO MIL PESOS (5.425.000,00) M/CTE sin IVA. De conformidad con la Ley 2024 del 23 de julio de 2020 "por medio de la cual se adoptan normas de pago en plazos justos en el ámbito mercantil y se dictan otras disposiciones en materia de pago y facturación", los pagos se realizarán dentro de los cuarenta y cinco (45) días calendario siguientes a la radicación del Informe de supervisión, actividades y gestión. Documentos Soporte en Adquisiciones Efectuadas a No Obligados a Facturar y certificación de pago a Sistema de Seguridad Social y sus anexos correspondientes al pago de los aportes a Salud o FOSYGA (según aplique). Pensión (según aplique) y riesgos laborales, de acuerdo con el ingreso base de cotización establecido por ley y de conformidad con lo establecido en el artículo 23 de la Ley 1150 de 2007, previa situación de recursos por parte de la Dirección Nacional del Tesoro, cupo de PAC y demás tramites administrativos a que haya lugar. PARÁGRAFO PRIMERO: Para el primer informe de supervisión se deberá allegar: Acta de capacitación relacionada con: Sistema de Gestión de Seguridad y Salud en el Trabajo. Compromiso anticorrupción Acta capacitación código de integridad y servicio Público Colombiano realizada por el supervisor del contrato al contratista. (Esta capacitación está sujeta a la fecha de realización por parte del Departamento de Talento Humano). Acta de capacitación la cual el supervisor del contrato deberá dar a conocer al contratista la Política de Antisoborno implementada por el Ministerio de Defensa Nacional y los distintos canales dispuestos por el Ministerio – ESDEG denunciar cualquier acto de soborno o de corrupción (numeral 8.6.2. prácticas indebidas del Manual de Contratación y convenios emitido por el Ministerio de Defensa). PARÁGRAFO SEGUNDO: Para el ultimo tramite de pago se deberá anexar al informe de supervisión acta de entrega de las obligaciones contractuales, planilla del pago de aportes parafiscales y seguridad social la cual deberá evidenciar el pago total del valor contratado y la verificación por parte del supervisor que el contratista tiene publicado en el SIGEP el formato de publicación proactiva declaración de bienes, rentas y registro de conflicto de interés y la declaración del impuesto de renta y complementario actualizado, deberá aportar borrador acta cierre del expediente contractual digital y Certificado emitido por el Departamento de Seguridad. PARÁGRAFO TERCERO: De conformidad con lo establecido en la Directiva Presidencial No. 09 del 17 de Septiembre de 2020 "Lineamientos para el pago a los proveedores del Estado", en caso que el contratista este obligado a facturar electrónicamente, deberá presentar la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia, con lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020, y las normas que las modifiquen o sustituyan. Así mismo, el contratista deberá haber efectuado el proceso de Validación de la factura electrónica en el Sistema SECOP II, de

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

	conformidad con lo señalado sobre el particular por Colombia Compra Eficiente. PARÁGRAFO CUARTO: Los pagos de que trata esta cláusula se efectuarán mediante consignación en la Cuenta de Ahorros No. 91230625595 Banco Bancolombia, señalada por EL CONTRATISTA o en otro banco o cuenta que el Contratista designe con anterioridad al vencimiento del pago, con sujeción a lo previsto en las disposiciones cambiarias, por medio de aviso escrito con no menos de treinta (30) días calendario de anticipación, previa entrega de la certificación bancaria y activación de la cuenta en el SIIF. PARÁGRAFO QUINTO: EL CONTRATANTE no se responsabilizará por la demora presentada en el pago a EL CONTRATISTA cuando ella fuere ocasionada, por encontrarse incompleta la documentación que sirva de soporte para el trámite o no se ajuste a cualquiera de las condiciones establecidas en el presente contrato o sea allegada extemporáneamente y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza. PARÁGRAFO SEXTO: EL CONTRATANTE no se hará responsable de las sumas que excedan el valor total establecido en el presente contrato o no estén estipuladas dentro del objeto de este.

Modificatorio	**TIPO DE MODIFICATORIO**	**MODIFICATORIO No.**	**FECHA**	**CLAUSULA MODIFICADA No.**	**RESUMEN DEL MODIFICATORIO**
	ADICIÓN-REDUCCIÓN-SUSPENSIÓN-OTROS	NO APLICA	NO APLICA	NO APLICA	NO APLICA

Valor Final (+ modificatorio)	NO APLICA
Plazo De Ejecución Final (+ modificatorio)	NO APLICA
Nombre Del Supervisor	TE. RAMIREZ FLOR ENRIQUE
Número De Resolución De Nombramiento	001 DE 2026
Teléfono De Contacto	3135239402
Correo Electrónico	enrique.ramirez@esdeg.edu.co

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

1.1 CAMBIO DE SUPERVISOR

Nombre Del Supervisor	N/A
Número De Resolución De Nombramiento	N/A
Teléfono De Contacto	N/A
Correo Electrónico	N/A
Motivo del Cambio de supervisor	VACACIONES/PERMISOS/COMISIONES/TRASLADOS/INCAPACIDADES/OTROS (Explique)

2. GARANTÍAS

2.1. Las obligaciones contractuales se respaldan con la siguiente póliza:

Póliza No. 14-46- 101159880 de fecha 20 de enero 2026, expedida por Seguros del Estado y aprobada mediante acta No 052 de fecha 21 DE ENERO DE 2026 que cubre los siguientes amparos, así:

RIESGO ASEGURADO	DESDE	HASTA	VALOR ASEGURADO
Cumplimiento Del Contrato	20/01/2026	10/07/2027	11.935.000

2.2 Modificación de la póliza: **NO APLICA**

3. EJECUCIÓN CONTRACTUAL

No.	OBLIGACIONES ESPECIFICAS
1.	Implementar protocolos de seguridad informática en los equipos de seguridad perimetral de la ESDEG a los usuarios finales quienes se rigen por una política de seguridad de la información.
2.	Administrar la plataforma de servidores de virtualización de la ESDEG con VMWARE.
3.	Garantizar la cobertura y disponibilidad WIFI de la ESDEG.
4.	Administrar los equipos de seguridad perimetral y de Networking (Firewall, Fortinet, Fortiswitch, Fortiap, fortianalyzeer, forti autenticador, fortimanager, Configuración y mantenimiento de Fortinet Firewall. Administrar y optimizar la configuración del firewall para garantizar la seguridad perimetral y el rendimiento de la red. Monitoreo y actualización de políticas de seguridad.
5.	Revisar y actualizar regularmente las políticas de seguridad en el sistema antivirus XDR para adaptarse a las nuevas amenazas.
6.	Participar en los comités de contratación que estén relacionados a su objeto y obligaciones contractuales.
7.	Administrar la infraestructura de respaldo y recuperación incluyendo nodo de backup con Exagrid, Veeam Backup & Replication Console y Storage Advisor Embedded de Hitachi.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

8.	Gestionar la configuración de servidores y seguridad, incluyendo Ubuntu Server, WAF, Active Directory.
9.	Administrar las licencias y usuarios de Microsoft Office de la Comunidad Académica que integra la ESDEG.
10.	Cumplir con las demás actividades requeridas por el supervisor del contrato y que sean acordes al objeto a contratar.
11.	Guardar y mantener la debida reserva sobre algún tipo de información, estructura o composición organizacional de la guarnición militar que por efectos de la ejecución del presente contrato llegue a conocer de acuerdo con lo establecido en la Directiva de seguridad de la información.
12.	Asistir, a las reuniones virtuales y/o presenciales que sean citados por el supervisor del contrato.
13.	Hacer acta de entrega física de toda la documentación manejada y archivos digitales, informar sobre el estado actual de las obligaciones específicas objetos del contrato.
14.	Cumplir con la normatividad interna de ESDEG en especial con el manual de convivencia.
15.	Las demas obligaciones contenidas en el artículo 5 de la ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual.
16.	Cumplir con el objeto del contrato con plena autonomía técnica y administrativa bajo su propia responsabilidad. Por lo tanto, no existe, ni existirá ningún tipo de subordinación ni vinculo laboral alguno del CONTRATISTA con el MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - ESCUELA SUPERIOR DE GUERRA DEPARTAMENTO ADMINISTRATIVO.

PLAN DE TRABAJO

No	ACTIVIDADES DESARROLLADAS	ENTREGABLE
1.	Implementar y verificar que esté funcionando de manera correcta el Exagrid, Hitachi y Vee Backup.	Anexo Informe
2.	Validar el despliegue de los volúmenes de los Nodos de copias de seguridad.	Anexo Informe
3.	Presentar un volumen de mínimo 4 TB a la plataforma VMWare una vez configurado los Nodos.	Anexo Informe
4.		Anexo Informe
5.	Programar la realización de las copias de seguridad y respaldo de los servidores. Revisar el estado actual de la plataforma de servidores de virtualización de la ESDEG con PROXMOX Y VMWARE y realizar ajustes necesarios para garantizar su óptimo rendimiento y disponibilidad.	Anexo Informe
6.	Verificar regularmente la ejecución exitosa de las copias de seguridad de los servidores.	Anexo Informe
7.	Monitorear continuamente la capacidad de almacenamiento utilizada para prever y mitigar problemas de espacio. Recomendar proactivamente la reorganización o eliminación de copias de seguridad antiguas, garantizando así la disponibilidad y la protección de datos esenciales cuando el almacenamiento alcanza su capacidad máxima si se llega a presentar.	Anexo Informe

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

4. CUMPLIMIENTO DE OBLIGACIONES AL SISTEMA DE SEGURIDAD Y SOCIAL Y PARAFISCALES

El contratista manifiesta bajo la gravedad de juramento que se encuentra dando estricto cumplimiento a la obligación consagrada en el artículo 50 de la ley 789 de 2002, el parágrafo 2 del artículo 1 de la ley 828 de 2003, en concordancia con el artículo 23 de la ley 1150 de 2007, Decreto 0723 de 2013, Decreto 2353 de 2015, Decreto 780 de 2016, Decreto 1273 de 2018 y demás normas reglamentarias y complementarias vigentes durante la ejecución del presente contrato, se verificó y certifico que el Contratista cumple con las obligaciones frente al sistema de seguridad social integral, parafiscales (cajas de compensación familiar, Sena e Instituto Colombiano de Bienestar Familiar- cuando aplique) y se anexa para tal fin, las planillas soportes del cumplimiento por parte del contratista.

FECHA DE PAGO	NÚMERO DE PLANILLA	HONORARIOS MENSUALES	INGRESO BASE COTIZACIÓN (40%)	SISTEMA DE SALUD (12,5%)	SISTEMA DE PENSIÓN (16%)	ARL
NA	NA	NA	NA	NA	NA	SURA
16/03/2026	84449480	9.929.000	3.971.600	496.500	635.500	20.800

Nota: Deben relacionar todas las planillas pagas del presente contrato.

5. CRITERIO DE EVALUACIÓN MENSUAL

Yo, TE. RAMIREZ FLOR ENRIQUE supervisor del contrato, verifiqué las actividades realizadas por EL CONTRATISTA y certifico que están acorde a las obligaciones específicas y al plan de trabajo pactadas en el **CONTRATO DE PRESTACIÓN DE SERVICIOS PROFESIONALES NO. 052-MDN-COGFM-ESDEG-2026**, por lo tanto, se recibe a satisfacción el cumplimiento de las obligaciones correspondientes al pago No. 02 según forma y condiciones de pago y actividades del plan de trabajo descritas en el contrato.

CUMPLIMIENTO DE EJECUCIÓN PRESUPUESTAL
18,18 %

6. BALANCE

BALANCE	
DESCRIPCIÓN	**VALORES**
VALOR INCIAL CONTRATO	$ 59. 675.000
VALOR ADICIÓN	N/A
VALOR REDUCCIÓN	N/A
VALOR PAGADO	$ 5.425.000
PAGO PARA ESTE INFORME	$ 5.425.000
PENDIENTE POR PAGAR	$ 48.825.000

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

7. ANEXOS

ANEXO	HOJAS
Planilla 84449480	1
Certificado de aplicación Retención en la Fuente (Decreto No. 2231 del 22 de diciembre del 2023)	1
Informe actividades CCOCI	19
Informe Actividades	4

Atentamente,

CONTRATISTA:

Nombre: YESSID ARAMIS CÁCERES VÁSQUEZ.
Tipo y No. Documento C.C. 72.342.326

SUPERVISOR:

Grado y Nombre TE. RAMIREZ FLOR ENRIQUE
Tipo y No. Documento C.C. 1061743430
Cargo Oficial Gestión Gobierno Digital

Archivado en: 15.103.12.5 Contrato de prestación de servicios 2026.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Bogotá D.C. FECHA: marzo de 2026

Señora Teniente
ENRIQUE RAMIREZ FLOR
Supervisor contrato 052
Escuela Superior de Guerra "General Rafael Reyes Prieto"

ASUNTO: Informe acciones tomadas de acuerdo al Radicado No. 0126001351402 para los Caso: ID: ##378349## - Caso ID: ##378359## - ID :##378370## - ID: ##378368## - ID:## 378386## y ID: ##378383##

Por medio del presente me permito presentar el **informe consolidado de las acciones adelantadas en atención al Radicado No. 0126001351402**, correspondiente a los casos **ID: ##378349##, ##378359##, ##378370##, ##378368##, ##378386## y ##378383##**, con el propósito de unificar en un solo documento los análisis técnicos y las medidas implementadas frente a los eventos de seguridad reportados por las plataformas de monitoreo institucional CCOCI.

En el presente informe se describen las actividades de verificación realizadas sobre los registros del **FortiGate 600E**, el análisis de los eventos correlacionados en el **SIEM** y **FortiAnalyzer 300G**, así como las acciones de contención, bloqueo y validación técnica ejecutadas sobre las direcciones IP y servicios involucrados. Los eventos analizados corresponden principalmente a **intentos fallidos de autenticación SSL-VPN compatibles con patrones de fuerza bruta, intentos de conexión desde infraestructuras con reputación maliciosa y actividades de escaneo provenientes de múltiples direcciones IP externas**, evaluándose en cada caso el impacto potencial y las medidas aplicadas para preservar la **seguridad, integridad y disponibilidad de la infraestructura tecnológica institucional.**

A continuación, se relacionan las acciones efectuadas:

1. **Caso ID: ##378349## y Caso ID: ##378359## – Verificación de comunicaciones hacia direcciones IP externas**

En atención a los eventos reportados en los Casos ID: ##378349## y ##378359##, se llevó a cabo la verificación técnica de las conexiones identificadas desde equipos internos de la ESDEG hacia las direcciones IP externas 159.89.230.187 y 190.71.130.238. Las

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

actividades desarrolladas estuvieron orientadas a realizar la validación inmediata de los equipos involucrados, el análisis histórico de los registros disponibles en el Firewall FortiGate 600E y el FortiAnalyzer 300G para determinar el periodo de ocurrencia de dichas comunicaciones, así como la evaluación de posibles medidas de contención a nivel perimetral, con el fin de establecer el comportamiento del tráfico observado y garantizar la seguridad, integridad y estabilidad de la infraestructura tecnológica institucional.

1.1. Verificación inmediata de equipos relacionados

Dando seguimiento al análisis de tráfico saliente reportado bajo el Caso ID: ##378349##, se realizó la revisión técnica detallada de los registros del Firewall **FortiGate 600E** y del **FortiAnalyzer 300G** correspondiente a la comunicación hacia la **IP 159.89.230.187.**

En el análisis efectuado se identificó:

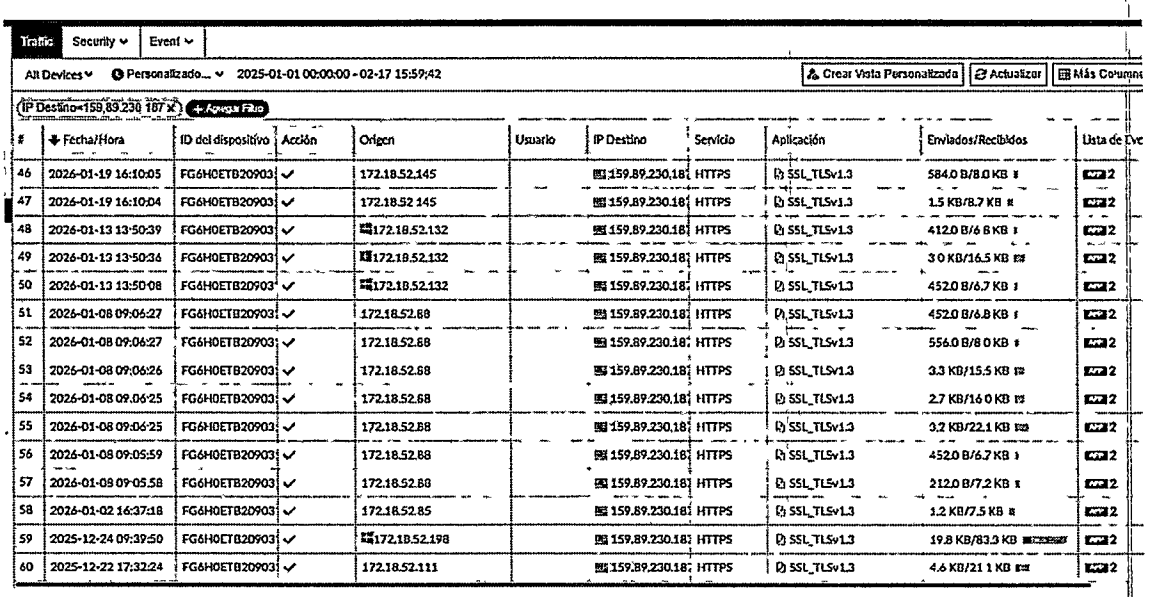
- 60 eventos totales
- 21 equipos internos diferentes
- Tráfico bajo protocolo HTTPS (TLS 1.3)
- Volumen bajo (aproximadamente 100 KB máximo por equipo)
- Duración promedio de sesión cercana a 30 segundos
- Sin patrón repetitivo periódico
- Sin equipo dominante
- Sin comportamiento persistente

No se evidencian:

- Conexiones sostenidas en el tiempo
- Incremento progresivo de actividad
- Exfiltración de información
- Comunicación periódica tipo comando y control (C2)

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

- Actividad anómala concentrada en un único host



Traffic | Security | Event

All Devices | Personalizado... | 2025-01-01 00:00:00 - 02-17 15:59:42 | Crear Vista Personalizada | Actualizar | Más Columnas

IP Destino=159.89.230.187 | + Agregar Filtro

#	Fecha/Hora	ID del dispositivo	Acción	Origen	Usuario	IP Destino	Servicio	Aplicación	Enviados/Recibidos	Lista de Eve
46	2026-01-19 16:10:05	FG6H0ETB20903	✓	172.18.52.145		159.89.230.187	HTTPS	SSL_TLSv1.3	584.0 B/8.0 KB	2
47	2026-01-19 16:10:04	FG6H0ETB20903	✓	172.18.52.145		159.89.230.187	HTTPS	SSL_TLSv1.3	1.5 KB/8.7 KB	2
48	2026-01-13 13:50:39	FG6H0ETB20903	✓	172.18.52.132		159.89.230.187	HTTPS	SSL_TLSv1.3	412.0 B/6.6 KB	2
49	2026-01-13 13:50:36	FG6H0ETB20903	✓	172.18.52.132		159.89.230.187	HTTPS	SSL_TLSv1.3	3.0 KB/16.5 KB	2
50	2026-01-13 13:50:08	FG6H0ETB20903	✓	172.18.52.132		159.89.230.187	HTTPS	SSL_TLSv1.3	452.0 B/6.7 KB	2
51	2026-01-08 09:06:27	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	452.0 B/6.8 KB	2
52	2026-01-08 09:06:27	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	556.0 B/8.0 KB	2
53	2026-01-08 09:06:26	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	3.3 KB/15.5 KB	2
54	2026-01-08 09:06:25	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	2.7 KB/16.0 KB	2
55	2026-01-08 09:06:25	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	3.2 KB/22.1 KB	2
56	2026-01-08 09:05:59	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	452.0 B/6.7 KB	2
57	2026-01-08 09:05:58	FG6H0ETB20903	✓	172.18.52.88		159.89.230.187	HTTPS	SSL_TLSv1.3	212.0 B/7.2 KB	2
58	2026-01-02 16:37:18	FG6H0ETB20903	✓	172.18.52.85		159.89.230.187	HTTPS	SSL_TLSv1.3	1.2 KB/7.5 KB	2
59	2025-12-24 09:39:50	FG6H0ETB20903	✓	172.18.52.198		159.89.230.187	HTTPS	SSL_TLSv1.3	19.8 KB/83.3 KB	2
60	2025-12-22 17:32:24	FG6H0ETB20903	✓	172.18.52.111		159.89.230.187	HTTPS	SSL_TLSv1.3	4.6 KB/21.1 KB	2

Imagen 1 – Listado de equipos que generaron tráfico registrado en los log

Se identificaron las direcciones MAC de los equipos de acuerdo con el análisis realizado en los registros del FortiAnalyzer-300G. Con base en dicha revisión, se procedió a ejecutar las acciones correspondientes a través del equipo de soporte técnico, verificando en cada uno de los equipos identificados la posible existencia de conexión activa con la IP 159.89.230.187.

Teniendo en cuenta que previamente se realizó el bloqueo perimetral mediante el FortiGate 600E, la validación se efectuó utilizando el comando **netstat -ano | findstr 159.89.230.187**, cuyo resultado fue nulo o vacío, evidenciando que no existe conectividad activa con la dirección IP mencionada.

Esta situación fue confirmada en los equipos JURID-0005, DGRAP-0004, elkin.velandia, AUTEV-0001, SESCO-0008, SEADP-0006, DETAH-0009, CREES-0002, SEADP-0001, CENTROC2, VACAD-53-37, AYUTI-0022, SESET-0002, VINVE-0015, CENTROC-53-129, así como en los equipos DETIC-0030, COMES-0005 y CREESW-0007, donde se realizó la validación correspondiente.

En todos los casos, el resultado del comando ejecutado fue nulo, evidenciando que no existen conexiones activas hacia la IP 159.89.230.187, dejando constancia de que la acción

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

correctiva fue ejecutada satisfactoriamente. Se aporta la evidencia técnica correspondiente para cada caso verificado.

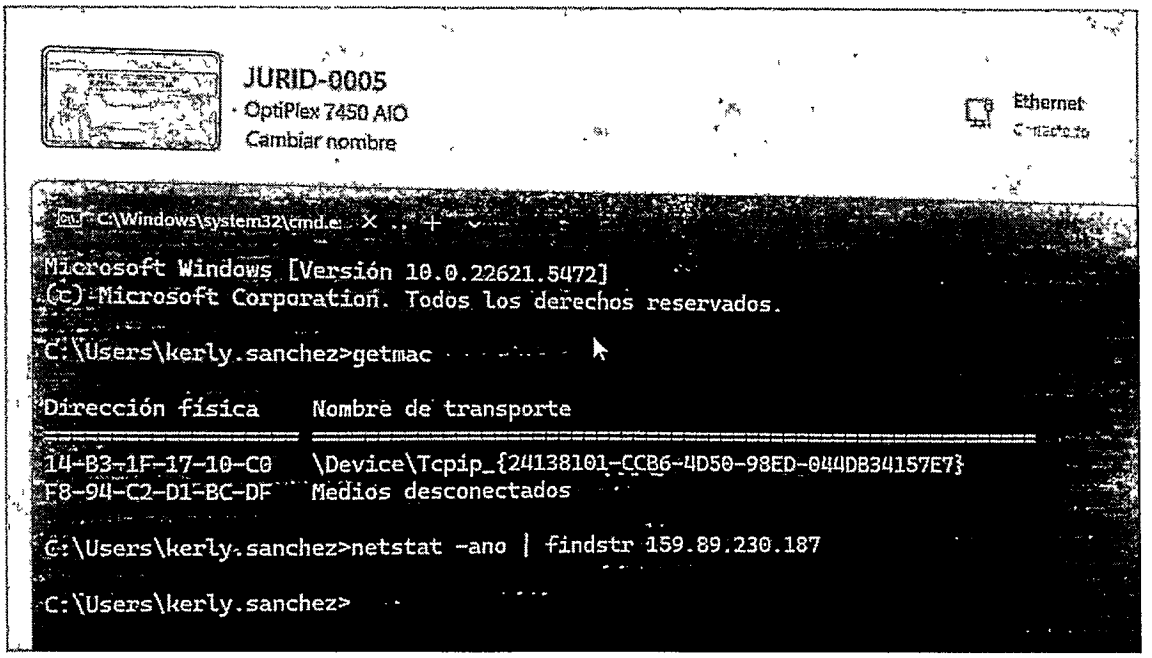


Imagen 1.2 – Verificación conexión equipo JURID-0005 - 14:b3:1f:17:10:c0

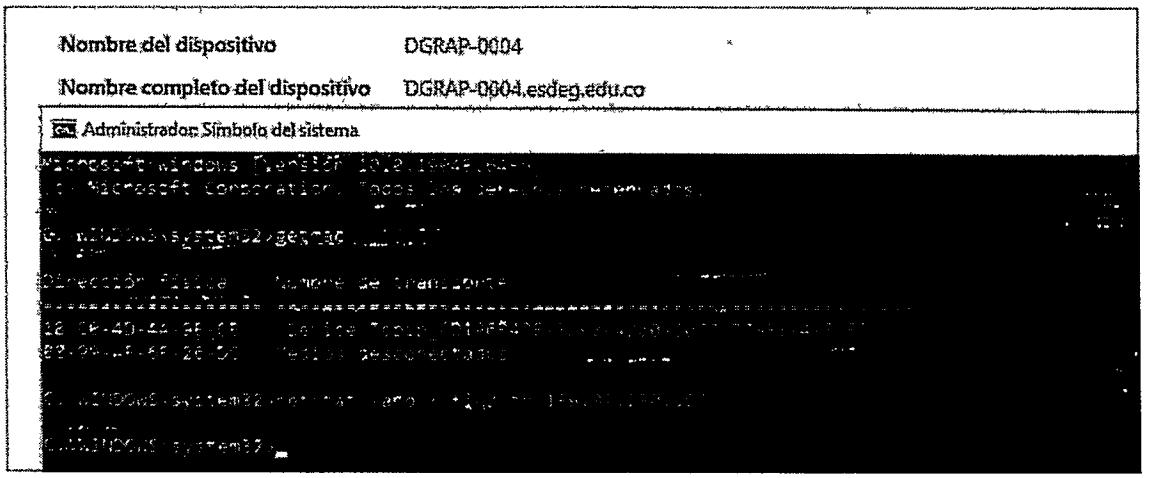


Imagen 1.3 – Verificación conexión equipo DGRAP-0004 - 18:c0:4d:4a:9e:ce

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

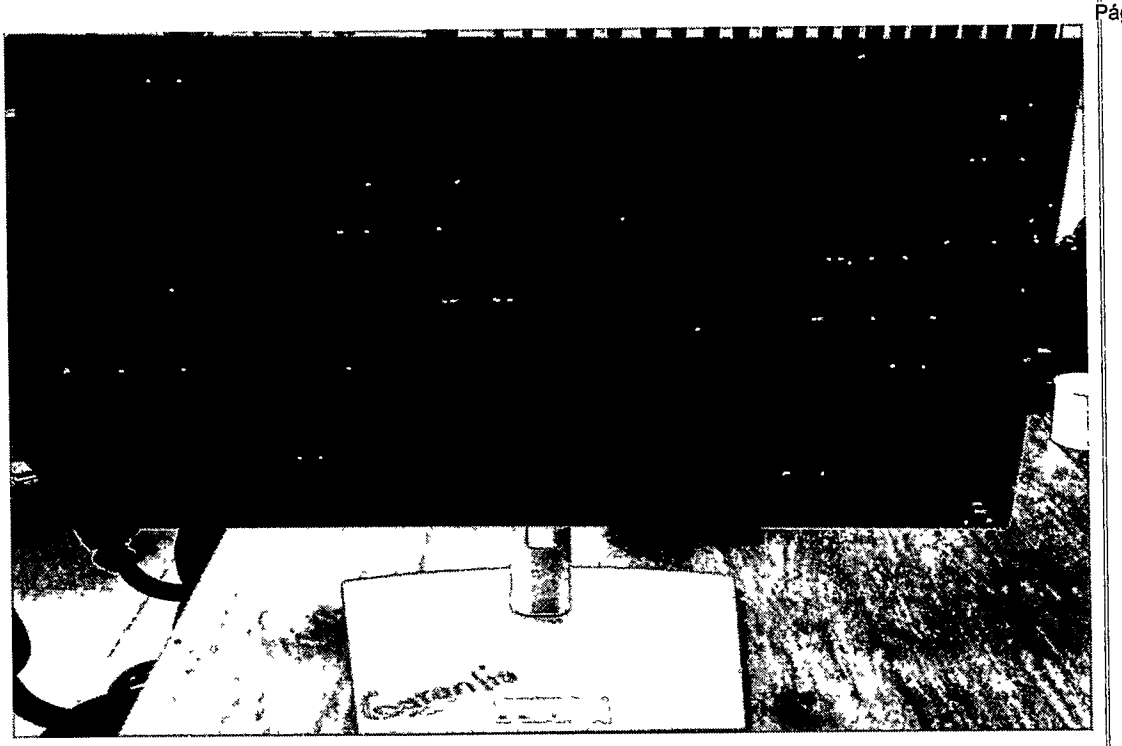


Imagen 1.4 – No se puede validar debido a que esta para garantía por Board

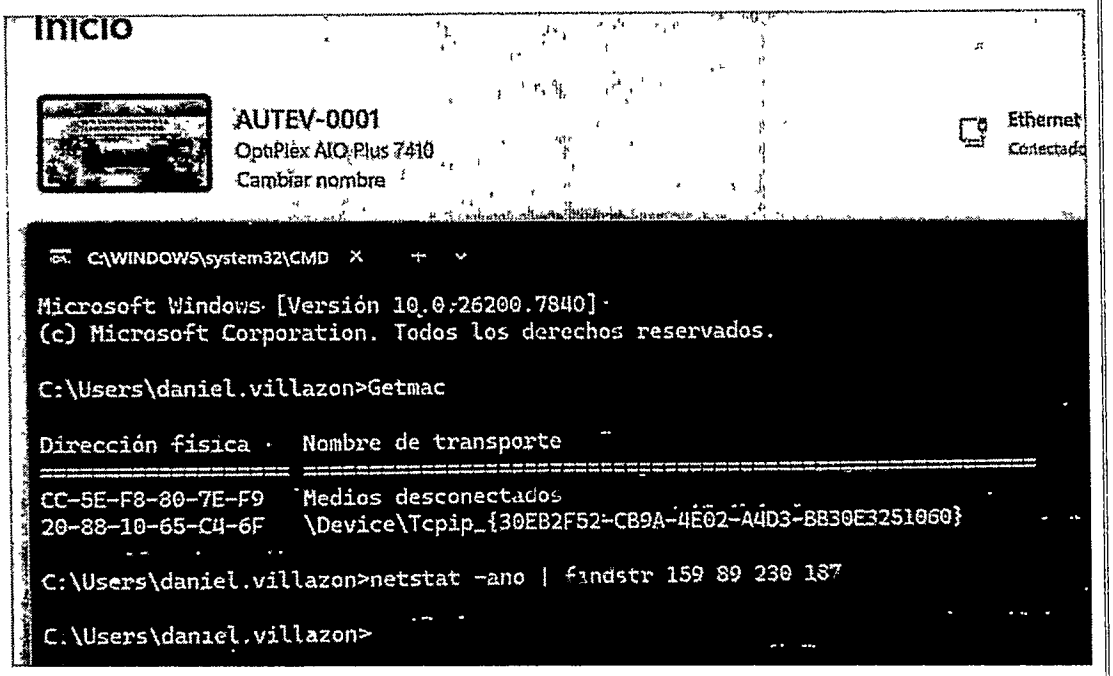


Imagen 1.5 – Verificación conexión equipo AUTEV-0001 - 20:88:10:65:c4:6f

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

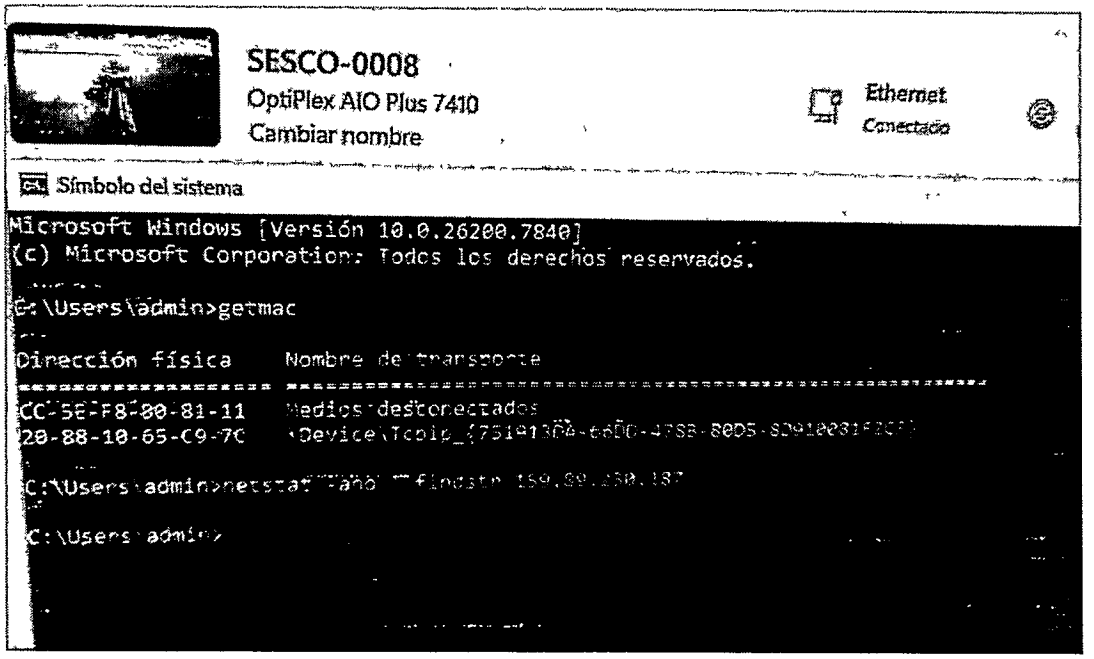


Imagen 1.6 – Verificación conexión equipo SESCO-0008 - 20:88:10:65:c9:7c

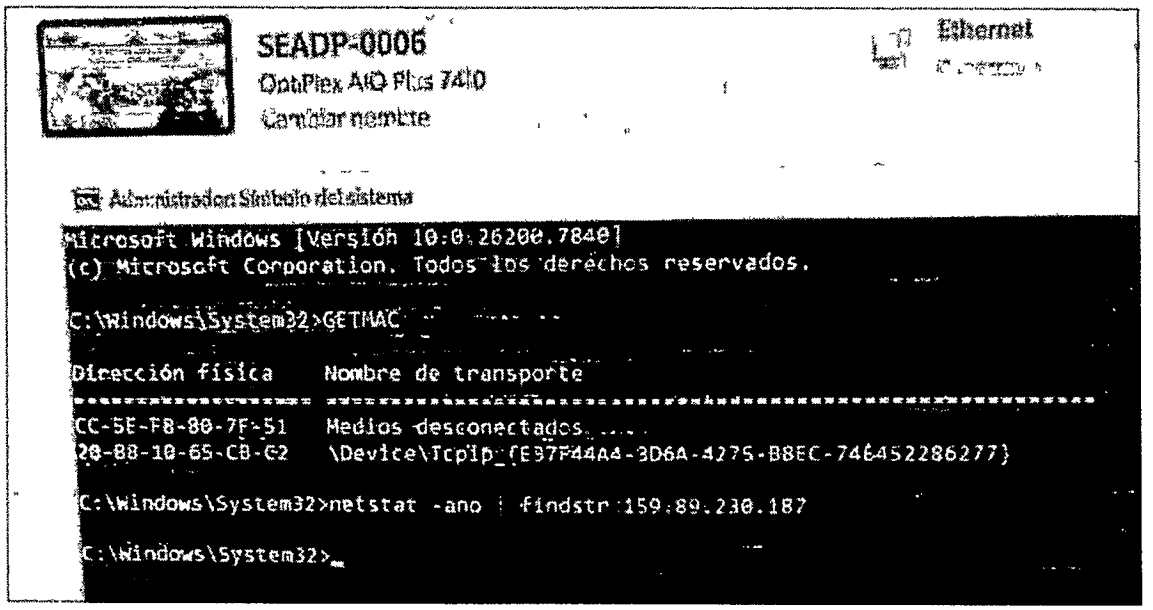


Imagen 1.7 – Verificación conexión equipo SEADP-0006 - 20:88:10:65:cb:c2

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

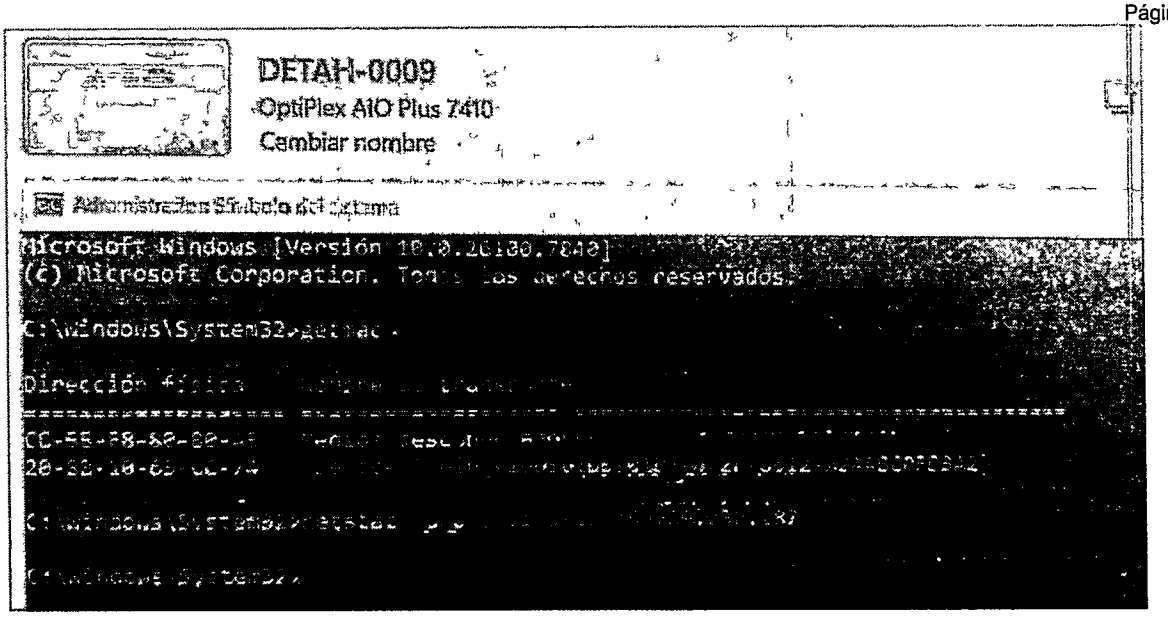


Imagen 1.8 – Verificación conexión equipo DETAH-0009 - 20:88:10:65:cc:74

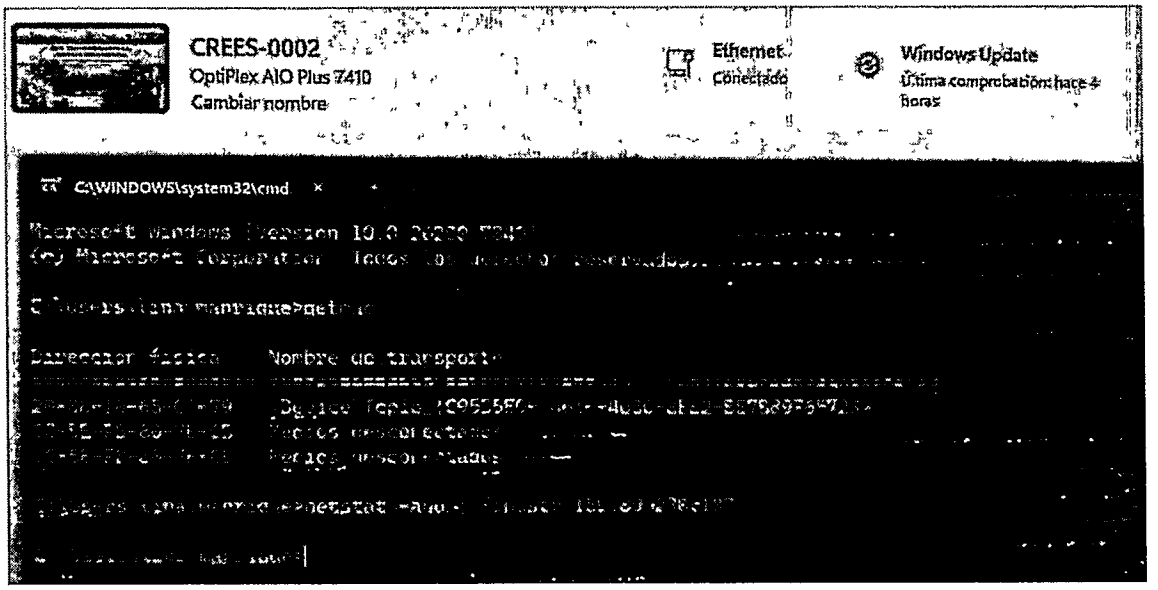


Imagen 1.9 – Verificación conexión equipo CREES-0002 - 20:88:10:65:cc:79

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

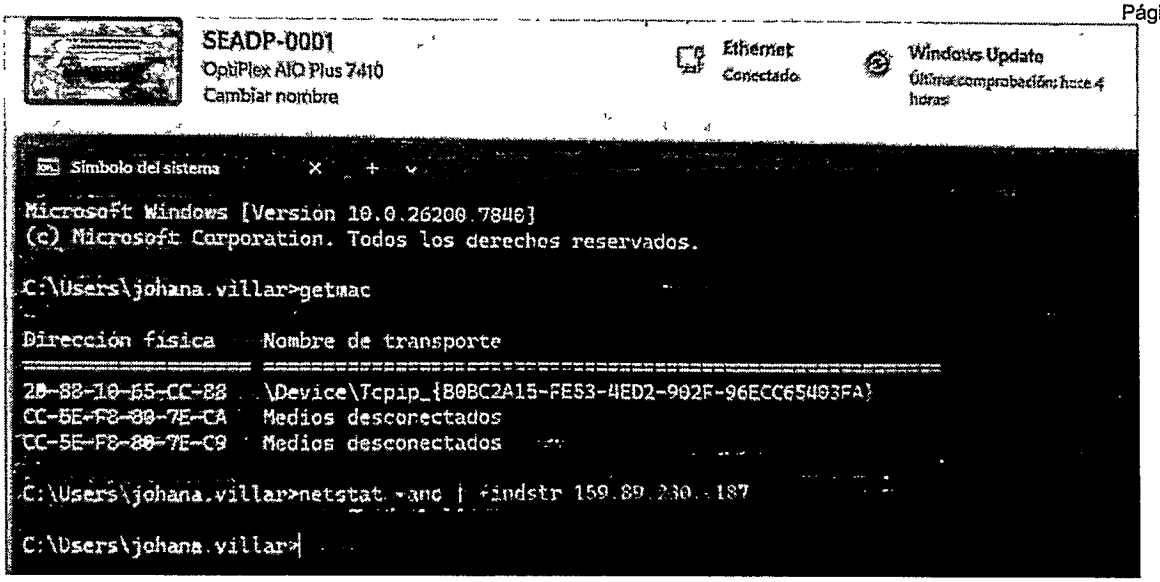


Imagen 1.10 – Verificación conexión equipo SEADP-0001 - 20:88:10:65:cc:88

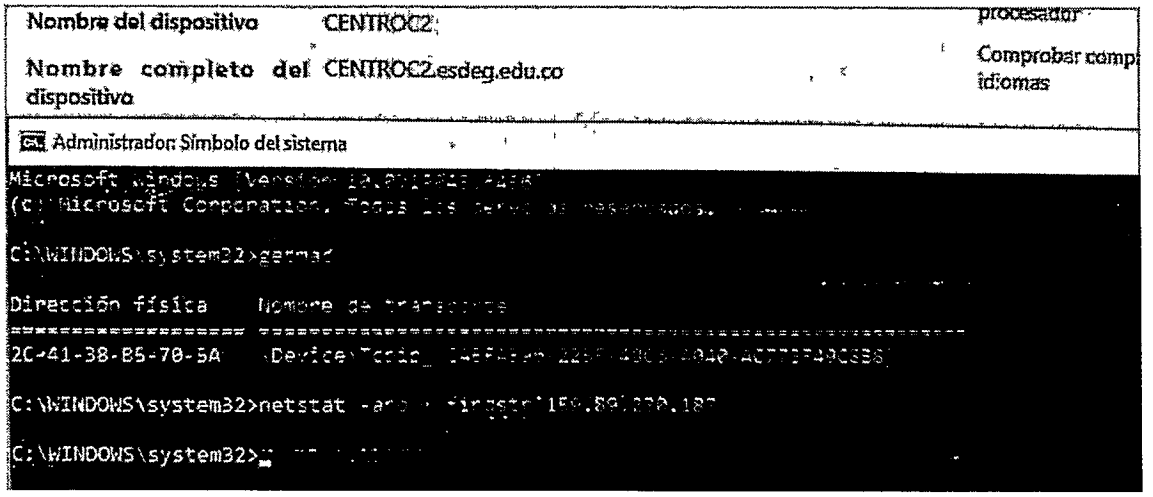


Imagen 1.11 – Verificación conexión equipo CENTROC2 - 2c:41:38:b5:70:5a

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

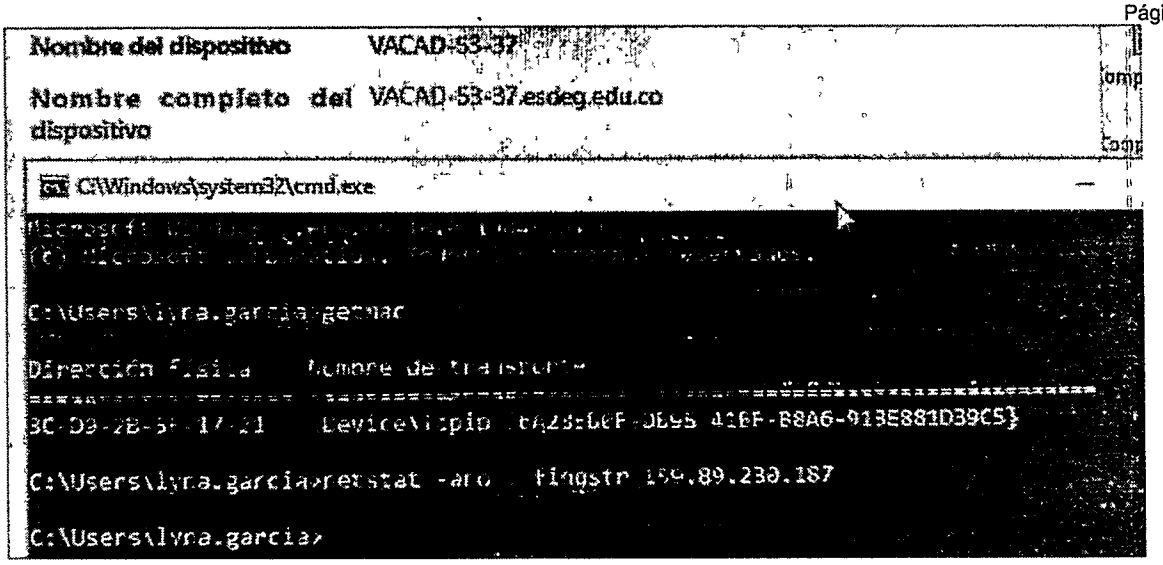


Imagen 1.12 – Verificación conexión equipo VACAD-53-37- 3c:d9:2b:5f:17:21

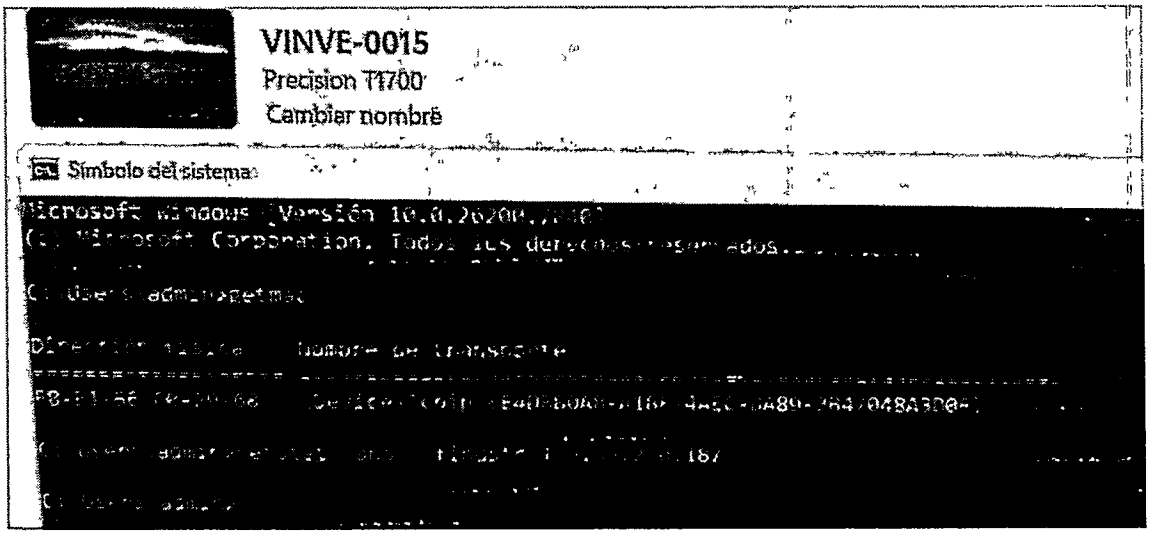


Imagen 1.13 – Verificación conexión equipo VINVE-0015 - f8:b1:56:c0:29:68

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

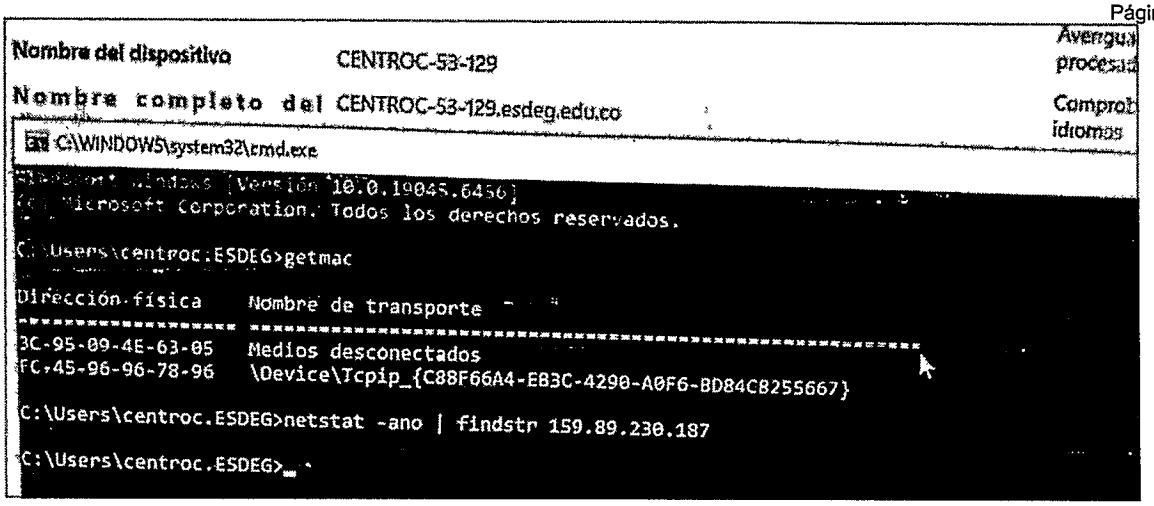


Imagen 1.14 – Verificación conexión equipo CENTROC-53-129 - fc:45:96:96:78:96

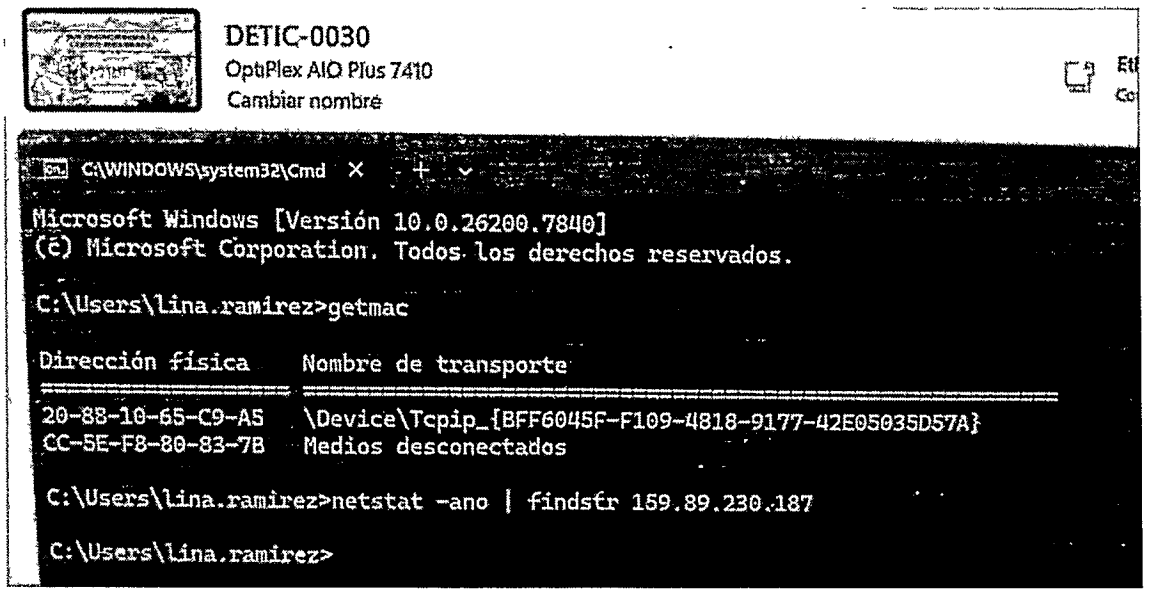


Imagen 1.15 – Verificación conexión equipo DETIC-0030 – 20:88:10:65:c9:a5

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

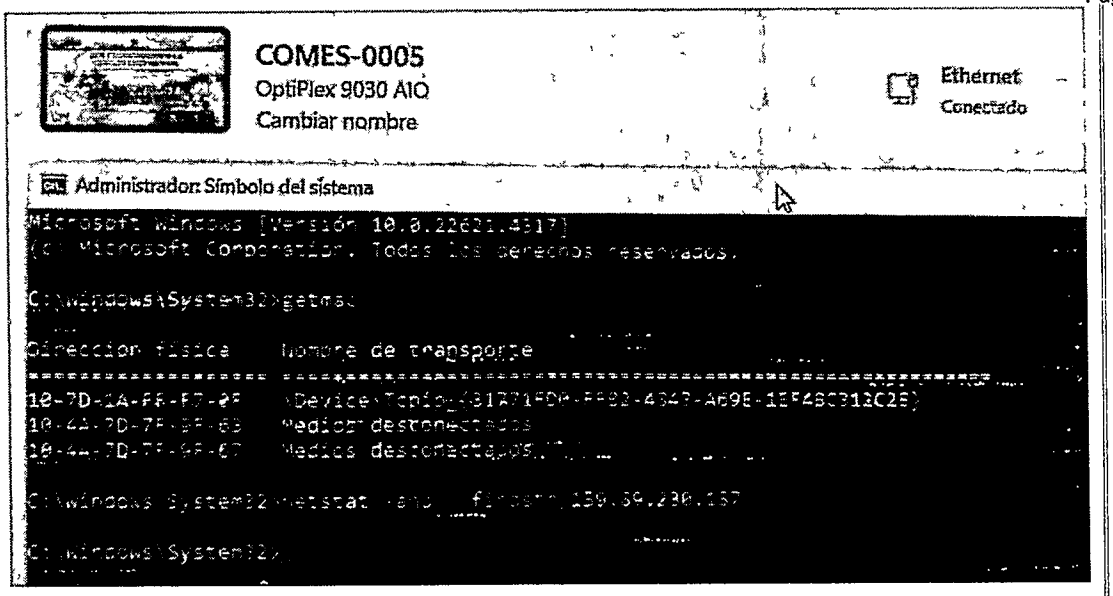


Imagen 1.16 – Verificación conexión equipo COMES-0005 – 10:7D:1A:FF:F7:0F

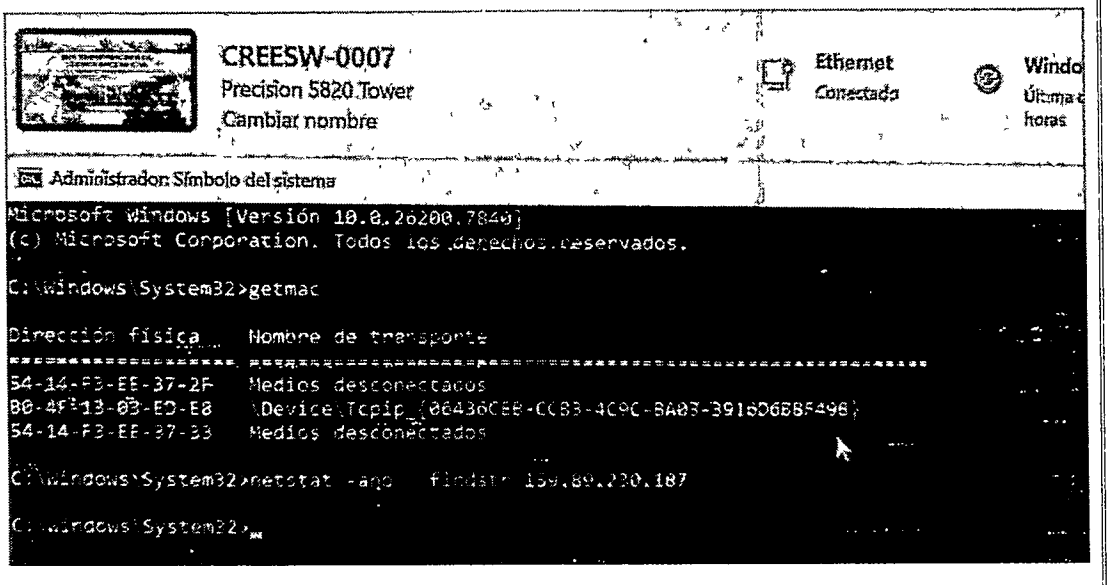


Imagen 1.17 – Verificación conexión equipo CREESW-0007 – B0:4F:13:03:ED:E8

Con respecto a la IP **190.71.130.238**, no se encontraron registros adicionales de conexión en los logs institucionales, teniendo en cuenta que la IP mencionada se encontraba previamente bloqueada desde el 09 de febrero de 2026.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

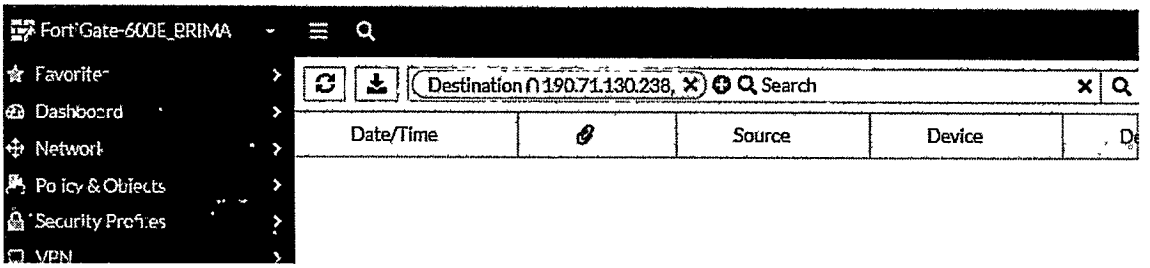


Imagen 1.18 – Consulta de log del firewall de conexiones a las IP's 190.71.130.238

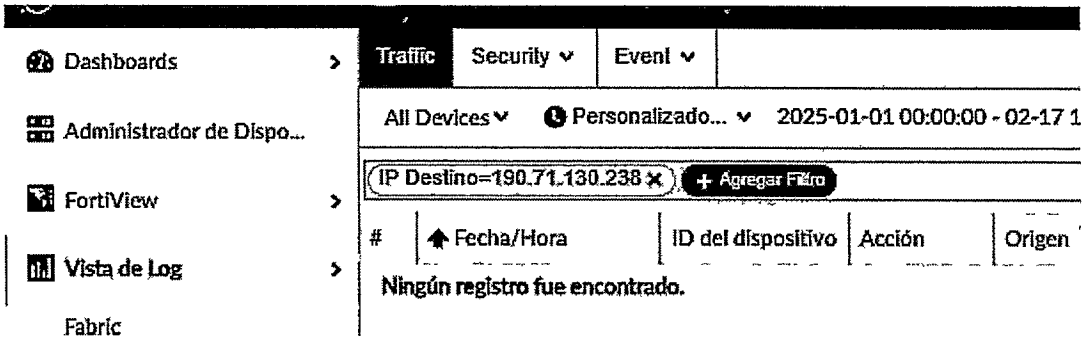


Imagen 18 – Consulta de log del Forigate de conexiones a las IP's 190.71.130.238

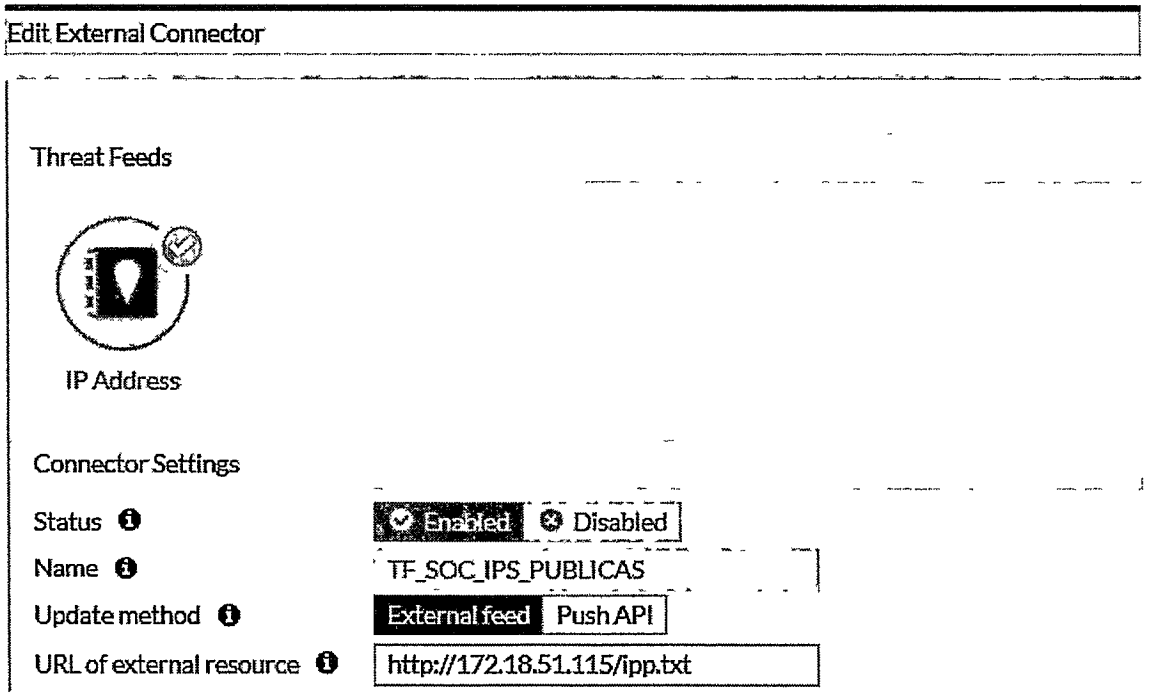


Imagen 1.19 - Existencia de un Threat Feeds para bloqueo de ip's por listado

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

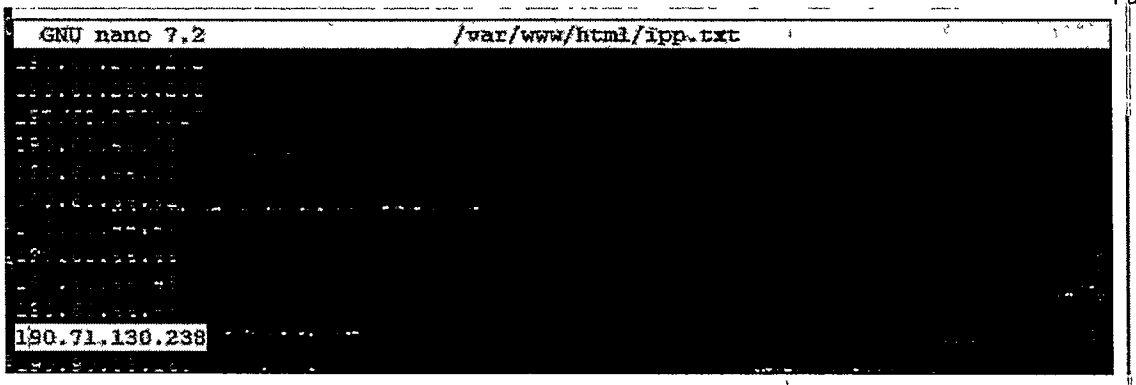


Imagen 1.20 – Listado de ip's asociado al Threat Feeds

1.2. Periodo desde el cual se tiene registro en el Firewall

De acuerdo con los registros históricos disponibles en el firewall institucional, se evidencian eventos dentro de las siguientes fechas:

Desde: 01 de diciembre de 2025
Hasta: 17 de febrero de 2026

Dentro de dicho periodo:

- No se observa crecimiento progresivo
- No existe incremento reciente anormal
- No se identifica escalamiento en el tiempo

De acuerdo con lo analizado anteriormente, no se observa actividad sostenida ni comportamiento escalonado que sugiera compromiso activo o persistente.

1.3. Medidas de contención implementadas

El departamento de tecnología como medida preventiva y sin perjuicio de los hallazgos técnicos, procedió a realizar las siguientes actividades:

- Bloquear la IP **159.89.230.187** a nivel de política de salida en el Firewall FortiGate.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

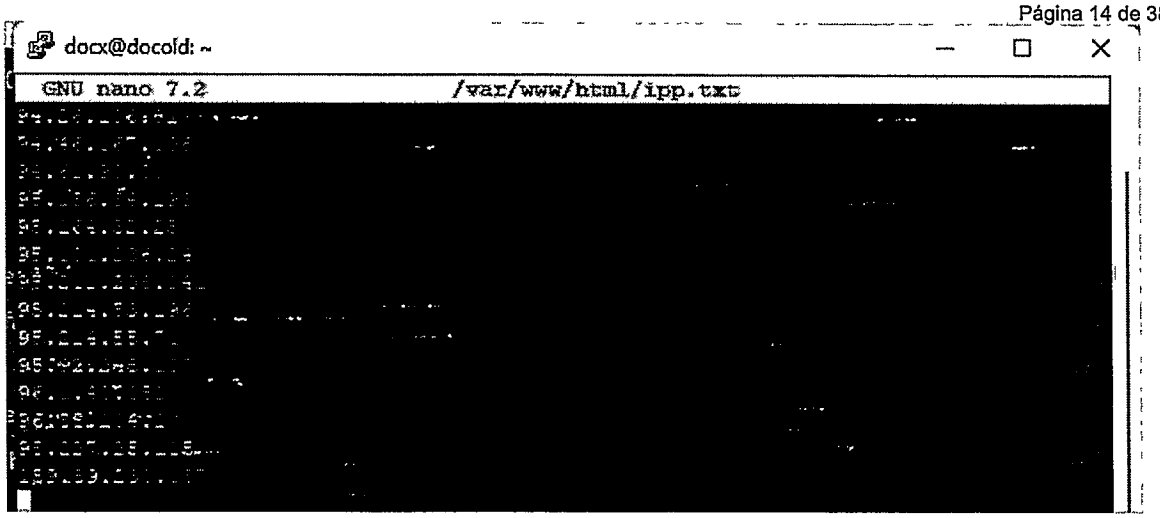


Imagen 1.21 – Relación de IP's Bloqueadas para este caso

De acuerdo con el punto dos se utilizó el mismo método para bloqueo actual de la ip 159.89.230.187

- Confirmar el bloqueo previo de la IP **190.71.130.238 (desde el 09 de febrero de 2026).**
- Restringir los dominios identificados que están asociados a esta IP identificados en FortiAnalyzer, incluyendo:
    - sync.cootlogix.com
    - sync.kueezrtb.com
    - sync.omni-dex.io
    - sync.programmaticx.ai

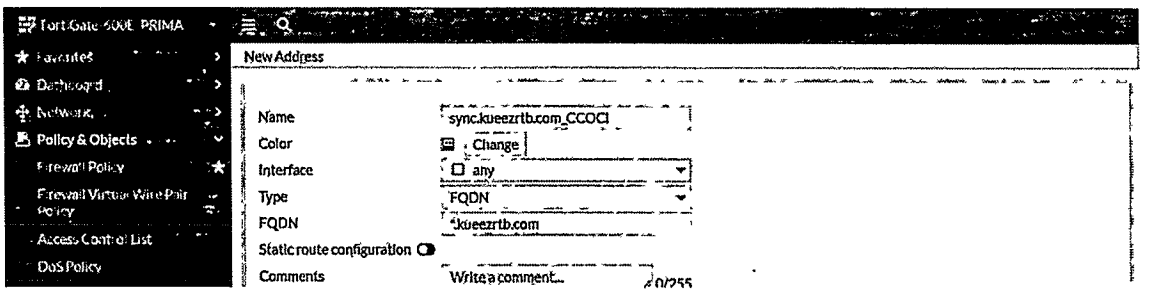


Imagen 1.22 – Creación de los FQDNs para su respectivo Bloqueo

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

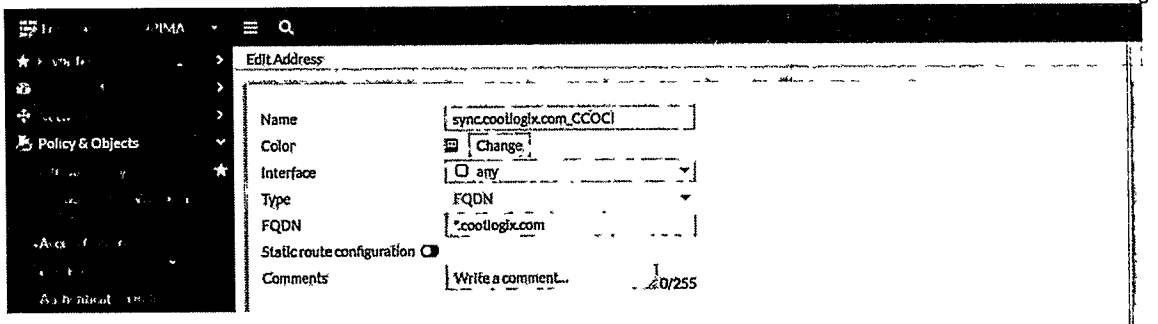


Imagen 1.23 – Creación de los FQDNs para su respectivo Bloqueo

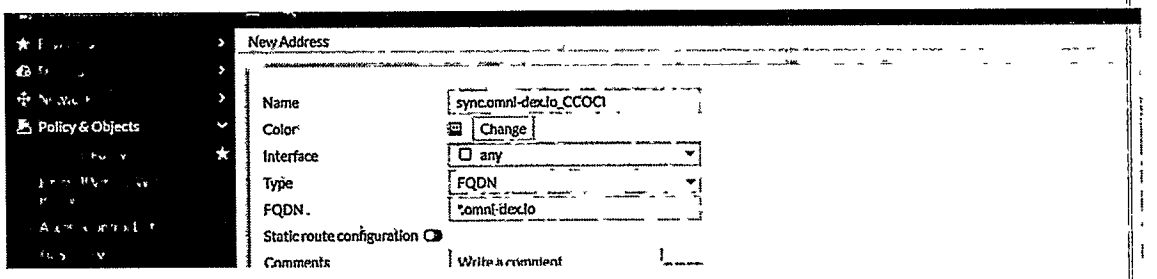


Imagen 1.24 – Creación de los FQDNs para su respectivo Bloqueo

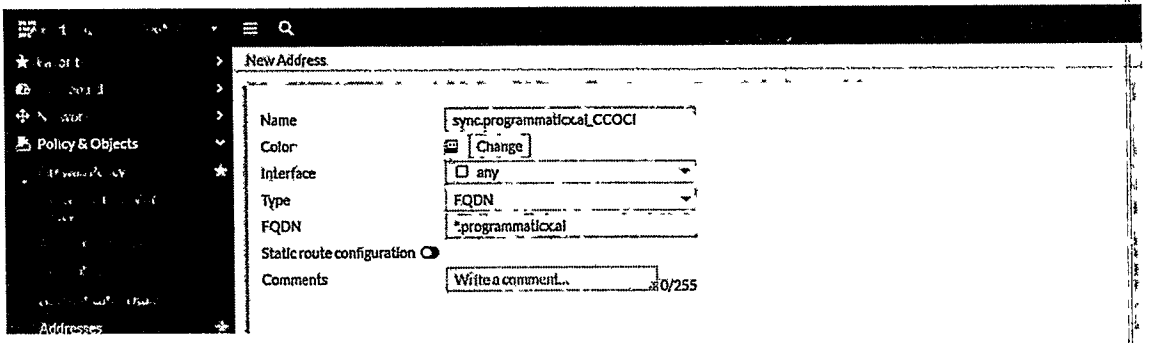


Imagen 1.25 – Creación de los FQDNs para su respectivo Bloqueo

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

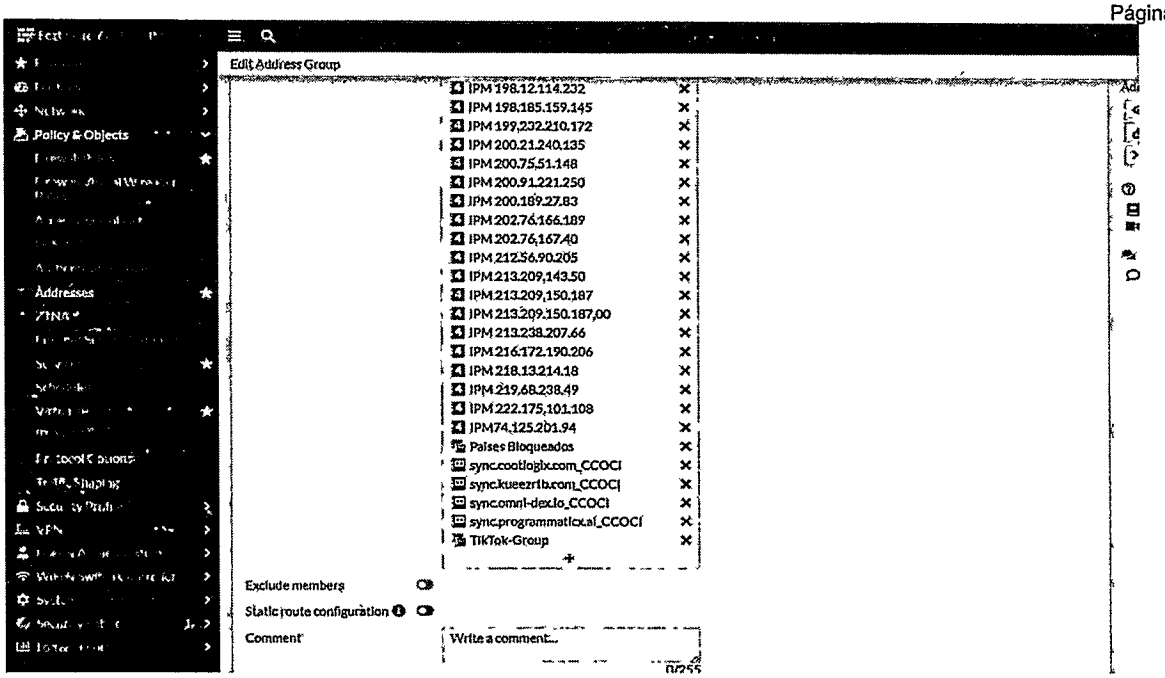


Imagen 1.26 – Asociación al grupo de los FQDNs Bloqueados

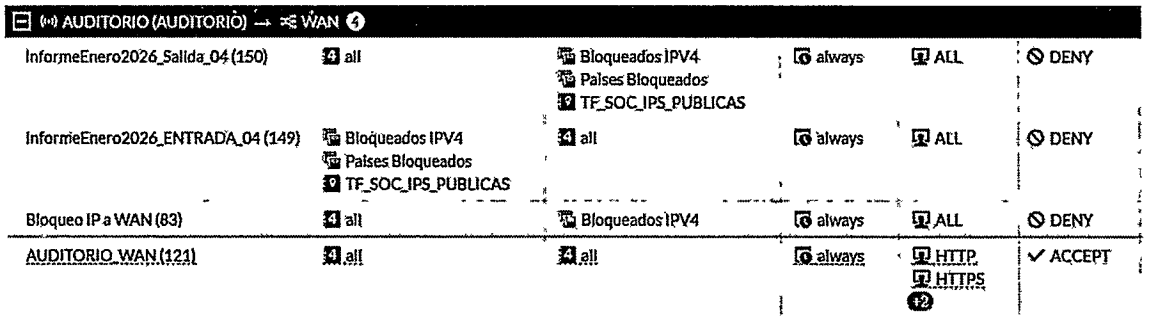


Imagen 1.27 – Reglas previamente existentes a las que se les asoció los FQDN bloqueados

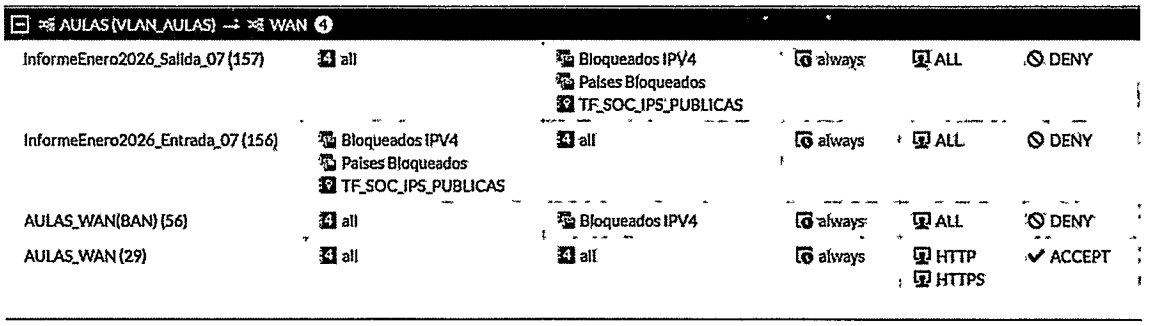


Imagen 1.28 – Reglas previamente existentes a las que se les asoció los FQDN bloqueados

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

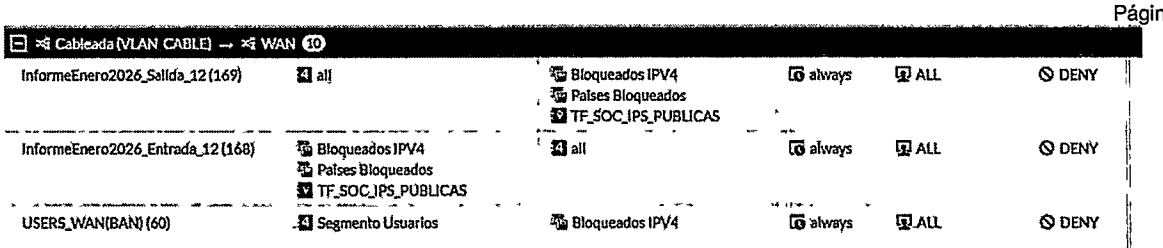


Imagen 1.29 – Reglas previamente existentes a las que se les asoció los FQDN bloqueados

Se aplicó restricciones a los subdominios asociados a la IP, reforzando así la postura de seguridad perimetral.

1.4. Otras actividades

Adicionalmente, se informa que dentro de las actividades establecidas en el plan de trabajo del presente año se encuentra contemplado el proceso progresivo de formateo y reinstalación controlada de los equipos institucionales, como medida preventiva de fortalecimiento de la seguridad y estandarización de configuraciones.

A la fecha, se han formateado y configurado **120 equipos** de la ESDEG, siguiendo lineamientos básicos de seguridad, actualización de sistema operativo y validación de políticas institucionales.

En atención al evento reportado y de acuerdo con las instrucciones del mando, se le ha otorgado **prioridad a los 21 equipos identificados en los registros**, incorporándolos de manera inmediata al cronograma de intervención, con el fin de reforzar la postura preventiva y mitigar cualquier riesgo potencial asociado.

1.5. Conclusión técnica

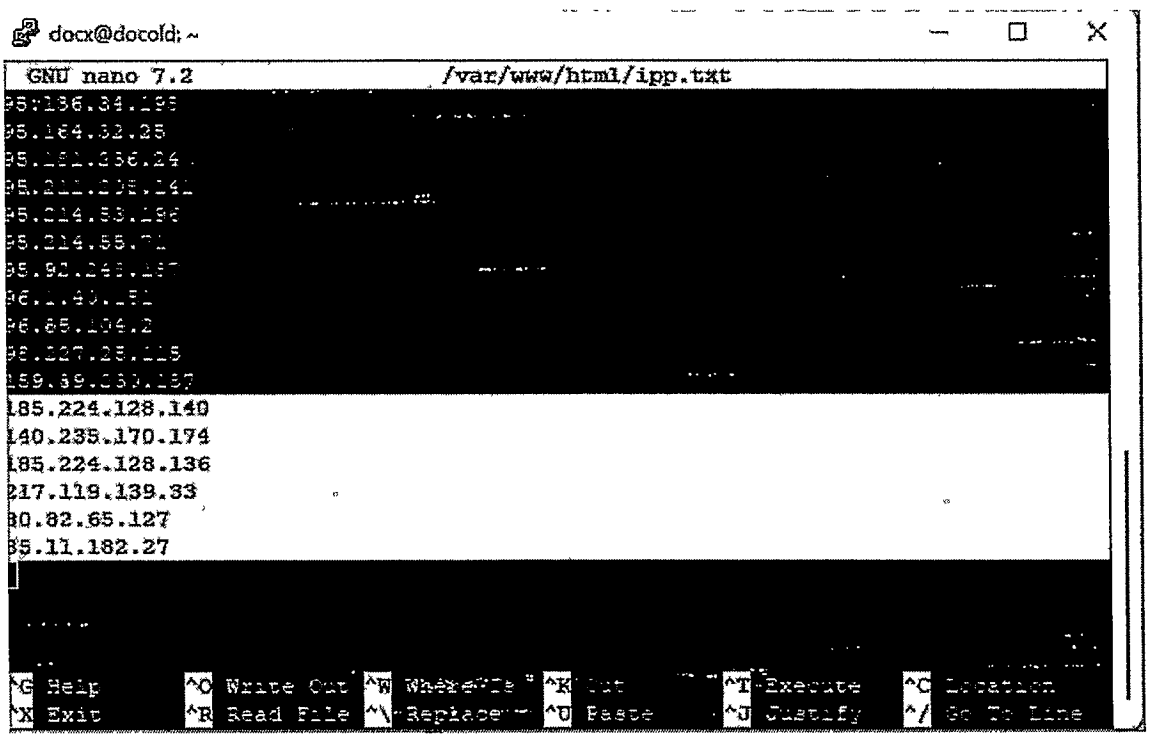
Con base en el análisis técnico realizado, no se identifican indicadores de compromiso activo, exfiltración de datos ni comportamiento tipo C2 en los equipos evaluados. No obstante, y en aplicación del principio de seguridad, se implementaron medidas preventivas de bloqueo y restricción perimetral, manteniendo monitoreo reforzado sobre cualquier intento futuro de comunicación hacia los destinos mencionados.

"Documento propiedad SIG - ESDEG, Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

2. Caso ID: ##378370## – Intentos fallidos de autenticación SSL-VPN compatibles con ataque de fuerza bruta

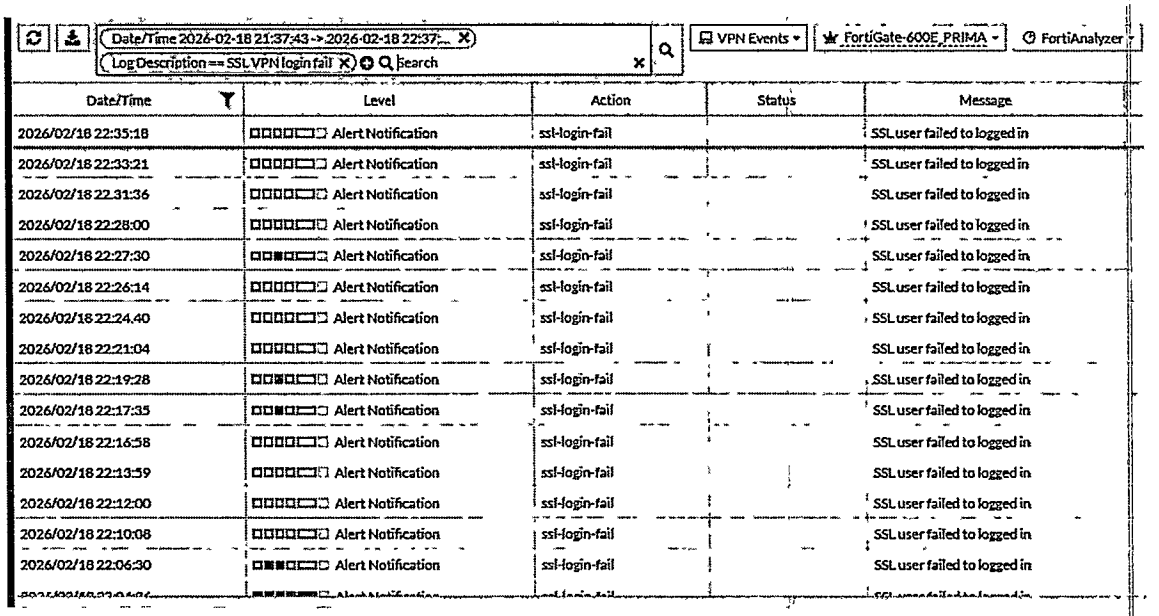
En atención a los eventos reportados en el **Caso ID: ##378370## – Radicado No. 0126001351402**, se realizó el análisis de múltiples intentos fallidos de autenticación detectados por el **SIEM** bajo la regla **"Failed VPN Logon From Outside My Country"**, los cuales evidencian un patrón compatible con intentos de **fuerza bruta o password spraying** contra credenciales del **Directorio Activo** a través del servicio **SSL-VPN del FortiGate 600E**.

En el proceso de verificación técnica se revisaron detalladamente los registros del **FortiGate 600E y su correlación en el FortiAnalyzer**, identificando diversas direcciones IP externas desde las cuales se generaron intentos reiterativos de autenticación fallida. Como medida inmediata de contención, se procedió al **bloqueo a nivel perimetral de las direcciones IP 217.119.139.33, 80.82.65.127 y 85.11.182.27**, reportadas inicialmente en el caso, así como de las IP **185.224.128.140, 140.235.170.174 y 185.224.128.136**, las cuales también registraron múltiples intentos fallidos de acceso con comportamiento consistente con intentos automatizados de validación de credenciales.



"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Imagen 2. – Bloqueo de las IP's relacionadas en el informe.



Date/Time	Level	Action	Status	Message
2026/02/18 22:35:18	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:33:21	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:31:36	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:28:00	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:27:30	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:26:14	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:24:40	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:21:04	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:19:28	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:17:35	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:16:58	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:13:59	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:12:00	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:10:08	Alert Notification	ssl-login-fail		SSL user failed to logged in
2026/02/18 22:06:30	Alert Notification	ssl-login-fail		SSL user failed to logged in

Imagen 2.1 – Registro de conexiones adicionales a las reportas en el Casao

Como medida adicional de fortalecimiento de la seguridad administrativa del dispositivo, se configuró el mecanismo de bloqueo automático por intentos fallidos (**Imagen 2.2**) de autenticación mediante el ajuste de los parámetros admin-lockout-threshold y admin-lockout-duration, estableciendo un umbral de **3 intentos fallidos consecutivos** y un tiempo de bloqueo de **600 segundos (10 minutos)**.

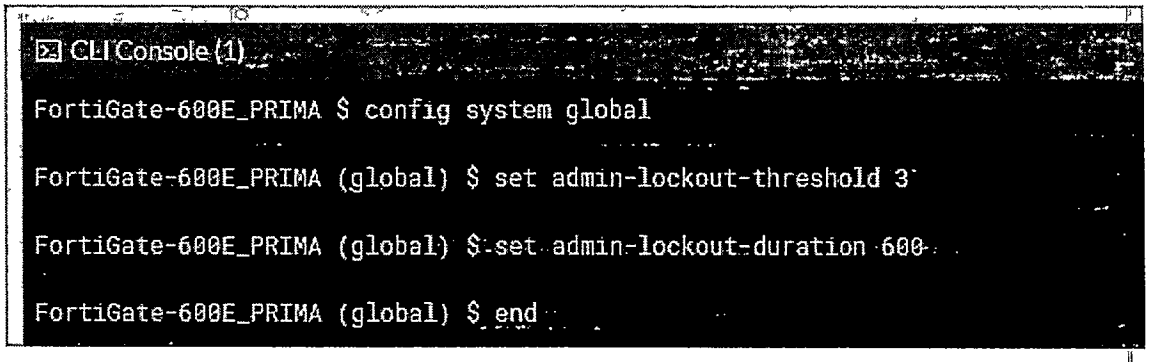


Imagen 2.2 – configuración mecanismo de bloqueo automático por intentos fallidos

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Con esta configuración, cualquier origen que supere el límite definido queda temporalmente bloqueado, mitigando eficazmente intentos automatizados de fuerza bruta contra cuentas administrativas y reduciendo el riesgo de validación masiva de credenciales.

Adicionalmente, se deshabilitó el acceso en modalidad Web Mode del servicio SSL-VPN **(Imagen 2.3)**, manteniendo únicamente habilitado el modo túnel para conexión mediante cliente FortiClient autorizado. Es importante precisar que, aunque la URL del servicio SSL-VPN continúa respondiendo debido a que el modo túnel permanece activo, no se encuentra habilitado el acceso a portal web, recursos publicados ni funcionalidades de navegación vía navegador, reduciendo así la superficie de exposición sin afectar la operación institucional.

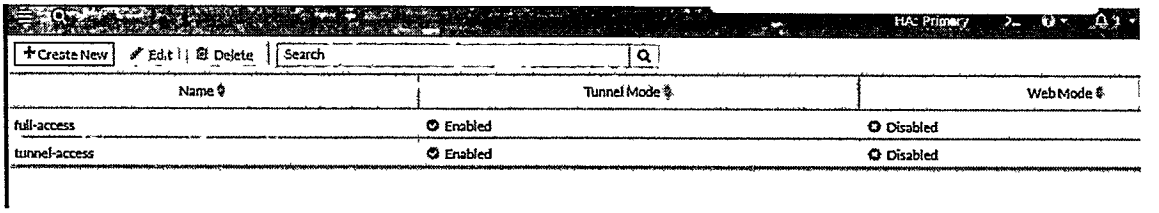
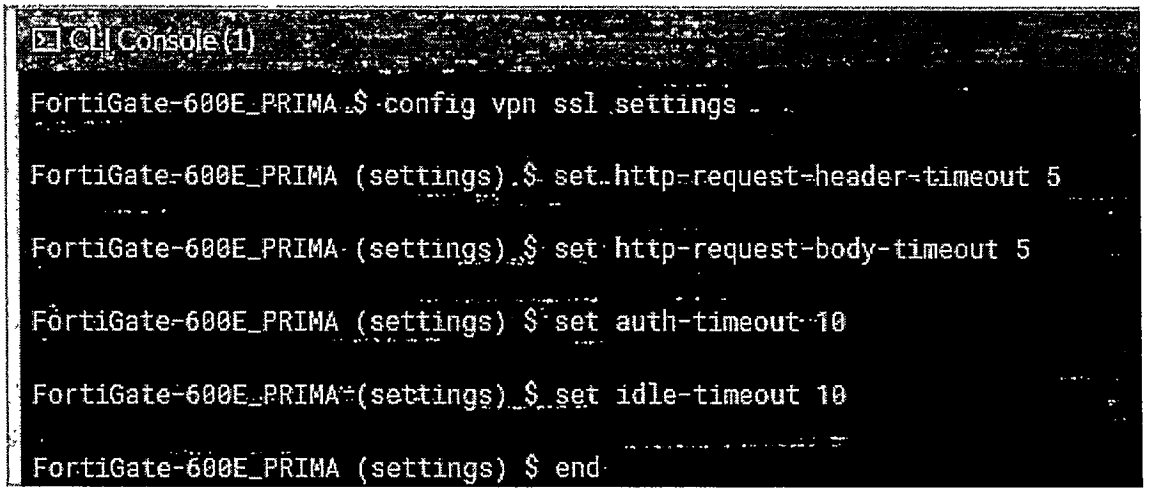


Imagen 2.3 - Des habilitación del acceso en modalidad Web Mode del servicio SSL-VPN

De igual manera, se fortaleció el servicio SSL-VPN, ajustando los parámetros de control de sesión y autenticación dentro de la configuración global del VPN, reduciendo los tiempos de espera asociados a solicitudes HTTP y sesiones activas. Se configuraron valores restrictivos para http-request-header-timeout, http-request-body-timeout, auth-timeout e idle-timeout, limitando la ventana de interacción y permanencia de conexiones no autenticadas.



"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Imagen 2.4 – Reducción de tiempos de espera a solicitudes HTTP y sesiones activas

Con esta configuración se disminuye la exposición frente a intentos automatizados de fuerza bruta y sesiones persistentes no legítimas, reduciendo la capacidad de los atacantes de mantener procesos de validación masiva de credenciales o conexiones inactivas prolongadas contra el servicio SSL-VPN.

2.1. Conclusión Técnica

En atención a la descripción del evento emitida por el SIEM, donde se hace referencia a posibles intentos de explotación asociados a vulnerabilidades como CVE-2023-27997, se precisa que la infraestructura institucional no se encuentra expuesta a dicha vulnerabilidad. El equipo técnico institucional ejecutó previamente la actualización del clúster FortiGate 600E en alta disponibilidad (HA) junto con los dispositivos asociados de la infraestructura Fortinet (FortiAP, switch core y FortiSwitch), dejando la plataforma en la versión **v7.4.11 build 2878**, versión reciente, estable y soportada por el fabricante, la cual —de acuerdo con la información oficial de Fortinet— no presenta vulnerabilidad frente al CVE-2023-27997 ni exposición a ejecución remota de código.

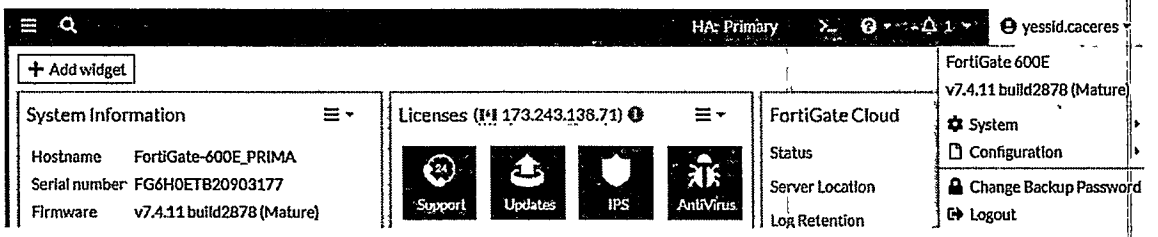


Imagen 2.5 – Versión actual Fortigate 600E (v7.4.11 build 2878)

Del análisis técnico realizado sobre los registros de autenticación SSL-VPN, se determinó que los eventos corresponden a múltiples intentos fallidos de autenticación, compatibles con técnicas de *brute force* o *password spraying*, orientadas a la validación de credenciales y no a la explotación de una vulnerabilidad del software.

En consecuencia, el escenario identificado se clasifica como intentos de fuerza bruta contra el mecanismo de autenticación, frente al cual se aplicaron medidas inmediatas de

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

contención mediante el bloqueo perimetral de las IP involucradas, el endurecimiento de los parámetros de autenticación y la reducción de la superficie de exposición del servicio SSL-VPN, conforme se detalla en el presente informe

3. Caso ID: ##378368## – Verificación de posible intento de comunicación de Comando y Control (C2)

En atención al evento reportado como posible intento de comunicación de Comando y Control (C2), relacionado con conexión entrante desde la dirección IP pública **185.93.89.171** hacia el puerto destino **21443** de la IP pública **179.1.128.134**, se realizaron las siguientes acciones:

3.1. Bloqueo perimetral inmediato:

Se procedió al bloqueo de la dirección IP de origen 185.93.89.171 a nivel de firewall, a través del External Connector institucional previamente configurado, agregando la IP al listado centralizado de bloqueo, impidiendo nuevos intentos de conexión desde dicho origen hacia la infraestructura institucional.

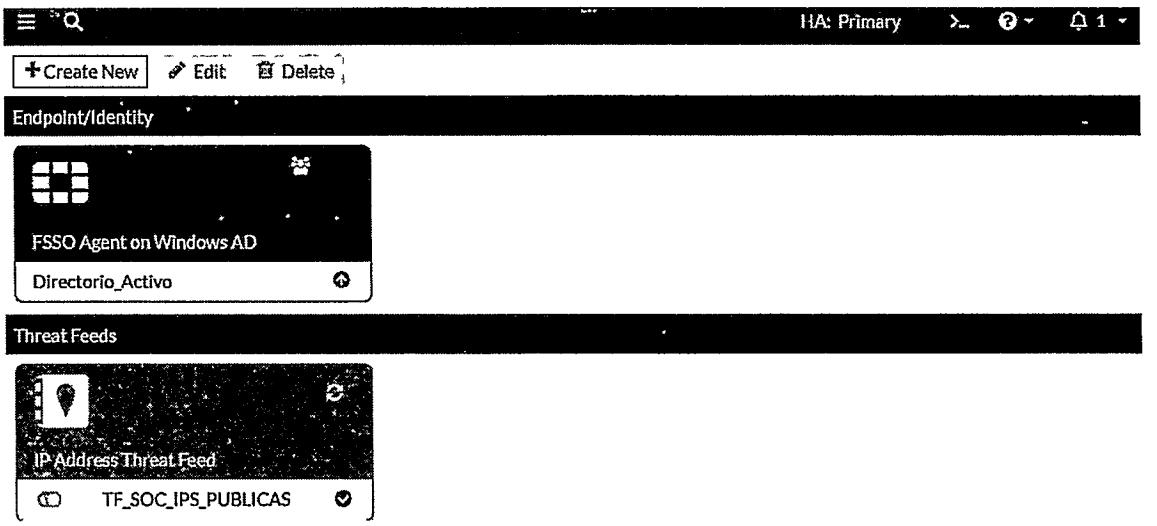


Imagen 3 – Threat Feeds configurado para cargar IP's Bloqueadas

"Documento propiedad SIG – ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

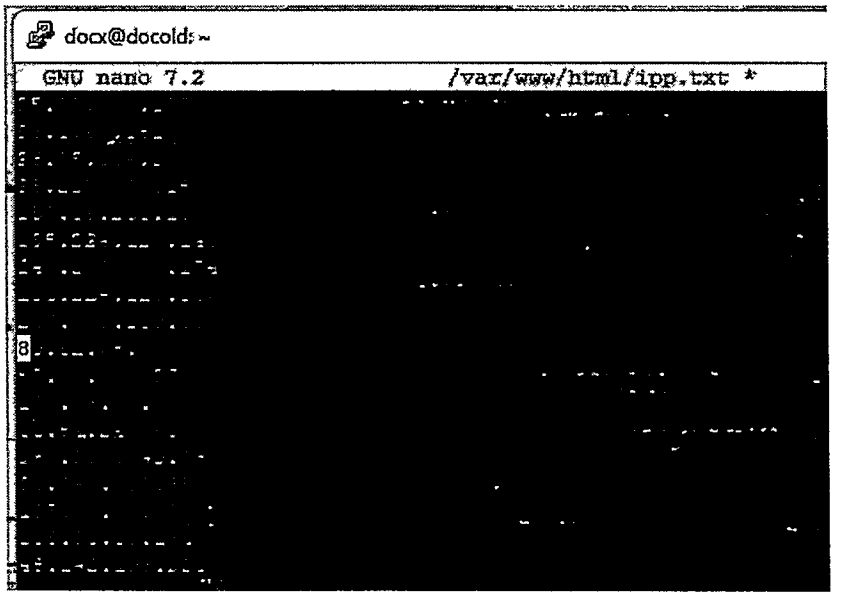


Imagen 1 – registro de las IP's nuevas adicionadas al listado de bloqueadas

Con lo anterior, se mantiene activo el monitoreo permanente del servicio SSL-VPN, la revisión continua de logs y la verificación de recurrencia desde las mismas u otras IP externas, dejando constancia de que no se evidenciaron accesos exitosos asociados a los intentos descritos.

5. Caso ID: ##378386## – Detección de intentos de conexión desde múltiples direcciones IP externas asociadas a actividades de escaneo

En atención a los eventos reportados en el Caso ID: ##378386## – Radicado No. 0126001351402, se realizó la verificación técnica de múltiples intentos de conexión provenientes de direcciones IP externas identificadas por el SIEM y asociadas, según inteligencia de amenazas (GTI), a actividades de escaneo, reconocimiento y posible infraestructura utilizada para pruebas automatizadas sobre servicios expuestos.

Como parte del proceso de análisis, se revisaron detalladamente los registros del FortiGate 600E y su correlación en el FortiAnalyzer, evidenciando que tres de las cinco direcciones IP reportadas (207.90.244.2, 71.6.134.235 y 154.197.56.163) registran intentos de conexión en los logs del firewall. No obstante, en todos los casos los eventos se encuentran en estado rechazado (deny) por las políticas de seguridad perimetral, sin establecimiento

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

de sesión ni transferencia de datos, lo que confirma el correcto funcionamiento de los mecanismos de protección implementados en la infraestructura institucional.

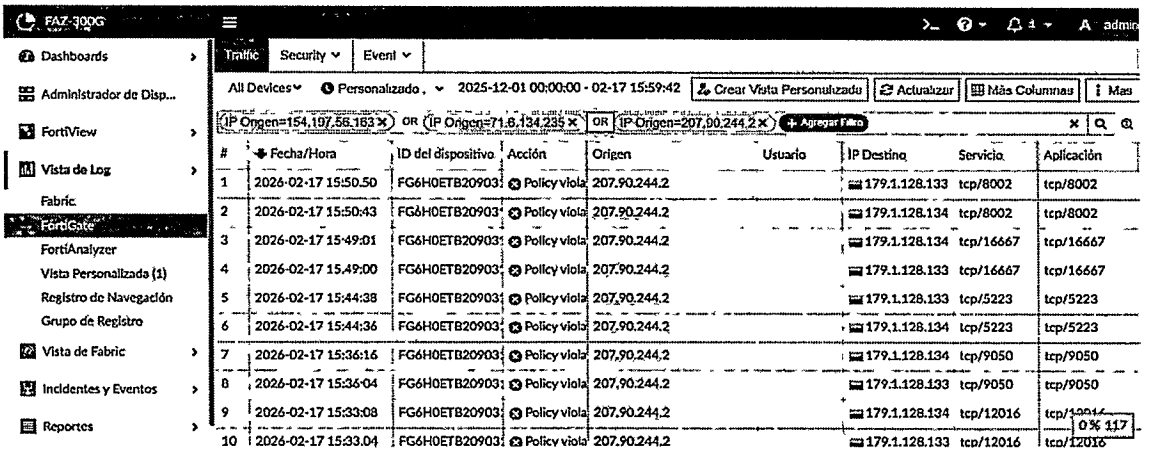


Imagen 5.1 - Registro de los intentos de conexión de las IPs donde se evidencia que todas están rechazadas

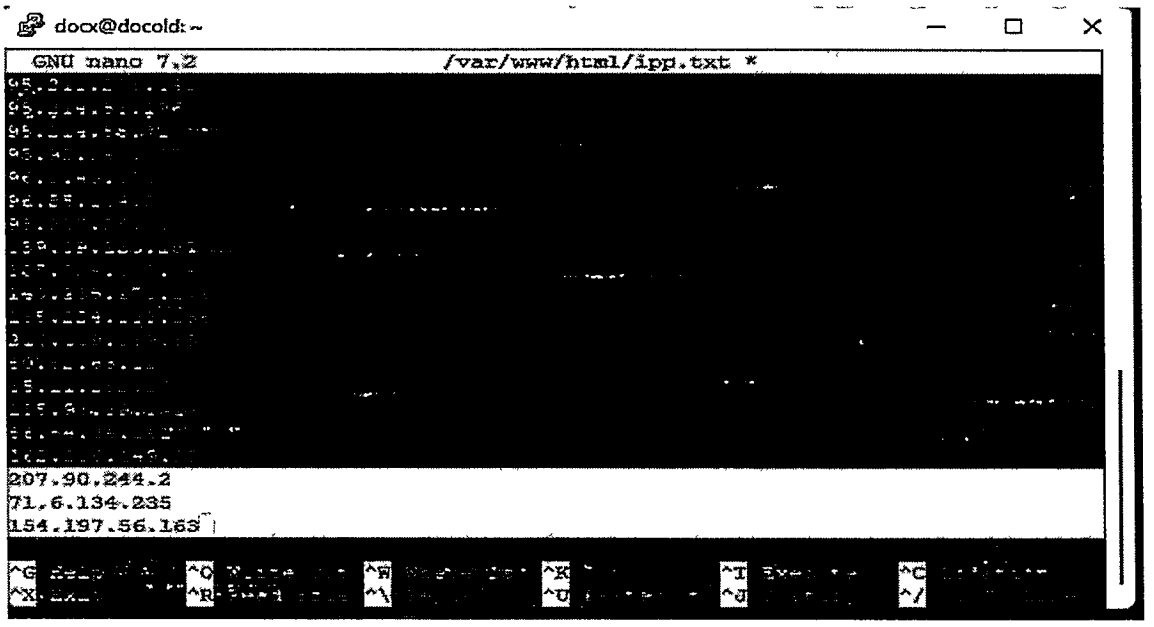


Imagen 5.2 – Adición de IP's al Threat Feeds

Respecto a las direcciones IP 80.82.77.33 y 66.240.236.116, tras la validación de logs también se evidenciaron intentos de conexión; no obstante, estas ya se encontraban previamente incluidas en el listado de IP bloqueadas con fecha 16 de enero, en atención a las indicaciones recibidas mediante el informe DATA LEAK remitido por la Armada, donde se identificó el hallazgo "Found topic".

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

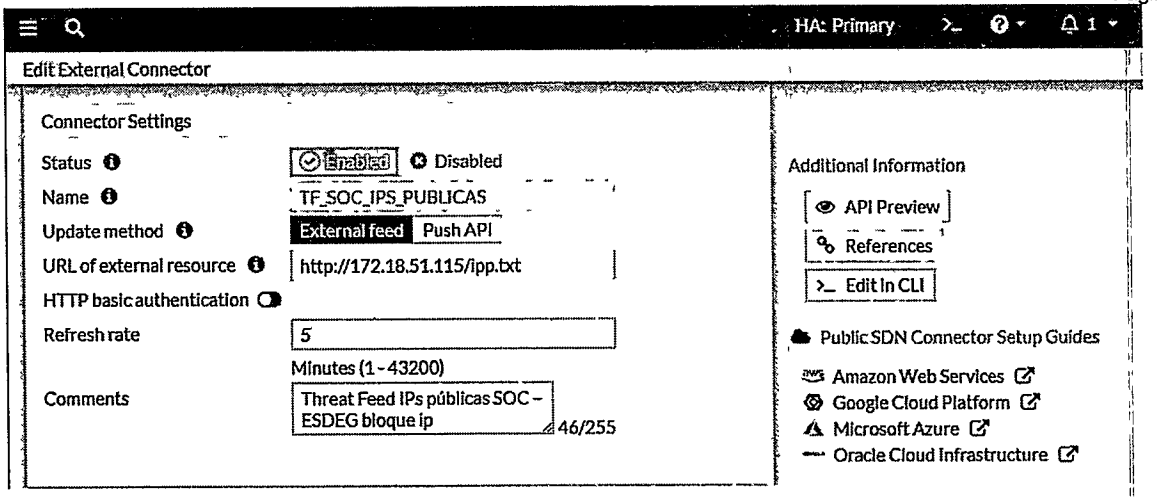


Imagen 3.1 – Configuración del Threat Feeds

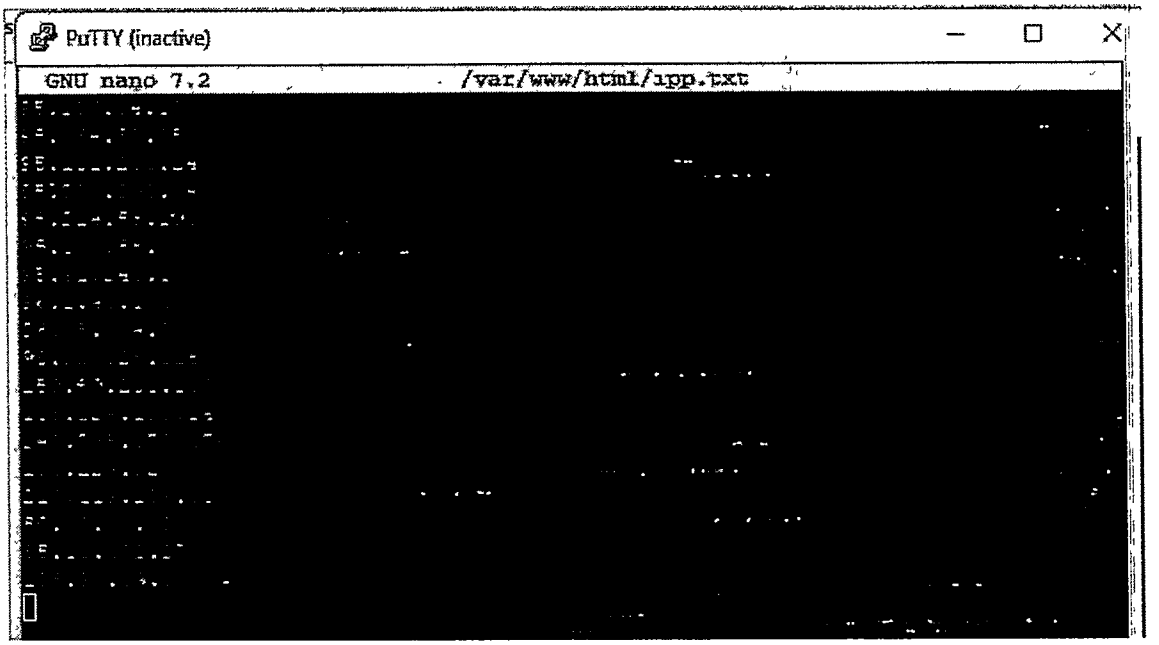


Imagen 3.2 listado donde se agregan nuevas IP's bloqueadas

3.2. Validación del puerto TCP 21443:

Se verificó que el puerto 21443 corresponde al servicio institucional de SSL-VPN, el cual se encuentra publicado de manera controlada para acceso remoto autorizado. Del análisis de los registros no se evidenció establecimiento de sesión válida, autenticación exitosa ni

"Documento propiedad SIG – ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

tráfico bidireccional que indique compromiso o canal activo de comunicación, tratándose únicamente de intentos de conexión entrante sin éxito.

3.3. Revisión de registros y recurrencia:

Se realizó análisis de los logs del FortiGate, confirmando que el evento corresponde a un intento aislado de conexión entrante, sin evidencia de persistencia, establecimiento de canal de comunicación ni transferencia de datos.

4. Caso ID: ##378370## – Intentos adicionales de autenticación fallida SSL-VPN compatibles con ataque de fuerza bruta

En atención a los eventos reportados en el Caso ID: ##378370## – Radicado No. 0126001351402, se realizó la verificación técnica de múltiples intentos de conexión no autorizados detectados por el SIEM y registrados en los logs del FortiGate 600E bajo el evento "SSL VPN login fail" (acción: ssl-login-fail). Dichos eventos evidencian intentos reiterativos de autenticación contra diferentes cuentas de acceso, provenientes de direcciones IP externas con reputación maliciosa, comportamiento consistente con patrones de fuerza bruta y validación automatizada de credenciales contra el servicio SSL-VPN institucional.

Es preciso indicar que estos eventos guardan relación con las acciones previamente informadas mediante Radicado No. 0126105888, correspondiente al Caso ID ##378357##; no obstante, tras la revisión detallada de los registros del FortiGate 600E y su correlación en el SIEM, se identificaron direcciones IP adicionales (185.93.89.170, 185.93.89.164 y 45.142.193.221) que no habían sido incluidas en el informe anterior. En consecuencia, se procedió a su bloqueo inmediato a nivel perimetral, con el fin de complementar y reforzar las medidas de contención previamente implementadas.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

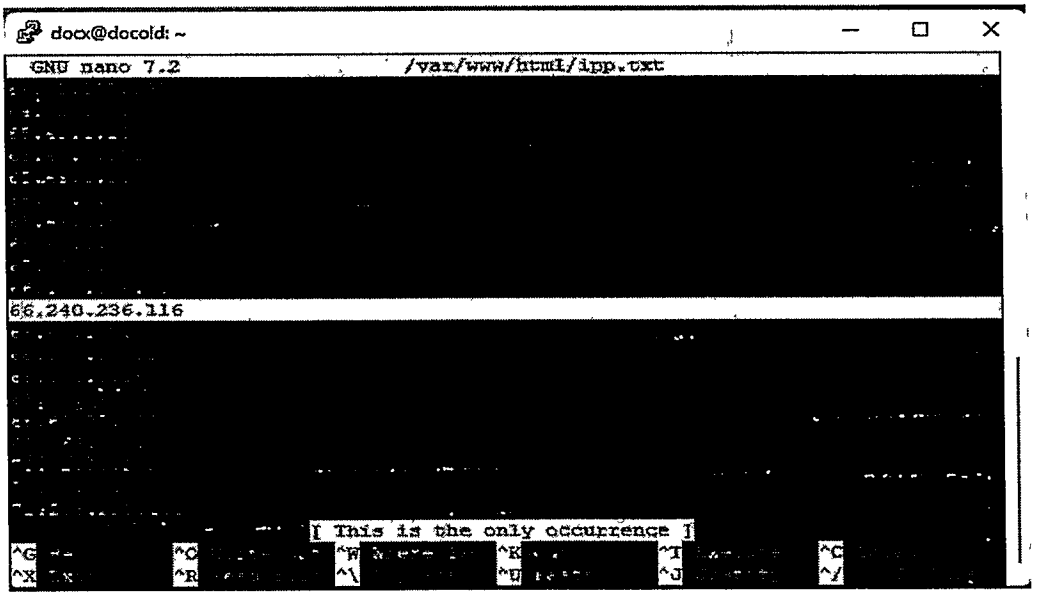


Imagen 5.3 – IP's registradas al listado de bloqueadas basado en los Casos Anteriores dentro del mismo radicado

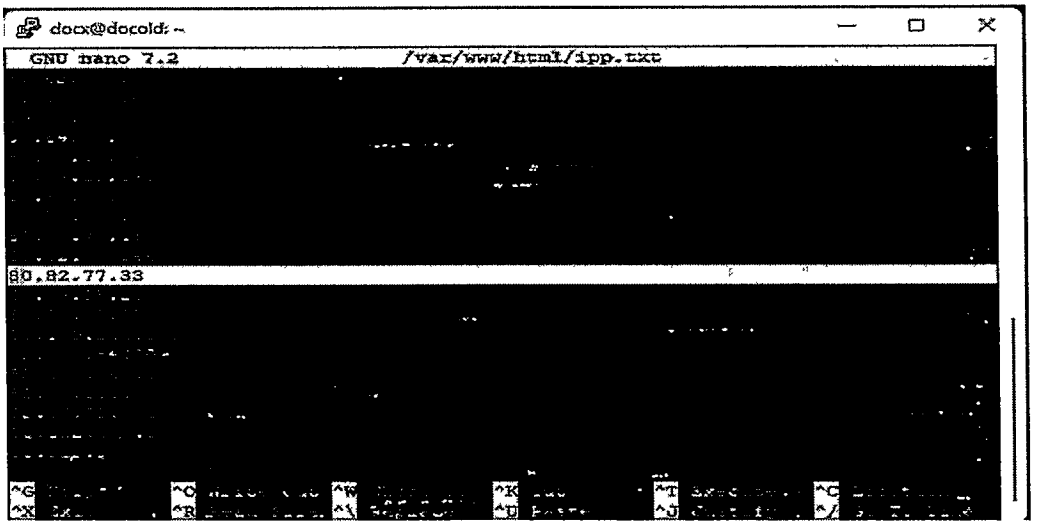


Imagen 2 – IP's registradas al listado de bloqueadas basado en los Casos Anteriores dentro del mismo radicado

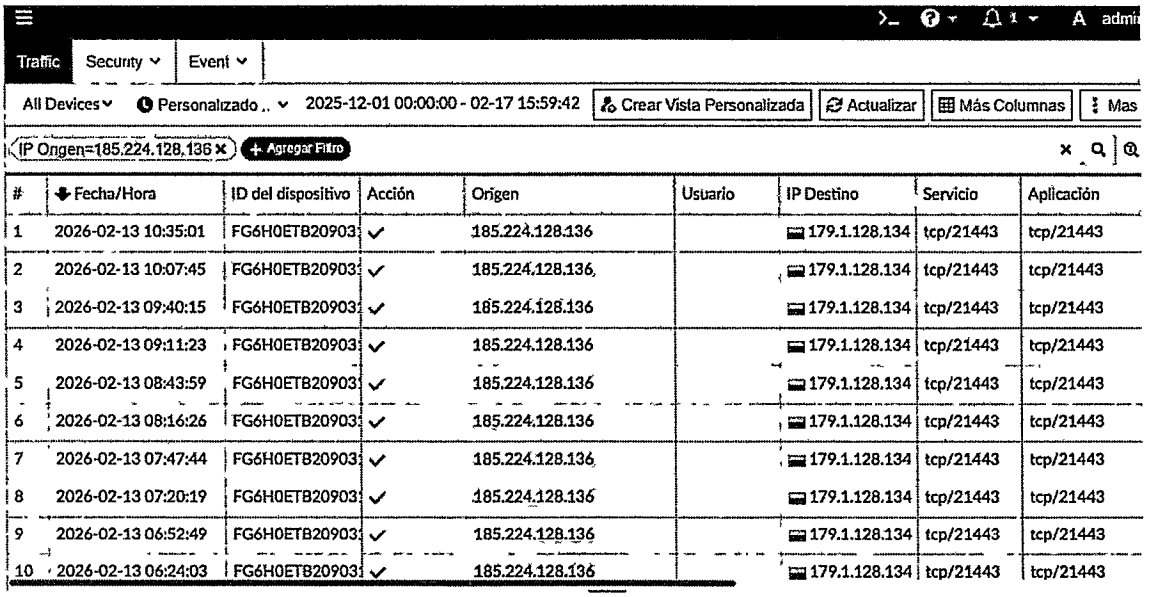
Se deja constancia que no se evidenciaron accesos exitosos, autenticaciones válidas ni compromiso de servicios internos asociados a las direcciones IP mencionadas, manteniéndose activo el monitoreo permanente del tráfico entrante y la revisión continua de eventos correlacionados en el SIEM y el firewall institucional.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

6. Caso ID: ##378383## – Evento de tráfico permitido identificado como IPSum Malware IP

En atención a los eventos reportados en el Caso ID: ##378383## – Radicado No. 0126001351402, se realizó la verificación técnica de un evento de tráfico permitido hacia el plano de control del dispositivo FortiGate 600E, identificado por el SIEM bajo la alerta "Permitted Traffic from IPSum Malware IP".

El evento analizado corresponde a una conexión proveniente de la dirección IP 185.224.128.136, geolocalizada en Países Bajos, dirigida al puerto 21443 de la IP pública institucional, puerto configurado para el servicio SSL-VPN del firewall FortiGate 600E. Dicho evento fue detectado el 13 de febrero, motivo por el cual se realizó la verificación de los registros correspondientes en el FortiGate 600E y su correlación en el FortiAnalyzer, procediéndose como medida preventiva al bloqueo inmediato de la dirección IP a nivel perimetral con el fin de evitar nuevos intentos de conexión hacia el servicio expuesto.



#	Fecha/Hora	ID del dispositivo	Acción	Origen	Usuario	IP Destino	Servicio	Aplicación
1	2026-02-13 10:35:01	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
2	2026-02-13 10:07:45	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
3	2026-02-13 09:40:15	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
4	2026-02-13 09:11:23	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
5	2026-02-13 08:43:59	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
6	2026-02-13 08:16:26	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
7	2026-02-13 07:47:44	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
8	2026-02-13 07:20:19	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
9	2026-02-13 06:52:49	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
10	2026-02-13 06:24:03	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443

El registro evidencia que el tráfico fue procesado bajo subtype="local" y policytype="local-in-policy" (policyid=0), lo que confirma que la comunicación fue dirigida directamente al dispositivo y no a infraestructura interna. Aunque se registró un intercambio inicial de paquetes (sentpkt=10 / rcvdpkt=11), la sesión finalizó mediante client-rst, sin autenticación exitosa ni establecimiento de túnel VPN.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Del análisis técnico se determinó que el comportamiento corresponde a una actividad de reconocimiento o intento de negociación inicial del servicio SSL-VPN, sin evidencia de explotación de vulnerabilidad ni compromiso del sistema.

6.1. Verificación de bloqueo previo:

Se confirmó que la IP 185.224.128.136 ya se encontraba bloqueada a nivel perimetral como parte de las acciones ejecutadas en el Caso ID ##378370##, asociado a intentos de fuerza bruta contra el servicio SSL-VPN.

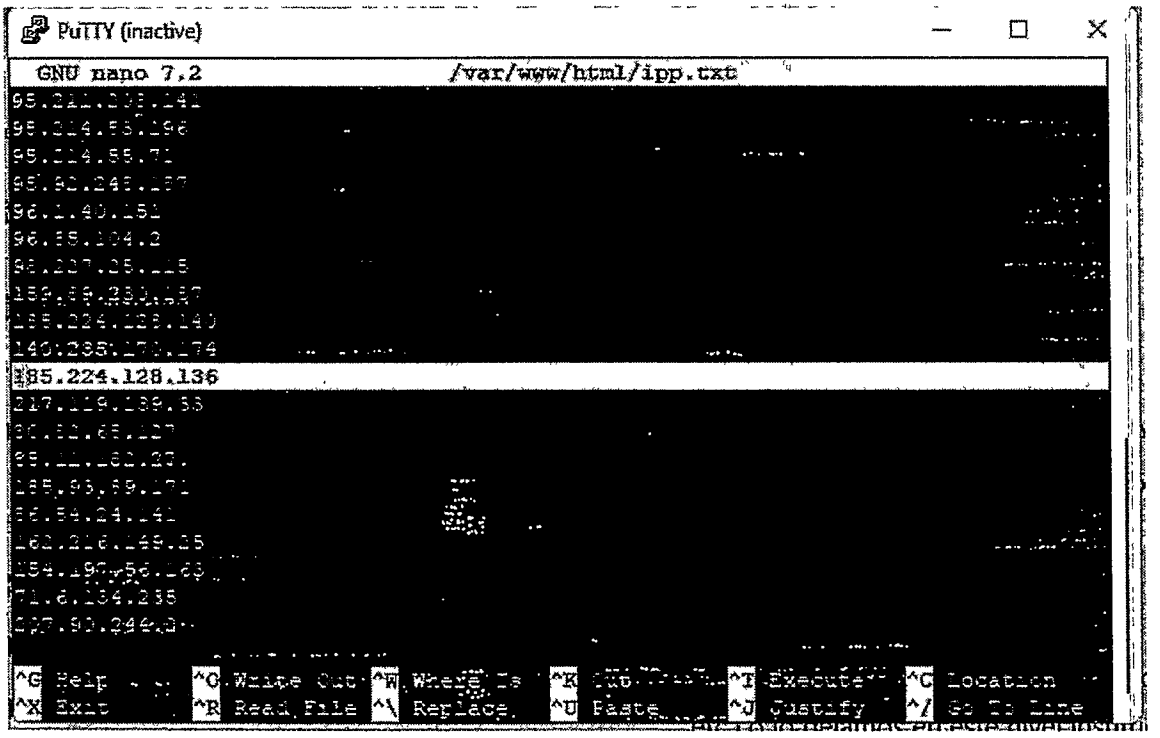


Imagen 6.1 – Bloueo previo de la IP con Threat Feeds

6.2. Implementación de geobloqueo en Local-In Policy:

Se configuró una política de tráfico entrante (Local-In Policy) para el servicio SSL-VPN en la interfaz WAN, permitiendo únicamente conexiones provenientes de Colombia y bloqueando explícitamente el resto de los orígenes no autorizados. Con esta medida, cualquier intento de negociación desde países no permitidos es rechazado antes de que alcance el servicio.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

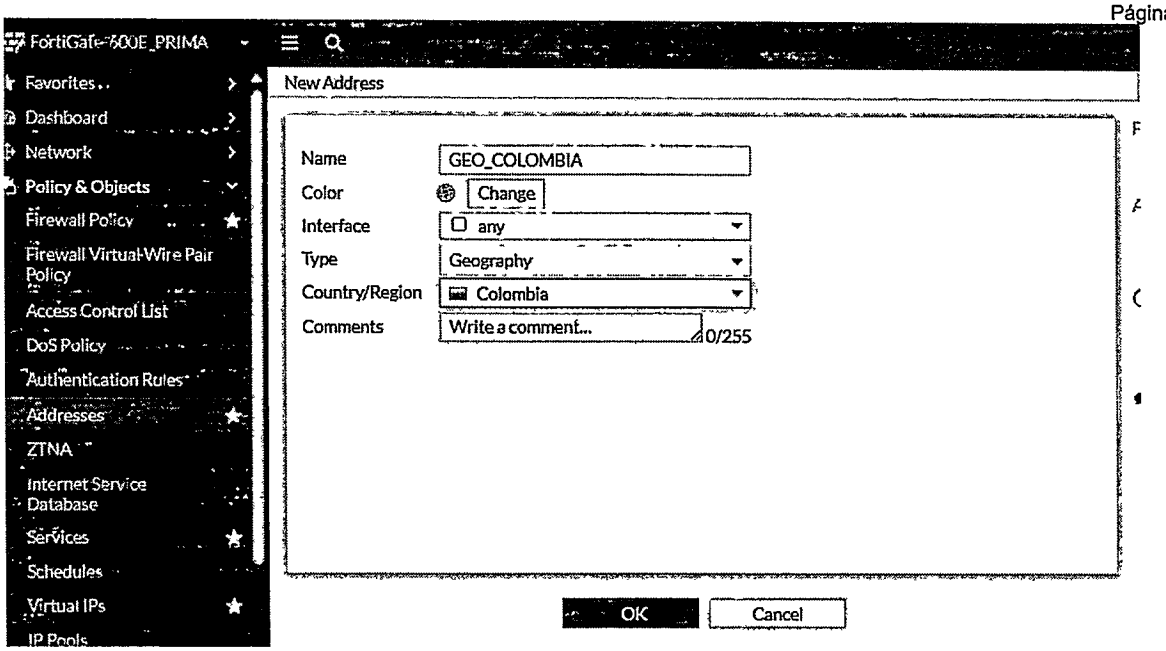


Imagen 6.2 – Creación de la Zona Geografica de Colombia

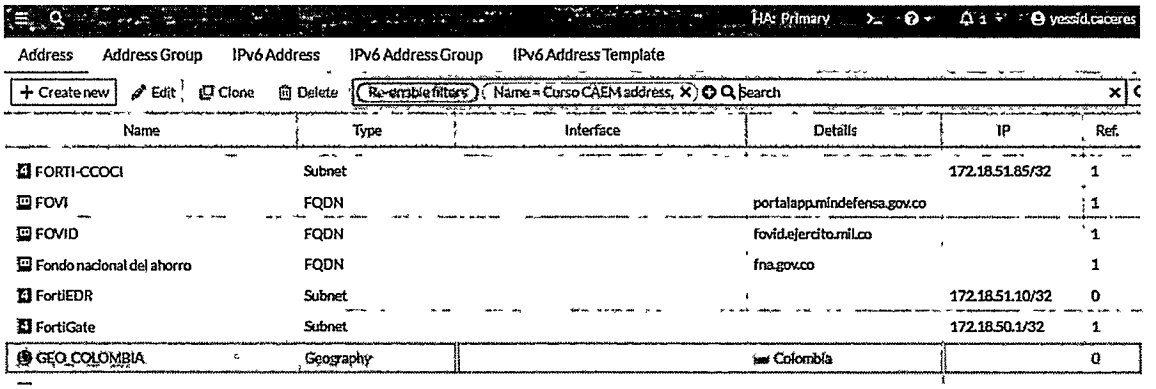


Imagen 6.3 – Zona Geografica de Colombia creada

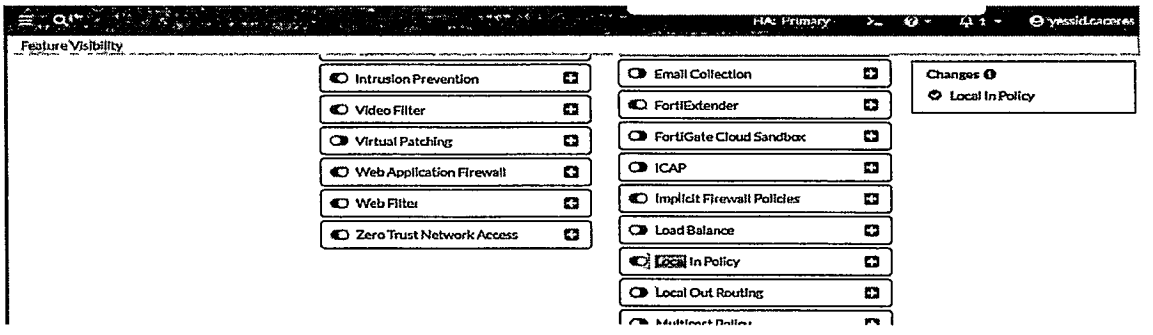


Imagen 6.4 - Activación de Local In Policy

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

6.3. Ajuste explícito de Local-In Policy para SSL-VPN:

Se definieron reglas específicas para el puerto 21443 (SSL-VPN), aceptando únicamente los orígenes autorizados y denegando de forma explícita cualquier otro intento externo, eliminando la permisividad implícita observada bajo policyid=0.

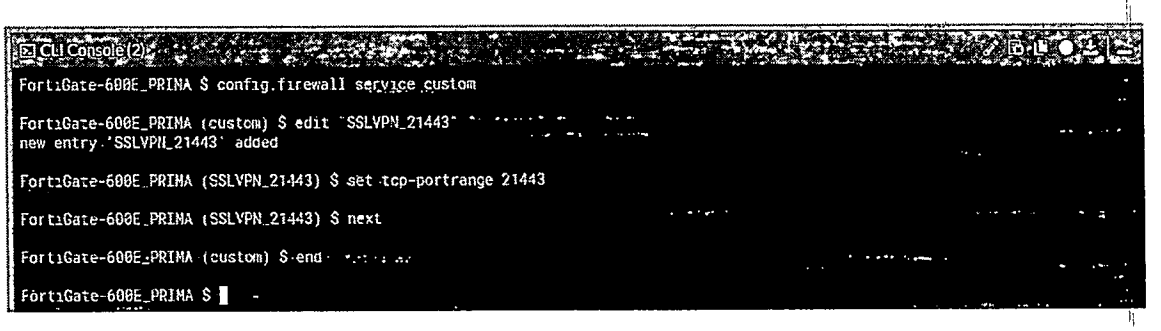


Imagen 6.5 – Creación del servicio 21443 para su implementación en el bloqueo

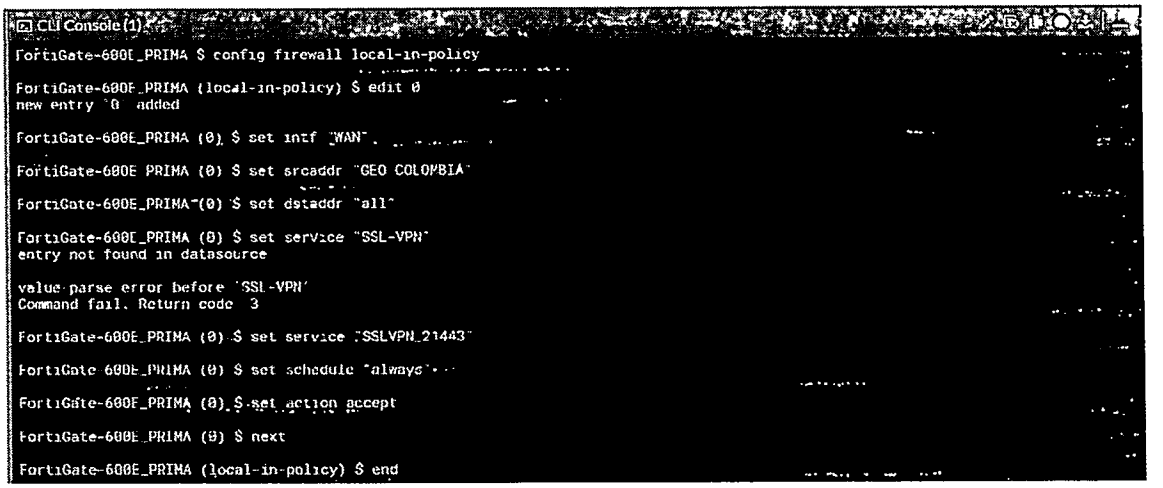


Imagen 6.6 – Creación de la política de permitir conexión solo desde Colombia

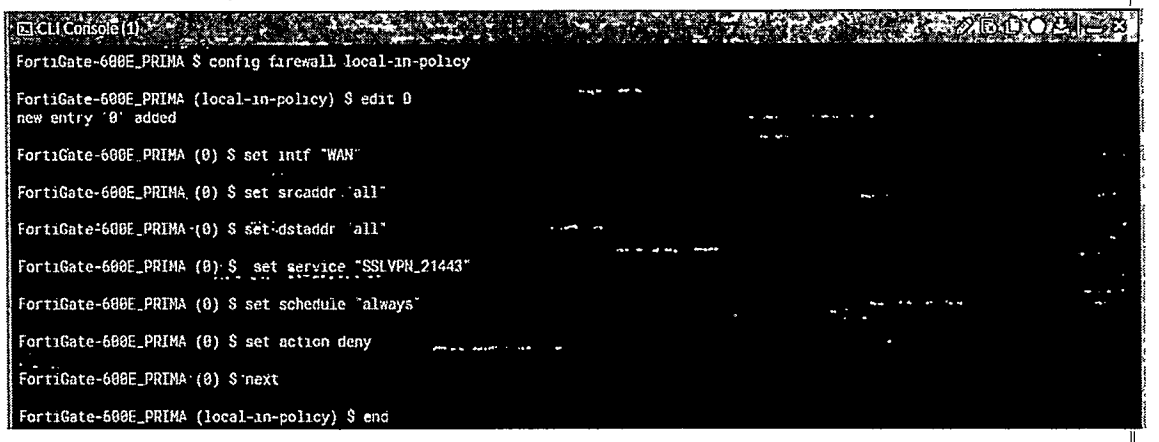


Imagen 6.7 – Creación de la política de denegación de conexión fuera de Colombia

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Imagen 6.8 – Verificación de la Creación de las política de conexión y denegación de conexión

6.4. Revisión de exposición del plano administrativo:

Se verificó que el puerto 21443 corresponde exclusivamente al servicio SSL-VPN y no a la administración directa del equipo. Se programó el cambio del puerto actual por uno no estándar, previa notificación a los directivos institucionales, con el fin de evitar afectaciones operativas previa coordinación con mi Te Ramírez Flor Enrique..

6.5. Plan de implementación de MFA:

Se programó la implementación de Autenticación de Doble Factor (MFA) previa coordinación con mi Te Ramírez Flor Enrique, para el servicio SSL-VPN mediante FortiToken o solución equivalente, la cual será ejecutada en el transcurso de la presente semana, previa coordinación con los usuarios y directivos autorizados. Esta medida tiene como finalidad reforzar el mecanismo de autenticación y mitigar el riesgo asociado a intentos de validación masiva de credenciales.Estado actual del riesgo

Con las medidas implementadas:

- El acceso al servicio SSL-VPN desde orígenes no autorizados queda bloqueado a nivel de plano de control.
- No se evidenció autenticación exitosa ni establecimiento de túnel.
- No se identificó explotación de vulnerabilidad ni ejecución remota de código.

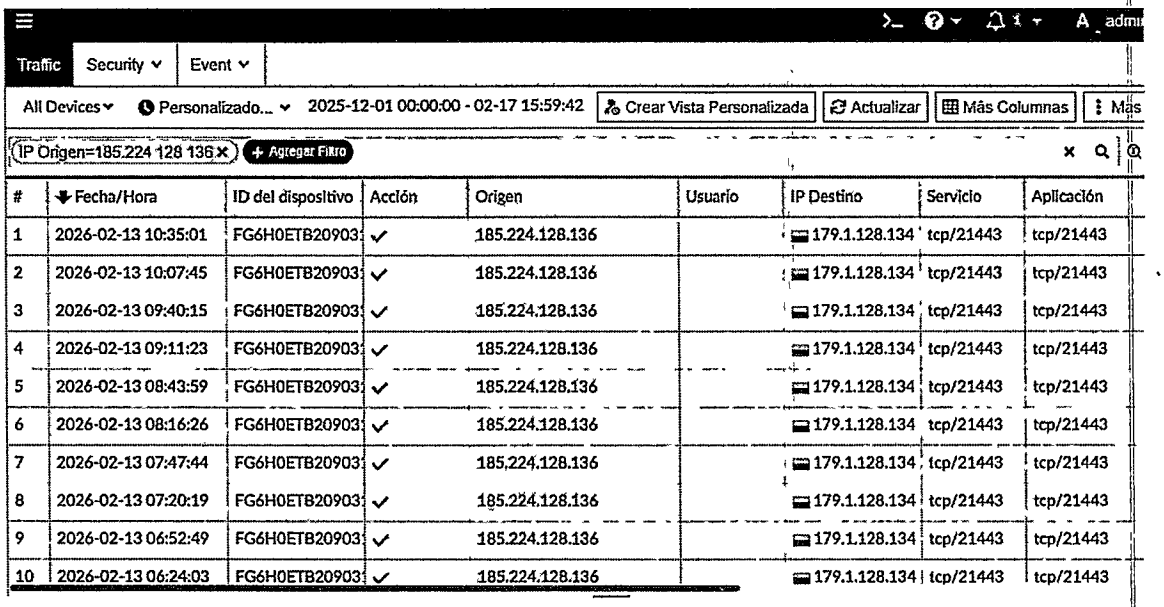
"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

- El evento se clasifica como actividad de reconocimiento externo, mitigada mediante endurecimiento de políticas de acceso.

En consecuencia, el incidente no derivó en compromiso de la infraestructura institucional y se encuentra contenido conforme a las acciones descritas.

7. Caso ID: ##378383## – Evento de tráfico permitido identificado como IPSum Malware IP

En atención a los eventos reportados en el Caso ID: ##378383## – Radicado No. 0126001351402, se realizó la verificación técnica de un evento de tráfico permitido hacia el plano de control del dispositivo FortiGate 600E, identificado por el SIEM bajo la alerta "Permitted Traffic from IPSum Malware IP".



#	Fecha/Hora	ID del dispositivo	Acción	Origen	Usuario	IP Destino	Servicio	Aplicación
1	2026-02-13 10:35:01	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
2	2026-02-13 10:07:45	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
3	2026-02-13 09:40:15	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
4	2026-02-13 09:11:23	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
5	2026-02-13 08:43:59	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
6	2026-02-13 08:16:26	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
7	2026-02-13 07:47:44	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
8	2026-02-13 07:20:19	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
9	2026-02-13 06:52:49	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443
10	2026-02-13 06:24:03	FG6H0ETB20903	✓	185.224.128.136		179.1.128.134	tcp/21443	tcp/21443

Imagen 6.9 – Verificación de la Creación de las política de conexión y denegación de conexión

El registro evidencia que el tráfico fue procesado bajo subtype="local" y policytype="local-in-policy" (policyid=0), lo que confirma que la comunicación fue dirigida directamente al dispositivo y no a infraestructura interna. Aunque se registró un intercambio inicial de paquetes (sentpkt=10 / rcvdpkt=11), la sesión finalizó mediante client-rst, sin autenticación exitosa ni establecimiento de túnel VPN.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Del análisis técnico se determinó que el comportamiento corresponde a una actividad de reconocimiento o intento de negociación inicial del servicio SSL-VPN, sin evidencia de explotación de vulnerabilidad ni compromiso del sistema.

7.1. Verificación de bloqueo previo:

Se confirmó que la IP 185.224.128.136 ya se encontraba bloqueada a nivel perimetral como parte de las acciones ejecutadas en el Caso ID ##378370##, asociado a intentos de fuerza bruta contra el servicio SSL-VPN.

Imagen 7.2 – Bloueo previo de la IP con Threat Feeds

7.2. Implementación de geobloqueo en Local-In Policy:

Se configuró una política de tráfico entrante (Local-In Policy) para el servicio SSL-VPN en la interfaz WAN, permitiendo únicamente conexiones provenientes de Colombia y bloqueando explícitamente el resto de orígenes no autorizados. Con esta medida, cualquier intento de negociación desde países no permitidos es rechazado antes de que alcance el servicio.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

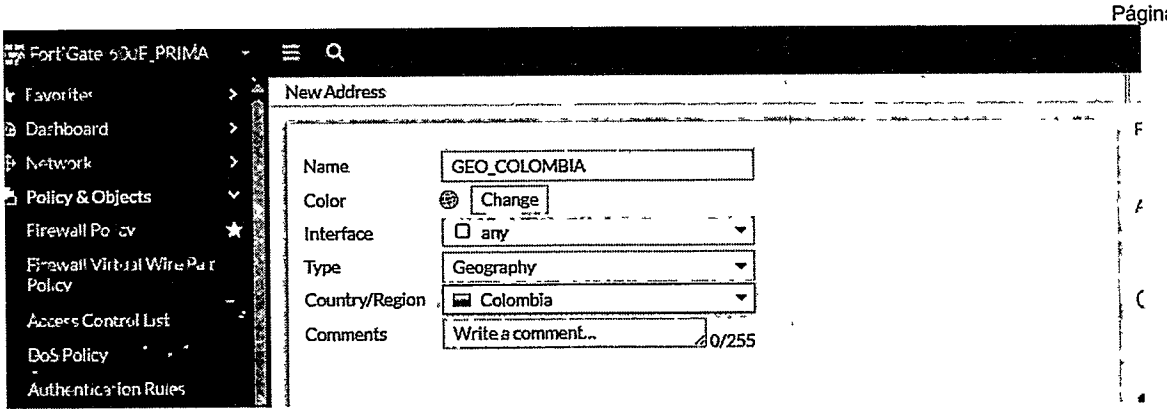


Imagen 7.3 – Creación de la Zona Geografica de Colombia

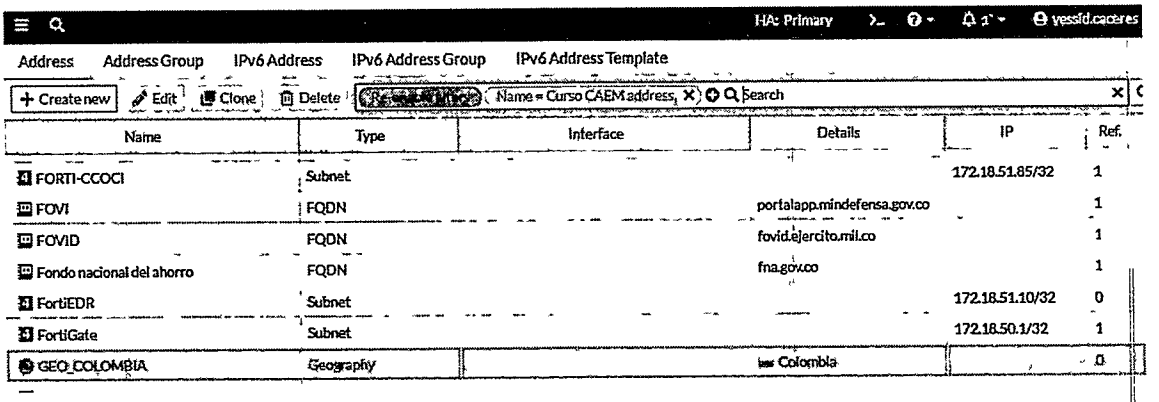


Imagen 3 – Zona Geográfica de Colombia creada

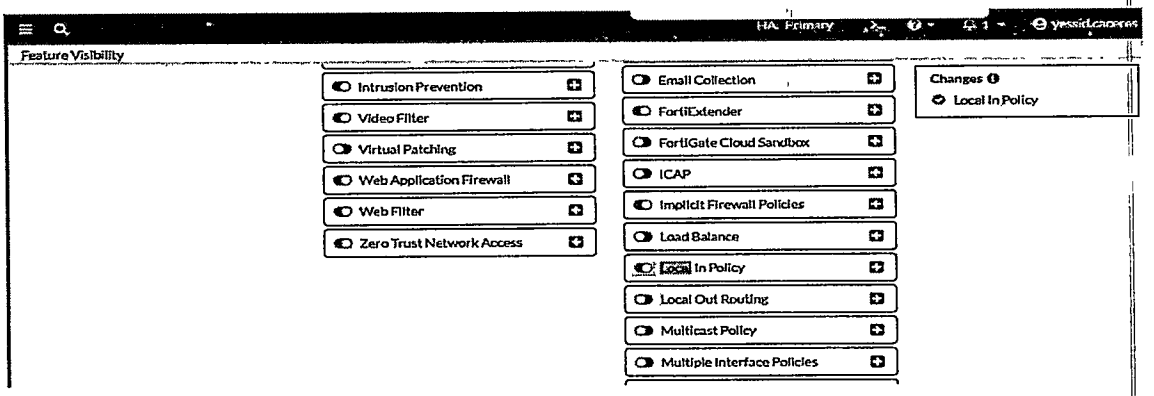


Imagen 4 - Activación de Local In Policy

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

7.3. Ajuste explícito de Local-In Policy para SSL-VPN:

Se definieron reglas específicas para el puerto 21443 (SSL-VPN), aceptando únicamente los orígenes autorizados y denegando de forma explícita cualquier otro intento externo, eliminando la permisividad implícita observada bajo policyid=0.

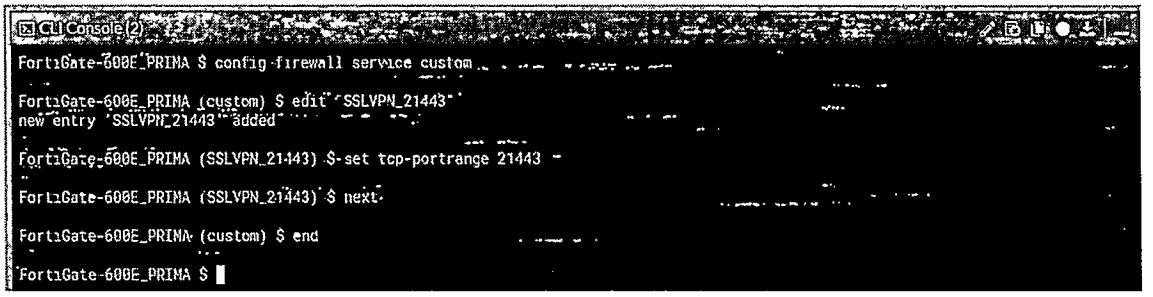


Imagen 5 – Creación del servicio 21443 para su implementación en el bloqueo

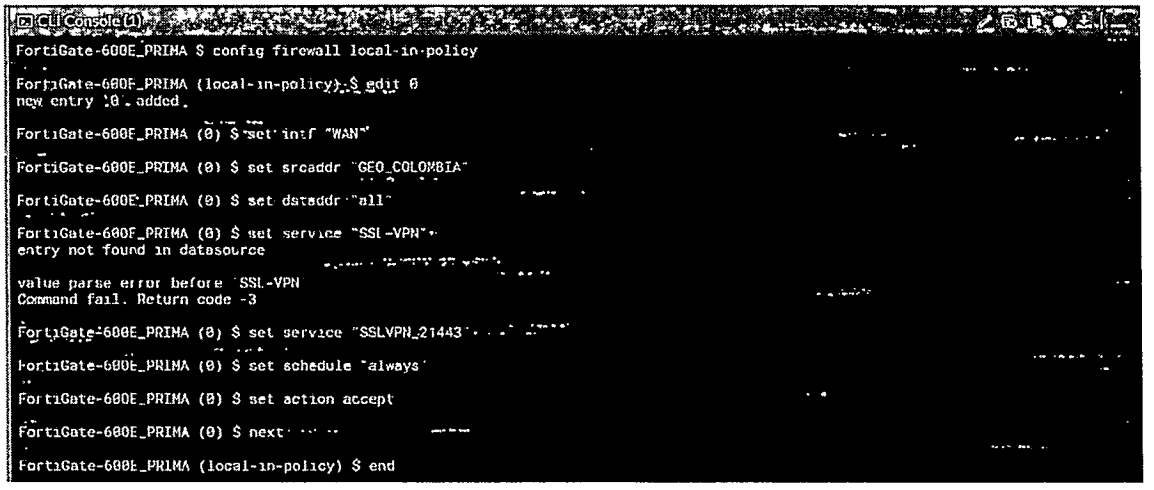


Imagen 6 – Creación de la política de permitir conexión solo desde Colombia

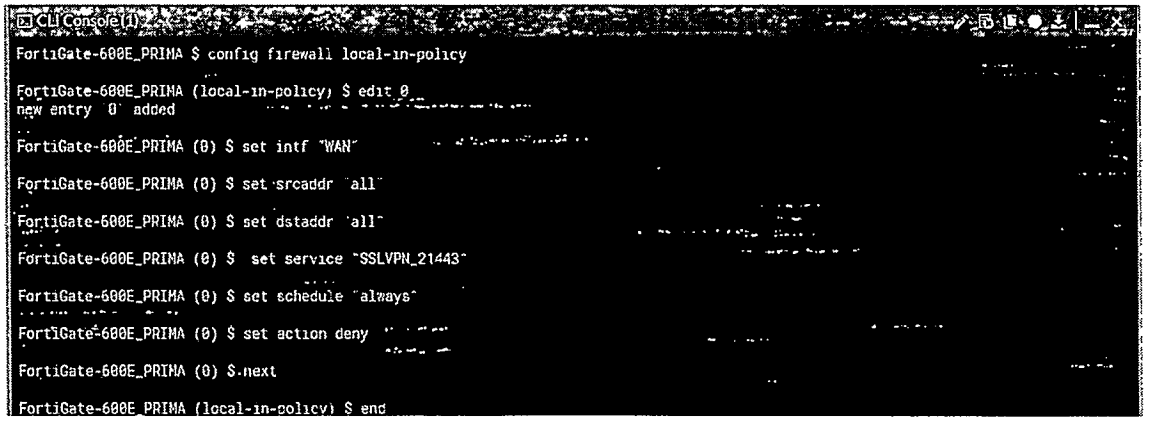


Imagen 7 – Creación de la política de denegación de conexión fuera de Colombia

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

Imagen 8 – Verificación de la Creación de las política de conexión y denegación de conexión

7.4. Revisión de exposición del plano administrativo:

Se verificó que el puerto 21443 corresponde exclusivamente al servicio SSL-VPN y no a la administración directa del equipo. Se programó el cambio del puerto actual por uno no estándar, previa notificación a los directivos institucionales, con el fin de evitar afectaciones operativas previa coordinación con mi Te Ramírez Flor Enrique..

7.5. Plan de implementación de MFA:

Se programó la implementación de Autenticación de Doble Factor (MFA) previa coordinación con mi Te Ramírez Flor Enrique, para el servicio SSL-VPN mediante FortiToken o solución equivalente, la cual será ejecutada en el transcurso de la presente semana, previa coordinación con los usuarios y directivos autorizados. Esta medida tiene como finalidad reforzar el mecanismo de autenticación y mitigar el riesgo asociado a intentos de validación masiva de credenciales.Estado actual del riesgo

Con las medidas implementadas:

- El acceso al servicio SSL-VPN desde orígenes no autorizados queda bloqueado a nivel de plano de control.
- No se evidenció autenticación exitosa ni establecimiento de túnel.
- No se identificó explotación de vulnerabilidad ni ejecución remota de código.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

- El evento se clasifica como actividad de reconocimiento externo, mitigada mediante endurecimiento de políticas de acceso.

En consecuencia, el incidente no derivó en compromiso de la infraestructura institucional y se encuentra contenido conforme a las acciones descritas.

El evento analizado corresponde a una conexión proveniente de la dirección IP 185.224.128.136, geolocalizada en Países Bajos, dirigida al puerto 21443 de la IP pública institucional, puerto configurado para el servicio SSL-VPN del firewall FortiGate 600E. Dicho evento fue detectado el 13 de febrero, por lo cual se realizó la verificación de los registros correspondientes en el FortiGate 600E y su correlación en el FortiAnalyzer, procediéndose como medida preventiva al bloqueo inmediato de la dirección IP a nivel perimetral, con el fin de evitar nuevos intentos de conexión hacia el servicio expuesto y reforzar las medidas de seguridad sobre la infraestructura institucional.

Nombre: YESSID ARAMIS CACERES VASQUEZ
Tipo y No. Documento CC. 72.342.326
Ingeniero de Sistemas DETIC - ESDEG

Atentamente,

Archivado en: 15.103.12.5 Contrato de prestación de servicios 2026.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

SuAporte | REPORTE INDIVIDUAL

Fecha creación reporte 2026-03-17, 09:15:00 AM **Tipo Planilla** I **Número Planilla** 84449480

Periodo Cotización 202602 **Periodo Servicio** 202602

Cliente:

PAGADA 2026-03-17

I. DATOS DEL APORTANTE

Razón Social	CACERES VASQUEZ YESSID ARAMIS				
Documento	CC 72342326	**Dirección**	CR 116A #15 C - 70 BLOQUE 10 APTO 603		
Tipo de Empresa	INDEPENDIENTE	**Teléfono**	3907300		
Tipo Persona	NATURAL	**Forma Presentación**	ÚNICO	**Total Afiliados**	1
Ciudad	BOGOTA D.C.	**Departamento**	BOGOTA D.C.		
Representante Legal		**Identificación**			

II. DATOS DEL AFILIADO

Documento	CC 72342326		**Residente**		**Exonerado**	N	**Apellidos y Nombres**	**Código Ciudad - Departamento**	**Centro de Trabajo**	**Ubicación Laboral**
Tipo Cotizante	59	00					CACERES VASQUEZ YESSID ARAMIS	11001000 - 11		BOGOTA D.C.

III. APORTE POR CADA UNA DE LAS ADMINISTRADORAS ASOCIADAS AL AFILIADO:

Novedades																			Extranjero	Tipo salario	Salario	Pensión							Salud						Riesgos					Caja				Parafiscales			
ING	RET	TDE	TAE	TDP	TAP	VSP	COR	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRP	Días AFP	Días EPS	Días ARP	Días CCF			Código AFP	Código Tras. AFP	Tarifa AFP	IBC	Total Aporte AFP	Total Aporte FSP	Total Aporte FSPS	Código EPS	Código Tras. EPS	Tarifa EPS	IBC EPS	Aporte Salud	Aporte UPC	Código ARL	Clase Riesgo	Tarifa ARL	IBC ARL	Aporte Riesgos	Código CCF	Tarifa CCF	IBC CCF	Aporte Caja	Tarifa SENA	Aporte SENA	Tarifa ICBF	Aporte ICBF
X															0	30	30	30	0			231001		16 %	$ 3.971.600	$ 635.500	$ 0	$ 0	EPS005		12,5 %	$ 3.971.600	$ 496.500	$ 0	14-11	1	0,522 %	$ 3.971.600	$ 20.800	NIN-CC	0 %	$ 0	$ 0	0 %	$ 0	0 %	$ 0

IV.TOTALES

Total Aportes Pensión	Total Aportes FSP	Total Aportes FSPS	Total Aportes Salud	Total Aportes Riesgos	Total Aportes Cajas	Total Aportes SENA	Total Aportes ICBF	Total Aportes ESAP	Total Aportes MEN	Total Final
COLFONDOS	FSP SOLIDARIDAD	FSP SUBSISTENCIA	EPS SANITAS	ARL SURA	NINGUNA CCF	SENA	ICBF	ESAP	MEN	
$ 635.500	$ 0	$ 0	$ 496.500	$ 20.800	$ 0	$ 0	$ 0	$ 0	$ 0	$ 1.152.800

Enlace Operativo – Línea Expertos en PILA: Barranquilla (605) 385 24 44 · Bogotá (601) 742 44 88 · Bucaramanga (607) 697 87 27 · Cali (602) 485 94 44 · Cartagena (605) 693 77 27 · Pereira (606) 340 13 27 · Manizales (606) 892 80 27 · Medellín (604) 604 27 27 · Desde otras ciudades: 01 8000 51 99 77 · WhatsApp: 3164416952

EXPERTOS en PILA

enlace operativo

SuAporte | AUTOLIQUIDACION CONSOLIDADA

Fecha creación reporte: 2026-03-19, 12:01:51 PM **Tipo Planilla:** I: PLANILLA INDEPENDIENTES **Numéro Planilla:** 84510656

Periodo Cotización: enero de 2026 **Periodo Servicio:** enero de 2026

PAGADO 19/03/2026

I. DATOS DEL APORTANTE

Razón Social	CACERES VASQUEZ YESSID ARAMIS		
Documento	CC72342326	**Dirección**	CR 116A #15 C - 70 BLOQUE 10 APTO 603
Tipo de Empresa	INDEPENDIENTE	**Teléfono**	3907300
Tipo Persona	NATURAL	**Forma Presentación**	ÚNICO
Ciudad	BOGOTA D.C.	**Departamento**	BOGOTA D.C.
Representante Legal		**Identificación**	
Total Afiliados	1	**ARP**	NINGUNA ARP

I. DETALLE DEL APORTANTE

Datos del Afiliado				Novedades																		Pensiones			Salud			Riesgos			Cajas			Parafiscales			
Identificación	Apellidos y Nombres	Tipo Cotizante	Subtipo Cotizante	ING	RET	RET P	TDE	TAE	TDP	TAP	VSP	COR	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRP	Días APP	Días EPS	Días ARP	Días CCF	Administradora	IBC Pensión	Aporte Pensión	Administradora	IBC Salud	Aporte Salud	Tarifa	IBC Riesgos	Aporte Riesgos	Administradora	IBC Caja	Aporte Caja	Aporte SENA	Aporte ICBF	ESAP	Apo Mini
72342326	YESSID ARAMIS CACERES VASQUEZ	03	00	X																	0	4	4	0	0	(231001) COLFONDOS	$ 233,454	$ 37,400	(EPS005) EPS SANITAS	$ 233,454	$ 29,200	0,000	$ 0	$ 0	(NIN-CC) NINGUNA CCF	$ 0	$ 0	$ 0	$ 0	$ 0	

III.TOTALES

IBC Pensión	IBC Salud	IBC Riesgos	IBC Cajas	Aportes Pensión	Aportes Salud	Aportes Riesgos	Aportes Cajas	Aportes Sena	Aportes ICBF	Aportes ESAP	Aportes Min Educación	(Incapacidades, Licencias, Saldos a Favor) EPS	Incapacidades ARP	SUBTOTAL SIN INTERESES DE MORA	TOTAL INTERESES DE MORA	TOTAL FINAL
$ 233.454	$ 233.454	$ 0	$ 0	$ 37.400	$ 29.200	$ 0	$ 0	$ 0	$ 0	$ 0	$ 0	$ 0	$ 0	$ 66.600	$ 1.800	$ 68.400

Enlace Operativo – Línea Expertos en PILA: Barranquilla (605) 385 24 44 · Bogotá (601) 742 44 88 · Bucaramanga (607) 697 87 27 · Cali (602) 485 94 44 · Cartagena (605) 693 77 27 · Pereira (606) 340 13 27 · Manizales (606) 892 80 27 · Medellín (604) 604 27 27 · Desde otras ciudades: 01 8000 51 99 77 · WhatsApp: 3164416952

Antes de imprimir, asegúrese que sea realmente necesario. Proteger el medio ambiente está en nuestras manos.

CERTIFICACIÓN APLICACIÓN

Decreto No. 2231 del 22 de diciembre del 2023

Yo YESSID ARAMIS CÁCERES VÁSQUEZ en mi calidad de prestador de servicios de **LA ESCUELA SUPERIOR DE GUERRA "RAFAEL REYES PRIETO".**, certifico bajo la gravedad de juramento que los ingresos recibidos como persona natural por concepto de renta de trabajo no proveniente de una relación laboral, legal o reglamentaria correspondiente a los servicios prestados a la **ESCUELA SUPERIOR DE GUERRA "RAFAEL REYES PRIETO"** durante el año 2026 se les dará el siguiente tratamiento:

Seleccione con una X el tratamiento que dará a sus ingresos en la declaración de renta:

a. Se restará el 25% de renta exenta asociada a estas rentas en desarrollo de mi actividad **(numeral 10 del artículo 206 del estatuto tributario)** [X]

b. Se tomarán costos o deducciones asociados a estas rentas en desarrollo de mi actividad. [ ]

Esta certificación se expide a los 18 días del mes de marzo del año 2026

Firma: _____

Nombres y Apellidos: YESSID ARAMIS CÁCERES VASQUEZ

No. de Cédula: 72342326

Con el fin de atender lo establecido en la Ley 2277 del año 2022 (Reforma tributaria) reglamentada con él con el Decreto 2231 de diciembre 22 de 2023 el cual se definirá si durante el año 2024 a las personas naturales residentes del régimen ordinario que obtengan ingresos por rentas de trabajo no laborales (honorarios. comisiones, servicios. emolumentos, etc.) se les practicaría la retención en la fuente a título de renta con la tabla del artículo 383 del ET (a) o con las tarifas del artículo 392 del ET y sus decretos reglamentarios (b)

COMANDO GENERAL

ENTRADA DE BIENES
POR CONCEPTO DE: ENTRADA DE SERVICIOS

Doc. Material
5003868590-2026
MOVIMIENTO: ML81N

...DAD	NIT	CODIGO	ALMACEN	FECHA	CIUDAD
Escuela Superior de Guerra	830002634-1	ESSG		19.03.2026	Bogota

PROVEEDOR	NIT	CODIGO	No. PEDIDO	DESTINO
CÃ#CERES VÃ#SQUEZ YESSID ARAMI	72342326		4500554513	

TRAZABILIDAD: PAGO 2 / 052-MDN-COGFM-ESDEG-2026 / PROFESIONALES ASISTENCIALES

MATNR	LOTE/UBIC	EQUIPO	No.PARTE	DESCRIPCION	IMPUTACN./SERIE	CANT	UD	VR.UNITARIO	VR.TOTAL
				YESSID ARAMIS CACERES VASQUE		1,00	UN	5.425.000,00	5.425.000,00

TOTALES 5.425.000,00

MONTO: CINCO MILLONES CUATROCIENTOS VEINTICINCO MIL PESOS CON- CERO /100 M.CTE

RECIBI

ALMACENISTA

POST-FIRMA

Fecha: 24.03.2026 14:45:19 DANIMARC

SIIF Nación

Cuenta por pagar Comprobante

Usuario Solicitante:	MHlcortez	LUIS HERNANDO CORTES LEON
Unidad ó Subunidad Ejecutora Solicitante:	15-01-02-001	ESCUELA SUPERIOR DE GUERRA
Fecha y Hora Sistema:	2026-03-19-3:22 p. m.	

CUENTAS POR PAGAR

Número:	31726	Fecha Registro:	2026-03-19	Unidad / Subunidad Ejecutora:	15-01-02-001 ESCUELA SUPERIOR DE GUERRA		
Estado:	Radicada	Tipo de Cuenta x Pagar:	Rentas de trabajo NO obligados a facturar	Nro. Compromiso:	7026	Nro. Cdp:	6926
Caja Menor-Identif.:		Caja Menor-Fecha Registro:		Tipo de Moneda:	COP-Pesos	Tasa de Cambio:	0,00
Valor Antes del Iva:	5.425.000,00	Valor Iva:	0,00	Valor Total:	5.425.000,00	Valor Total Moneda Original:	0,00

TERCERO

Identificación:	72342326	Razón Social:	YESSID ARAMIS CACERES VASQUEZ

DOCUMENTOS SOPORTE RECIBIDOS

CODIGO	DESCRIPCION
11	CUENTA DE COBRO

Objeto.:	052-MDN-COGFM-ESDEG-2026

LUIS HERNANDO CORTÉS LEÓN
CC 3.159.633 DE SAN FRANCISCO CUND.

SIIF Nación

Anexo Obligación

Usuario Solicitante:	MHnvillar	NELCY JOHANA VILLAR PEREZ
Unidad ó Subunidad Ejecutora Solicitante:	15-01-02-001	ESCUELA SUPERIOR DE GUERRA
Fecha y Hora Sistema:	2026-03-24-11:20 a. m.	

ANEXO COMPROBANTE OBLIGACION

Numero:	31326	**Fecha Registro:**	2026-03-20	**Unidad / Subunidad ejecutora:**	15-01-02-001 ESCUELA SUPERIOR DE GUERRA			
Vigencia Presupuestal	Actual	**Estado:**	Generada	**Requiere DIP:** No	**Nro. Compromiso:**	7026	**Nro. Cdp:**	6926
Valor Inicial:	5.425.000,00	**Valor Total Operaciones:**	0,00		**Valor Actual:**	5.425.000,00	**Atributo Contable:**	05-NINGUNO
Valor Deducciones:	46.322,00	**Valor Neto:**	5.378.678,00		**Saldo x Ordenar:**	5.425.000,00	**Comprobante Contable:**	141164

TERCERO

Identificacion:	72342326	**Razon Social:**	YESSID ARAMIS CACERES VASQUEZ	**Medio de Pago:**	Abono en cuenta

DOCUMENTO SOPORTE

Numero:	PAGO 2 CTTO 052/2026	**Tipo:**	CONTRATO DE PRESTACION DE SERVICIOS - PROFESIONALES	**Fecha:**	2026-03-20

AFECTACIONES CONTABLES -Comprobante 141164 EPG066 - Registro Obligación Presupuestal con Deducciones con marca aplica usos contables

Código	Descripción	Debe	Haber
243627001	Retenido	0,00	46.322,00
249054001	Honorarios	0,00	5.378.678,00
511179001	Honorarios	5.425.000,00	0,00
	Sumatoria	5.425.000,00	5.425.000,00

USOS PRESUPUESTALES

ITEM DE AFECTACION DE GASTO						USOS PRESUPUESTALES		
DEPENDENCIA	**POSICION CATALOGO DE GASTO**	**FUENTE**	**RECURSO**	**SITUAC.**	**VALOR**	**RUBRO**	**DESCRIPCION**	**VALOR**
001 ESCUELA SUPERIOR DE GUERRA	A-02-02-02-008-003 SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS SERVICIOS DE INVESTIGACION, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)	Nación	10	CSF	5.425.000,00	A-02-02-02-008-003-09	OTROS SERVICIOS PROFESIONALES, TÉCNICOS Y EMPRESARIALES N.C.P.	5.425.000,00

Objeto:	

PD. ALBERTO MORA CASTAÑEDA
CONTADOR - ESDEG-

SIIF Nación

Obligación Presupuestal Comprobante

Usuario Solicitante: MHjlopezl JAIRO ALEJANDRO LOPEZ LARA
Unidad ó Subunidad Ejecutora Solicitante: 15-01-02-001 ESCUELA SUPERIOR DE GUERRA
Fecha y Hora Sistema: 2026-03-24-11:32 a. m.

REGISTRO PRESUPUESTAL DE OBLIGACION.

Numero:	31326	**Fecha Registro:**	2026-03-20	**Unidad / Subunidad ejecutora:**		15-01-02-001 ESCUELA SUPERIOR DE GUERRA			
Vigencia Presupuestal	Actual	**Estado:**	Generada	**Requier**	No	**Tipo de DIP:**		**Nro. Compromiso:**	7026
Valor Inicial:	5.425.000,00	**Valor Total Operaciones:**	0,00			**Valor Actual:**	5.425.000,00	**Saldo x Ordenar:**	5.425.000,00
Valor Inicial Moneda	0,00	**Valor Total Operaciones Moneda**	0,00			**Valor Actual**	0,00	**Saldo x Ordenar**	0,00
Valor Deducciones:	46.322,00	**Valor Neto:**	5.378.678,00			**Valor IVA:**	0,00	**Nro. Cdp:**	6926
Valor Deducciones	0,00	**Valor Neto Moneda:**	0,00			**Atributo**	05-NINGUNO	**Comprobante**	141164

TERCERO

Identificacion:	72342326	**Razon Social:**	YESSID ARAMIS CACERES VASQUEZ	**Medio de Pago:**	Abono en cuenta

CUENTA BANCARIA

Numero:	91230625595	**Banco:**	BANCOLOMBIA S.A.	**Tipo:**	Ahorro	**Estado:**	Activa

CUENTA X PAGAR				**CAJA MENOR**			
Numero:	31726	**Tipo:**	Rentas de trabajo	**Identificacion:**		**Fecha de Registro:**	

DOCUMENTO SOPORTE

Numero:	PAGO 2 CTTO 052/2026	**Tipo:**	CONTRATO DE PRESTACION DE SERVICIOS - PROFESIONALES	**Fecha:**	2026-03-20

ITEM PARA AFECTACION DE GASTO

DEPENDENCIA	POSICION CATALOGO DE GASTO	FUENTE	RECURSO	SITUAC.	ATRIBUTO CONTABLE	FECHA OPERACION	VALOR INICIAL	VALOR OPERACION	VALOR ACTUAL	SALDO X ORDENAR
001 ESCUELA SUPERIOR DE GUERRA	A-02-02-02-008-003 SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS SERVICIOS DE INVESTIGACION, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)	Nación	10	CSF	05-NINGUNO					
						Total:	5.425.000,00	0,00	5.425.000,00	5.425.000,00

Objeto:	

PLAN DE PAGOS

DEPENDENCIA DE AFECTACION DE PAC	POSICION DEL CATALOGO DE PAC	FECHA DE PAGO	ESTADO	VALOR A PAGAR
001 ESCUELA SUPERIOR DE GUERRA	1-2 ANC - GASTOS GENERALES NACION CSF	2026-03-20	Generada	5.425.000,00

POSICIONES DEL CATALOGO PARA PAGO NO PRESUPUESTAL

POSICION DEL CATALOGO DE PAGO	IDENTIFICACION	NOMBRE BENEFICIARIO	BASE GRAVABLE	TARIFA	VALOR	SALDO
2-01-05-01-01-03-05 RETENCION ICA COMERCIAL SERVICIOS DEMÁS ACTIVIDADES DE SERVICIOS	NIT 899999061	BOGOTA DISTRITO CAPITAL	4.795.250,00	0,966 %	46.322,00	46.322,00

CF. CLAUDIA PATRICIA PEREZ RODRIGUEZ
JEFE DEPARTAMENTO ADMINISTRATIVO Y ORDENADOR DEL GASTO ESDEG

SIIF Nación

Orden de pago Presupuestal de gastos Comprobante

Usuario Solicitante: MHjduranp JOHN EDINSON DURAN PLATA
Unidad ó Subunidad Ejecutora Solicitante: 15-01-02-001 ESCUELA SUPERIOR DE GUERRA
Fecha y Hora Sistema: 2026-04-08-11:29 a. m.

ORDEN DE PAGO PRESUPUESTAL

Número:	89313226	Fecha Registro:	2026-03-24	Unidad / Subunidad ejecutora:	15-01-02-001 ESCUELA SUPERIOR DE GUERRA		
Vigencia Presupuestal	Actual	Estado:	Pagada	Nro Obligación:	31326	Comprobante Contable de la Generación:	
Fecha Máxima Pago:	2026-03-26	Código de Referencia:	04500079700089313226	Tipo de Moneda:	COP-Pesos	Tasa de Cambio:	0,00
Valor Bruto:	5.425.000,00	Valor Deducciones:	46.322,00	Valor Neto:	5.378.678,00	Saldo x Pagar:	0,00

VALORES PAGADOS

TRM Pago		Valor Bruto	5.425.000,00	Valor Deducciones	46.322,00	Valor Neto	5.378.678,00	Moneda Base Compra		Valor MBC

REINTEGROS

Números				No Recaudo:	
Bruto Reintegrado Pesos:	0,00	Reintegrado Deducciones Pesos:	0,00	Reintegrado Neto Pesos:	0,00
Bruto Reintegrado Moneda:	0,00	Reintegrado Deducciones Moneda:	0,00	Reintegrado Neto Moneda:	0,00

TERCERO DE LA ORDEN DE PAGO

Identificación:	72342326	Razón Social:	YESSID ARAMIS CACERES VASQUEZ	Medio de Pago:	Abono en cuenta

CUENTA BANCARIA

Número:	91230625595	Banco:	BANCOLOMBIA S.A.	Tipo:	Ahorro	Estado:	Activa

TESORERIA	DOCUMENTO SOPORTE				
13-01-01-DT - DIRECCION TESORO NACION DGCPTN	Número:	052-MDN-CUGFM-ESDEG-2026	Tipo:	CONTRATO DE PRESTACION	Fecha: 2026-03-24

Tipo Beneficiario Pago: 01 - Beneficiario final

ITEM PARA AFECTACION DE GASTOS

DEPENDENCIA / POSICION CATALOGO DE GASTO	FUENTE	REC	SIT	VALOR		VALOR PAGADO	VALOR REINTEGRADO		USO DE PROYECTOS ESPECIALES			
				PESOS	MONEDA	PESOS	PESOS	MONEDA EXTRANJERA	USO DE PROYECTO	MONEDA	TASA DE CAMBIO	VALOR MONEDA
001 ESCUELA SUPERIOR DE GUERRA / A-02-02-02-008-003 SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS SERVICIOS DE INVESTIGACION, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)												
	Nación	10	CSF	5.425.000,00	0,00	5.425.000,00				Pesos	0,00	0,00

DEDUCCIONES

POSICIONES DEL CATALOGO PARA PAGO NO PRESUPUESTALES		TERCERO		TARIFA	VALOR	VALOR AJUSTADO PAGO	VALOR REINTEGRADO
2-01-05-01-01-03-05	RETENCION ICA COMERCIAL SERVICIOS DEMÁS ACTIVIDADES DE SERVICIOS	899999061	BOGOTA DISTRITO CAPITAL	0,966 %	46.322,00	46.322,00	

LINEAS DE PAGO VINCULADA

DEPENDENCIA PARA AFECTACION DE PAC	POSICION DEL CATALOGO DE PAC	FECHA	VALOR	ATRIBUTO LINEA DE PAGO	ESTADO
001 - ESCUELA SUPERIOR DE GUERRA	1-2 - ANC - GASTOS GENERALES NACION CSF	2026-03-20	5.425.000,00	05 NINGUNO	Pagada

SV. JOHN EDINSON DURAN PLATA
TESORERO ESDEG