



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

Bogotá D.C. FECHA: febrero 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. 01 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. 1 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 ✓



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

Recurso presupuestal	R10
Forma Y Condiciones De Pago	<p>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.</p> <p>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.</p> <p>PARÁGRAFO PRIMERO: Para el primer informe de supervisión se deberá allegar:</p> <p>Acta de capacitación relacionada con: Sistema de Gestión de Seguridad y Salud en el Trabajo. Compromiso anticorrupción</p> <p>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).</p> <p>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).</p> <p>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.</p> <p>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</p>

FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

Página 3 de 7

	<p>conformidad con lo señalado sobre el particular por Colombia Compra Eficiente.</p> <p>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.</p> <p>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.</p> <p>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.</p>				
Modificadorio	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 (+ modificadorio)	NO APLICA				
Plazo De Ejecución Final (+ modificadorio)	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				



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

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 ESPECÍFICAS
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.



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

Página 5 de 7

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.	Realizar la verificación integral del estado de la plataforma tecnológica y de copias de seguridad, incluyendo Veeam Backup, ExaGrid y almacenamiento Hitachi, así como la validación de las barreras perimetrales (FortiGate 600E en alta disponibilidad, FortiSwitch y FortiAP), asegurando su correcto funcionamiento posterior al cierre del año anterior.	Anexo Informe
2.	Monitorear el estado de capacidad de almacenamiento en los Nodos de backup y en las cabinas de almacenamiento, anticipando crecimiento y generando recomendaciones para evitar saturación durante el primer trimestre.	Anexo Informe
3.	Realizar revisión general de la plataforma de virtualización en Proxmox y VMware, identificando oportunidades de optimización de rendimiento, balanceo de carga y estabilidad para el inicio del año.	Anexo Informe
4.	Acompañar y ajustar la configuración de red perimetral según necesidades detectadas (Firewall Fortinet, FortiSwitch, FortiAP, FortiAnalyzer, FortiAuthenticator, FortiManager), asegurando continuidad operativa durante el retorno de actividades institucionales.	Anexo Informe



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

5.	Verificar la correcta disponibilidad de la red WIFI institucional, validando cobertura y conectividad.	Anexo Informe
6.	Realizar revisión preventiva de certificados digitales, configuraciones SSL/TLS y servicios expuestos, verificando vigencias y reforzando mecanismos de protección perimetral.	Anexo Informe
7.	Monitorear continuamente los equipos perimetrales de seguridad y realizar ajustes según necesidades detectadas y/u órdenes recibidas (Firewall Fortinet, FortiSwitch, FortiAP, FortiAnalyzer, FortiAuthenticator, FortiManager, Veeam Backup).	Anexo Informe

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

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. 01 según forma y condiciones de pago y actividades del plan de trabajo descritas en el contrato.

CUMPLIMIENTO DE EJECUCIÓN PRESUPUESTAL
9,09 %



FORMATO INFORME DE SUPERVISIÓN ACTIVIDADES DE
EJECUCIÓN CONTRATOS PRESTACIÓN SERVICIOS
PROFESIONALES Y/O DE APOYO A LA GESTIÓN

6. BALANCE

BALANCE	
DESCRIPCIÓN	VALORES
VALOR INICIAL CONTRATO	\$ 59.675.000
VALOR ADICIÓN	N/A
VALOR REDUCCIÓN	N/A
VALOR PAGADO	\$ 0
PAGO PARA ESTE INFORME	\$ 5.425.000
PENDIENTE POR PAGAR	\$ 54.250.000

7. ANEXOS

ANEXO	HOJAS
Acta de Soporte de información SGSST	6
Acta capacitación código de integridad y servicio Publico colombiano	5
Acta de capacitación la cual el supervisor del contrato deberá dar a conocer al contratista la Política de Antisoborno implementada por el MDN.	3
Compromiso antisoborno y anticorrupción.	1
Copia de póliza de seguro con sus anexos	3
Certificado de afiliación ARL	1
Certificado de aplicación Retención en la Fuente (Decreto No. 2231 del 22 de diciembre del 2023)	1
Informe Avance CCOCI	18
Informe Actividades	6

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.



CONSTANCIA: 253-2026

**EL SUSCRITO JEFE DEL DEPARTAMENTO DE TALENTO HUMANO DE LA ESCUELA
SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"
NIT: 830.002.634-1**

HACE CONSTAR:

Que el señor YESSID ARAMIS CÁCERES VÁSQUEZ, identificado con cédula de ciudadanía No 72342326, vinculado mediante contrato de prestación de servicios No 052, realizó inducción X reinducción del Sistema de Gestión de Salud y Seguridad en el Trabajo para la vigencia 2026 de la Escuela Superior de Guerra "General Rafael Reyes Prieto" el día 16 de febrero del 2026.

Para efectos de verificación de la presente información, al correo derhily.giraldo@esdeg.edu.co

La presente constancia se expide en la ciudad de Bogotá D.C., a los 17/02/2026.

Coronel PABLO ENRIQUE CARDENAS CASTIBLANCO
Jefe Departamento Talento Humano "ESDEG"


Elaboró: PS. Derhily Giraldo Rodriguez
Profesional en Seguridad y Salud en el Trabajo Talento Humano "ESDEG"

Archivado en: 15103.12.5 Contrato de prestación de servicios 2026



Acta N°	0126105660	MDN-COGFM-JEMCO-ESDEG-DIESG-SBESG-VIADM-DEADM-DETAH	
Asunto	Capacitación relacionada con: Sistema de Gestión de Seguridad y Salud en el Trabajo		
Lugar y Fecha	Bogotá D.C., 30 de enero de 2026		
Hora Inicio	09:00 Horas	Hora Finalización	09:30 Horas
Unidad /Proceso y/o Dependencia Productora		Sección de Contratación	
Ausentes	N/A		

Orden del día:

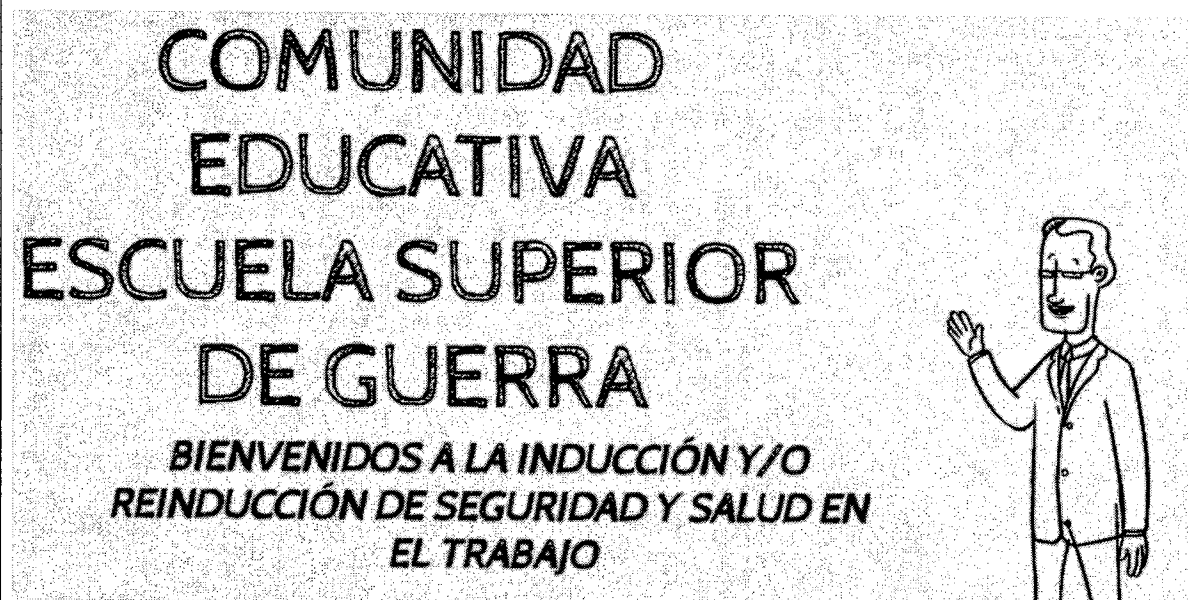
Se realizó la capacitación relacionada con el Sistema de Gestión de Seguridad y Salud en el Trabajo

Moderador:

PS. DERHLLY JOHANNA GIRALDO RODRIGUEZ

Desarrollo:

En el desarrollo de la capacitación se presento el siguiente video:



¿EN QUE CONSISTE EL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO?

El Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua. Con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y la salud en el trabajo.



La aplicación de las medidas de Seguridad y Salud en el Trabajo.

El mejoramiento del comportamiento del personal, las condiciones y el medio ambiente laboral.

El control y prevención de los peligros y riesgos en el lugar de trabajo.

Participación del personal y/o contratistas.

CUENTA CON: POLÍTICA DE SEGURIDAD Y SALUD EN EL TRABAJO

La Escuela Superior de Guerra "General Rafael Reyes Prieto" - ESDEG, como Institución de Educación Superior, se compromete desde la Alta Dirección, en el fortalecimiento del Sistema de Gestión de Seguridad y Salud en el Trabajo - SG-SST, promoviendo ambientes de trabajo seguros y saludables, ejerciendo el control de los riesgos presentes en los procesos y actividades de la institución, para minimizar la ocurrencia de incidentes, accidentes y enfermedades laborales, de acuerdo con lo establecido en la normatividad legal vigente.

 CREATED USING

CUENTA CON: OBJETIVOS DE LA POLÍTICA DEL SISTEMA DE GESTIÓN.

- 1. Promover y mantener en los trabajadores de la ESDEG el bienestar físico, mental y social en pro de la mejora continua.*
- 2. Asegurar la efectividad de los controles implementados para la prevención de enfermedades y accidentes laborales.*
- 3. Proveer los recursos físicos, tecnológicos, de infraestructura y económicos para el fortalecimiento y permanencia en el tiempo del SG-SST.*
- 4. Fortalecer el SG-SST, a través del ciclo PHVA.*
- 5. Determinar medidas conducentes a prevenir la materialización de accidentes y enfermedades laborales relacionadas con la misión institucional.*

CUENTA CON: QUIENES TIENEN ROLES Y RESPONSABILIDADES EN EL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO.

- *Alta Dirección (Dirección, Subdirección) y Comité de Desempeño Institucional.*
- *Vicedirecciones, Jefe de Departamentos y Oficinas de la Dirección.*
- *Oficiales, Suboficiales, Civiles de planta, Docentes, Pasantes, Contratistas y Subcontratistas.*
- *Estudiantes.*
- *Responsable de Seguridad y Salud en el Trabajo.*
- *Comité Paritario de Seguridad y Salud en el Trabajo -COPASST.*
- *Comité de Convivencia Laboral - CONVILAB.*

CUENTA CON:

1. *Cumplir con los requisitos legales en Seguridad y Salud en el Trabajo aplicables a la ESDEG.*
2. *Desarrollar las acciones necesarias del Sistema de Gestión de la Seguridad y la Salud en el Trabajo, para prevenir los accidentes y/o enfermedades laborales promoviendo una cultura de autocuidado y prevención.*
3. *Fomentar el aprendizaje por medio del desarrollo de actividades de promoción y prevención en materia de Seguridad y Salud en el Trabajo.*

CUENTA CON: IDENTIFICACIÓN DE PELIGROS A LOS QUE ESTAMOS EXPUESTOS.

BIOMECÁNICO: Posturas prolongadas.
CONTROL: Buena higiene postural.

LOCATIVO: Superficies irregulares.
CONTROL: No haga uso del celular mientras baja o sube escaleras.

PSICOSOCIAL: Gestión organizacional.
CONTROL: Actividades recreo deportivas para disminuir el estrés.

FÍSICO: Iluminación.
CONTROL: Aprovechar la iluminación natural.

FENÓMENOS NATURALES: Sismos, terremotos, inundaciones.
CONTROL: Participar en los simulacros.

QUÍMICO: Material particulado.
CONTROL: Uso de protección respiratoria y mantener la ventilación.

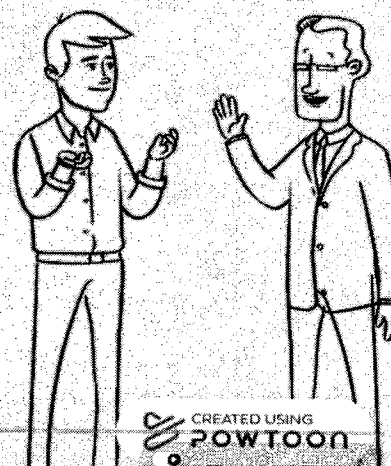
PÚBLICO: Atracos, robos, atentados.
CONTROL: Reportar cualquier anomalía.

BIOLÓGICO: Virus, bacterias.
CONTROL: Lavar las manos constantemente.

CREATED USING
POWTOON

PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS.

Establecer los procedimientos y acciones que debe realizar el personal de oficiales, suboficiales, civiles de planta, docentes, estudiantes, prestadores de servicio, pasantes, contratistas, proveedores, visitantes y todo aquel que ingrese a las instalaciones de la Escuela Superior de Guerra "General Rafael Reyes Prieto", para prevenir o afrontar una situación de emergencia, con el fin de organizar el control de la misma, evitar pérdidas humanas, materiales y económicas, haciendo uso de los recursos existentes en las instalaciones.



INDICACIONES EN CASO DE EMERGENCIAS.

- Al escuchar un timbre continuo evacue el edificio por emergencia de Sismo.
- Al escuchar dos timbres el ultimo continuo, evacue el edificio por emergencia de incendio.
- Al escuchar tres timbres el ultimo continuo, evacue el edificio por emergencia atentado terrorista.
- Ante cualquier emergencia suspenda inmediatamente la actividad que se encuentre realizando.
- Siga las instrucciones del personal brigadista.
- Utilice las rutas de evacuación correctamente señalizadas.
- Evacue por las escaleras, mientras se desplaza no haga uso del celular.
- No corra, no grite.
- No utilice ascensores.
- No forme aglomeraciones, camine con firmeza en fila y orden.
- Aléjese de ventanales u objetos que lo pongan en peligro "puedan caer".
- En caso de existir humo, desplácese lo más cercano al suelo y cúbrase la boca con un pañuelo o similar.
- Si tiene que bajar escaleras realicelo cercano a la pared y en fila y sin hacer uso del celular.
- Por ningún motivo se detenga o regrese a su área de trabajo o estudio.
- Diríjase al punto de encuentro y ubíquese en el lugar correspondiente.
- Hágase censar.
- Después de evaluar la emergencia y que el edificio reúna las condiciones de seguridad, se ordenará el ingreso.

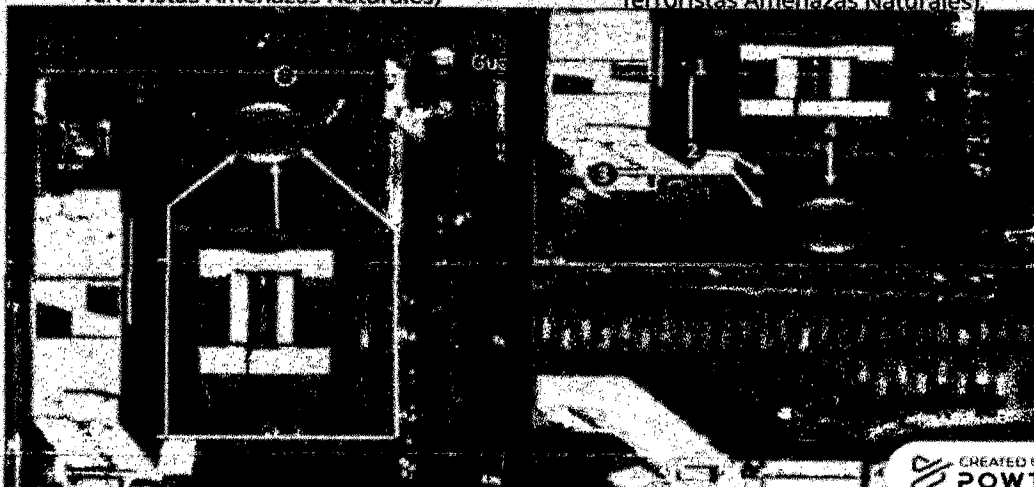


CREATED USING
POWTOON

PUNTOS DE ENCUENTRO.

Punto 1 Zona de Banderas. (Amenazas Terroristas Amenazas Naturales)

Punto 2 Zona verde Auditorio (Amenazas Terroristas Amenazas Naturales).



CREATED USING
POWTOON

COMITÉ PARITARIO DE SEGURIDAD Y SALUD EN EL TRABAJO.

Es un órgano bipartito y paritario, constituido por representantes del empleador y de los trabajadores, con las facultades y obligaciones previstas por la legislación y la práctica nacionales, destinado a la consulta regular y periódica de las actuaciones de la empresa en materia de prevención de riesgos.

FZA	GDO	APELLIDOS Y NOMBRES	CARGO O FUNCIÓN
EJC	CR	SERRANO CUERVO ALDEMAR	SUBDIRECTOR ENCARGADO/REPRESENTANTE DEL EMPLEADOR/ PRESIDENTE DEL COPASST
EJC	CR	SUÁREZ BAUTISTA CÉSAR ORLANDO	JEFE DEPARTAMENTO TALENTO HUMANO/ REPRESENTANTE DEL EMPLEADOR
EJC	TC	REYES CELY PAULA NATHALIA	JEFE DE PLANEACIÓN ESTRATÉGICA/ SUPLENTE DEL REPRESENTANTE DEL EMPLEADOR
ARC	MY	SORIA NIETO JESUS DARIO	JEFE DEPARTAMENTO SEGURIDAD/ SUPLENTE DEL REPRESENTANTE DEL EMPLEADOR
COGFM	PD8	CARDENAZ ORTIZ ADRIANA MARLENE	PROFESIONAL DE DEFENSA (ABOGADA)/ REPRESENTANTE DE LOS TRABAJADORES
COGFM	AA13	MORALES PATIÑO CAROL LORENA	AUXILIAR DE SERVICIOS(SECRETARIA)/ REPRESENTANTE DE LOS TRABAJADORES
COGFM	TS14	PUERTO REYES YENY ASTRID	TECNICO DE SERVICIOS/ SUPLENTE DEL REPRESENTANTE DE LOS TRABAJADORES
COGFM	AA13	MARTINEZ GOMEZ MARISOL	AUXILIAR PARA APOYO DE SEGURIDAD Y DEFENSA/ SUPLENTE DEL REPRESENTANTE DE LOS TRABAJADORES/ SECRETARIA DEL COMITÉ

CREATED USING
POWTOON

REPORTE DE ACCIDENTES Y/O ENFERMEDADES LABORALES.

Todo accidente laboral "A.T" o enfermedad laboral "E.L" que ocurra en la Escuela Superior de Guerra, deberá ser informado por el respectivo empleador, a la entidad administradora de riesgos laborales a la que se encuentra afiliado y a la entidad promotora de salud, en forma simultánea.

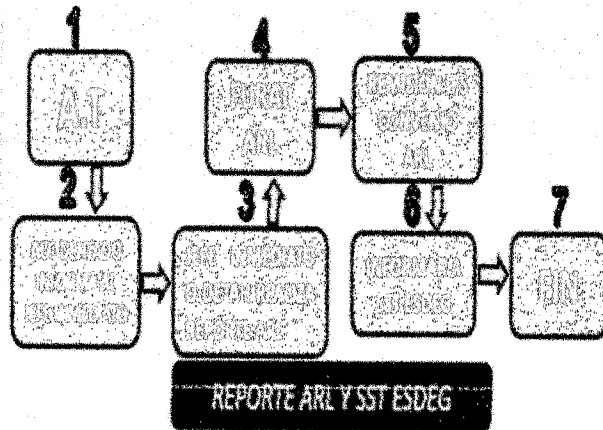
- A.T "Accidente de Trabajo": 48 Horas.
- E.L "Enfermedad Laboral": 2 Días hábiles.

En caso de accidente laboral:

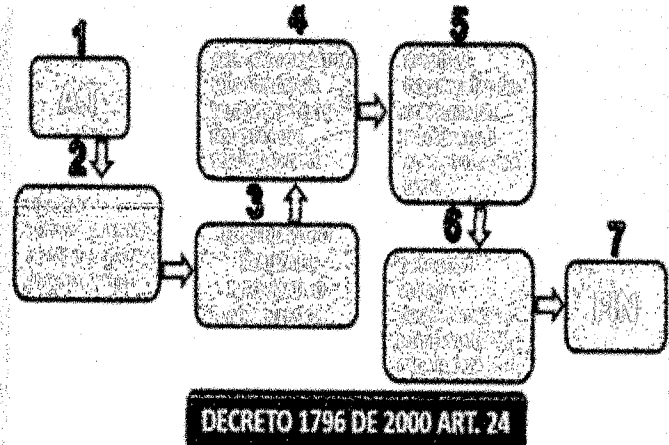
1. Datos personales del accidentado.
2. Datos de la empresa como Nit y dirección.
3. Hechos y testigos: Breve narración del suceso, testigos.

CÓMO REPORTAR UN ACCIDENTE LABORAL.

PERSONAL CIVIL.



PERSONAL MILITAR.



CREATED USING
POWTOON

DENTRO DE LAS INSTALACIONES DE LA ESDEG ESTA PROHIBIDO FUMAR O VAPEAR.



Dando cumplimiento a la Ley 2354 del 2024 y a la Política de prevención del consumo de sustancias psicoactivas, tabaco y alcohol de la ESDEG.

CREATED USING
POWTOON

**RECUERDE QUE PUEDE REPORTAR LAS
CONDICIONES INSEGURAS EVIDENCIADAS
EN LAS INSTALACIONES DE LA ESDEG EN:**

***CORREO:
DERHILLY.GIRALDO@ESDEG.EDU.CO***

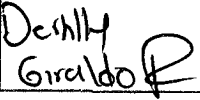


2. Se desarrollo un cuestionario por parte de los asistentes

Conclusiones:
N/A

Actividades a realizar:		
Actividad	Responsable	Fecha de Entrega
N/A	N/A	N/A

Convocatoria Próxima Reunión			
Tema:	N/A		
Fecha - Hora:	N/A	Lugar:	N/A

Intervienen y/o Asistentes						
Grado	Nombres y Apellidos	Cédula	Cargo	Teléfono	E-mail	Firma
PS.	YESSID ARAMIS CACERES VASQUEZ	72342326	INGENIERO DE SISTEMAS ESDEG	3015550697	yessid.caceres@esdeg.edu.co	
PS.	DERHLLY JOHANNA GIRALDO RODRIGUEZ	1024538570	Encargada SG-SSI	3193784459	derhilly.giraldo@esdeg.edu.co	

Archivado en: 15103.12.5 contrato de prestación de servicios 2026



ACTA GENERAL

Página de

Acta N°	01260110	MDN-COGFM-JEMCO-ESDEG- SBESG-VIADM-DETAH	
Asunto	Capacitación sobre código de integridad y sana convivencia laboral		
Lugar y Fecha	Bogotá D.C., 28 de enero de 2026		
Hora Inicio	14:30	Hora Finalización	15:30
Unidad /Proceso y/o Dependencia Productora	DETAH		
Ausentes	NO APLICA		

Orden del día:

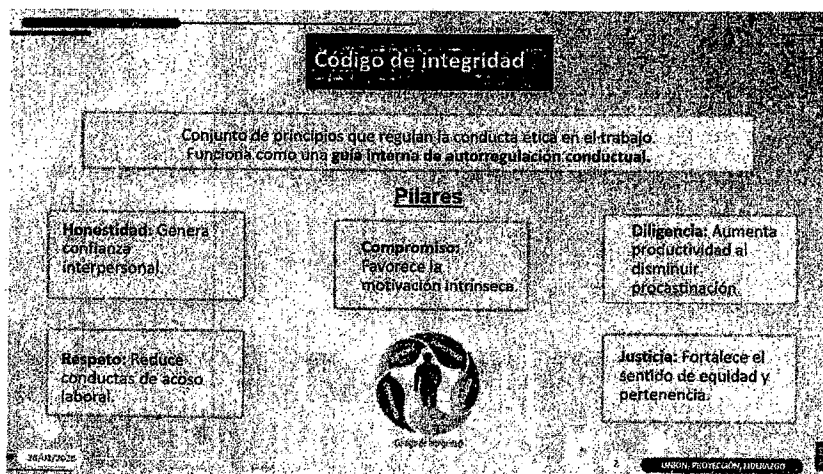
- Saludo inicial por parte de la psicóloga de la ESDEG
- Que es el código de integridad y sus pilares
- Convivencia laboral
- Valores para una sana convivencia
- No discriminación
- Clima organizacional positivo
- Del saber hacer
- Protocolo de prevención y atención por violencias basadas en género
- Activación de las rutas.
- Agradecimiento
- Cierre de la capacitación

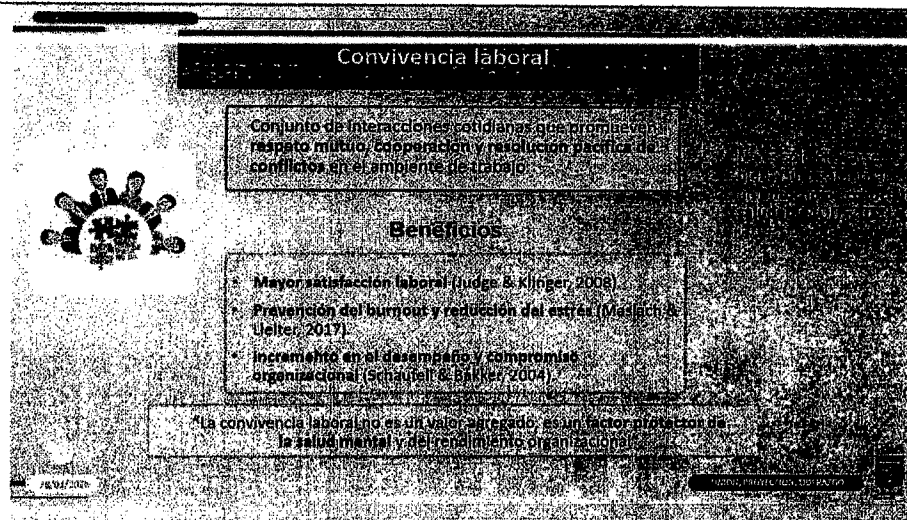
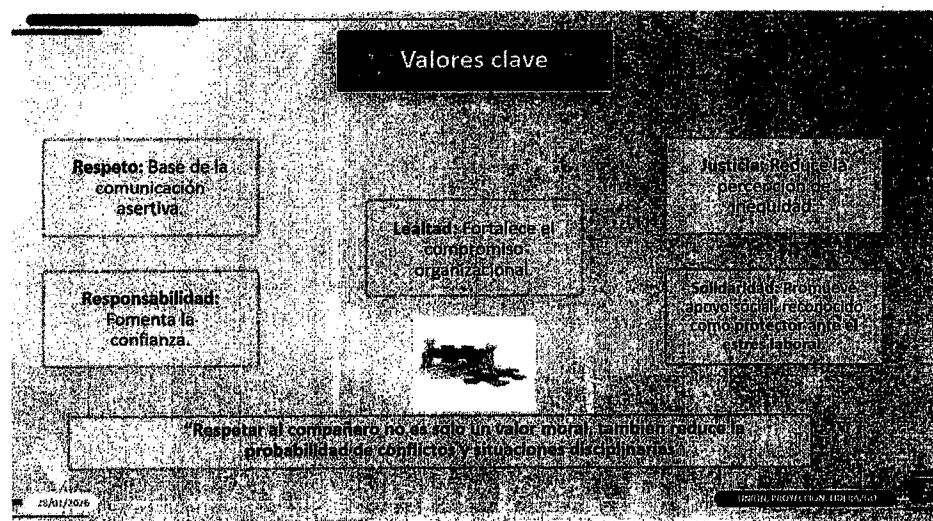
Moderador:

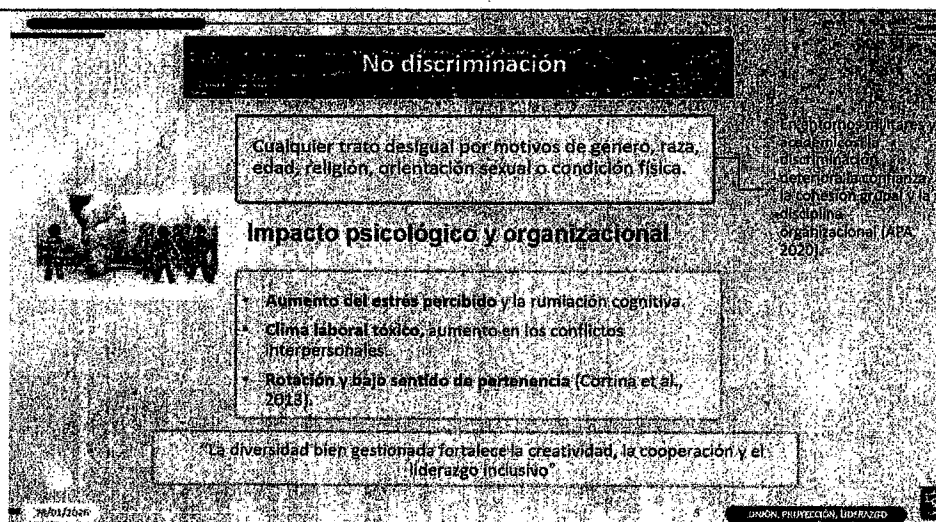
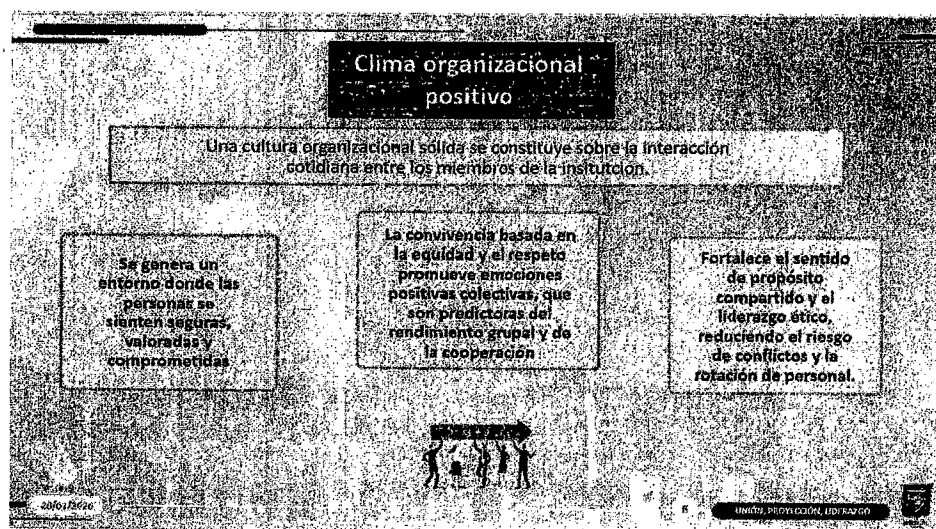
CT. Natalia Rodriguez Monroy

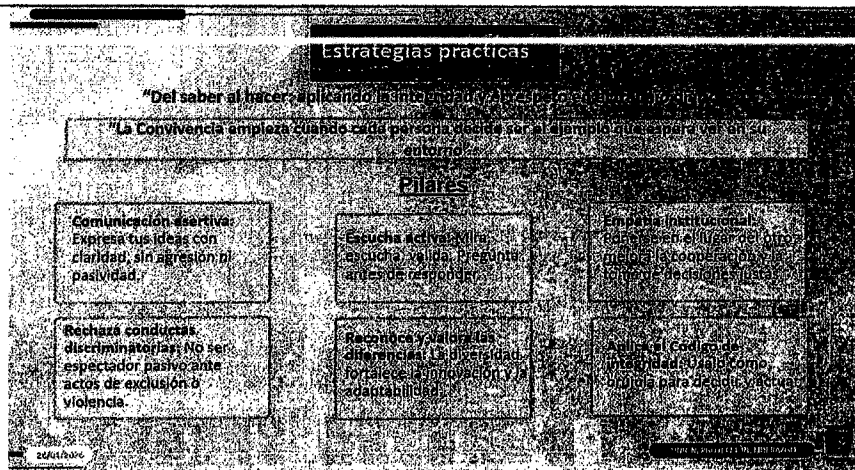
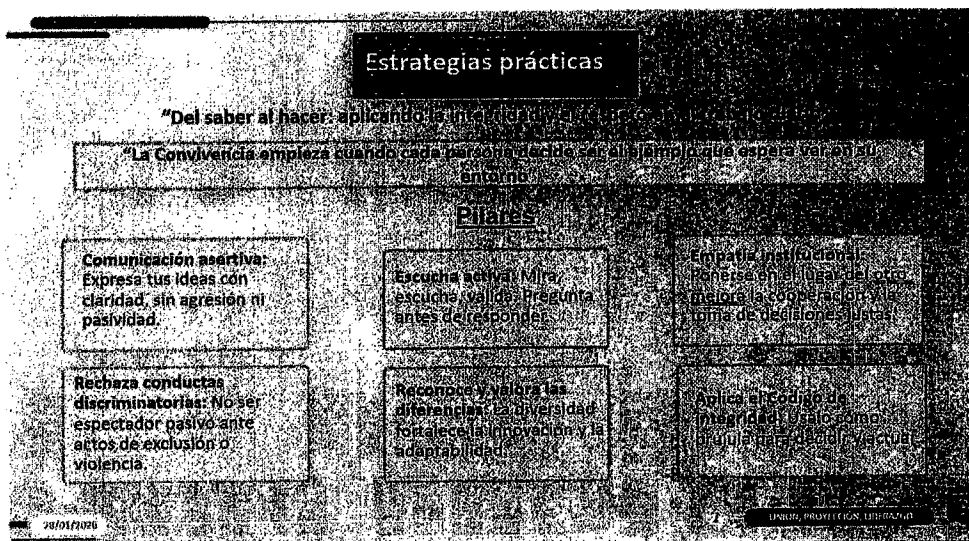
Desarrollo:

Se da inicio a la capacitación por parte de la psicóloga de la ESDEG dando un saludo inicial e indicando el objetivo de la capacitación, seguido a esto se tocan los siguientes temas expuestos en las ayudas anexadas así :











Dentro de la capacitación se abordan temas relacionados con el tema del código de integridad y cómo éstos de manera directa permiten un óptimo clima organizacional y convivencia, teniendo como pilar valores como respeto, honestidad, lealtad entre otros.

Se le da a conocer al personal los beneficios de un clima organización optimo, así como también la importancia del empoderamiento del código de integridad dentro de nuestro actuar como método para la generación de ambientes laborales saludables y el desarrollo de una excelente labor como servidores públicos.

Por ultimo se les da a conocer las rutas de atención en caso tal de un presunto caso de violencia basada en género, discriminación y/o posible caso de acoso laboral con el fin de que puedan recurrir a estas de ser necesario.

Conclusiones:

- Se capacita al personal sobre el código de integridad y los valores que fomentan el actuar como servidores públicos
- Se capacita sobre la importancia de generar un excelente clima organizacional, generando ambientes sanos y libres de violencias
- Se da a conocer el protocolo establecido por la ESDEG para el manejo de posibles casos de violencias basadas en género, discriminación y/o acoso laboral.
- Se sensibiliza al personal frente el rol de cada uno ante el desarrollo de ambientes laborales saludables indicando la importancia de la generación de conductas basadas en el respeto, cumplimiento de funciones y buen trato.

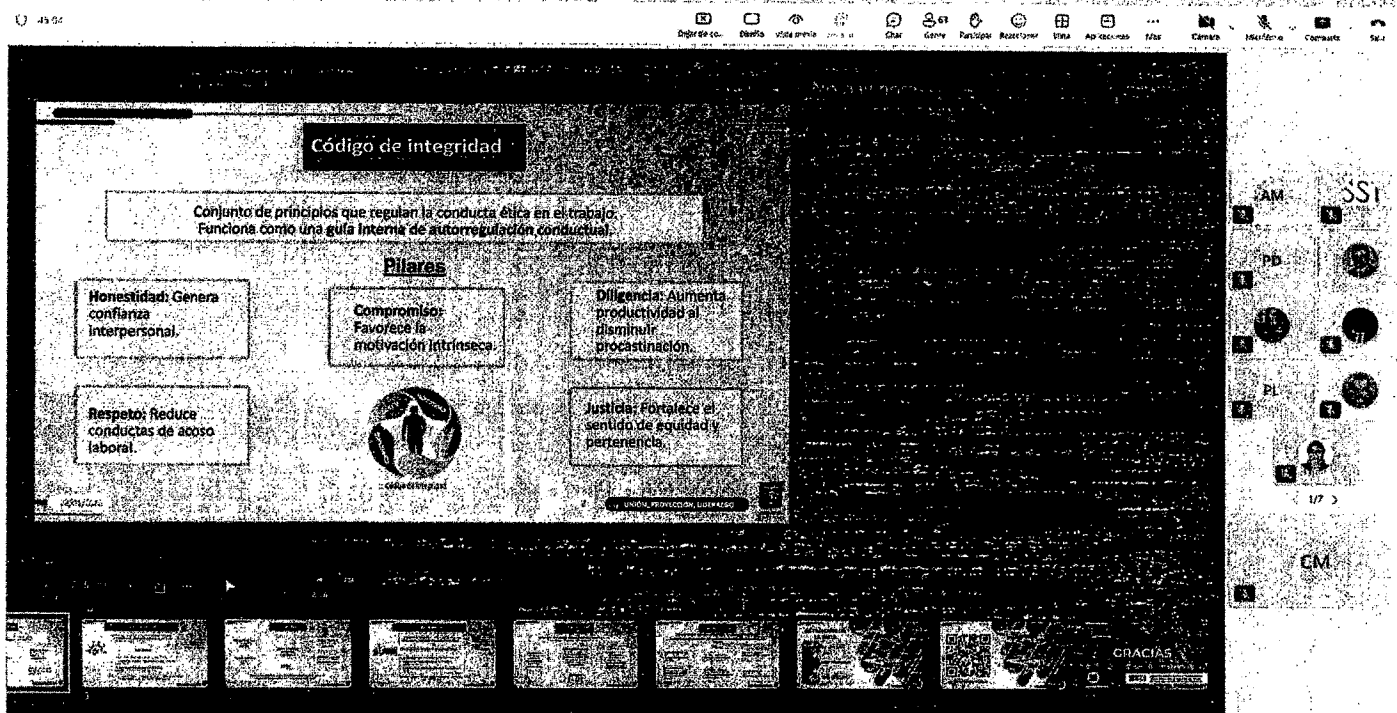
No aplica

Actividades a Realizar:

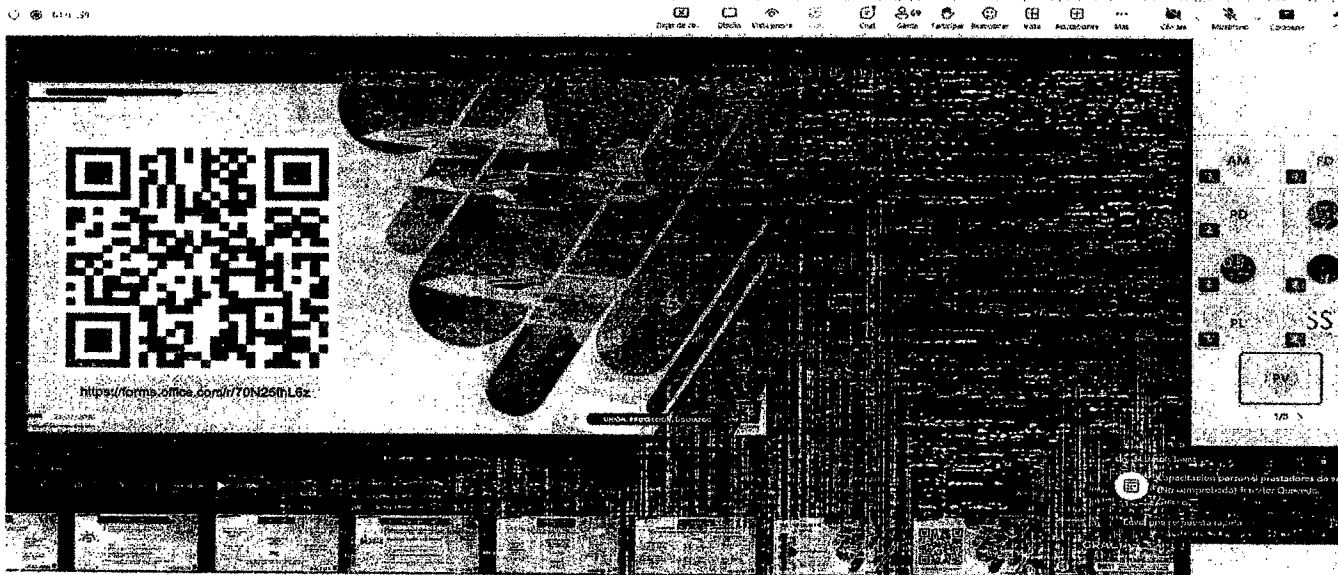
Actividad	Responsable	Fecha de Entrega
No aplica		

Convocatoria Próxima Reunión			
Tema:			
Fecha - Hora:		Lugar:	

44. Exprimación personal prestadores de servicios sobre Código de Integridad.



45. Capacitación personal prestadores de servicios sobre Código de Integridad.



01260110

Acta N°

/ MDN-COGFM-JEMCO-ESDEG- SBESG-VIADM- DETAH

Página

de

8

MY. PAOLA ANDREA RODRIGUEZ VARGAS	29687998	JEFE COEST	3128335090	paola.rodriguezv@esdeg.edu.co
HERNAN ALFONSO CONTRERAS RUIZ	79249358	GESTOR ACADEMICO DEPARTAMENTO EJERCITO	3143312858	halfonsocr@gmail.com
MARIA ALEJANDRA ROMERO	1033777730	ASISTENTE ADMINISTRATIVO DEESD	3214232129	maria.romeror@esdeg.edu.co
Luz Marina Cuervo Gamboa	52810326	Profesional Autoevaluación	3204962463	Luz.cuervo@esdeg.edu.co
BRYAN STEVEN HERRERA DIAZ	1234789320	WEBMASTER	3213910268	bryan.herrera@esdeg.edu.co
Henry Giovanni torres	79726886	Ing. Simulación	3214207456	Henry.torres@esdeg.edu.co
KATY ELENA VILLACOB RIOS	1102825386	ASESORA JURIDIA	3025552106	katy.villacob@esdeg.edu.co
Carmen Cecilia castillo antonio	46679228	Auxiliar de enfermería	3202209658	ceciliaantonio2178@gmail.com
Rosemary García Portilla	36544411	Profesional SIG Autev	3157071816	Rosemary.garcia@esdeg.edu.co
Nehil Jhon casallas estevez	93406400	Gestor académico maestría en derechos humanos y DICA	3102152441	nejhoca@hotmail.com
Fernando Enrique Farfan Castro	12139946	PS	3108031483	farfancastro2005@yahoo.com.mx
Jennifer Rocio Quevedo Ardila	1014202000	Técnico en Relaciones Internacionales y Estudios Políticos	3228131318	jennifer.quevedo@esdeg.edu.co
Yuli Natali Castellanos Muñoz	53101297	Gestora de Investigación Maestría en Derechos Humanos	3107517030	natalicastellanosm@gmail.com - natha131@hotmail.com
Cr. Pablo Ernesto Ramírez Gómez	86056092	Jefe de Departamento DELOG-DETL	3105599784	pablo.ramirezg@esdeg.edu.co
JACQUELINE DEL PILAR GARCIA PINCHAO	37013423	ASISTENTE CEMCI	3112893210	jacqueline.garcia@esdeg.edu.co
Mónica Alexandra López Lesmes	1016111552	Profesional DGRAP	3197774566	monica.lopez@esdeg.edu.co
Cindy Alexandra Ovalle trujillo	1032433591	Técnico enfermería	3017521559	alexandra.ovalle.1@hotmail.com
Ct Natalia Rodríguez Monroy	1095932089	Psicóloga	3161315997	natalia.rodriguez@esdeg.edu.co
Andersson Andres Salas Tapia	1083883677	Jefe Departamento DEINT	3124287572	andersson.salas@esdeg.edu.co
Edwing javier vargas garcia	91509702	Jefe dpto relaciones civiles y militares	3208474392	edwing.vargas@esdeg.edu.co
TF Lozada León Angie	1047502795	Jefe sección administrativo y presupuesto	3162481520	Angie.lozada@esdeg.edu.co
Rene Alejandro Garcia Chacon	79960574	Jefe DEEST	3106800687	rene.garcia@esdeg.edu.co
Javier Alejandro Durán Roa	79884558	Cesac	3208507474	Javier.duranr@esdeg.edu.co
TN Diego Alejandro Martínez Rodríguez	1016082032	Ayudantía Dirección	3125103048	diego.martinez@esdeg.edu.co
Ivan alberto pintor acosta	13.721.822	Director Centro doctrina conjunta	317 427 2575	Ivan.pintor@esdeg.edu.co
IVAN ALBERTO PINTOR ACOSTA	13721822	JEFE CEDCO	3174272575	Iván.pintor@esdeg.edu.co
Zulema Patricia Cobos Chico	52489695	Asesor Economico	3138343442	Zulma.cobos@esdeg.edu.co
Linda Julieth Blanco Lopez	1026289692	Abogada Talento Humano	3503998889	Linda.blanco@esdeg.edu.co
Diana Lopera Davila	31571245	Contadora Detah	3132419904	diana.lopera@esdeg.edu.co

01260110

Acta Nº

/ MDN-COGFM-JEMCO-ESDEG- SBESG-VIADM- DETAH

Página

de

9

Jenny Carolina Cubillos Mondragón	1015396376	Gestor Académico Especialización en Seguridad y Defensa Nacionales y Cursos de Extensión	3216342667	gacademica.esdn@esdeg.edu.co
Jorge Esteban Bettin Betin	1087940434	Ingeniero civil	3215407335	jorge.bettin@esdeg.edu.co
Andrea Luque Villegas	1015458464	Profesional de cultura física y deporte	3213613824	andrea.luque@esdeg.edu.co
Valentina Skinner Aguilar	1000595322	Asistente de VPROI	3188118223	Valentina.skinner@esdeg.edu.co
Veronica Viviana Urrea Pérez	1054544697	Contratista	3124598952	veronicaurrea1587@gmail.com
VIVIANA ALEJANDRA CALLES ARIAS	1104704704	GESTORA DE INVESTIGACIÓN	3228957886	viviana.calles@esdeg.edu.co
Yessid Aramis Caceres Vasquez	72342326	Ingeniero de infraestructura y seguridad	3015550697	yessid.caceres@esdeg.edu.co
JOSE DAVID MARCELO VARGAS ESCOBAR	19490124	GENERADOR Y ESTANDARIZADOR DE DOCTRINA	3214683238	jodamarva@yahoo.com
Daniel Alfonso Martinez Caro	79879695	Módulo SAP compras	3115459699	daniel.martinez@esdeg.edu.co
Enrique Ramirez	1061743430	Oficial Gestión Gobierno Digital	3135239402	enrique.ramirez@esdeg.edu.co
LYDA JAZMIN ZAMORA MONTAÑEZ	52474951	GESTORA ACADEMICA MAESD	3153480004	lyda.zamora@esdeg.edu.co
MARIA ANGELICA VERGARA	52934653	PROFESIONAL SEGUIMIENTO CONTRACTUAL	3115237038	angelica.vergara@esdeg.edu.co
FERNANDO ANDRES RAMOS DIAZ	80217734	GESTOR DE INVESTIGACION MAESD	3112879898	ginvestMAESD@esdeg.edu.co
Rosa Cristina Perdomo Torres	55168797	Tecnico Administrativo MAESD	3108777708	Asistente.maesd@esdeg.edu.co
ANDRES FELIPE BELTRAN ZAPATA	94150838	ASISTENTE PLAES	3122734025	ANDRES.BELTRAN@ESDEG.EDU.CO
Jorge Ricardo Espinel Bermúdez	72179153	Gestor de Doctrina	3106019158	jorgerespinel@gmail.com
Rosana Andrade Fuentes	38144903	Gestora académica MAEEG	3125778089	Rosana16@hotmail.com
Gustavo Adolfo Patiño Díaz	79786389	PS Corrector de estilo CEDCO	3108541316	gustavopatinocorrector@gmail.com
Boris José Mendoza Bonilla	79779608	Asesor	3112630583	borismendozaab@gmail.com
Carmen Cecilia castillo antonio	46679228	Auxiliar de enfermería	3202109658	Ceciliaantonio2178@gmail.com
MARIA LUCRECIA LEGUIZAMON	52086124	Asistente VACAD	3142311547	Maria.Leguiamon@esdeg.edu.co
JOSE DAVID MARCELO VARGAS ESCOBAR	19490124	GESTOR DOCTRINA	3214683238	jodamarva@yahoo.com
LUDY MARCELA MORENO SUAREZ	37626709	Técnico Archivo	3132688963	ludy.moreno@esdeg.edu.co
Javier Arturo Quintero Poveda	2234981	Asesor SIG	3102515859	Javier.quintero@esdeg.edu.co
William Restrepo	79592503	Asesor doctrina	3104911891	willrestrepo@hotmail.com
JAVIER Alejandro Durán Roa	79884558	CESAC	3208507474	Javier.duranr@esdeg.edu.co
Walter Hugo Agreda Hincapié	80049817	Supervisor de Contrato PS.	3102342207	walter.agreda@esdeg.edu.co
LUCIA BARRIGA	52791337	Adm sistema académico	3132702412	Lucia.barriga@esdeg.edu.co
Mario Fernando Canales Eodriguez	16645172	Asesor PLAES	3108556227	Mario.canales@esdeg.edu.co
Eliana Sierra Diaz	33379614	Asesora Jurídica	3143790378	Gladys.sierra@esdeg.edu.co
José Vicente Gómez	88207998	Diagramador Cedco	3125683513	Jotavfox@gmail.com
ANDRES HERNANDEZ	1026267760	ASESOR ECONOMICO	3214830811	ANDRESHAZ2021@GMAIL.COM
Nidia Patricia Herrera G.	39758277	Ps. Asesora académica educación virtual	3112434823	nidia.herreta@esdeg.edu.co
Fredy José Blanco Portillo	1032415038	Prestador de servicios	3505951149	Fredy.blanco@esdeg.edu.co

Código: MDN-COGFM-A05-ESDEG-AC.2-2 TRD: 2. Versión 5 25/OCT/2024
 Archivado en: 15200.29.19 planes institucionales de capacitación

LISTA DE ASISTENTES DIGITAL A TRAVES DEL LINK

LISTA DE ASISTENCIA CAPACITACIÓN SOBRE CÓDIGO DE INTEGRIDAD Y CONVIVENCIA : Rellenar formulario

NOMBRE COMPLETO	CEDULA	CARGO	TELÉFONO	CORREO ELECTRONICO
JUAN MANUEL JIMÉNEZ HERNÁNDEZ	79466532	Gestor académico de DEEST	3108103602	Juan.jimenezh@esdeg.edu.co
WILLIAM HERNANDO PINZÓN PÁEZ	79063382	ASESOR PROAC	3502656780	william.pinzonp@esdeg.edu.co
Diego Cortés	80188476	Administrador AVAFP	3196636747	diego.cortes@esdeg.edu.co
Derhily Johanna Giraldo Rodríguez	1024538570	Profesional en seguridad ocupacional	3193784459	derhily.giraldo@esdeg.edu.co
Andres Roberto Solano Ricaurte	1110459262	Ingeniero en Simulación y Modelado 3D	3153759449	andres.solano@esdeg.edu.co
Henry Leonardo Quiroga Morillo	80082170	Asesor Proyectos de Inversión	3192560678	Henry.Quiroga@esdeg.edu.co
Angie Catherine Vargas Fonseca	1013588111	Técnico Gestor Secop	3004029988	angie.vargas@esdeg.co
Robert Navarro Mateus	1030602309	Diseñador gráfico	3045565356	Robert.navarro@esdeg.edu.co
Edwin Jefferson Alarcón Silva	1032451566	Asesor Económico - SESET	3186222960	edwinalarcon14@hotmail.com
KAREN STEFANNY BECERRA CORREA	1030682179	Ingeniera Ambiental - geógrafa	3208287824	Karen.becerra@esdeg.edu.co
Lyna Johanna García Silva	1019052079	Abogada	3138155082	Lina1005g@hotmail.com
DIANA CAROLINA FERNANDEZ DIAZ	1014263622	PERIODISTA	3104232234	carolina.fernandez@esdeg.edu.co
Carlos Alberto Torres Chamorro	80817941	Diseñador Gráfico	3103025877	carlos.torresc@esdeg.edu.co
Martín Santos	91269607	Planeacion y programación presupuestal	3125976023	martin.santos@esdeg.edu.co
Gustavo Camberos hernandez	79382308	Asesor PLAGE	3114817924	gustavo.camberos@esde.edu.co
JUAN DAVID MÉNDEZ MENDIETA	1018430187	Ingeniero de sonido	3204711926	juan.mendezd@esdeg.edu.co
Bertsy Oriana Guzmán Alvarado	1073230641	Gestora de Investigación MAEEG	3224817437	oriana.guzman@esdeg.edu.co
Mary Iuz Vargas guzman	52354139	Asistente gestión académica	3015876682	Maryzury001@gmail.com
Lina Natalia Barrera Zea	1022324740	Gestora Académica	3242526628	Lina.barrera@esdeg.edu.co
Lesly Carolina Revelo Castro	1085259740	Asistente PROAC	3222556758	lesly.revelo@ESDEG.edu.co
Pablo Alejandro García Mora	1014238122	Diseñador Gráfico	3115562709	pablo.garciam@esdeg.edu.co
María Alejandra Hitomy Orjuela Mendez	1005771485	Economista	3224111674	maria.orjuela@esdeg.edu.co
ALEJANDRA GARZÓN BUSTAMANTE	1010201650	INGENIERA AMBIENTAL	3114818442	ALEJANDRA.GARZON@ESDEG.EDU.CO
LUDY MARCELA MORENO SUAREZ	37626709	TECNICO ARCHIVO	3132688963	LUDY.MORENO@ESDEG.EDU.CO
Nelcy Johana Villar Pérez	1121711989	Auxiliar Contable	3123134910	Johana.villar@esdeg.edu.co
Luis Hernando Cortés León	3159633	Facturación Electrónica	3118135889	luis.cortes@esdeg.edu.co
Alejandro Lopez	79633863	Asesor contable	3124138305	alejandro.lopezl@esdeg.edu.co
Johana Katherine Jimenez Zapata	1061727608	Ps abogada sesco	3137010274	Johanawhats90@gmail.com
Hugo Armando Galeano Valbuena	1020715904	Ingeniero de simulación	3115037139	hugo.galeano@esdeg.edu.co



Acta N°	0126105721	COGFM-JEMCO-ESDEG-SBESG- VIADM-DETAH	
Asunto	Aplicación del Código de integridad y servicio Público Colombiano		
Lugar y Fecha	Bogotá D.C., 02 de febrero de 2026		
Hora Inicio	10:00 Horas	Hora Finalización	10:30 Horas
Unidad /Proceso y/o Dependencia Productora		Sección de Contratación	
Ausentes	N/A		

Orden del día:

Se realizó la capacitación de aplicación del Código de integridad y servicio Público Colombiano y socialización de la política antisoborno y corrupción de acuerdo al numeral (8.6.2. practicas indebidas del Manual de Contratación y convenios emitido por el Ministerio de Defensa)

Moderador:

TE. RAMIREZ FLOR ENRIQUE

Supervisor de contrato

Desarrollo:

1. Se realizó capacitación de aplicación del Código de integridad y servicio Público Colombiano

»» Código de integridad

El Código de Integridad elaborado por la Función Pública constituye una herramienta para ser implementada por las entidades públicas de la Rama Ejecutiva colombiana.

La adopción del Código debe contemplar el siguiente aspecto:

Adoptar y apropiar el Código de Integridad, y de conformidad con las particularidades y autonomía de cada entidad pública, adicionar principios de acción ("lo que hago" y "lo que no hago") a los cinco valores establecidos en el Código e incluir hasta dos valores adicionales."

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad

El Código de Integridad establece los mínimos de integridad homogéneos para todos los servidores públicos del país e incluye los siguientes valores:

- Honestidad
- Respeto
- Compromiso
- Diligencia
- Justicia

Los valores determinan una línea de acción cotidiana para los servidores públicos y contratistas de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad

LO QUE HAGO

• Siempre digo la verdad, incluso cuando cometo errores, porque es humano cometerlos, pero no es correcto esconderlos.

• Cuando tengo dudas respecto a la aplicación de mis deberes busco orientación en las instancias pertinentes al interior de mi entidad. Se vale no saberlo todo, y también se vale pedir ayuda.

• Facilito el acceso a la información pública completa, veraz, oportuna y comprensible a través de los medios destinados para ello.

• Denuncio las faltas, delitos o violación de derechos de los que tengo conocimiento en el ejercicio de mi cargo, siempre.

LO QUE NO HAGO

• No le doy trato preferencial a personas cercanas para favorecerlos en un proceso en igualdad de condiciones.

• No acepto incentivos, favores, ni ningún otro tipo de beneficio que me ofrezcan personas o grupos que estén interesados en un proceso de toma de decisiones.

• No uso recursos públicos para fines personales relacionados con mi familia, mis estudios y mis pasatiempos (esto incluye el tiempo de mi jornada laboral, los elementos y bienes asignados para cumplir con mi labor, entre otros).

• No soy descuidado con la información a mi cargo, ni con su gestión.



HONESTIDAD

Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad

Lo que hago:

Atiendo con amabilidad, igualdad y equidad a todas las personas en cualquier situación a través de mis palabras, gestos y actitudes, sin importar su condición social, económica, religiosa, étnica o de cualquier otro orden.

Soy amable todos los días, esa es la clave, siempre.

Estoy abierto al diálogo y a la comprensión a pesar de perspectivas y opiniones distintas a las mías.

No hay nada que no se pueda solucionar hablando y escuchando al otro.

Lo que no hago:

Actuar de manera discriminatoria, grosera o hiriente, en ninguna circunstancia.

Basar mis decisiones en presunciones, estereotipos, o prejuicios.

Agredir, ignorar o maltratar a los ciudadanos o a otros servidores públicos.



RESPECTO

Reconozco, valoro y trato de manera digna a todas las personas con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad

Lo que hago:

Asumo mi papel como servidor público, entendiendo el valor de los compromisos y responsabilidades que he adquirido frente a la ciudadanía y al país.

Siempre estoy dispuesto a ponerme en los zapatos de las personas. Entender su contexto, necesidades y requerimientos es el fundamento de mi servicio y labor.

Escucho, atiendo y oriento a quien necesite cualquier información o guía en algún asunto público.

Estoy atento siempre que interactúo con otras personas, sin distracciones de ningún tipo.

Lo que no hago:

Trabajar con una actitud negativa. No se vale afectar mi trabajo por no ponerle ganas a las cosas.

Pensar que mi trabajo como servidor es un "favor" que le hago a la ciudadanía. Es un compromiso y un orgullo.

Asumir que mi trabajo como servidor es irrelevante para la sociedad.



COMPROMISO

Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad



Lo que hago:

Uso responsablemente los recursos públicos para cumplir con mis obligaciones. Lo público es de todos y no se desperdicia.

Cumplo con los tiempos estipulados para el logro de cada obligación laboral. A fin de cuentas, el tiempo de todos es oro.

Aseguro la calidad en cada uno de los productos que entrego bajo los estándares del servicio público. No se valen cosas a medias.

Siempre soy proactivo comunicando a tiempo propuestas para mejorar continuamente mi labor y la de mis compañeros de trabajo.

Lo que no hago:

Malgastar el recurso público.

Postergar las decisiones y actividades que den solución a problemáticas ciudadanas o que hagan parte del funcionamiento de mi cargo. Hay cosas que sencillamente no se dejan para otro día.

Demostrar desinterés en mis actuaciones ante los ciudadanos y los demás servidores públicos.

Evadir mis funciones y responsabilidades.

Trasladar los problemas y responsabilidades a otras dependencias, siempre apporto a la solución.



DILIGENCIA

• Cumplir con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.

UNIÓN, PROYECCIÓN, LIDERAZGO

»» Código de integridad



Lo que hago:

Tomo decisiones informadas y objetivas basadas en evidencias y datos confiables. Es muy grave fallar en mis actuaciones por no tener las cosas claras.

Reconozco y protejo los derechos de cada persona de acuerdo con sus necesidades y condiciones.

Tomo decisiones estableciendo mecanismos de diálogo y concertación con todas las partes involucradas.

Lo que no hago:

Promover y ejecutar políticas, programas o medidas que afectan la igualdad y la libertad de personas.

Favorecer el punto de vista de un grupo de interés sin tener en cuenta a todos los actores involucrados en una situación.

Permitir que odios, simpatías, antipatías, caprichos, presiones o intereses de orden personal o grupal interfieran en mi criterio, toma de decisión y gestión pública.

Dar un trato inequitativo a nuestros usuarios y prelacones indebidas para favorecer alguna persona.



JUSTICIA

• Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

UNIÓN, PROYECCIÓN, LIDERAZGO

2- Socialización Política de Antisoborno implementada por el Ministerio de Defensa Nacional y los distintos canales dispuestos por el Ministerio - ESDEG de acuerdo al numeral (8.6.2. practicas indebidas del Manual de Contratación y convenios emitido por el Ministerio de Defensa), respecto de los actos de soborno o de corrupción.

Conclusiones:

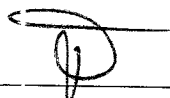
N/A

Actividades a realizar:

Actividad	Responsable	Fecha de Entrega
N/A	N/A	N/A

Convocatoria Próxima Reunión

Tema:	N/A		
Fecha - Hora:	N/A	Lugar:	N/A

Intervienen y/o Asistentes						
Grado	Nombres y Apellidos	Cédula	Cargo	Teléfono	E-mail	Firma
TE	RAMIREZ FLOR ENRIQUE	1061743430	Cargo Oficial Gestión Gobierno Digital	3135239402	enrique.ramirez@esdeg.edu.co	
PS	CACERES VASQUEZ YESSID ARAMIS	72342326	INGENIERO INFRAESTRUCTURA Y SEGURIDAD	3015550697	yessid.caceres@esdeg.edu.co	

Archivado en: 15103.12.5 contrato de prestación de servicios 2024

El Ministerio de Defensa Nacional, ha declarado el compromiso institucional de cero tolerancias con el soborno y la corrupción, adoptando prácticas e impulsando campañas y mecanismos que permitan prevenir y detectar potenciales situaciones de soborno o conductas irregulares en el accionar de los contratistas de la entidad, mediante el desarrollo de actividades, planes y programas en el marco de los valores y la integridad aplicadas en el Código de Integridad de la entidad.

Por lo anterior, se suscribe el siguiente compromiso antisoborno:

Yo, YESSID ARAMIS CÁCERES VASQUEZ identificado(a) con C.C. 72.342.326 expedida en Barranquilla en mi calidad de PROVEEDOR, del contrato de prestación de servicios profesionales y de apoyo a la gestión, de manera voluntaria y libre de coacción, coerción, amenaza, dádiva y/o promesa remuneratoria, directa o indirecta, mediante la suscripción de este documento a título de aporte unilateral a favor del MINISTERIO DE DEFENSA-COMANDO GENERAL – ESCUELA SUPERIOR DE GUERRA - "GENERAL RAFAEL REYES PRIETO", en cumplimiento del compromiso de lucha contra la corrupción, declaro que asumo los siguientes compromisos:

1. Manifiesto públicamente que conozco el alcance y el contenido de la Política, objetivo y alcance del Sistema de Gestión de Antisoborno del Ministerio de Defensa Nacional, y como consecuencia de ello me comprometo a tomar una actitud de cero tolerancias ante el soborno y la corrupción.
2. Rechazar, NO aceptar y/o solicitar, NO ofrecer, NO prometer y NO entregar para sí o para otro, dádivas, regalos, bonificaciones, comisiones y/o promesa remuneratoria, directa o indirectamente; tanto en el Ministerio como fuera de él, a cambio de obtener beneficios ilegales en la ejecución de las obligaciones contractuales.
3. Rechazar y NO aceptar ningún tipo de fiestas, recepciones, homenajes, o cualquier tipo de atención social de servidores del Ministerio de Defensa Nacional, interventores, consultores o contratistas de la entidad o de personas con interés en los diferentes momentos del contrato que me fue adjudicado.
4. Prevenir el soborno por, o en nombre de, o en beneficio de quien suscribe en relación con la operación correspondiente, proyecto, actividad o relación.
5. Fomentar y aplicar mecanismos, instrumentos y/o controles al interior de la empresa que represento y/o en nombre propio para la prevención de prácticas de conductas asociadas al soborno, el fraude o la corrupción.
6. Fomentar el reporte de las conductas o hechos que puedan llegar a configurar prácticas de soborno, corrupción o fraude con fundamento en la buena fe o en una sospecha razonable.
7. Promover acciones encaminadas a la formación para la aplicación de la Sistema de gestión de Antisoborno basados en los requerimientos de la Norma ISO 37001 y la normativa aprobada por el Ministerio de Defensa Nacional que tienen la finalidad de combatir el soborno y la corrupción en las relaciones inherentes a mi cargo, entre ellos el Código de Ética e Integridad.
8. Garantizar la confidencialidad de los datos de quien reporte hechos de corrupción soborno o fraude en la entidad.
9. Proteger la identidad de los informantes y de las personas que participan en la denuncia.
10. Aceptar que la violación de Política del Sistema de Gestión Antisoborno del Ministerio de Defensa Nacional dará lugar al inicio de investigaciones por parte de la Oficina de Control Interno Disciplinario del Ministerio de Defensa Nacional o al traslado de las denuncias correspondientes a las demás autoridades competentes, con la finalidad de establecer la responsabilidad administrativa, fiscal, disciplinaria, civil a que haya lugar, así mismo se da a conocer los canales dispuestos por el MDN.

✓ Correo electrónico: lineadelhonor@mindefensa.gov.co
antisoborno@mindefensa.gov.co

FORMATO ANTISOBORNO Y ANTICORRUPCION
CONTRATOS PRESTACION DE SERVICIOS
PROFESIONALES Y DE APOYO A LA GESTION

Página 2 de 2

- ✓ Línea telefónica: Línea del honor -antisoorno PBX: 3150111 ext. 40135
- ✓ Buzones físicos en punto de atención presencial
- ✓ APP: Mindefensa
- ✓ Sede electronica:
<https://wasedeelectronicaapro.azurewebsites.net/Imindefensa.html?#/home>

11. Que, conociendo los mecanismos dispuestos de denuncia planteados en la política de Antisoorno del Ministerio de Defensa, recibir y dar traslado oportuno de las denuncias.
12. Respetar los valores representados en el Código de Integridad del Ministerio.
13. Colaborar de buena fe en cualquier investigación llevada a cabo por el Ministerio de Defensa Nacional y sus representantes, en caso de que se produzca algún incumplimiento de estos compromisos.
14. Aceptar que el MINISTERIO DE DEFENSA-COMANDO GENERAL – ESCUELA SUPERIOR DE GUERRA - "GENERAL RAFAEL REYES PRIETO", puede poner fin a la relación contractual en caso comprobado de soborno por parte de, o en nombre de, o en beneficio de quien suscribe, en relación con la transacción correspondiente, proyecto, actividad o relación. Hago constar que soy consciente de la responsabilidad que implica la suscripción de este acuerdo.

Con la firma de este documento, doy prueba de que conozco y me comprometo para aplicar la Política Antisoorno del Ministerio de Defensa Nacional.

Firma: 

Nombre **YESSID ARAMIS CÁCERES VÁSQUEZ**

Cedula: **72.342.326 de Barranquilla**

Archivado en: 15.103.12.5 Contrato de prestación de servicios 2026.

PÓLIZA DE SEGURO DE CUMPLIMIENTO ENTIDAD ESTATAL
DECRETO 1082 DE 2015

CIUDAD DE EXPEDICIÓN:			SUCURSAL:			COD. SUC:		NO. PÓLIZA:		ANEXO:	
BOGOTÁ, D.C.			CHAPINERO			14		14-46-101159880		0	
FECHA EXPEDICIÓN:			VIGENCIA DESDE:			A LAS:		VIGENCIA HASTA:		A LAS:	
DÍA:	MES:	AÑO:	DÍA:	MES:	AÑO:	HORAS:	DÍA:	MES:	AÑO:	HORAS:	
20	01	2026	20	01	2026	00:00	10	07	2027	23:59	
TIPO MOVIMIENTO:											
EMISIÓN ORIGINAL											

DATOS DEL TOMADOR / GARANTIZADO											
NOMBRE O RAZÓN SOCIAL: CACERES VASQUEZ YESSID ARAMIS										IDENTIFICACIÓN: C.C. :72,342,326	
DIRECCIÓN: CARRERA 116 A NO 15C -70.						CIUDAD: BOGOTÁ, D.C. - DISTRITO CAPITAL				TELÉFONO: 3015550697	
DATOS DEL ASEGURADO / BENEFICIARIO											
ASEGURADO/BENEFICIARIO: MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES ESCUELA SUPERIOR DE GUERRA GENERAL RAFAEL REYES PRIETO DEPARTAMENTO ADMINISTRATIVO										IDENTIFICACIÓN: NIT. :830,002,634-1	
DIRECCIÓN: CRA 11 NO 102 50						CIUDAD: BOGOTÁ, D.C. - DISTRITO CAPITAL				TELÉFONO: 3102739049	
ADICIONAL:											

OBJETO DEL SEGURO											
CON SUJECCIÓN A LAS CONDICIONES GENERALES DE LA PÓLIZA QUE SE ANEXAN ECU010B, QUE FORMAN PARTE INTEGRANTE DE LA MISMA Y QUE EL ASEGURADO Y EL TOMADOR DECLARAN HABER RECIBIDO Y HASTA EL LÍMITE DE VALOR ASEGURADO SEÑALADO EN CADA AMPARO, SEGUROS DEL ESTADO S.A., GARANTIZA:											
EL CUMPLIMIENTO DE LAS OBLIGACIONES DERIVADAS DEL CONTRATO NO. 052-MDN-COGFM-ESDEG-2026 DE PRESTACION DE SERVICIOS CUYO OBJETO ES: PRESTACION DE SERVICIOS PROFESIONALES EN LA CATEGORIA H, COMO INGENIERO DE SISTEMAS CON EL FIN DE GESTIONAR LA INFRAESTRUCTURA TECNOLÓGICA Y DE SEGURIDAD PARA EL DEPARTAMENTO DETECNOLOGIAS DE LA INFORMACIDN Y COMUNICACIONES DE LA ESCUELA SUPERIOR DE GUERRA GENERALRAFAEL REYES PRIETO											

AMPAROS											
RIESGO: PRESTACION DE SERVICIOS											
AMPAROS:											
VIGENCIA DESDE: VIGENCIA HASTA: SUMA ASEG/ACTUAL:											
CUMPLIMIENTO DEL CONTRATO 20/01/2026 10/07/2027 \$ 11,935,000.00											
ACLARACIONES:											
SE AMPARA EL CUMPLIMIENTO DEL CONTRATO, EL PAGO DE LAS MULTAS Y DE LA CLAUSULA PENAL PECUNIARIA CONVENIDA. SEGUROS DEL ESTADO RENUNCIA AL BENEFICIO DE EXCUSION											

VALOR PRIMA NETA:	GASTOS EXPEDICIÓN:	IVA:	TOTAL A PAGAR:	VALOR ASEGURADO TOTAL:	PLAN DE PAGO:
\$ 43,816.16	\$ 8,000.00	\$ 9,845.07	\$ 61,661.23	\$ 11,935,000.00	CONTADO

INTERMEDIARIO			DISTRIBUCIÓN COASEGURO		
NOMBRE:	CLAVE:	% PART:	NOMBRE COMPAÑIA:	% PART:	VALOR ASEGURADO:
AGENCIA DE SEGUROS AFIRMAR LTDA	153870	100,00			

QUEDA EXPRESAMENTE CONVENIDO QUE LAS OBLIGACIONES DE SEGUROS DEL ESTADO S.A. SE REFIERE UNICAMENTE AL OBJETO Y OBSERVACIONES DE LA(S) GARANTÍA(S) QUE SE ESPECIFICAN EN ESTE CUADRO

PARA EFECTO DE NOTIFICACIONES LA DIRECCIÓN DE SEGUROS DEL ESTADO S.A. ES CRA. 7 NO. 57 -67 - TELÉFONO: 2172417 - BOGOTÁ, D.C.

14-46-101159880

FIRMA AUTORIZADA: Jose Luis Ojeda Acaveado - Vicepresidente de Fianzas

FIRMA TOMADOR

USTED PUEDE CONSULTAR ESTAR PÓLIZA EN WWW.SEGUROSDELESTADO.COM

Oficina Principal: Autopista Norte # 103 - 60, Piso 5 Bogotá D.C. Piso 5.Teléfono: 601-2186977, 601-6019330

900691207

NO EFECTUAR RETENCIÓN EN LA FUENTE POR NINGUN CONCEPTO * RESPONSABLE IVA



SEGUROS
DEL
ESTADO S.A.

NIT. 860.008.578-6

CONSTANCIA DE NO REVOCATORIA NI CANCELACIÓN POR FALTA DE PAGO DE LA PRIMA

Hacemos constar, que la póliza No. 14-46-101159880, anexo 0, no expirará por falta de pago de la prima, ni por revocatoria unilateral del tomador de la póliza o de la aseguradora.

Lo anterior de conformidad con lo establecido en el decreto 1082 de 2015, el cual regula las garantías ante entidades estatales.

Dado en BOGOTÁ, D.C., a los 20 días del mes de Enero de 2026

FIRMA AUTORIZADA: Jose Luis Ojeda Acevedo - Vicepresidente de Fianzas

Oficina Principal: Autopista Norte # 103 - 60, Piso 5 Bogotá D.C. Teléfono: 601-2186977, 601-6019330
ASISTENCIA CELULAR #388 - FUERA DE BOGOTÁ 018000123010

www.segurosdelestado.com

SUPERINTENDENCIA FINANCIERA
DE COLOMBIA

VIGILADO

**SEGUROS DEL ESTADO S.A.**

Hace constar que:

RECIBO DE PAGO N°:

14461011598800

FECHA				
CONTADO				
RECIBIMOS DE:	CACERES VASQUEZ YESSID ARAMIS		C.C. C.C. :72,342,326	
LA SUMA DE:	SESENTA Y UN MIL SEISCIENTOS SESENTA Y UN CON VEINTITRES CENTAVOS PESOS M/CTE			
POR CONCEPTO DE:	PAGO DE PÓLIZA NRO.: 14-46-101159880			
SUC - RAMO - PÓLIZA - ENDOSO - CUOTA		PRIMA	GASTOS EXPEDICION	IVA
CHAPINERO - CU. ESTATAL - 101159880 - 0 - 0		\$ 43,816.16	\$ 8,000.00	\$ 9,845.07
FORMA DE PAGO				
				EFFECTIVO:
				\$ 61,661.23
				CHEQUE:
				\$ 0.00
				TARJETA:
				\$ 0.00
				BD:
				\$ 0.00
				OTROS:
				\$ 0.00
INTERMEDIARIO:	AGENCIA DE SEGUROS AFIRMAR LTDA - 153870			TOTAL:
			\$ 61,661.23	
CAJERO: RAPIESTADO				

ORIGINAL

**SEGUROS DEL ESTADO S.A.**

Hace constar que:

RECIBO DE PAGO N°:

14461011598800

FECHA				
CONTADO				
RECIBIMOS DE:	CACERES VASQUEZ YESSID ARAMIS		C.C. C.C. :72,342,326	
LA SUMA DE:	SESENTA Y UN MIL SEISCIENTOS SESENTA Y UN CON VEINTITRES CENTAVOS PESOS M/CTE			
POR CONCEPTO DE:	PAGO DE PÓLIZA NRO.: 14-46-101159880			
SUC - RAMO - PÓLIZA - ENDOSO - CUOTA		PRIMA	GASTOS EXPEDICION	IVA
CHAPINERO - CU. ESTATAL - 101159880 - 0 - 0		\$ 43,816.16	\$ 8,000.00	\$ 9,845.07
FORMA DE PAGO				
				EFFECTIVO:
				\$ 61,661.23
				CHEQUE:
				\$ 0.00
				TARJETA:
				\$ 0.00
				BD:
				\$ 0.00
				OTROS:
				\$ 0.00
INTERMEDIARIO:	AGENCIA DE SEGUROS AFIRMAR LTDA - 153870			TOTAL:
			\$ 61,661.23	
CAJERO: RAPIESTADO				

COPIA



**SEGUROS
DEL
ESTADO S.A.**
NIT. 860.006.579-6

**PÓLIZA ÚNICA DE SEGURO DE CUMPLIMIENTO EN FAVOR DE ENTIDADES ESTATALES
SOMETIDA AL DECRETO 1082 DE 2015 No.14-46-101159880**

1. AMPAROS.

SEGUROS DEL ESTADO S.A., QUE EN ADELANTE SE DENOMINARÁ SEGUROESTADO OTORGA A LA ENTIDAD ESTATAL ASEGURADA, HASTA EL MONTO DEL VALOR ASEGURADO PACTADO, LOS AMPAROS MENCIONADOS EN LA CARÁTULA DE LA PRESENTE PÓLIZA, CUBRIENDO CON ELLOS, SIEMPRE LOS PERJUICIOS DIRECTOS QUE CON SUJECCIÓN A LA DEFINICIÓN DE LAS CONDICIONES ADELANTE INDICADAS, LLEGARÉ A CAUSAR EL GARANTIZADO POR EL INCUMPLIMIENTO QUE, ATRIBUIBLE A SU ACCIÓN U OMISIÓN, PRODUCIERE.

LOS AMPAROS QUE SE OTORGAN EN ESTA PÓLIZA SERÁN INDEPENDIENTES UNOS DE OTROS RESPECTO DE SUS RIESGOS Y DE SUS VALORES ASEGURADOS. SEGÚN LAS DEFINICIONES QUE A CONTINUACIÓN SE INDICAN:

1.1 AMPARO DE SERIEDAD DE LA OFERTA.

EL AMPARO DE SERIEDAD DE LA OFERTA, CUBRE A LA ENTIDAD ESTATAL ASEGURADA, LA SANCIÓN DERIVADA DEL INCUMPLIMIENTO DE LA OFERTA, EN LOS SIGUIENTES EVENTOS:

1.1.1 LA NO AMPLIACIÓN DE LA VIGENCIA DE LA GARANTÍA DE SERIEDAD DE LA OFERTA CUANDO EL PLAZO PARA LA ADJUDICACIÓN O PARA SUSCRIBIR EL CONTRATO ES PRORROGADO, SIEMPRE QUE TAL PRÓRROGA SEA INFERIOR A TRES (3) MESES.

1.1.2 EL RETIRO DE LA OFERTA DESPUÉS DE VENCIDO EL PLAZO FIJADO PARA LA PRESENTACIÓN DE LAS OFERTAS.

1.1.3 LA NO SUSCRIPCIÓN DEL CONTRATO SIN JUSTA CAUSA POR PARTE DEL ADJUDICATARIO.

1.1.4 LA FALTA DE OTORGAMIENTO POR PARTE DEL PROPONENTE SELECCIONADO DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

1.2 AMPARO DE BUEN MANEJO Y CORRECTA INVERSIÓN DEL ANTICIPO.

EL AMPARO DE BUEN MANEJO Y CORRECTA INVERSIÓN DEL ANTICIPO CUBRE A LA ENTIDAD ESTATAL ASEGURADA, DE LOS PERJUICIOS QUE SE LE LLEGUEN A CAUSAR, CON OCASIÓN DE (I) LA NO INVERSIÓN DEL ANTICIPO, (II) EL USO INDEBIDO DEL ANTICIPO Y (III) LA APROPIACIÓN INDEBIDA DE LOS RECURSOS RECIBIDOS POR EL CONTRATISTA GARANTIZADO EN CALIDAD DE ANTICIPO.

1.3 AMPARO DE DEVOLUCIÓN DE PAGO ANTICIPADO.

EL AMPARO DE DEVOLUCIÓN DE PAGO ANTICIPADO CUBRE A LA ENTIDAD ESTATAL ASEGURADA, DE LOS PERJUICIOS QUE SE LE CAUSEN POR LA NO DEVOLUCIÓN TOTAL O PARCIAL, DEL DINERO ENTREGADO AL CONTRATISTA GARANTIZADO A TÍTULO DE PAGO ANTICIPADO, CUANDO A ELLO HUBIERE LUGAR.

1.4 AMPARO DE CUMPLIMIENTO DEL CONTRATO.

EL AMPARO DE CUMPLIMIENTO, CUBRE A LA ENTIDAD ESTATAL ASEGURADA, POR LOS PERJUICIOS DIRECTOS DERIVADOS DE: (A) EL INCUMPLIMIENTO TOTAL O PARCIAL DEL CONTRATO, CUANDO EL INCUMPLIMIENTO ES IMPUTABLE AL CONTRATISTA; (B) EL CUMPLIMIENTO TARDÍO O DEFECTUOSO DEL CONTRATO, CUANDO EL INCUMPLIMIENTO ES IMPUTABLE AL CONTRATISTA; (C) LOS DAÑOS IMPUTABLES AL CONTRATISTA POR ENTREGAS PARCIALES DE LA OBRA, CUANDO EL CONTRATO NO PREVÉ ENTREGAS PARCIALES; Y (D) EL PAGO DEL VALOR DE LAS MULTAS Y DE LA CLÁUSULA PENAL PECUNIARIA SIEMPRE QUE SE HUBIEREN PACTADO PREVIAMENTE EN EL CONTRATO GARANTIZADO.

EN VIRTUD DE LO SEÑALADO POR EL ARTÍCULO 44 DE LA LEY 610 DE 2000, LA GARANTÍA DE CUMPLIMIENTO CUBRIRÁ LOS PERJUICIOS CAUSADOS A LA ENTIDAD ESTATAL COMO CONSECUENCIA DE LA CONDUCTA DOLOSA O CULPOSA, IMPUTABLE AL CONTRATISTA GARANTIZADO, DERIVADOS DE UN PROCESO DE RESPONSABILIDAD FISCAL, SIEMPRE Y CUANDO ESOS PERJUICIOS DERIVEN DEL INCUMPLIMIENTO DE LAS

OBLIGACIONES SURGIDAS DEL CONTRATO AMPARADO POR LA GARANTÍA.

1.5 AMPARO DE PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES.

EL AMPARO DE PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES DE NATURALEZA LABORAL, CUBRE A LA ENTIDAD ESTATAL ASEGURADA, POR LOS PERJUICIOS QUE SE LE OCASIONEN, A RAÍZ DEL INCUMPLIMIENTO DE LAS OBLIGACIONES LABORALES A QUE ESTÉ OBLIGADO EL CONTRATISTA GARANTIZADO, DERIVADAS DE LA CONTRATACIÓN DEL PERSONAL UTILIZADO PARA LA EJECUCIÓN DEL CONTRATO AMPARADO EN EL TERRITORIO NACIONAL.

ESTA GARANTÍA NO SE APLICARÁ PARA LOS CONTRATOS QUE SE EJECUTEN EN SU TOTALIDAD FUERA DEL TERRITORIO NACIONAL POR PERSONAL CONTRATADO BAJO UN RÉGIMEN JURÍDICO DISTINTO AL NACIONAL.

1.6 AMPARO DE ESTABILIDAD Y CALIDAD DE LA OBRA.

EL AMPARO DE ESTABILIDAD Y CALIDAD DE LA OBRA, CUBRE A LA ENTIDAD ESTATAL ASEGURADA, DE LOS PERJUICIOS QUE SE LE GENEREN COMO CONSECUENCIA DE CUALQUIER TIPO DE DAÑO O DETERIORO, PRESENTADOS EN LA OBRA ENTREGADA Y RECIBIDA A SATISFACCIÓN DE DICHA ENTIDAD ESTATAL O SUS REPRESENTANTES, CUYA CAUSA SEA IMPUTABLE AL CONTRATISTA GARANTIZADO.

1.7 AMPARO DE CALIDAD DEL SERVICIO

EL AMPARO DE CALIDAD DEL SERVICIO CUBRE A LA ENTIDAD ESTATAL ASEGURADA, DE LOS PERJUICIOS IMPUTABLES AL CONTRATISTA GARANTIZADO, QUE SE OCASIONEN CON POSTERIORIDAD A LA TERMINACIÓN DEL CONTRATO GARANTIZADO, Y QUE SE DERIVEN DE LA DEFICIENTE CALIDAD DEL SERVICIO PRESTADO.

EN LOS CONTRATOS DE INTERVENTORIA, LA VIGENCIA DE ÉSTE AMPARO DEBE SER IGUAL AL PLAZO DE LA GARANTÍA DE ESTABILIDAD DEL CONTRATO PRINCIPAL EN CUMPLIMIENTO DEL PARAGRAFO DEL ARTÍCULO 85 DE LA LEY 1474 DE 2011.

1.8 CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES Y EQUIPOS SUMINISTRADOS.

ESTE AMPARO CUBRE A LA ENTIDAD ESTATAL ASEGURADA DE LOS PERJUICIOS OCASIONADOS IMPUTABLES AL CONTRATISTA, SUFRIDOS POR LA DEFICIENTE CALIDAD E INCORRECTO FUNCIONAMIENTO DE LOS BIENES QUE RECIBE LA ENTIDAD ESTATAL ASEGURADA EN CUMPLIMIENTO DEL CONTRATO GARANTIZADO.

2. EXCLUSIONES.

LOS AMPAROS OTORGADOS EN LA PRESENTE PÓLIZA NO OPERARÁN CUANDO LOS DAÑOS A LA ENTIDAD ESTATAL ASEGURADA SE GENEREN POR:

2.1 CAUSA EXTRAÑA, ESTO ES, LA FUERZA MAYOR O CASO FORTUITO, EL HECHO DE UN TERCERO O LA CULPA EXCLUSIVA DE LA VÍCTIMA.

2.2 DAÑOS CAUSADOS POR EL CONTRATISTA GARANTIZADO, A LOS BIENES DE LA ENTIDAD ESTATAL ASEGURADA, NO DESTINADOS AL CUMPLIMIENTO DEL OBJETO CONTRACTUAL.

2.3. EL USO INDEBIDO O INADECUADO O LA FALTA DE MANTENIMIENTO PREVENTIVO A QUE SE ENCUENTRE OBLIGADA LA ENTIDAD ESTATAL ASEGURADA.

2.4. EL DETERIORO NORMAL QUE SUFRAN LOS BIENES ENTREGADOS CON OCASIÓN DEL CONTRATO GARANTIZADO, COMO CONSECUENCIA DEL TRANSURSO DEL TIEMPO.

3. SUMA ASEGURADA.

DE CONFORMIDAD CON EL ARTÍCULO 1079 DEL CÓDIGO DE COMERCIO, SEGURESTADO NO ESTARÁ OBLIGADO A RESPONDER SI NO HASTA CONCURRENCIA DE LA SUMA ASEGURADA EN CASO DE SINIESTRO, DETERMINADA EN LA CARÁTULA DE ESTA PÓLIZA PARA CADA AMPARO.

4. VIGENCIA.

LA VIGENCIA DE LOS AMPAROS OTORGADOS EN LA PRESENTE PÓLIZA, SE HARÁ BAJO LOS LINEAMIENTOS DEL DECRETO 1082 DE 2015 Y CONSTARÁN EN LA CARÁTULA DE LA MISMA O EN SUS ANEXOS.

5. EFECTIVIDAD DE LA GARANTÍA.

PARA HACER EFECTIVOS CUALQUIERA DE LOS AMPAROS OTORGADOS POR SEGURESTADO, LA ENTIDAD ESTATAL ASEGURADA DEBERÁ GARANTIZAR EL DEBIDO PROCESO DE SEGURESTADO Y EL CONTRATISTA, MEDIANTE EL AGOTAMIENTO DEL PROCEDIMIENTO ESTABLECIDO EN EL ARTÍCULO 86 DE LA LEY 1474 DE 2011 O LAS NORMAS QUE LO SUSTITUYAN O MODIFIQUEN.

LA ENTIDAD ESTATAL ASEGURADA, LE CORRESPONDERÁ DEMOSTRAR LA OCURRENCIA DEL SINIESTRO Y ACREDITAR LA CUANTÍA DE LA PÉRDIDA SI FUERE EL CASO.

EL PROCEDIMIENTO QUE DEBERÁ SEGUIR LA ENTIDAD ESTATAL ASEGURADA, PARA LA EFECTIVIDAD DE LOS AMPAROS OTORGADOS POR ESTA PÓLIZA, SERÁ:

5.1. RESPECTO DEL AMPARO DE SERIEDAD DE LA OFERTA, LA ENTIDAD ESTATAL ASEGURADA PROFERIRÁ EL ACTO ADMINISTRATIVO QUE IMPONGA LA SANCIÓN PREVIAMENTE ESTABLECIDA POR LA OCURRENCIA DE UNO CUALQUIERA DE LOS EVENTOS PREVISTOS EN LA CONDICIÓN 1.1 DE ÉSTA PÓLIZA, Y DISPONGA LA EFECTIVIDAD DE ÉSTE AMPARO A SEGURESTADO.

5.2. EN CASO DE DECRETARSE LA CADUCIDAD, LA ENTIDAD ESTATAL ASEGURADA PROFERIRÁ EL ACTO ADMINISTRATIVO CORRESPONDIENTE EN EL CUAL, ADEMÁS DE LA DECLARATORIA DE LA MISMA, HARÁ EFECTIVA LA CLÁUSULA PENAL O CUANTIFICARÁ EL MONTO DEL PERJUICIO, ORDENANDO SU PAGO TANTO AL CONTRATISTA COMO A SEGURESTADO. DICHO ACTO ADMINISTRATIVO SERÁ CONSTITUTIVO DEL SINIESTRO.

5.3. EN EL EVENTO DE IMPOSICIÓN DE MULTAS, LA ENTIDAD ESTATAL ASEGURADA, PROFERIRÁ EL ACTO ADMINISTRATIVO CORRESPONDIENTE ORDENANDO SU PAGO AL CONTRATISTA Y SEGURESTADO. DICHO ACTO ADMINISTRATIVO SERÁ CONSTITUTIVO DEL SINIESTRO.

5.4. EN LOS DEMÁS EVENTOS DE INCUMPLIMIENTO DEL CONTRATISTA GARANTIZADO, LA ENTIDAD ESTATAL ASEGURADA, PROFERIRÁ EL ACTO ADMINISTRATIVO CORRESPONDIENTE, EN EL CUAL, ADEMÁS DE DECLARAR EL INCUMPLIMIENTO, PROCEDERÁ A CUANTIFICAR EL MONTO DE LA PÉRDIDA O A HACER EFECTIVA LA CLÁUSULA PENAL, ORDENANDO SU PAGO AL CONTRATISTA Y SEGURESTADO. EL ACTO ADMINISTRATIVO CORRESPONDIENTE ES LA RECLAMACIÓN PARA LA COMPAÑÍA DE SEGURO.

LOS ACTOS ADMINISTRATIVOS EMITIDOS POR LA ENTIDAD ESTATAL CONTRATANTE QUE SEAN CONSTITUTIVOS O DECLARATIVOS DEL SINIESTRO, DEBERÁN ESTAR EJECUTORIADOS Y DEBIDAMENTE NOTIFICADOS, DE ACUERDO CON EL ARTÍCULO 87 DE LA LEY 1437 DE 2011.

6. COMPENSACIÓN.

EN VIRTUD DE LA COMPENSACIÓN COMO MEDIO DE EXTINCIÓN DE LAS OBLIGACIONES RECONOCIDA EL ARTÍCULO 17 DE LA LEY 1150 DE 2007, SEGURESTADO TENDRÁ EN CUENTA TODAS LAS SUMAS DE DINERO QUE LA ENTIDAD ESTATAL ASEGURADA LE ADEUDE AL CONTRATISTA GARANTIZADO, POR CUALQUIER CONCEPTO. PARA TALES EFECTOS, SE DEBERÁ TENER EN CUENTA LA LIQUIDACIÓN DEL CONTRATO GARANTIZADO, EFECTUADA EN LOS TÉRMINOS LEGALES O CONVENCIONALES.

7. FORMAS DE PAGO DE LA INDEMNIZACIÓN.

LA INDEMNIZACIÓN SERÁ PAGADERA EN DINERO, O MEDIANTE LA REPOSICIÓN, REPARACIÓN O RECONSTRUCCIÓN DE LA COSA ASEGURADA, A OPCIÓN DE SEGURESTADO, SIN PERJUICIO QUE LA ENTIDAD ESTATAL ASEGURADA EN EL EVENTO DE DECLARATORIA DE CADUCIDAD DECIDA CONTINUAR LA EJECUCIÓN DEL OBJETO CONTRATADO A TRAVÉS DE SEGURESTADO O DE OTRO CONTRATISTA, A QUIEN A SU VEZ SE LE PODRÁ DECLARAR LA CADUCIDAD, SI A ELLO HUBIERE LUGAR.

EN EL EVENTO EN QUE POR INCUMPLIMIENTO DEL CONTRATISTA GARANTIZADO, SEGURESTADO RESOLVIERA CONTINUAR, COMO CESIONARIO, CON LA EJECUCIÓN DEL CONTRATO Y LA ENTIDAD ESTATAL ASEGURADA ESTUVIESE DE ACUERDO CON ELLO, EL CONTRATISTA GARANTIZADO ACEPTA DESDE EL MOMENTO DE LA CONTRATACIÓN DE ESTA PÓLIZA, LA CESIÓN DEL CONTRATO GARANTIZADO A FAVOR DE SEGURESTADO.

8. PLAZO PARA EL PAGO.

DE CONFORMIDAD CON EL ARTÍCULO 1080 DEL CÓDIGO DE COMERCIO, SEGURESTADO DEBERÁ EFECTUAR EL PAGO DEL SINIESTRO DENTRO DEL MES SIGUIENTE AL CUAL LA ENTIDAD ESTATAL ASEGURADA HAYA ACREDITADO LOS REQUISITOS DEL ARTÍCULO 1077 DEL CÓDIGO DE COMERCIO, A TRAVÉS DEL ACTO ADMINISTRATIVO A QUE HACE REFERENCIA EL NUMERAL 5. DE ESTAS CONDICIONES.

9. CERTIFICADOS O ANEXOS DE MODIFICACIÓN.

PARA LOS CASOS EN QUE LA SUMA ASEGURADA DE ESTA PÓLIZA DEBA SER AUMENTADA O DISMINUIDA Y PARA AQUELLOS EN LOS CUALES LAS ESTIPULACIONES DEL CONTRATO GARANTIZADO SEAN MODIFICADAS, SEGURESTADO A SOLICITUD PREVIA DEL CONTRATISTA GARANTIZADO Y DE LA ENTIDAD ESTATAL ASEGURADA (O EL INTERVENTOR, SUPERVISOR, ETC., EN SU CASO), EXPEDIRÁ UN CERTIFICADO O ANEXO DE MODIFICACIÓN DE LA PÓLIZA, EN EL CUAL CONSTEN LAS MODIFICACIONES CORRESPONDIENTES. PARA TAL EFECTO SE HACE INDISPENSABLE ACOMPAÑAR A LA SOLICITUD DE MODIFICACIÓN A SEGURESTADO EL DOCUMENTO (OTOSÍ, CLÁUSULA ADICIONAL, ETC.) QUE CONTENGA LAS MODIFICACIONES AL CONTRATO GARANTIZADO.

EL ÚLTIMO ANEXO O CERTIFICADO DE MODIFICACIÓN, SERÁ EL QUE LA ENTIDAD ESTATAL ASEGURADA HARÁ EFECTIVO, DE CONFORMIDAD CON EL NUMERAL 5. DE ESTAS CONDICIONES.

10. VIGILANCIA SOBRE LA EJECUCIÓN DEL CONTRATO GARANTIZADO.

SEGURESTADO TENDRÁ LA FACULTAD DE EJERCER LA VIGILANCIA DEL CONTRATO, PARA LO CUAL LA ENTIDAD ESTATAL ASEGURADA LE PRESTARÁ LA COLABORACIÓN NECESARIA PARA ELLO. EN LOS CASOS EN LOS CUALES EL CONTRATO GARANTIZADO TENGA POR OBJETO ASUNTOS RELACIONADOS CON EL ORDEN PÚBLICO Y LA SEGURIDAD NACIONAL, LA ENTIDAD ESTATAL ASEGURADA PODRÁ PROHIBIR O LIMITAR ÉSTA FACULTAD.

11. NO CANCELACIÓN DE LA PÓLIZA POR FALTA DE PAGO DE LA PRIMA E IRREVOCABILIDAD DE ESTE SEGURO.

LA PRESENTE PÓLIZA NO EXPIRARÁ POR FALTA DE PAGO DE LA PRIMA NI PODRÁ SER REVOCADA UNILATERALMENTE.

12. CLÁUSULAS INCOMPATIBLES

EN CASO DE INCONGRUENCIA PRESENTADA ENTRE LAS CONDICIONES PARTICULARES Y LAS CONDICIONES GENERALES DE ESTA PÓLIZA, PREVALECEERÁN LAS PRIMERAS.

13. COASEGURO

EN CASO DE EXISTIR COASEGURO, ESTO ES LA DISTRIBUCIÓN ENTRE VARIAS ASEGURADORAS DE DETERMINADO RIESGO, AL NO EXISTIR SOLIDARIDAD ENTRE LAS MISMAS, EL IMPORTE DE LA INDEMNIZACIÓN SE DISTRIBUIRÁ Y HARÁ EXIGIBLE ENTRE LOS COASEGURADORES, EN PROPORCIÓN A LAS CUANTÍAS DE SU RESPECTIVA PARTICIPACIÓN.

LA GERENCIA DE AFILIACIONES Y NOVEDADES

CERTIFICA QUE:

YESSID ARAMIS CACERES VASQUEZ identificado con CC. 72342326 registra la siguiente información en el ramo de Riesgos Laborales:

INFORMACIÓN DEL CONTRATANTE			
Nombres y/o Razón	ESCUELA SUPERIOR DE GUERRA		
Tipo y Numero de Documento	NI - 830002634		

INFORMACIÓN RELACIÓN LABORAL			
Fecha de inicio de cobertura	2026/01/27	Fecha inicio contrato	2026/01/26
Tipo de vinculación	Independiente con Contrato	Fecha de fin contrato	2026/12/31
Riesgo	1	Código actividad económica	1620202 - ACTIVIDADES DE CONSULTORIA INFORMATICA Y ACTIVIDADES DE ADMINISTRACION DE
Estado afiliación	Activo		
Fecha retiro		Estado del contrato	Activo

Esta certificación se expide a los 16 días del mes de febrero del 2026.

Tenga en cuenta que, una vez finalice la fecha de terminación del contrato, el sistema aplicará automáticamente el retiro. Si tiene un nuevo contrato o prórroga, registre la novedad en www.positivaenlinea.gov.co para mantener la cobertura.

Para verificar la autenticidad de este certificado, escanea el código QR incluido o visita nuestra página web. Selecciona la opción "Validar certificados de afiliación" e ingresa el siguiente código: **CC16022026Y72342326C9084213**. Este código es válido por un mes.

Cordialmente,

Gerencia de afiliaciones y novedades ARL

POSITIVA COMPAÑIA DE SEGUROS

Positiva Compañía de Seguros S.A.:

Nit. 860.011.153-6 | Línea Gratuita Nacional: (+57) 01-8000-111-170 - Teléfono: +57 (601) 330 7000

Defensor del Consumidor Financiero: Ana María Giraldo (Principal) - Pablo Valencia (Suplente) | defensordelcliente@positiva.gov.co | Carrera 10 #97A - 13, Oficina 502. Bogotá | +57 (601) 610 8164 | Lunes a Viernes 8:00 a. m. -- 6:00 p. m. | El Defensor, resolverá las quejas o reclamos, actuará como Conciliador ante Positiva.

Más información: <https://www.positiva.gov.co/web/guest/defensoria-del-consumidor>
Puedes interponer una queja ante Positiva, o el Defensor, o la SFC u otro organismo de

**LA ASEGURADORA
DE TODOS LOS
COLOMBIANOS**

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**) ☒
- 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 febrero 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 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 practicará 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)

Bogotá D.C. febrero de 2026

RADICADO No. 0126105718 / MDN-COGFM-JEMCO-ESDEG-SBESG-VIADM-DETI

Señor Teniente
Enrique Ramírez Flor
Supervisor del Contrato

ASUNTO: Informe mensual de actividades enero y febrero 2026

Me permito presentar el informe correspondiente a las actividades desarrolladas al inicio del año, orientadas a garantizar la estabilidad, continuidad operativa y seguridad de la plataforma tecnológica institucional tras el cierre de la vigencia anterior.

Las acciones adelantadas estuvieron enfocadas en la verificación integral de la infraestructura de copias de seguridad —incluyendo ExaGrid, almacenamiento Hitachi y Veeam Backup— así como en la revisión y validación de las barreras perimetrales, la infraestructura de red, la plataforma de virtualización en Proxmox y VMware, la capacidad de almacenamiento, la disponibilidad de la red WIFI institucional y los mecanismos de protección asociados a certificados digitales y configuraciones SSL/TLS. De igual manera, se realizaron ajustes preventivos y validaciones técnicas sobre los equipos de seguridad perimetral y sus componentes asociados, junto con la actualización de la documentación técnica correspondiente al estado inicial del año operativo.

A continuación, se relacionan las principales acciones desarrolladas:

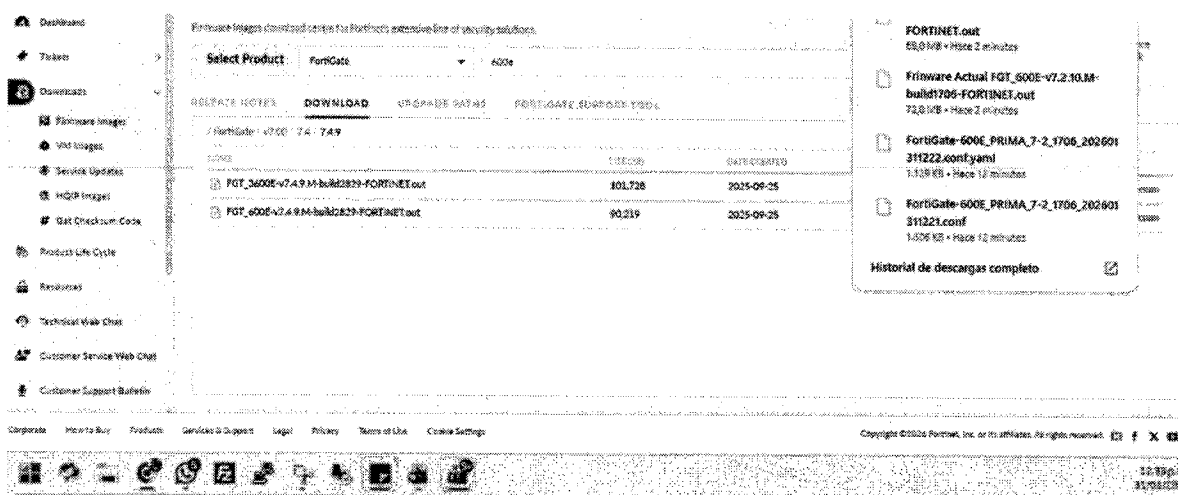
1. Se realizó verificación del estado operativo de las plataformas tecnológicas institucionales

1.1. Barreras perimetrales (FortiGate 600E en alta disponibilidad, switches core, switches de acceso y FortiAPs)

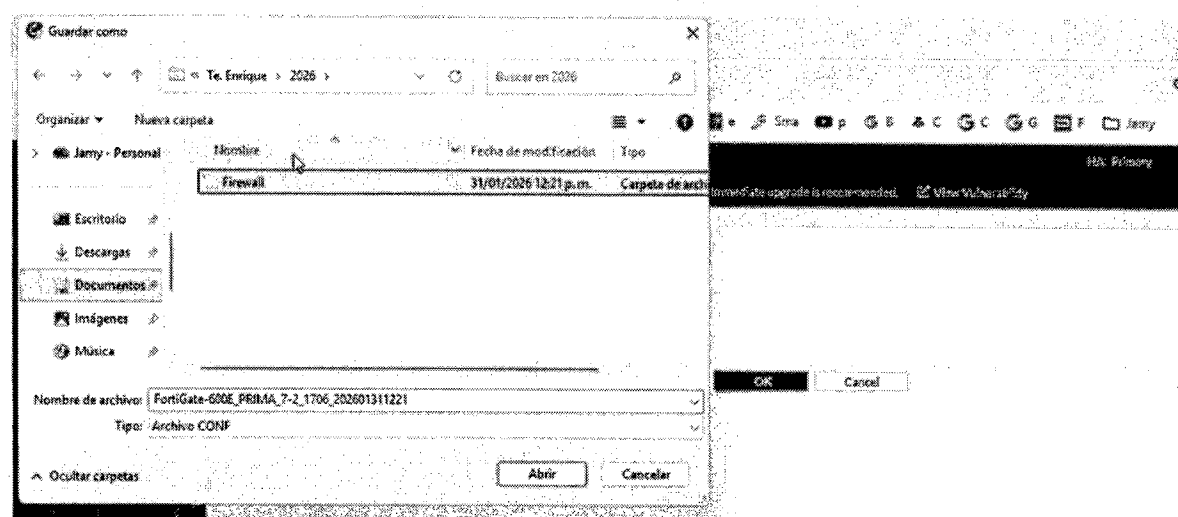
Se evidenció que el dispositivo FortiGate 600E (HA: Primary) se encontraba operando bajo la versión 7.2.10 (build 1706 – Mature) y presentaba una alerta crítica de vulnerabilidad, indicada en la franja roja del sistema (“This FortiGate is subject to a critical severity vulnerability. Immediate upgrade is recommended”), lo cual motivó la ejecución del proceso de actualización de firmware para mitigar el riesgo identificado y fortalecer la postura de seguridad perimetral institucional.

Previo a la actualización del firmware del dispositivo FortiGate 600E, se realizaron verificaciones exhaustivas y se recopilaron evidencias para asegurar que la actividad no tuviera efecto negativo sobre la infraestructura tecnológica. Estas validaciones fueron fundamentales para documentar el estado inicial de la infraestructura.

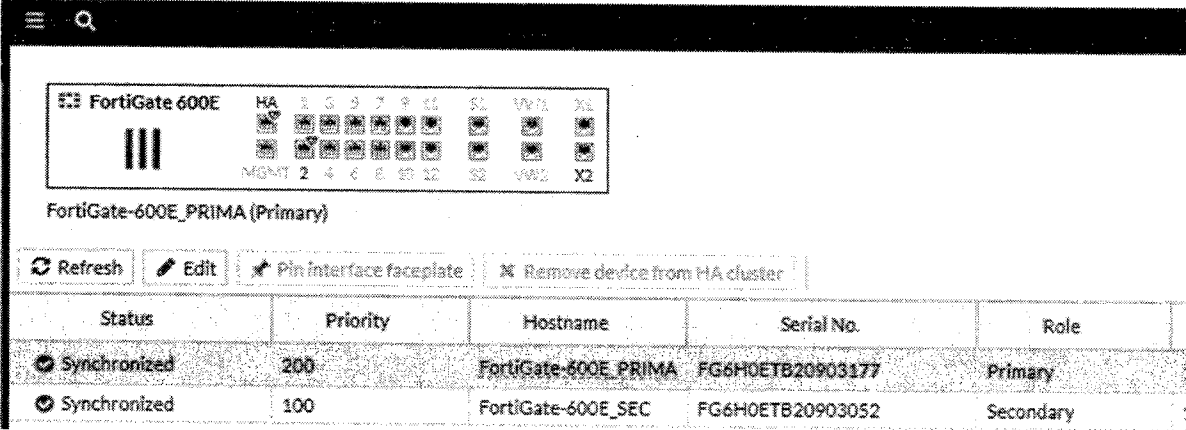
Se realizó la descarga de las imágenes de firmware correspondientes al modelo FortiGate 600E, específicamente las versiones **FGT_600E-v7.4.9.M-build2829-FORTINET.out** y **FGT_600E-v7.4.7.M-build2829-FORTINET.out**, conforme a la ruta oficial de actualización disponible en el portal de soporte de Fortinet, dejando los archivos preparados para su posterior carga y ejecución controlada en el dispositivo.



Para asegurar la operatividad, se realiza un backup de las configuraciones actuales



Se efectuó la validación técnica de los dispositivos FortiGate 600E configurados en alta disponibilidad (HA), verificando estado primario/secundario, correcta sincronización de configuración, estabilidad del firmware actualizado a versión 7.4.11, integridad de políticas de seguridad, reglas internas asociadas a servidores y almacenamiento, funcionamiento de SD-WAN, VPN y servicios integrados (Fabric). Se confirmó operación estable sin alertas críticas, sin reinicios inesperados y con consumo de recursos dentro de parámetros normales y se empieza el proceso de actualización .



The screenshot shows the FortiGate HA cluster configuration page. At the top, there is a diagram of the HA cluster with two nodes: FortiGate-600E_PRIMA (Primary) and FortiGate-600E_SEC (Secondary). Below the diagram, there are buttons for Refresh, Edit, Pin interface faceplate, and Remove device from HA cluster. A table below shows the status of the HA cluster.

Status	Priority	Hostname	Serial No.	Role
Synchronized	200	FortiGate-600E_PRIMA	FG6H0ETB20903177	Primary
Synchronized	100	FortiGate-600E_SEC	FG6H0ETB20903052	Secondary

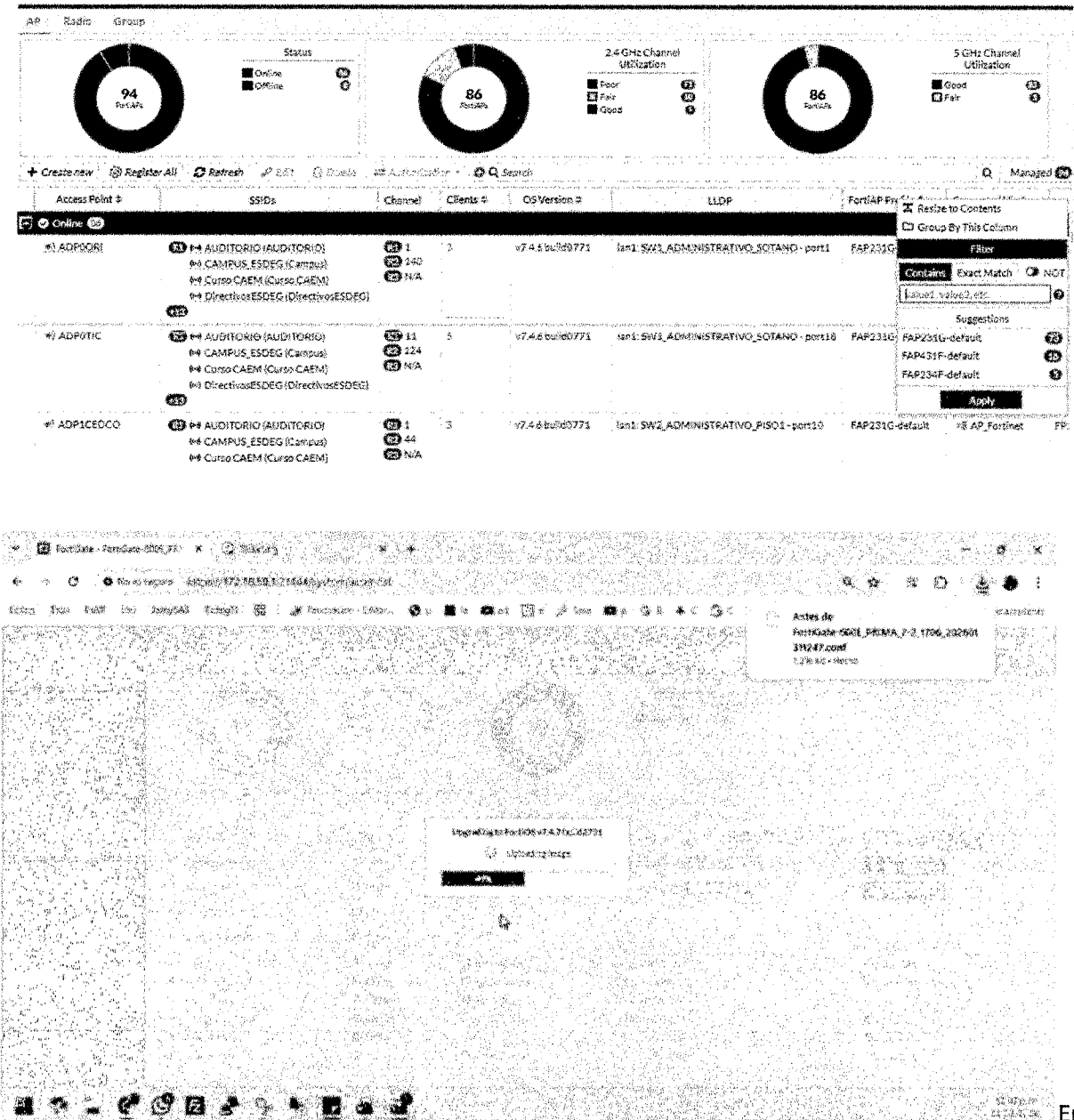
HA Fortigate 600 E (Principal y Secundario)



The screenshot shows the FortiGate switch configuration page. At the top, there are two donut charts showing the status of the switches: 34 Online and 34 Offline. Below the charts, there are buttons for Create New, Edit, Delete, Authorization, Upgrade, Register All, and Search. A table below shows the configuration of the switches. A dropdown menu is open, showing the filter options: Contains, Does Not Contain, and Regex. The table has columns for Name, Switch Group, Status, Model, and Firmware Version.

Name	Switch Group	Status	Model	Firmware Version
SW_CORE_PRIN (FS1E48T423002199)		Online	FortiSwitch 1048E	
SW_CORE_SEC (FS1E48T423001673)		Online	FortiSwitch 1048E	
SW1_ADMINISTRATIVO_PISO3 (S124FNTF23009104)		Online	FortiSwitch 124F	
SW1_ADMINISTRATIVO_PISO4 (S148FPTF23003136)		Online	FortiSwitch 148F-POE	
SW2_AULAS_PISO1 (S148FPTF23005514)		Online	FortiSwitch 148F-POE	
SW3_AULAS_PISO1 (S148FPTF23004549)		Online	FortiSwitch 148F-POE	
SW4_AULAS_PISO1 (S148FPTF23002164)		Online	FortiSwitch 148F-POE	
SW5_AULAS_PISO1 (S148FPTF23003121)		Online	FortiSwitch 148F-POE	
SW1_AULAS_PISO3 (S148FPTF23002081)		Online	FortiSwitch 148F-POE	
SW1_AULAS_PISO6 (S148FPTF23004881)		Online	FortiSwitch 148F-POE	
SW2_AULAS_PISO6 (S148FPTF23002314)		Online	FortiSwitch 148F-POE	
SW1_ADMINISTRATIVO_SOTANO (S148FPTF23003091)		Online	FortiSwitch 148F-POE	
SW2_AULAS_PISO3 (S148FPTF23002995)		Online	FortiSwitch 148F-POE	

FortiSwitch 148F-POE / FortiSwitch 124F / FortiSwitch 1048E / FortiSwitch 1048E-POE / FortiSwitch 1048F- POE

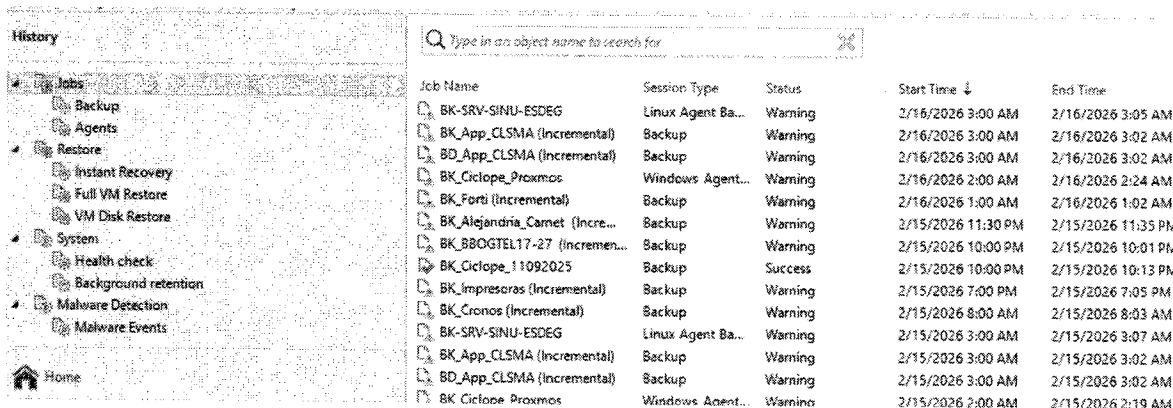


total se actualizaron 34 FortiSwitch, 2 Core, 2 Fortigate y 94 AP.

Para este proceso podemos concluir que: La ejecución de la actualización del FortiGate se realizó de manera exitosa, cumpliendo con los objetivos establecidos y garantizando la estabilidad del sistema. Durante el proceso, se siguieron los protocolos de planificación, pruebas y validación, lo que permitió minimizar riesgos y asegurar una transición sin impacto en los servicios

1.2. Se realizó verificación del estado operativo de la plataforma Veeam Backup.

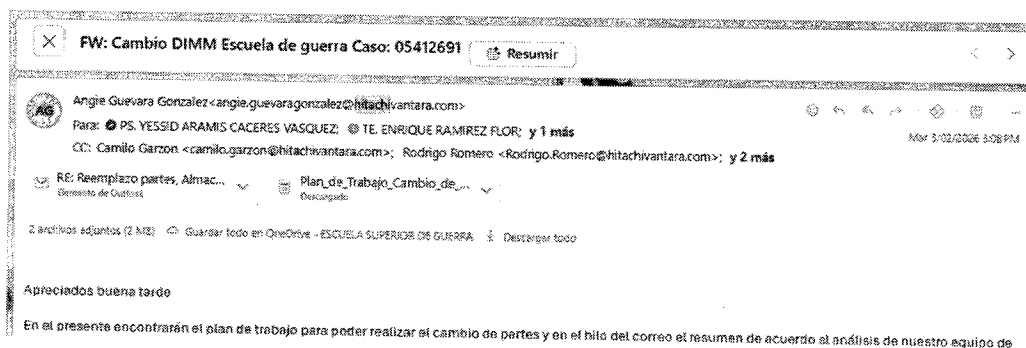
Se evidenció en consola que el servidor se encontraba operativo, con los servicios activos y sin alertas críticas (las únicas alertas son de no envío de correo). Se validó la ejecución reciente de los trabajos de respaldo, confirmando finalización satisfactoria y correcta disponibilidad de los repositorios configurados en ExaGrid.



Job Name	Session Type	Status	Start Time	End Time
BK-SRV-SINU-ESDEG	Linux Agent Ba...	Warning	2/16/2026 3:00 AM	2/16/2026 3:05 AM
BK_App_CLSMA (Incremental)	Backup	Warning	2/16/2026 3:00 AM	2/16/2026 3:02 AM
BD_App_CLSMA (Incremental)	Backup	Warning	2/16/2026 3:00 AM	2/16/2026 3:02 AM
BK_Ciclope_Proximos	Windows Agent...	Warning	2/16/2026 2:00 AM	2/16/2026 2:24 AM
BK_Forti (Incremental)	Backup	Warning	2/16/2026 1:00 AM	2/16/2026 1:02 AM
BK_Alejandria_Carnet (Incre...	Backup	Warning	2/15/2026 11:30 PM	2/15/2026 11:35 PM
BK_BBOTTEL17-27 (Incremen...	Backup	Warning	2/15/2026 10:00 PM	2/15/2026 10:01 PM
BK_Ciclope_11092025	Backup	Success	2/15/2026 10:00 PM	2/15/2026 10:13 PM
BK_Impresoras (Incremental)	Backup	Warning	2/15/2026 7:00 PM	2/15/2026 7:05 PM
BK_Cronos (Incremental)	Backup	Warning	2/15/2026 8:00 AM	2/15/2026 8:03 AM
BK-SRV-SINU-ESDEG	Linux Agent Ba...	Warning	2/15/2026 3:00 AM	2/15/2026 3:07 AM
BK_App_CLSMA (Incremental)	Backup	Warning	2/15/2026 3:00 AM	2/15/2026 3:02 AM
BD_App_CLSMA (Incremental)	Backup	Warning	2/15/2026 3:00 AM	2/15/2026 3:02 AM
BK Ciclope Proximos	Windows Agent...	Warning	2/15/2026 2:00 AM	2/15/2026 2:19 AM

1.3. Se realizó verificación del estado operativo de la plataforma Hitachi VSP E590

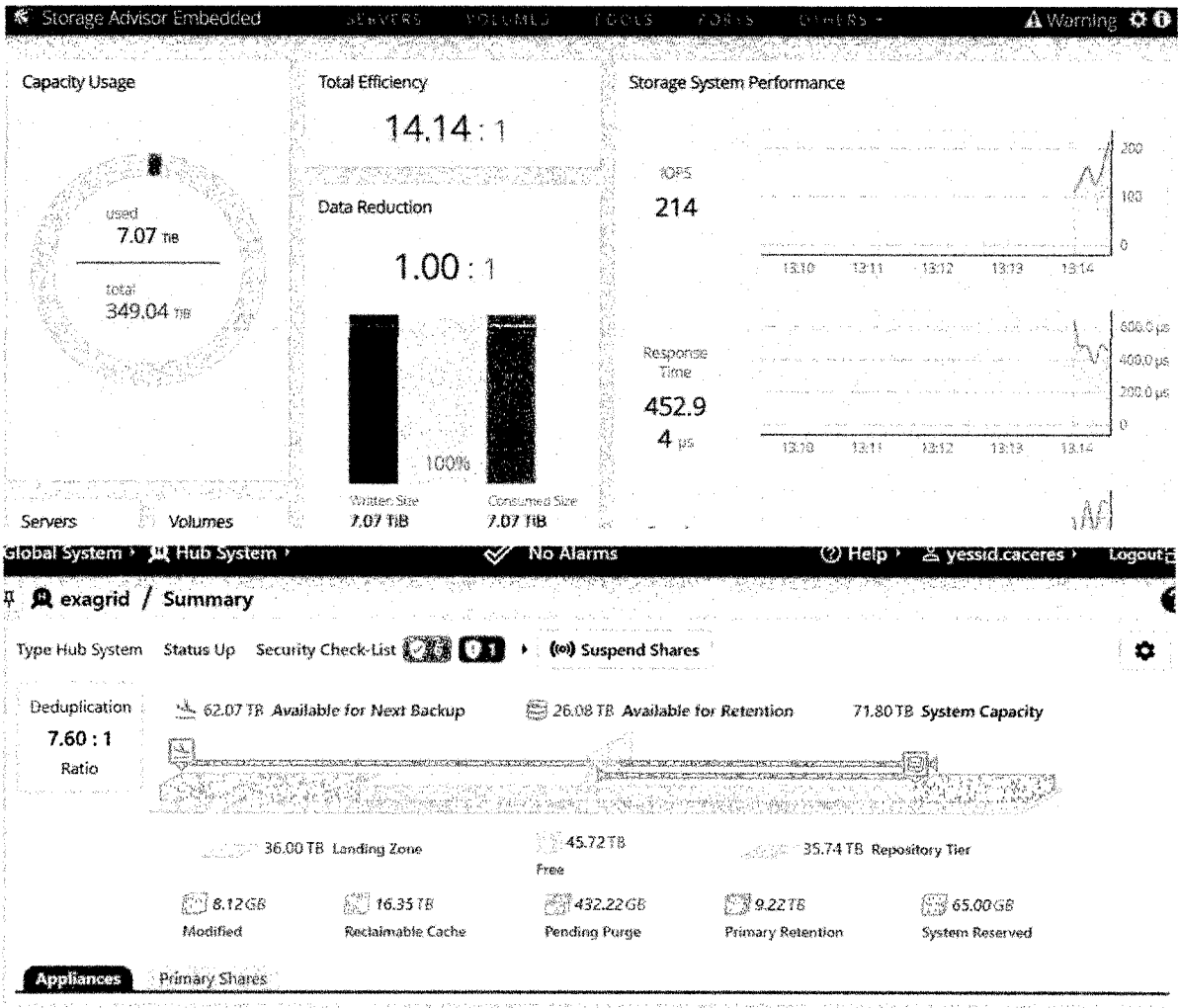
Se evidenció una notificación técnica relacionada con un *cache correctable error* en el módulo de memoria DIMM 02 de la Controladora 2. El sistema continúa operando, sin afectación inmediata al servicio; sin embargo, en atención a esta condición, se gestionó el caso 05412691 con el fabricante y se recibió el plan formal de trabajo para el reemplazo preventivo del componente, incluyendo análisis técnico, prerequisites, impacto y plan de mitigación. La actividad fue coordinada y cuenta con ventana de mantenimiento programada, conforme a las recomendaciones técnicas emitidas.



2. Monitorear el estado de capacidad de almacenamiento en los Nodos de backup y en las cabinas de almacenamiento, anticipando crecimiento y generando recomendaciones para evitar saturación durante el primer trimestre.

Se realizó monitoreo del estado de capacidad en los nodos de backup y en el servidor de almacenamiento Hitachi y Exagrid, verificando porcentaje de uso, espacio disponible y tendencia de crecimiento actual. Al momento de la revisión, los sistemas operan dentro de parámetros normales, sin evidencia de saturación ni alertas críticas asociadas a capacidad.

Se mantiene seguimiento preventivo sobre el comportamiento del almacenamiento, con el fin de anticipar posibles incrementos de consumo durante el primer trimestre y garantizar disponibilidad continua de los recursos de respaldo y virtualización.

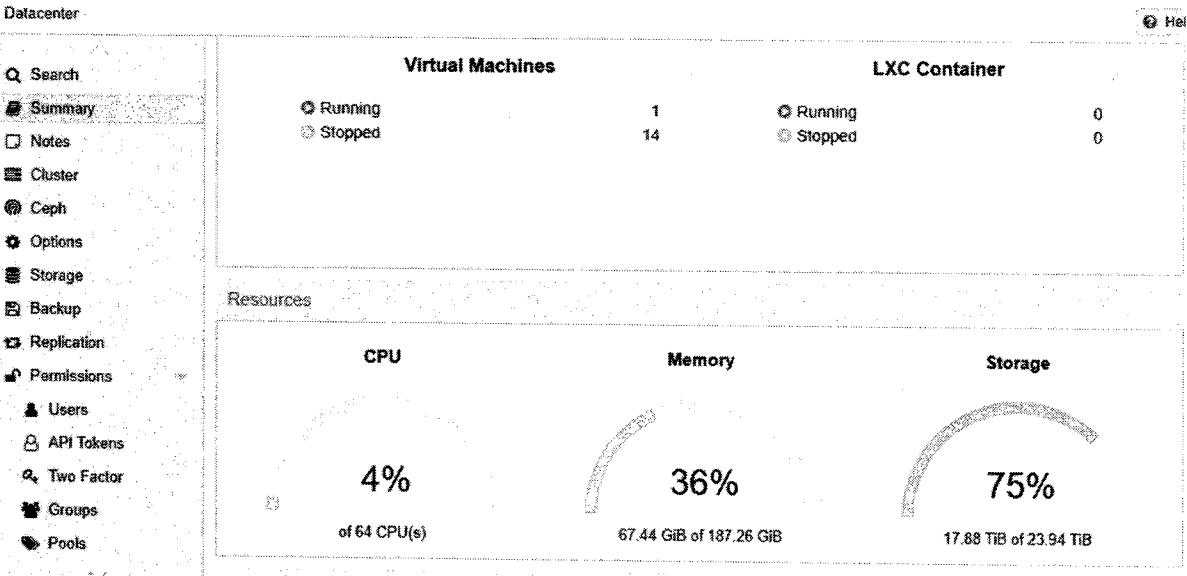


3. Realizar revisión general de la plataforma de virtualización en Proxmox y VMware, identificando oportunidades de optimización de rendimiento, balanceo de carga y estabilidad para el inicio del año. Se realizó revisión general del estado de la plataforma de virtualización en Proxmox y VMware:

3.1. Estado de Proxmox

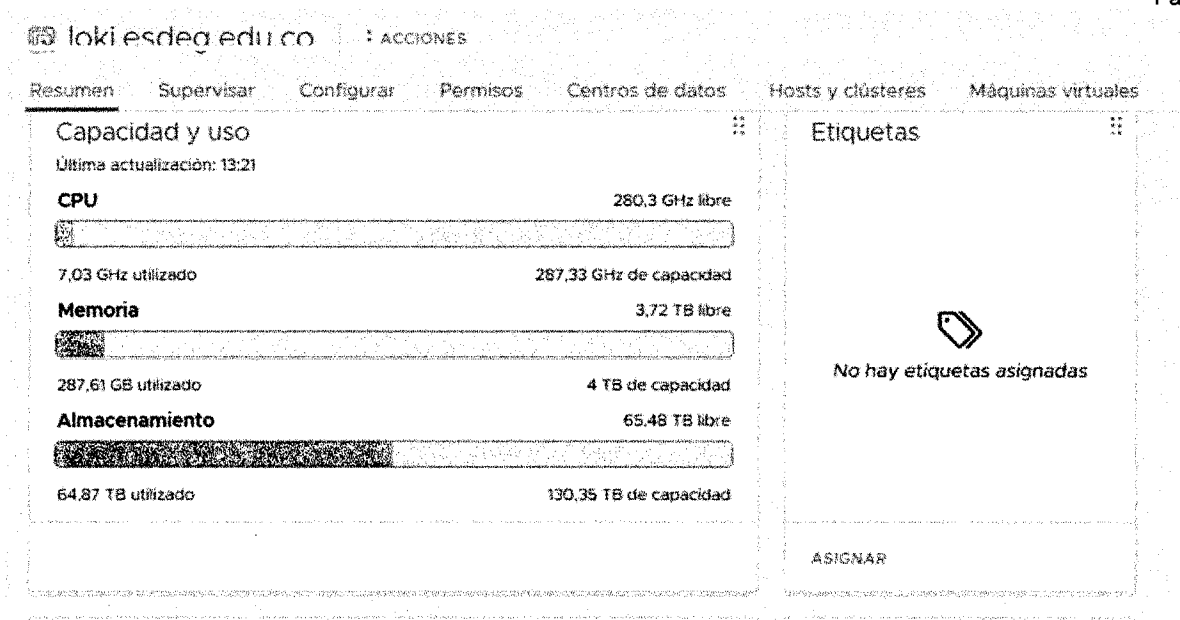
Se encuentra operativo y estable. Actualmente la infraestructura está soportando una máquina virtual productiva y dos de pruebas, evidenciando baja utilización de recursos (CPU y memoria dentro de parámetros normales) y capacidad suficiente para crecimiento controlado.

El almacenamiento presenta un nivel de ocupación del 75%, manteniéndose dentro de umbral aceptable; no obstante, se continuará monitoreo preventivo para evitar acercamiento a niveles críticos durante el primer trimestre.



3.2. Estado de VMWare

Se realizó revisión general del entorno VMware desde vCenter, evidenciando que la infraestructura se encuentra operativa y con baja utilización de recursos. Se registró consumo de 7.03 GHz de CPU sobre una capacidad total de 287.33 GHz, uso de 287.61 GB de memoria sobre 4 TB disponibles y 64.87 TB utilizados sobre 130.35 TB de almacenamiento, manteniéndose amplia capacidad libre y sin condiciones de sobrecarga para el inicio del año operativo.

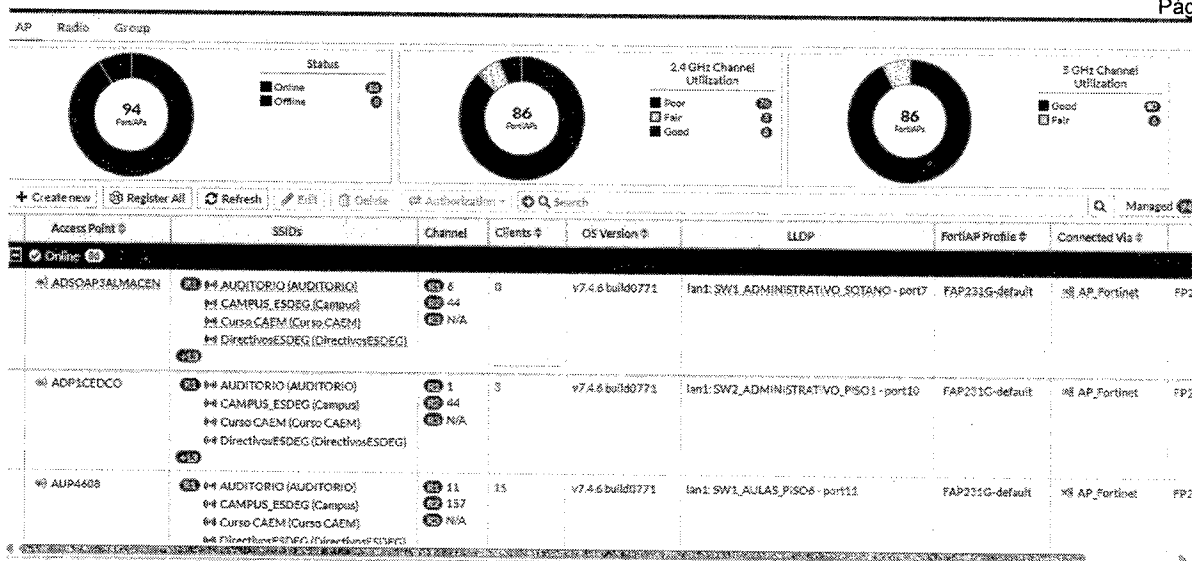


4. **Acompañar y ajustar la configuración de red perimetral según necesidades detectadas (Firewall Fortinet, FortiSwitch, FortiAP, FortiAnalyzer, FortiAuthenticator, FortiManager), asegurando continuidad operativa durante el retorno de actividades institucionales.**

Se presentó informe parcial de avance sobre las actividades de ajuste y fortalecimiento de la configuración de red perimetral (Fortinet y componentes asociados) y servidores, en el cual se detallan las acciones que actualmente se encuentran en ejecución. Dicho documento se anexa al presente corte para su respectivo conocimiento y seguimiento.

5. **Verificar la correcta disponibilidad de la red WIFI institucional, validando cobertura y conectividad.**

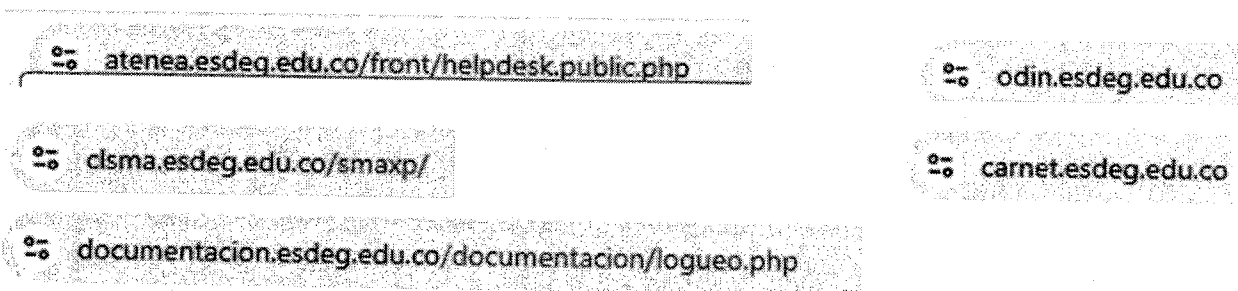
Se realizó verificación de la disponibilidad de la red WIFI institucional, validando cobertura, estado operativo de los puntos de acceso y conectividad en los segmentos habilitados. No se evidenciaron fallas generalizadas ni interrupciones del servicio al momento de la revisión, confirmándose continuidad operativa para el retorno de actividades institucionales.



6. Realizar revisión preventiva de certificados digitales, configuraciones SSL/TLS y servicios expuestos, verificando vigencias y reforzando mecanismos de protección perimetral.

Se realizó revisión preventiva de los certificados digitales y configuraciones SSL/TLS asociados a los servicios expuestos institucionales, incluyendo atenea.esdeg.edu.co, odin.esdeg.edu.co, carnet.esdeg.edu.co, clsma.esdeg.edu.co y documentacion.esdeg.edu.co, verificando vigencia de certificados, cadena de confianza, protocolos habilitados y correcta publicación a través de la infraestructura perimetral.

Durante la validación se confirmó disponibilidad de los servicios, correcta negociación TLS y ausencia de certificados expirados al momento de la revisión. Se reforzaron controles de protección perimetral asociados a la publicación de estos servicios, asegurando cumplimiento de buenas prácticas de seguridad y continuidad operativa.



Inf

visor de certificados: documentacion.esdeg.edu.co

General Detalles

Enviado a

Nombre común (CN)	documentacion.esdeg.edu.co
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	E8
Organización (O)	Let's Encrypt
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

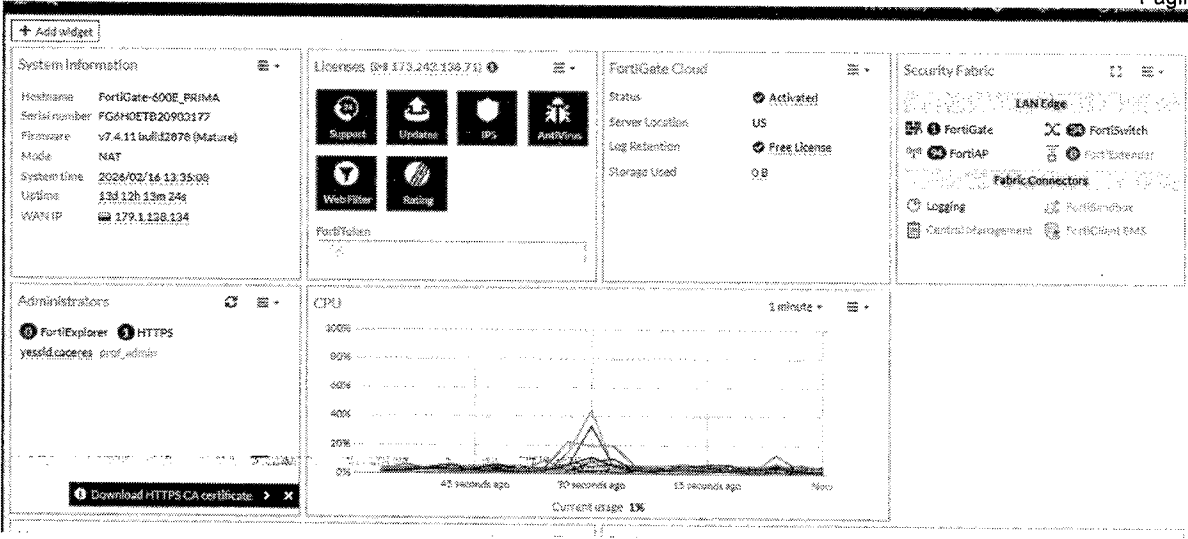
Emitido el	domingo, 8 de febrero de 2026, 18:47:54
Vencimiento el	sábado, 9 de mayo de 2026, 18:47:53

Huellas digitales SHA-256

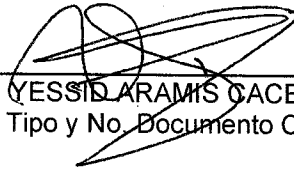
Certificado	0c2bc2392a72bd3774e1be2b761af8f1a76cf31ea460b8b1d49cfc983864c928
Clave pública	67dbce3c656e3f733999842c316909e16d323c12ddbd1d30af16c9db267cbf80

7. Monitorear continuamente los equipos perimetrales de seguridad y realizar ajustes según necesidades detectadas y/u órdenes recibidas (Firewall Fortinet, FortiSwitch, FortiAP, FortiAnalyzer, FortiAuthenticator, FortiManager, Veeam Backup).

Se mantuvo monitoreo continuo sobre los equipos perimetrales de seguridad y plataformas asociadas, realizando ajustes técnicos conforme a las necesidades detectadas y directrices impartidas, garantizando estabilidad operativa y fortalecimiento de los controles de seguridad institucionales.



Atentamente,


Nombre: **YESSID ARAMIS CACERES VASQUEZ**
Tipo y No. Documento CC. 72.342.326

Bogotá D.C. FECHA: febrero 09 de 2026

RADICADO No.0126105141 / MDN-COGFM-JEMCO-ESDEG-SBESG-VIADM-DETC

Señor Teniente
Enrique Ramírez Flor
Supervisor del Contrato

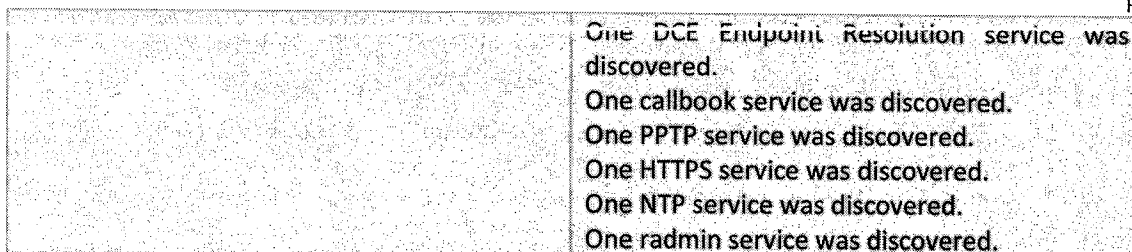
ASUNTO: Informe parcial de los avances de Remediación en respuesta a la actividad de Análisis de Vulnerabilidades realizado a la escuela

Por medio del presente, me permito comunicar el progreso y estado actual de las actividades desarrolladas en el área de Tecnologías de la Información. Durante el mes de enero y parte de febrero, se han llevado a cabo diversos despliegues y ajustes en la infraestructura, enfocados principalmente en el fortalecimiento de la seguridad en cumplimiento al plan de remediación impartido por el CCOCI, así como otras medidas adoptadas conforme a las necesidades identificadas, con el fin de garantizar la seguridad de la información.

A continuación, se presentan los puntos evaluados, las vulnerabilidades o hallazgos identificados y las acciones de remediación implementadas. Las actividades descritas se encuentran alineadas con el plan de trabajo establecido para el presente año así:

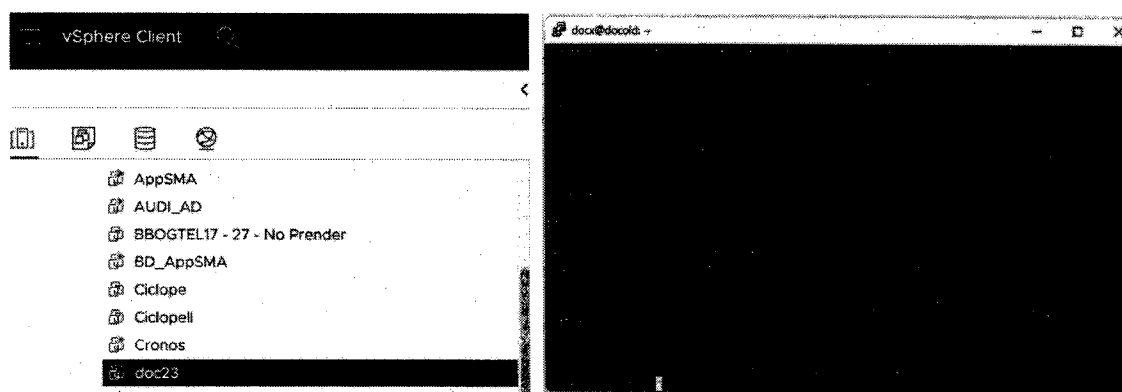
1. BBOGTEL17 – Windows Server 2008R2

IP	Vulnerabilidades
172.18.51.27	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>145 critical vulnerabilities were discovered.</p> <p>318 severe vulnerabilities were discovered.</p> <p>14 moderate vulnerabilities were discovered.</p> <p>One MySQL service was discovered.</p> <p>6 DCE RPC services were discovered.</p> <p>3 HTTP services were discovered.</p> <p>2 <unknown> services were discovered.</p> <p>2 CIFS services were discovered.</p> <p>One ISAKMP service was discovered.</p> <p>One CIFS Name Service service was discovered.</p> <p>One fics (Free Internet Chess Server) service was discovered.</p> <p>One RDP service was discovered.</p> <p>One SNMP service was discovered.</p>



Remediación: El servidor identificado con IP **172.18.51.27**, correspondiente a un **Windows Server 2008 R2** con **XAMPP y PHP 5.x**, fue retirado completamente de operación debido a la obsolescencia del sistema operativo y del stack de aplicaciones, los cuales ya no cuentan con soporte ni actualizaciones de seguridad del fabricante. Como acción correctiva, se implementó un nuevo servidor sobre **Ubuntu Server en su versión estable más reciente** con IP **172.18.51.115**, denominado **doc23**, con **PHP 8.3** y **MySQL en su versión actual soportada**, aplicando actualizaciones de seguridad, hardening inicial y reducción de la superficie de ataque. El servicio web identificado opera bajo un subdominio de uso exclusivamente interno, no publicado en Internet, aun así por medio de técnicas de **Lets Encrypt Certbot** se logró aplicar la emisión de certificados públicos para uso interno a través de **Registros DNS TXT**, práctica técnicamente válida para entornos cerrados. En consecuencia, las **145 vulnerabilidades críticas, 318 severas y 14 moderadas** quedan cerradas, al no existir ya el activo vulnerable.

Para lograr este ejercicio, nos vimos en la necesidad de actualizar el código fuente de la aplicación y el motor de la base de datos implementado que como se mencionó en el párrafo anterior, se encontraba obsoleto. Así mismo se cerraron todos los puertos dejando abiertos únicamente el 80, 443 y 3306.



[illegible]

```

Rule added
Rule added (v6)
doxx@doxxlidi:~$ sudo xfw status
Status: active

To                                     Action
--                                     -
80/tcp                                ALLOW
3306/tcp                              ALLOW
80/tcp (v6)                           ALLOW
3306/tcp (v6)                         ALLOW

```

[illegible]

```

docx@docold: ~
GNU nano 2.2.1
network:
version: 2
ethernets:
  ens34:
    dhcp4: false
    addresses:
      - 172.18.51.115/24
    routes:
      - to: default
        via: 172.18.51.33
    nameservers:
      addresses:
        - 8.8.8.8

```

ESCUELA SUPERIOR DE GUERRA | Manejo Documental Institucional

INICIO DE SESIÓN

IMPORTANTE: Esta plataforma quedará fuera de servicio próximamente. Estamos en proceso de transición al nuevo sistema SDGA - Dominium y al portal de solicitudes FORSD. Le sugerimos guardar los siguientes enlaces:

Acceso SDGA - Dominium

Portal PORSO OGEM

Usuario

Human Instructions

Contraseña

2008年12月15日

Ingresar al Sistema

Cancel

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...
aulas		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
documentacion		Carpeta de...	14/01/2026 02...	drwxr-xr-x	documenta...
forbidden		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
includes		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
restricted		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
wampp		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
wampp		Carpeta de...	13/01/2026 06...	drwxr-xr-x	documenta...
apache_pb.gif	2,326	Archivo GIF	13/01/2026 06...	-rw-r--r--	documenta...
apache_pb.png	1,385	Archivo PNG	13/01/2026 06...	-rw-r--r--	documenta...
apache_pb2.gif	2,414	Archivo GIF	13/01/2026 06...	-rw-r--r--	documenta...
apache_pb2.png	1,463	Archivo PNG	13/01/2026 06...	-rw-r--r--	documenta...

8 archivos y 7 directorios. Tamaño total: 182,163 bytes

```

100 <div class="login-card">
101   <h2>Inicio de Sesión</h2>
102
103   <div class="aviso-transicion">
104     <p><strong>¡IMPORTANTE!</strong> Esta plataforma quedará <strong>fuera de servicio</strong> próximamente.
105       Estamos en proceso de transición al nuevo sistema <strong>SSEA - Dominio</strong> y al portal de
106       solicitudes <strong>PQRSD</strong>. Le sugerimos guardar los siguientes enlaces:
107     </p>
108     <div class="enlaces-contenedor">
109       <a href="https://dominio.cgfe.mil.co" class="link-item" target="_blank"><img alt="Dominio icon" data-bbox="285 418 305 438"/> Acceso SSEA - Dominio</a>
110       <a href="https://pqrdd.cgfe.mil.co" class="link-item" target="_blank"><img alt="PQRSD icon" data-bbox="285 428 305 448"/> Portal PQRSD CGFE</a>
111     </div>
112   </div>
113
114   <form id="login" name="login" method="post" action="autenticar.php" onSubmit="return valida(this);">
115     <div class="form-group">
116       <label>Usuario</label>
117       <input type="text" name="usuario" id="usuario" placeholder="Usuario institucional" />
118     </div>
119
120     <div class="form-group">
121       <label>Contraseña</label>
122       <input type="password" name="clave" id="clave" placeholder="*****" />
123     </div>
124
125     <div class="btn-group">
126       <input type="submit" name="aceptar" value="Ingresar al Sistema" />
127       <input type="reset" name="cancelar" value="Cancelar" />
128     </div>
129   </form>

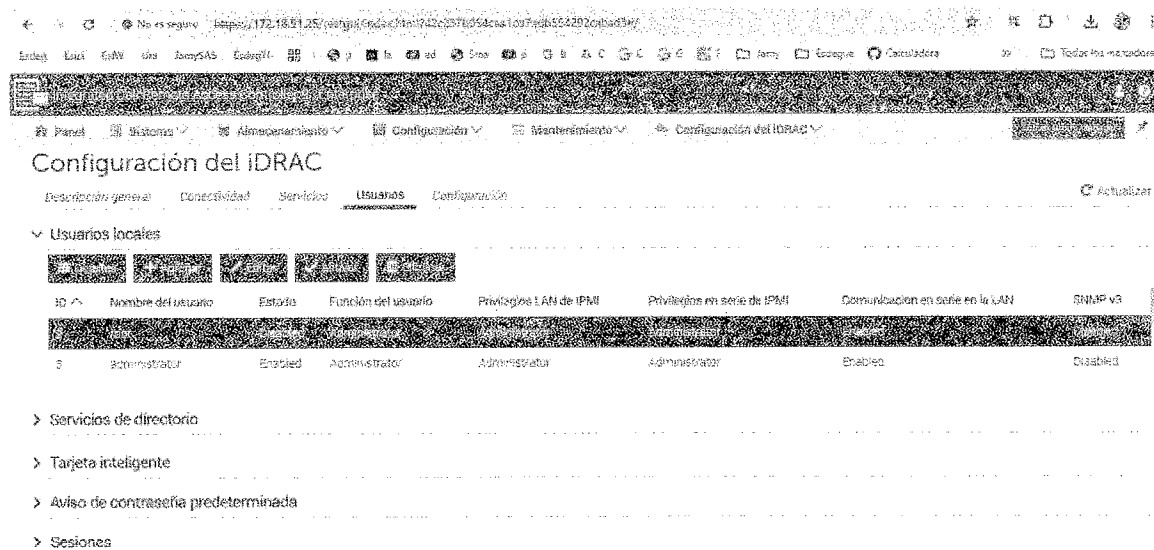
```

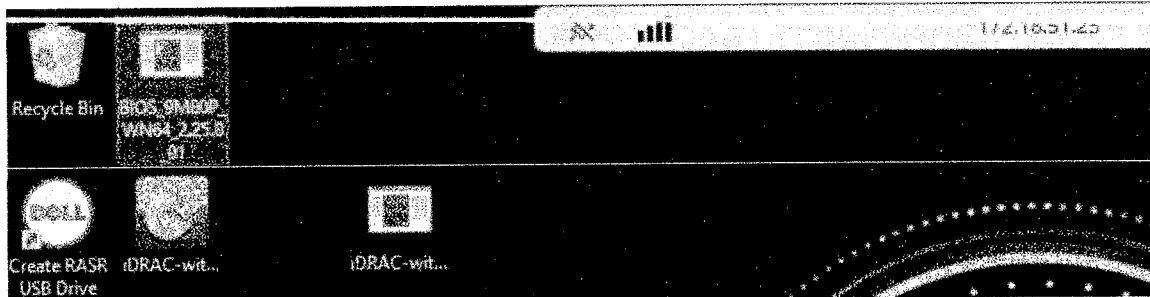
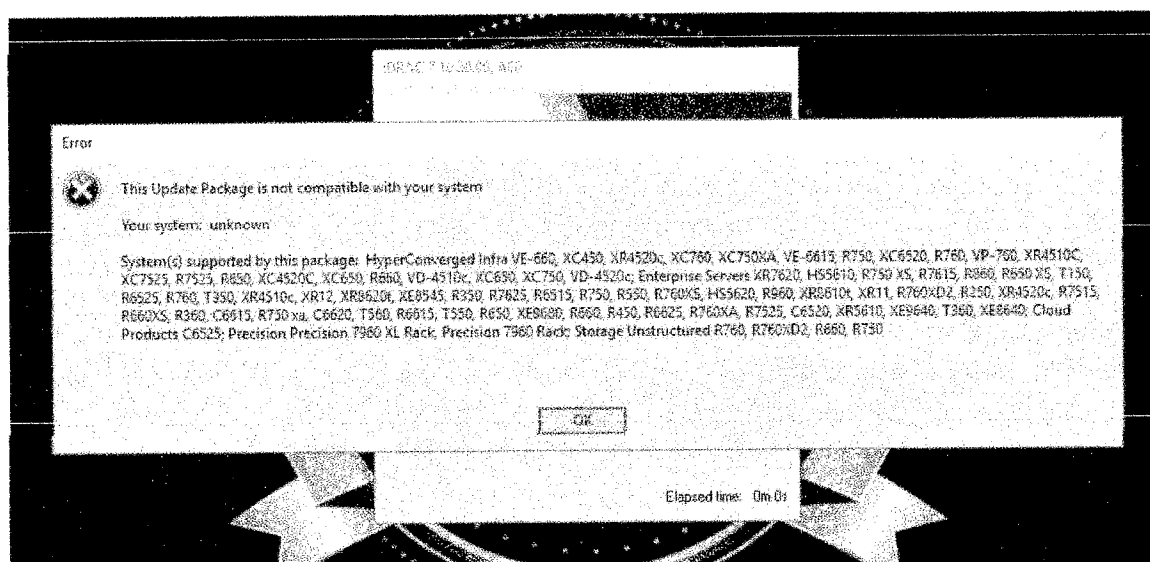
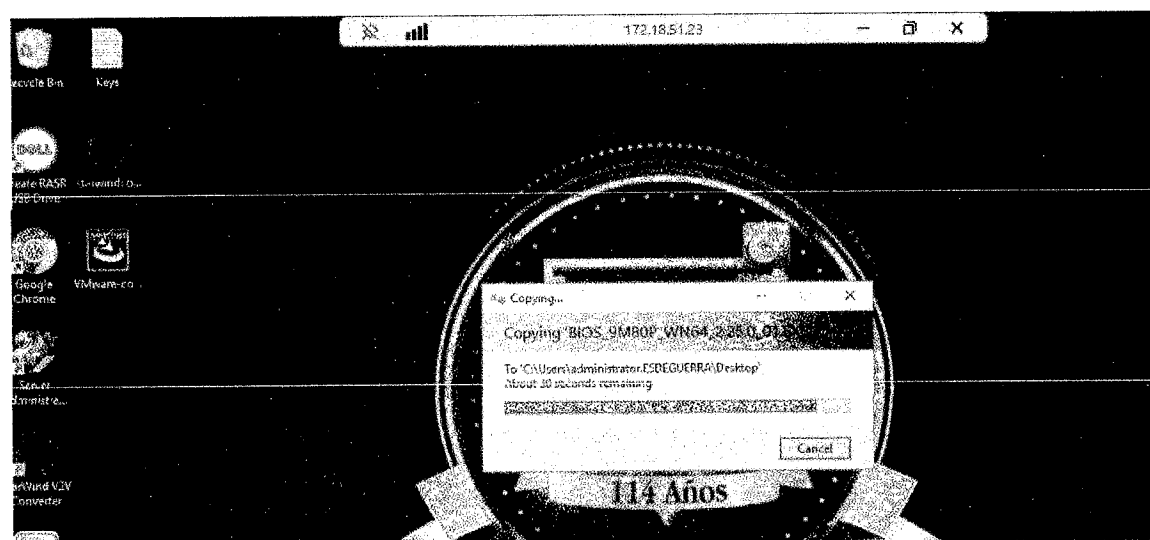
2. Dell EMC NX3240 - iDRAC

Valor	Importancia
172.18.51.25	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>19 critical vulnerabilities were discovered.</p> <p>22 severe vulnerabilities were discovered.</p> <p>4 HTTPS services were discovered.</p> <p>2 <unknown> services were discovered.</p> <p>2 callbook services were discovered.</p> <p>2 ASF-RMCP services were discovered.</p> <p>2 HTTP services were discovered.</p> <p>One SNMP service was discovered.</p> <p>One SSH service was discovered.</p>

Remediación: El activo identificado con IP **172.18.51.25** corresponde a la interfaz de gestión **iDRAC** del equipo **Dell EMC NX3240**, la cual utiliza un servicio web embebido propio del fabricante. Como acciones de remediación, se realizó la **actualización del firmware iDRAC**, quedando instalada la **versión 7.00.00.183**, correspondiente a la versión más reciente compatible con el modelo, incorporando correcciones de seguridad y actualización del stack criptográfico. Adicionalmente, se **deshabilitó el acceso por HTTP**, forzando el uso exclusivo de **HTTPS**, se fortalecieron las **credenciales de acceso** mediante la eliminación de cuentas por defecto y el uso de contraseñas robustas, y se deshabilitaron **servicios y funcionalidades internas no utilizadas** (proxy, redirecciones, scripting y servicios auxiliares), reduciendo la superficie de ataque del servicio web embebido. Finalmente, se implementaron **controles de acceso por red**, restringiendo la interfaz de gestión a la **VLAN administrativa** y bloqueando accesos desde redes no autorizadas. En consecuencia, las vulnerabilidades críticas y severas identificadas quedan **mitigadas o cerradas**, al tratarse de controles compensatorios aplicados sobre un servicio de gestión de hardware que no permite la administración tradicional de módulos Apache.

Para completar esta remediación, se hizo necesario que se instalaran en el sistema operativo del huésped (**172.18.51.23 – La NAS**) actualizaciones necesarias (BIOS_9M80P_WN64_2.25.0_01, iDRAC-with-Lifecycle-Controller_Firmware_HV310_WN64_7.10.30.00_A00 y iDRAC-with-Lifecycle-Controller_Firmware_VP556_WN64_7.00.00.183_A00) como se aprecia en las imágenes, esto no implica remediación para el huésped, solo la necesidad de realizarlo des esta maquina.





172.18.51.23

Manager ▶ Dashboard

Administrator: Windows PowerShell

PS C:\Users\administrator.ESDEGUERRA> Get-SmbSession

SessionId	ClientComputerName	ClientUserName	NumOpens
3934726914137	172.18.51.22	ESDEG\DETAH-52-245\$	2
3934794023013	172.18.51.22	ESDEG\CEDCO-53-93\$	6
3934794023037	172.18.51.22	ESDEG\AULA603_8\$	2
3934726914185	172.18.51.22	ESDEG\omar.acosta	9
3934726914189	172.18.51.6	ESDEG\Administrator	0
3934190043369	172.18.51.109	ESDEG\Administrator	0
3934726914557	172.18.51.22	ESDEG\DEEJC-0009\$	2
3934190044101	172.18.51.241	ESDEGUERRA\backupSINU	1

PS C:\Users\administrator.ESDEGUERRA> Get-SmbShare

Name	ScopeName	Path	Description
ADMIN\$	*	C:\Windows	Remote Admin
Backups	*	E:\Backups	
C\$	*	C:\	Default share
D\$	*	D:\	Default share
DEPENDENCIAS	*	E:\DEPENDENCIAS	
DETIC	*	E:\DETIC	
E\$	*	E:\	Default share
F\$	*	F:\	Default share
IPCS	*		Remote IPC
SERVIDORES	*	E:\SERVIDORES	
SINU	*	E:\SINU	
SINU_DOCUMENTOS	*	E:\SINU_DOCUMENTOS	
SOFTWARE	*	E:\SOFTWARE	

PS C:\Users\administrator.ESDEGUERRA> nbtstat -n

NIC4:

Node IpAddress: [0.0.0.0] Scope Id: []

No names in cache

Local Area Connection* 2:

Node IpAddress: [0.0.0.0] Scope Id: []

No names in cache

bond0:

Node IpAddress: [172.18.51.23] Scope Id: []

NetBIOS Local Name Table

no de inicio

Edadg Edcl EsW Onl JmmySAS Edclgll

Nueva pestaña Renovación Edición

IBRAV1 | Enterprise

Panel Sistema Almacenamiento Configuración Mantenimiento Configuración del iDRAC

Información de estado



Condición del sistema: **En buen estado** [Detalles»](#)

Estado del almacenamiento: **En buen estado** [Detalles»](#)

Información del sistema

Estado de la alimentación	On
Modelo	Dell EMC NX3240
Nombre de host	NAS1
Sistema operativo	Microsoft Windows 2016 Server
Versión del sistema operativo	Version 10.0 (Build 14293) (x64)
Etiqueta de servicio	G50V0Q2
Versión del BIOS	2.25.0
Versión de firmware de iDRAC	7.00.00.193
Dirección IP	172.16.51.26
Dirección MAC de iDRAC	6D:94:66:6a:03:ed
Licencia	Enterprise Editar

▼ Configuración de IPMI

Activar IPMI en la LAN: **Desactivado**

Límite de nivel de privilegio de canal: **Administrador**

Clave de cifrado*: 00000000000000000000

[Verificar contraseña](#) [Cancelar](#)

▼ Bloqueo de IP

Bloqueo de IP activado: **Activado**

Conteo de error de bloqueo de IP*: 3

Ventana de error de bloqueo de IP*: 60 segundos

Tiempo de penalización de bloqueo de IP*: 60 segundos

[Verificar contraseña](#) [Cancelar](#)

Configuración

Activado	Activado ▼
Protocolo HTTP/2	Desactivado ▼
N.º máx. de sesiones	8
Sesiones activas	1
Tiempo de espera*	1800 segundos
Bloquear puerto HTTP	☐
Redirección HTTPS	Activado ▼
Número de puerto HTTP*	80
Número de puerto HTTPS*	443
Cifrado SSL	128 bits o superior ▼
Protocolo TLS	Solo TLS 1.3 ▼

Panel Sistema Almacenamiento Configuración Mantenimiento

SSH

Activado	Desactivado ▼
N.º máx. de sesiones	4
Sesiones activas	0
Tiempo de espera	1800 segundos
Número de puerto	22

✓ |RACADM remoto

Activado	Desactivado ▾
Sesiones activas	0
<div></div> <div></div>	

✓ |Agente SNMP

Activado	Desactivado ▾
Nombre de comunidad SNMP	public
Protocolo de SNMP	Todos ▾
Número de puerto de detección de SNMP	161
<div></div> <div></div>	

✓ |Redfish

Activado	Desactivado ▾
<div></div> <div></div>	

3. Host OCS Inventory - Ubuntu Linux

Vulnerabilidades	
172.18.51.8	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>18 critical vulnerabilities were discovered.</p> <p>10 severe vulnerabilities were discovered.</p> <p>One moderate vulnerability was discovered.</p> <p>One SSH service was discovered.</p> <p>One <unknown> service was discovered.</p> <p>One HTTP service was discovered.</p> <p>One callbook service was discovered.</p>

Remediación: El Host identificado con IP **172.18.51.8** se le aplicaron las acciones de remediación sobre los servicios **Apache HTTPD** y **OpenSSH**, conforme a los hallazgos reportados. Se realizó la **actualización de Apache HTTPD** a una versión soportada mediante los repositorios del sistema operativo, corrigiendo vulnerabilidades asociadas a versiones desactualizadas y a módulos como *mod_proxy*, *mod_lua*, *mod_macro* y *mod_sed*. Adicionalmente, se aplicó **hardening de configuración**, deshabilitando el método **HTTP OPTIONS** para evitar la enumeración de métodos HTTP y reducir la superficie de ataque. En cuanto al servicio **OpenSSH**, se ejecutó la **actualización a la versión vigente**, incorporando los parches de seguridad correspondientes, y se fortaleció su configuración criptográfica mediante la **deshabilitación de algoritmos MD5 y HMAC de 96 bits**, permitiendo únicamente cifrados y mecanismos de autenticación seguros. Como resultado, las vulnerabilidades críticas, severas y moderadas identificadas para este activo quedan **mitigadas y cerradas**, de acuerdo con las recomendaciones del plan de remediación.

Nota: al igual que en el **172.18.51.115**, en este servidor de ocs inventory también se logró la implementación del protocolo seguro 443 https.

[illegible][illegible]

[illegible]

```

This certificate will not be automatically renewed if --manual certificates requires the use of an authentication howm
was not provided. To renew this certificate, repeat this same command before the certificate's expiry date.

-----[Cenral]-----
If you like Torobot, please consider supporting our work by:
 * Donating to ICRC / Let's Encrypt: https://letsencrypt.org/donate
 * Donating to EFF: https://eff.org/donate-us

root@rainbowcat:/var/lib/letsencrypt# sudo certbot
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Please enter the domain name(s) you want to ask for your certificate (comma sep/or
space separated) (Enter 'c' to cancel): rainbowcat.sageg.edu.us
Certificate not yet due for renewal

You have an existing certificate that has exactly the same domains as certificate name you requested and isn't close to expiry.
key: /etc/letsencrypt/live/rainbowcat.sageg.edu.us/cert.pem

That would you like to do?
-----
1. Rotate to existing non-expiring certificate
2. Renew & replace the certificate (may be SUPERT to OR else kind?)
0. Make the appropriate number [1-9] then (ENTER) press 'c' to cancel: 1
Renewing an existing certificate for rainbowcat.sageg.edu.us

Successfully received certificate.
Certificate is saved at /etc/letsencrypt/live/rainbowcat.sageg.edu.us/fullchain.pem
Key is saved at: /etc/letsencrypt/live/rainbowcat.sageg.edu.us/privatekey.pem
This certificate expires on 2026-05-08.
These files will be updated when the certificate renews.
Took me out of a scheduled task to automatically renew this certificate in the background.

Deploying Certificate
Successfully deployed certificate for rainbowcat.sageg.edu.us to /etc/apache2/sites-available/000-default-le-virtual.conf

Your existing certificate has been successfully renewed, and the new certificate has been installed.

-----
If you like Torobot, please consider supporting our work by:
 * Donating to ICRC / Let's Encrypt: https://letsencrypt.org/donate
 * Donating to EFF: https://eff.org/donate-us

root@rainbowcat:/var/lib/letsencrypt#

```

The screenshot shows the CCX-NG GUI with a warning message in the center. The message reads: "ADVERTENCIA: No podrá cargar ningún paquete de implementación con un tamaño superior a 2MB. Debe aumentar limit_max_size_toload_max, ubicado en su configuración de Visual part, aumentando este límite." Below the message, it says "Class de datos existente actualizada" and "versión actual 7057 - versión esperada 7079". At the bottom, there are two buttons: "Realice la actualización" and "Actualizar con confianza". The top of the window shows a menu bar with "No es seguro" and "Opciones de seguridad de los reportes". The bottom status bar says "Click aquí para entrar CCX-NG GUI".

ocsinventory.esdeg.edu.co/ocsreports/

Unl JamySAS EsdegIT Nueva pestaña Renovacion - Editor...



LANGUAGE

English

User :

User

Password :

Password

Send

4. Host HERMES - Ubuntu Linux

	Vulnerabilidades
172.18.51.21	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>16 critical vulnerabilities were discovered.</p> <p>10 severe vulnerabilities were discovered.</p> <p>2 moderate vulnerabilities were discovered.</p> <p>2 CIFS services were discovered.</p> <p>2 HTTP services were discovered.</p> <p>One callbook service was discovered.</p> <p>One CIFS Name Service service was discovered.</p> <p>One SSH service was discovered.</p> <p>One <unknown> service was discovered.</p> <p>One HTTPS service was discovered.</p>

Remediación: El servidor identificado con IP **172.18.51.21** fue objeto de un proceso de remediación conforme a los hallazgos reportados. Se realizó la **actualización de PHP** a versiones soportadas **8.2.x y 8.3.x**, corrigiendo vulnerabilidades asociadas a versiones obsoletas del lenguaje. De igual forma, se ejecutó la **actualización de Apache HTTPD** mediante los repositorios del sistema operativo, mitigando vulnerabilidades conocidas relacionadas con procesamiento de solicitudes, módulos internos y manejo de HTTP/2. Como medida de hardening adicional, se **forzó el uso exclusivo de HTTPS**, impidiendo el acceso por HTTP, y se **deshabilitó el método HTTP OPTIONS** para evitar la enumeración de métodos soportados. En cuanto a servicios de acceso remoto, se actualizó **OpenSSH** a la versión vigente y se reforzó su configuración criptográfica, eliminando algoritmos MD5 y HMAC de 96 bits. Finalmente, se aplicaron **controles de red a nivel de firewall**, restringiendo el acceso a servicios **CIFS/NetBIOS (puertos 137–139 y 445)** exclusivamente a la red administrativa **172.18.50.0/23**, bloqueando cualquier acceso desde redes no confiables. Con estas acciones, las vulnerabilidades críticas, severas y moderadas identificadas para este activo quedan **mitigadas y cerradas** conforme al plan de remediación.

- **PERMITIR solo red administrativa Hermes .21**
 - `sudo iptables -A INPUT -p tcp -s 172.18.50.0/23 --dport 445 -j ACCEPT`
 - `sudo iptables -A INPUT -p tcp -s 172.18.50.0/23 --dport 139 -j ACCEPT`
 - `sudo iptables -A INPUT -p udp -s 172.18.50.0/23 --dport 137 -j ACCEPT`
 - `sudo iptables -A INPUT -p udp -s 172.18.50.0/23 --dport 138 -j ACCEPT`
- **BLOQUEAR todo lo demás**
 - `sudo iptables -A INPUT -p tcp --dport 445 -j DROP`
 - `sudo iptables -A INPUT -p tcp --dport 139 -j DROP`
 - `sudo iptables -A INPUT -p udp --dport 137 -j DROP`
 - `sudo iptables -A INPUT -p udp --dport 138 -j DROP`
- **Verificar reglas**
 - `sudo iptables -L INPUT -n --line-numbers`
- **Persistir reglas (IMPORTANTE)**
 - `sudo apt install iptables-persistent -y`
 - `sudo netfilter-persistent save`

[illegible][illegible]

```

GNU nano 6.2
[global]
workgroup = WORKGROUP
usershare allow guests = yes
security = user
map to guest = Bad User
guest account = nobody
server signing = mandatory

[ADConnect]
path = /srv/codex/
guest ok = yes
read only = no
create mask = 0777
directory mask = 0777
force user = esdegue

```

```

VirtualHost *:80 {
    ServerName steneas.esdegue.edu.co

    DocumentRoot /var/www/gipi/public

    # To add more vhosts, place this in a subfolder of your own, eg. /etc/httpd/sites,
    # and place the corresponding vhost record in the main configuration file.

    # AllowOverride None
    # Required for mod_rewrite to work. Relatively unused.
    #ErrorLog /usr/local/apache/logs/error_log
    #CustomLog /usr/local/apache/logs/access_log combined

    <Directory /var/www/gipi/public>
        Require all granted

        RewriteEngine On

        # If you need to use the %HIST% directive, you must use the %HIST%
        # directive in the RewriteRule.
        RewriteRule ^(.*)$ index.php [QSA,L]
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
}
VirtualHost *:80 {
    ServerName steneas.esdegue.edu.co

    DocumentRoot /var/www/gipi/public

    # To add more vhosts, place this in a subfolder of your own, eg. /etc/httpd/sites,
    # and place the corresponding vhost record in the main configuration file.

    # AllowOverride None
    # Required for mod_rewrite to work. Relatively unused.
    #ErrorLog /usr/local/apache/logs/error_log
    #CustomLog /usr/local/apache/logs/access_log combined

    <Directory /var/www/gipi/public>
        Require all granted

        RewriteEngine On

```

```

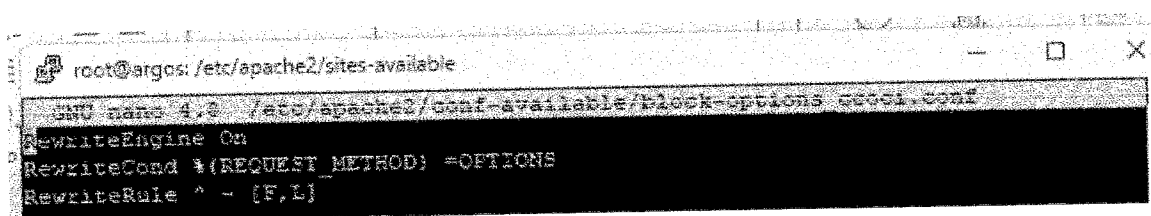
884 sudo ufw status verbose
885 sudo iptables -A INPUT -p tcp -s 172.18.50.0/23 --dport 445 -j ACCEPT
886 sudo iptables -A INPUT -p tcp -s 172.18.50.0/23 --dport 139 -j ACCEPT
887 sudo iptables -A INPUT -p udp -s 172.18.50.0/23 --dport 137 -j ACCEPT
888 sudo iptables -A INPUT -p udp -s 172.18.50.0/23 --dport 138 -j ACCEPT
889 sudo iptables -A INPUT -p tcp --dport 445 -j DROP
890 sudo iptables -A INPUT -p tcp --dport 139 -j DROP
891 sudo iptables -A INPUT -p udp --dport 137 -j DROP
892 sudo iptables -A INPUT -p udp --dport 138 -j DROP
893 sudo iptables -L INPUT -n --line-numbers
894 sudo apt install iptables-persistent -y
895 sudo netfilter-persistent save
896 cd /var/www/gipi
897 ls

```

5. Host ARGOS - Ubuntu Linux 20.04

Vulnerabilidad	
172.18.51.13	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>9 critical vulnerabilities were discovered.</p> <p>3 severe vulnerabilities were discovered.</p> <p>One moderate vulnerability was discovered.</p> <p>One HTTP service was discovered.</p> <p>One callbook service was discovered.</p> <p>One <unknown> service was discovered.</p> <p>One HTTPS service was discovered.</p> <p>One SSH service was discovered.</p>

Remediación: El servidor identificado con IP **172.18.51.13** fue objeto de acciones de remediación orientadas a corregir hallazgos asociados a servicios **Apache HTTPD**, **TLS/SSL** y **OpenSSH**. Se verificó y mantuvo el servidor web en versión soportada (**Apache/2.4.63 – Ubuntu**), y se aplicó hardening para reducir superficie de ataque, incluyendo la **deshabilitación del método HTTP OPTIONS** a nivel global en la configuración de Apache. Adicionalmente, se fortaleció el componente **TLS** implementando un **certificado interno** específico para backend con **SAN (DNS e IP)**, corrigiendo el hallazgo de **mismatch de CN** y asegurando que el servicio HTTPS del backend presente un certificado coherente para validaciones internas y escaneo. Finalmente, se actualizó y endureció **OpenSSH**, restringiendo algoritmos criptográficos inseguros (eliminando MD5 y HMAC de 96 bits) y dejando únicamente suites seguras. Con estas acciones, los hallazgos críticos y severos relacionados con **HTTP/HTTPS** y **SSH** para este activo quedan **mitigados y cerrados** conforme al plan de remediación./etc/apache2/conf-available/block-options.conf



```

root@argos: /etc/apache2/sites-available
GNU nano 4.8 /etc/apache2/conf-available/block-options.conf
RewriteEngine On
RewriteCond %{REQUEST_METHOD} =OPTIONS
RewriteRule ^ - [F,L]

```

```

sudo a2enmod rewrite
sudo a2enconf block-options
sudo apachectl configtest
sudo systemctl reload apache2

```

```

root@waf:~# nano /etc/ssl/openssl-backend.cnf
GNU nano 4.3 /etc/ssl/openssl-backend.cnf
[ req ]
default_bits      = 2048
prompt            = no
default_md        = sha256
distinguished_name = dn
x509_extensions   = v3_req
req_extensions    = req_ext

[ dn ]
CN = backend-waf.local

[ v3_req ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = backend-waf.local
IP.1  = 172.18.51.13

```

```
sudo nano /etc/ssl/openssl-backend.cnf
```

```
[ req ]
default_bits      = 2048
prompt            = no
default_md        = sha256
distinguished_name = dn
req_extensions    = req_ext
```

```
[ dn ]
CN = backend-waf.local
```

```
[ req_ext ]
subjectAltName = @alt_names
```

```
[ alt_names ]
DNS.1 = backend-waf.local
IP.1  = 172.18.51.13
```

```

root@argos:/etc/apache2/sites-available# sudo nano /etc/ssl/openssl-backend.cnf
root@argos:/etc/apache2/sites-available# sudo openssl req -new -x509 -days 825 \
  -keyout /etc/ssl/private/backend-waf.key \
  -out /etc/ssl/certs/backend-waf.crt \
  -config /etc/ssl/openssl-backend.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/backend-waf.key'
Enter PEM pass phrase:[]

```

```

sudo openssl req -new -x509 -days 825 \
-keyout /etc/ssl/private/backend-waf.key \
-out /etc/ssl/certs/backend-waf.crt \
-config /etc/ssl/openssl-backend.cnf

```

```

sudo chmod 600 /etc/ssl/private/backend-waf.key

```

```

root@argos:/etc/apache2/sites-available# sudo nano /etc/ssl/openssl-backend.cnf
root@argos:/etc/apache2/sites-available# sudo openssl req -new -x509 -days 825 \
  -keyout /etc/ssl/private/backend-waf.key \
  -out /etc/ssl/certs/backend-waf.crt \
  -config /etc/ssl/openssl-backend.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/backend-waf.key'
Enter PEM pass phrase:
140631314965824:error:28072065:UI routines:UI_set_result_ex:result too small:../
crypto/ui/ui_lib.c:905:You must type in 4 to 1024 characters
140631314965824:error:2807106B:UI routines:UI_process:processing error:../crypto
/ui/ui_lib.c:1545:while reading strings
140631314965824:error:0906406D:PEM routines:PEM_def_callback:problems getting pa
ssword:../crypto/pem/pem_lib.c:159:
140631314965824:error:0907E06F:PEM routines:read_pktpkey:read key:../crypto/pem/p
em_lib.c:183:
root@argos:/etc/apache2/sites-available#

```

sudo nano /etc/apache2/sites-available/backend-waf-ssl.conf

```

root@argos:/etc/apache2/sites-available
GNU nano 4.8 /etc/apache2/sites-available/backend-waf-ssl.conf
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName backend-waf.local

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/backend-waf.crt
    SSLCertificateKeyFile /etc/ssl/private/backend-waf.key

    ProxyPreserveHost On
    ProxyPass "/" "http://172.18.51.X:PUERTO/"
    ProxyPassReverse "/" "http://172.18.51.X:PUERTO/"
</VirtualHost>
</IfModule>

```

```

root@argos:/etc/apache2/sites-available
root@argos:/etc/apache2/sites-available# sudo nano /etc/apache2/sites-available/
backend-waf-ssl.conf
root@argos:/etc/apache2/sites-available# sudo a2ensite backend-waf-ssl.conf
Enabling site backend-waf-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@argos:/etc/apache2/sites-available# sudo apachectl configtest
AH00526: Syntax error on line 6 of /etc/apache2/sites-enabled/backend-waf-ssl.co
nf:
SSLCertificateFile: file '/etc/ssl/certs/backend-waf.crt' does not exist or is e
mpty
root@argos:/etc/apache2/sites-available# sudo systemctl reload apache2
Job for apache2.service failed.
See "systemctl status apache2.service" and "journalctl -xe" for details.
root@argos:/etc/apache2/sites-available#

```

```

root@argos:/etc/apache2/sites-available
root@argos:/etc/apache2/sites-available# sudo ls -l /etc/ssl/certs/backend-waf.c
rt /etc/ssl/private/backend-waf.key
ls: cannot access '/etc/ssl/certs/backend-waf.crt': No such file or directory
-rw----- 1 root root 0 ene 22 15:27 /etc/ssl/private/backend-waf.key
root@argos:/etc/apache2/sites-available# sudo ls -l /etc/ssl/openssl-backend.cnf
-rw-r--r-- 1 root root 273 ene 22 15:27 /etc/ssl/openssl-backend.cnf
root@argos:/etc/apache2/sites-available# sudo openssl req -new -x509 -days 325 -
key /etc/ssl/private/backend-waf.key -out /etc/ssl/certs/backend-waf.crt -config
/etc/ssl/openssl-backend.cnf
unable to load Private Key
140422013671748:error:0909006C:FEM routines:get_name:no start line:../crypto/pem
/pem_lib.c:749:Expecting: ANY PRIVATE KEY
root@argos:/etc/apache2/sites-available# sudo ls -l /etc/ssl/certs/backend-waf.c
rt
ls: cannot access '/etc/ssl/certs/backend-waf.crt': No such file or directory
root@argos:/etc/apache2/sites-available#

```

```

root@argos:/etc/apache2/sites-available
unable to load Private Key
140486813671744:error:09090060:PEM routines:get_name:no start line:../crypto/pem
/pem_lib.c:745:Expecting: ANY PRIVATE KEY
root@argos:/etc/apache2/sites-available# sudo ls -l /etc/ssl/certs/backend-waf.c
rt
ls: cannot access '/etc/ssl/certs/backend-waf.crt': No such file or directory
root@argos:/etc/apache2/sites-available# sudo rm -f /etc/ssl/private/backend-waf
.key
root@argos:/etc/apache2/sites-available# sudo openssl req -new -x509 -days 825 -
nodes \
  -keyout /etc/ssl/private/backend-waf.key \
  -out /etc/ssl/certs/backend-waf.crt \
  -config /etc/ssl/openssl-backend.cnf
Generating a RSA private key
.....+++++
.....+++++
Writing new private key to '/etc/ssl/private/backend-waf.key'
-----
root@argos:/etc/apache2/sites-available# sudo ls -l /etc/ssl/private/backend-waf
.key /etc/ssl/certs/backend-waf.crt
-rw-r--r-- 1 root root 1013 ene 22 16:04 /etc/ssl/certs/backend-waf.crt
-rw----- 1 root root 1704 ene 22 16:04 /etc/ssl/private/backend-waf.key
root@argos:/etc/apache2/sites-available#

```

sudo nano /etc/ssh/sshd_config

```

root@argos:/etc/apache2/sites-available
GNU nano 4.0 /etc/ssh/sshd_config
# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding ciphers on a per-host basis
#Match User admin
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand sftp-server

Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh
MACs hmac-sha2-512,hmac-sha2-256
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org

```

Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-
poly1305@openssh.com
MACs hmac-sha2-512,hmac-sha2-256
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org

sudo systemctl restart ssh

6. Host EXAGRID - Linux LINUX 4.4

	Vulnerabilidades
172.18.51.108	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>6 critical vulnerabilities were discovered. 3 severe vulnerabilities were discovered. 2 <unknown> services were discovered.</p> <p>One kerberos-adm (Kerberos admin/changepw) service was discovered. 5</p> <p>One HTTPS service was discovered. One SSH service was discovered. One dlip service was discovered. One HTTP service was discovered. One callbook service was discovered. One Kerberos service was discovered.</p>

Remediación: El Host identificado con IP **172.18.51.108 (ExaGrid)** fue objeto de análisis y gestión de remediación a partir de los hallazgos reportados en el escaneo de vulnerabilidades realizado sobre la infraestructura tecnológica. Dado que se trata de **un appliance especializado que cuenta con soporte directo del fabricante**, las acciones de remediación fueron elevadas formalmente al proveedor ExaGrid para su validación y ejecución.

Como resultado de esta gestión, el fabricante informó que la mayoría de los CVE reportados corresponden a componentes asociados a **Tomcat**, los cuales dejaron de utilizarse a partir de la versión 7.3.0, migrando el producto a Jetty, así como a condiciones que no aplican al funcionamiento del sistema ExaGrid (por ejemplo, autenticación personalizada de Jakarta, sistemas de archivos sensibles a mayúsculas/minúsculas o capacidades de carga de archivos). Adicionalmente, el proveedor confirmó que las vulnerabilidades comunes relevantes fueron corregidas en la versión 7.4 P6, la cual ya se encuentra aplicada en el sistema.

En consecuencia, los hallazgos identificados para este activo se consideran **mitigados por diseño o corregidos** a nivel de software del fabricante, **quedando pendiente únicamente la validación mediante un nuevo escaneo de vulnerabilidades** posterior a la actualización, con el fin de confirmar el cierre definitivo de los hallazgos reportados conforme al plan de remediación y a las buenas prácticas de gestión de vulnerabilidades.

Hola Katherine Murat, cordial saludo.

Me permito informarle que recientemente nuestra unidad superior realizó un escaneo de vulnerabilidades sobre la infraestructura tecnológica, dentro de la cual se encuentra el sistema ESDEG. Como resultado de dicho análisis, nos fue remitido un informe detallado con las posibles vulnerabilidades detectadas, así como las recomendaciones y acciones de remediación sugeridas.

En este sentido, quisiera solicitar su amable apoyo para validar conjuntamente los hallazgos reportados con ESDEG y revisar la viabilidad de las acciones propuestas. Adjunto le comparto las imágenes del reporte de vulnerabilidades junto con las respectivas recomendaciones de configuración para su análisis.

172.18.51	172	• Este servicio se encuentra en el sitio de servidores con normal importancia. • 10 vulnerabilidades graves descubiertas. • 2 vulnerabilidades moderadas descubiertas. • 7 DCE RPC servicios descubiertos. • 2 CIFS servicios descubiertos. • 2 <unknown> servicios descubiertos. • 2 portmapper servicios descubiertos. • 2 status servicios descubiertos. • One callbook service was discovered. • One RDP service was discovered. • One HTTP service was discovered. • One DCE Endpoint Resolution service was discovered. • One CIFS Name Service service was discovered.
-----------	-----	---

3.11. Remediation Plan for 172.18.51.108

Al momento de la revisión, la versión superior de la suite de herramientas de análisis de vulnerabilidades utilizada fue la versión 7.4.1.1. El informe de vulnerabilidades se encuentra adjunto al correo electrónico.

Miguel y equipo ESDEG.

La actualización a la versión 7.4.1.1 se completó con éxito. Miguel también pudo volver a conectar el servidor Linux de ESDEG en Ustream y ejecutar una serie de pruebas correctamente. Adjunto de nuevo las notas de la versión correspondientes.

Como mencionado en la reunión, en la versión 7.4.1.1 introdujimos una función de monitorización basada en inteligencia artificial (AI Monitor).

Con este cambio, se han producido algunas modificaciones en ciertas funciones y alarmas. Recomendamos que consulten la nueva Guía del Administrador de ESDEG para familiarizarse con estos cambios.

Algunas de las funciones más importantes incluyen:

- Ahora es posible configurar el tiempo de respuesta (RTT) a nivel de cada recurso conectado.
- Ahora un usuario tiene la posibilidad de suspender un recurso conectado específicamente desde la página de Shared and Remote.
- Ya no es posible ver ni resolver la configuración de administrador (root) desde la página web.
- Existe una nueva alarma que reemplaza a la alarma de "Shared Monitor" y elimina el monitor.

La nueva alarma ahora activa una función de la llamada intervención automatizada para el tiempo de respuesta (Automated Intervention for Time-Lock), que extiende el bloqueo temporal de la autenticación indefinidamente hasta que se resuelva la alerta. Esto significa que, en caso de activarse la alarma, ESDEG no eliminará los archivos. Esto puede provocar un comportamiento anómalo si no se resuelve durante períodos prolongados.

Por lo tanto, a partir de ahora, la persona encargada de detectar las alarmas en el diagnóstico ESDEG deberá seguir estos pasos para solucionar las alarmas que se encuentren activas "Shared anomaly detected. An anomaly detected on the (Shared Host)" - anomalía detectada en el recurso compartido. Se ha detectado una anomalía en el recurso compartido (Shared del Shared).

- Revisar el estado de los recursos de la alarma y confirmar que los recursos de la alarma están en un estado de normal funcionamiento y que los recursos de la alarma están en un estado de normal funcionamiento.
- En ESDEG, ahora hay un botón "AI" en el menú de recursos. Haga clic en el botón "AI" para ver el estado de los recursos. Haga clic en el botón "AI" para ver el estado de los recursos.
- Seleccione "View" para ver la alarma en detalle. Ahora podrá ver cuáles recursos se encuentran en estado de normal funcionamiento.
- Si no está al tanto de estos elementos y sospecha de un ataque, seleccione inmediatamente "Suspend" para suspender con Shared.

7. Host NAS1 – Windows Server 2016 Estándar

Vulnerabilidades	
172.18.51.23	This device is in the ESDEG-SERVIDORES site with normal importance. 10 severe vulnerabilities were discovered. 2 moderate vulnerabilities were discovered. 7 DCE RPC services were discovered. 2 CIFS services were discovered. 2 <unknown> services were discovered. 2 portmapper services were discovered. 2 status services were discovered. One callbook service was discovered. One RDP service was discovered. One HTTP service was discovered. One DCE Endpoint Resolution service was discovered. One CIFS Name Service service was discovered.

Remediación. En el host identificado con IP 172.18.51.23, en producción, se realizaron acciones de remediación orientadas a corregir vulnerabilidades críticas asociadas a los servicios SMB y a la configuración de cifrado del sistema operativo. Se deshabilitó el protocolo SMBv1 y se configuró la firma SMB como obligatoria, mitigando riesgos de ataques de tipo downgrade y man-in-the-middle.

Adicionalmente, se aplicó un proceso de hardening de seguridad sobre la capa criptográfica, deshabilitando los protocolos TLS 1.0 y TLS 1.1, así como los cifrados débiles RC4 y 3DES, y forzando el uso de TLS 1.2, conforme a buenas prácticas de seguridad. Estas acciones requirieron un reinicio controlado del sistema.

Como medida preventiva adicional, el servicio RDP fue deshabilitado con el fin de reducir la superficie de exposición durante el proceso de remediación. Con estas acciones se mitigaron los hallazgos identificados, quedando el host alineado con los lineamientos de seguridad establecidos.

```
PS C:\Users\administrator.ESDEGUERRA> Get-WindowsFeature FS-SMB1

Display Name                                     Name             Install State
-----
[X] SMB 1.0/CIFS File Sharing Support           FS-SMB1           Installed

PS C:\Users\administrator.ESDEGUERRA> Get-SmbServerConfiguration | Select EnableSMB1Protocol

EnableSMB1Protocol
-----
True

PS C:\Users\administrator.ESDEGUERRA> Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force

PS C:\Users\administrator.ESDEGUERRA>

PS C:\Users\administrator.ESDEGUERRA> Get-SmbServerConfiguration | Select EnableSecuritySignature, RequireSecuritySignature

EnableSecuritySignature RequireSecuritySignature
-----
False                  False

PS C:\Users\administrator.ESDEGUERRA> Get-SmbClientConfiguration | Select EnableSecuritySignature, RequireSecuritySignature

EnableSecuritySignature RequireSecuritySignature
-----
True                  False

PS C:\Users\administrator.ESDEGUERRA> Set-SmbServerConfiguration -EnableSecuritySignature $true -Force
PS C:\Users\administrator.ESDEGUERRA> Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
PS C:\Users\administrator.ESDEGUERRA> Get-SmbServerConfiguration | Select EnableSecuritySignature, RequireSecuritySignature

EnableSecuritySignature RequireSecuritySignature
-----
True                  True
```

```
PS C:\Users\Administrator\ESDEGUERRA> Get-ChildItem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols" -Recurse

Hive: HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Name      Property
-----
SSL 2.0

Hive: HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0

Name      Property
-----
Client    DisabledByDefault : 1
```

```
1 Get-ChildItem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols" -Recurse
2 ForEach-Object {
3     Write-Host "n[$($_.PSChildName)]"
4     Get-ItemProperty $_.PSPath -ErrorAction SilentlyContinue
5 }
6

MaxIdleTime REG_DWORD 0x0
MaxInstanceCount REG_DWORD 0xffffffff
MinEncryptionLevel REG_DWORD 0x2
MinLogonServer REG_SZ
OutBufCount REG_DWORD 0x6
OutBufDelay REG_DWORD 0x64
OutBufLength REG_DWORD 0x212
Password REG_SZ
PdClass REG_DWORD 0x2
PdClass1 REG_DWORD 0xb
PdDLL REG_SZ tcp
PdDll1 REG_SZ tssecsrv
PdFlag REG_DWORD 0x4e
PdFlag1 REG_DWORD 0x0
PdName REG_SZ tcp
PdName1 REG_SZ tssecsrv
PortNumber REG_DWORD 0xd3d
SecurityLayer REG_DWORD 0x2
SelectNetworkDetect REG_DWORD 0x1
SelectTransport REG_DWORD 0x2
Shadow REG_DWORD 0x1
UserAuthentication REG_DWORD 0x0
Username REG_SZ
WdFlag REG_DWORD 0x36
WdName REG_SZ Microsoft RDP 8.0
WdPrefix REG_SZ RDP
WdProfilePath REG_SZ
WorkDirectory REG_SZ

HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\TSWinRemotingAllowedApps
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\VideoRemotingWindowNames

PS C:\Users\Administrator\ESDEGUERRA>
```

```
PS C:\Users\Administrator\ESDEGUERRA> Get-Childitem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols"

Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Name      Property
-----
SSL 2.0


PS C:\Users\Administrator\ESDEGUERRA> Get-Childitem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers"

PS C:\Users\Administrator\ESDEGUERRA>

Get-Childitem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Force | Out-Null
Get-Childitem "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client" -Force | Out-Null
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name "Enabled" -Value 0 -PropertyType Word -Force
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Force | Out-Null
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -Force | Out-Null
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client" -Force | Out-Null
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -Name "Enabled" -Value 1 -PropertyType Word -Force
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client" -Name "Enabled" -Value 1 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168" -Name "Enabled" -Value 0 -PropertyType Word -Force
PS C:\Users\Administrator\ESDEGUERRA> New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Force | Out-Null
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client" -Name "Enabled" -Value 0 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" -Name "Enabled" -Value 1 -PropertyType Word -Force
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client" -Name "Enabled" -Value 1 -PropertyType Word -Force
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" -Force | Out-Null
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" -Name "Enabled" -Value 0 -PropertyType Word -Force
```

8. Host CENTROCOPY – Windows Server 2019 Standard

The enabled	
172.18.51.184	<p>This device is in the ESDEG-SERVIDORES site with normal importance.</p> <p>One critical vulnerability was discovered.</p> <p>7 severe vulnerabilities were discovered.</p> <p>3 moderate vulnerabilities were discovered.</p> <p>One Postgres service was discovered.</p> <p>9 DCE RPC services were discovered.</p> <p>6 HTTP services were discovered.</p> <p>4 HTTPS services were discovered.</p> <p>3 <unknown> services were discovered.</p> <p>2 remoting services were discovered.</p> <p>2 CIFS services were discovered.</p> <p>One RealAudio service was discovered.</p> <p>One RDP service was discovered.</p> <p>One Xwindows service was discovered.</p> <p>One callbook service was discovered.</p> <p>One CIFS Name Service service was discovered.</p> <p>One VNC service was discovered.</p> <p>One DCE Endpoint Resolution service was discovered.</p> <p>One NTP service was discovered.</p>

Remediación: En el host identificado con IP **172.18.51.184**, se ejecutaron las remediaciones para atender la vulnerabilidad crítica, las vulnerabilidades severas y moderadas detectadas durante el análisis. En cumplimiento del plan establecido, se corrigió el **Common Name (CN) del certificado digital** para que coincidiera con el nombre real del servidor y del servicio publicado, y se reemplazó el certificado anterior. Asimismo, se **eliminó la página por defecto del servidor IIS**, reduciendo la exposición innecesaria del servicio web.

Adicionalmente, se realizaron ajustes de seguridad sobre los servicios de red identificados. Se deshabilitó el protocolo **SMBv1** y se configuró la **firma SMB como obligatoria**, se restringió el acceso al servicio **PostgreSQL (puerto 5432)** permitiendo únicamente las direcciones IP autorizadas, y se implementaron reglas de firewall para bloquear la exposición del servicio **VNC (puerto 5900)**, validando desde otro host que no existiera acceso remoto. De igual manera, se restringió la exposición de servicios NetBIOS y se verificó la correcta configuración de los servicios compartidos.

Finalmente, se aplicó un proceso de fortalecimiento criptográfico, deshabilitando protocolos y cifrados obsoletos, forzando configuraciones seguras en los servicios HTTP y HTTPS, y verificando la correcta operación del servidor tras los reinicios controlados realizados. Con estas acciones se atendieron de manera integral los hallazgos asociados a los servicios detectados (HTTP, HTTPS, Postgres, CIFS, VNC y servicios remotos) y como medida preventiva adicional se **deshabilitó el servicio RDP** para todos dejando únicamente el servicio activo para dos equipos restringidos por IP, dejando el host en un estado seguro, operativo y alineado con los lineamientos institucionales.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\administrator> Disable-WindowsOptionalFeature -Online -FeatureName:SMB1Protocol

Path:
Online: True
RestartNeeded: False

PS C:\Users\administrator> systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
PS C:\Users\administrator> dir

Directorio: C:\Users\administrator

Mode                LastWriteTime         Length Name
----                -
d-r----- 23/01/2026 1:28 p. m.           30 Objects
d-r----- 23/01/2026 1:28 p. m.           Contacts
d-r----- 23/01/2026 1:28 p. m.           Desktop
d-r----- 23/01/2026 1:28 p. m.           Documents
d-r----- 26/01/2026 10:33 a. m.           Downloads
d-r----- 23/01/2026 1:28 p. m.           Favorites
d-r----- 23/01/2026 1:28 p. m.           Links
d-r----- 23/01/2026 1:28 p. m.           Music
d-r----- 23/01/2026 1:28 p. m.           OneDrive
d-r----- 21/12/2023 12:53 p. m.           Pictures
d-r----- 23/01/2026 1:28 p. m.           Saved Games
d-r----- 23/01/2026 1:28 p. m.           Searches
d-r----- 23/01/2026 1:28 p. m.           Videos
-a----- 23/01/2026 4:07 p. m.          27400 Get-TlsCipherSuite.txt
-a----- 26/01/2026 12:35 p. m.           14 start
-a----- 27/09/2024 12:03 p. m.          58535280 Topia_CMO_Setup_x64.exe
-a----- 27/09/2024 12:03 p. m.           6298936 vrx.exe

PS C:\Users\administrator> Get-WindowsFeature | Where-Object { $_.InstallState -eq "Installed" }

Display Name                                     Name                                     Install State
```

```

1 New-NetFirewallRule
2 -DisplayName "Postgres Allow 172.18.52.0-24"
3 -Direction Inbound
4 -Protocol TCP
5 -LocalPort 5432
6 -RemoteAddress 172.18.52.0/24
7 -Action Allow
8 -Profile Any
9

```

```

-Direction Inbound
-Protocol TCP
-LocalPort 5432
-RemoteAddress 172.18.52.0/24
-Action Allow
-Profile Any

```

```

Name : {08660aaa-ad89-44fa-a2b9-0efb2260cb99}
DisplayName : Postgres Allow 172.18.52.0-24
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

```

```

1 New-NetFirewallRule
2 -DisplayName "Postgres Block Others"
3 -Direction Inbound
4 -Protocol TCP
5 -LocalPort 5432
6 -RemoteAddress Any
7 -Action Block
8 -Profile Any
9

```

```

-Direction Inbound
-Protocol TCP
-LocalPort 5432
-RemoteAddress Any
-Action Block
-Profile Any

```

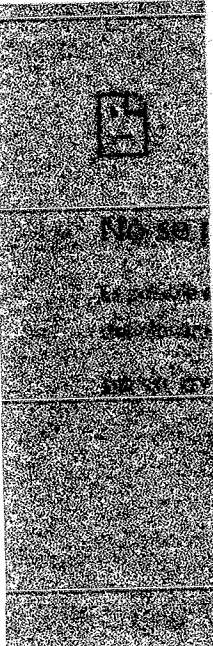
```

Name : {be71aced-4ed7-420f-bdde-dba9f75b6cb6}
DisplayName : Postgres Block Others
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Block
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

```

No es seguro http://centrocopy

Visor de certificados: centrocopy.esdeg.edu.co



General Detalles

Enviado a

Nombre común (CN)	centrocopy.esdeg.edu.co
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	centrocopy.esdeg.edu.co
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Período de validez

Emitido el	viernes, 6 de febrero de 2016, 10:53:48
Vencimiento el	viernes, 5 de febrero de 2027, 19:00:00

Huellas digitales SHA-256

Utilice esta característica para solicitar y administrar certificados que el servidor v

Filt

No

srv

Certificado

General Detalles Ruta de certificación

Información del certificado

Este certif. está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto
- Todas las directivas de emisión

Emitido para: centrocopy.esdeg.edu.co

Emitido por: centrocopy.esdeg.edu.co

Válido desde 6/02/2016 hasta 5/02/2027

Tiene una clave privada correspondiente a este certificado.

Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the

Server Protocols	Ciphers	Hashes	Key Exchanges
☐ Multi-Protocol Unified Hello ☐ PCT 1.0 ☐ SSL 2.0 ☐ SSL 3.0 ☐ TLS 1.0 ☐ TLS 1.1 ☒ TLS 1.2	☐ NULL ☐ DES 56/56 ☐ RC2 40/128 ☐ RC2 56/128 ☐ RC2 128/128 ☐ RC4 40/128 ☐ RC4 56/128 ☐ RC4 64/128 ☐ RC4 128/128 ☐ Triple DES 168 ☐ AES 128/128 ☒ AES 256/256	☒ MD5 ☒ SHA ☐ SHA 256 ☐ SHA 384 ☒ SHA 512	☒ Diffie-Hellman ☒ PKCS ☒ ECDH

Client Protocols

☒ Multi-Protocol Unified Hello ☐ PCT 1.0 ☐ SSL 2.0 ☐ SSL 3.0 ☐ TLS 1.0 ☐ TLS 1.1 ☐ TLS 1.2
--

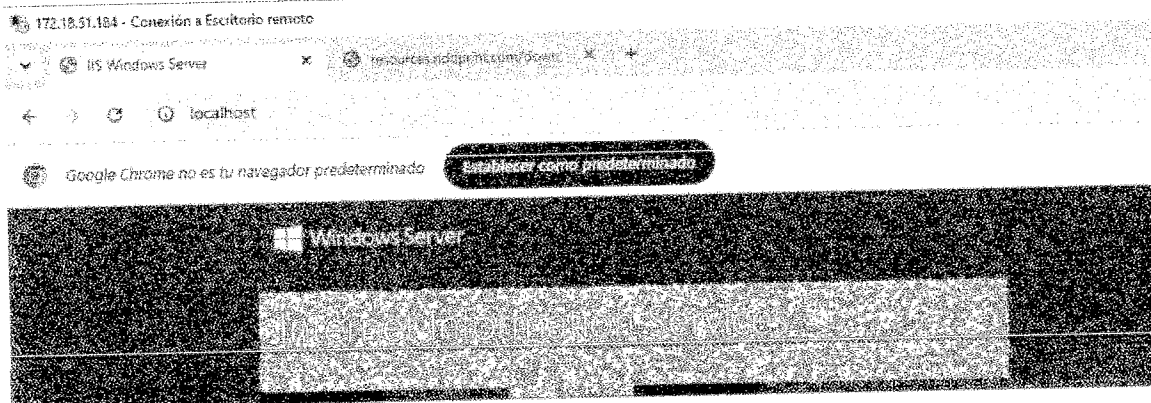
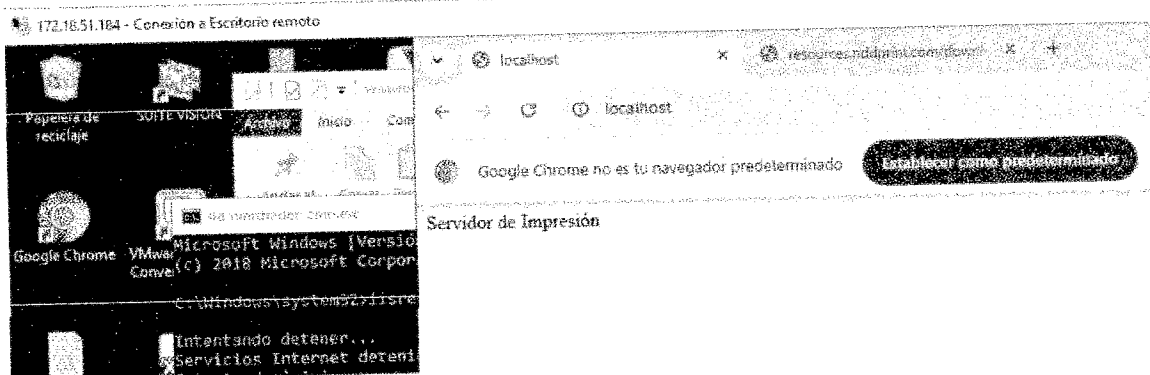
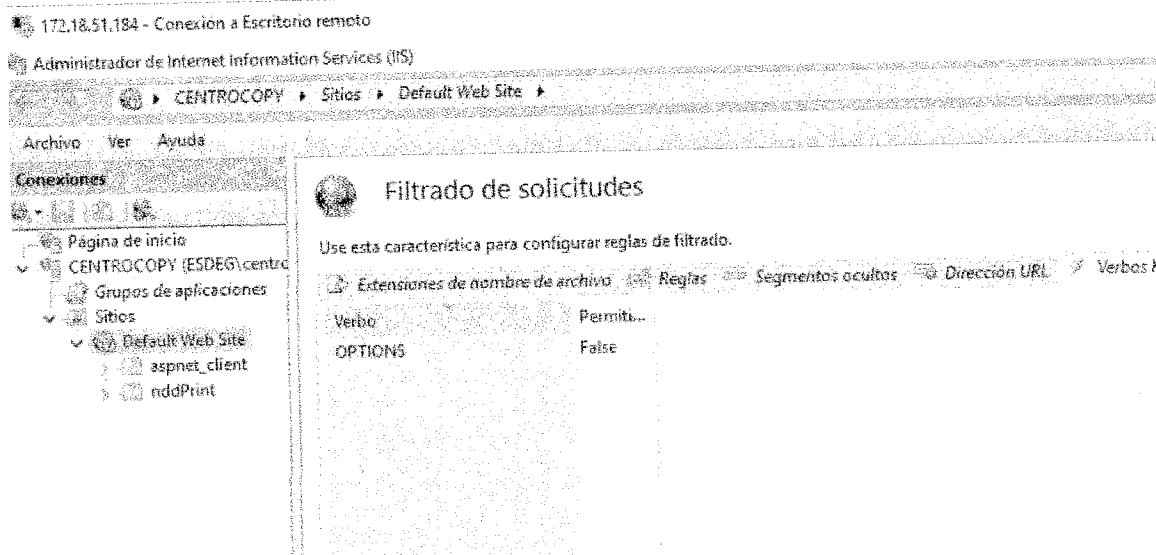
Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the

Server Protocols	Ciphers	Hashes	Key Exchanges
☐ Multi-Protocol Unified Hello ☐ PCT 1.0 ☐ SSL 2.0 ☐ SSL 3.0 ☐ TLS 1.0 ☐ TLS 1.1 ☒ TLS 1.2	☐ NULL ☐ DES 56/56 ☐ RC2 40/128 ☐ RC2 56/128 ☐ RC2 128/128 ☐ RC4 40/128 ☐ RC4 56/128 ☐ RC4 64/128 ☐ RC4 128/128 ☒ Triple DES 168 ☒ AES 128/128 ☒ AES 256/256	☒ MD5 ☒ SHA ☒ SHA 256 ☒ SHA 384 ☒ SHA 512	☒ Diffie-Hellman ☒ PKCS ☒ ECDH

Client Protocols

☐ Multi-Protocol Unified Hello ☐ PCT 1.0 ☐ SSL 2.0 ☐ SSL 3.0 ☐ TLS 1.0 ☐ TLS 1.1 ☒ TLS 1.2
--



Asignación de derechos de...	Seguridad de red: nivel de autenticación de LAN Manager	No está definido
Opciones de seguridad	Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
Windows Defender Firewall con	Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	No está definido
Directivas de Administrador de	Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	No está definido
Directivas de clave pública	Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Inter...	No está definido
Directivas de restricción de soft	Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
Directivas de control de aplicaci	Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio	No está definido
Directivas de seguridad IP en Eq	Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM	No está definido
Configuración de directiva de a	Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	No está definido
QoS basada en directiva	Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	No está definido
Plantillas administrativas	Seguridad de red: restringir NTLM: autenticación NTLM en este dominio	No está definido
Plantillas administrativas	Seguridad de red: restringir NTLM: tráfico NTLM entrante	No está definido
	Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos	No está definido
	Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 ...
	Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 ...
	Servidor de red de Microsoft: intentar SASLSelf para obtener información de notificaciones	No está definido
	Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada
	Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
	Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	No está definido

Propiedades: postgres Bloquear general

Opciones avanzadas Entidades de seguridad locales Usuarios remotos

General Programas y servicios Equipos remotos Protocolos y puertos Ambito

General

Nombre:

Descripción:

☒ Habilitado

Acción

☐ Permitir la conexión

☐ Permitir la conexión si es segura

☒ Bloquear la conexión

Propiedades: postgres Bloquear general

Propiedades: postgres Bloquear general

Opciones avanzadas Entidades de seguridad locales Usuarios remotos

General Programas y servicios Equipos remotos Protocolos y puertos **Ámbito**

Protocolos y puertos

Tipo de protocolo: TCP

Número de protocolo: 5432

Puerto local: Puertos específicos

Ejemplo: 80, 443, 5000-5010

Puerto remoto: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Configuración ICMP:

172.19.51.184 - Conexión a Escritorio remoto

Editor de directiva de grupo local

Archivo Acción Ver Ayuda

Directiva Equipo local

Configuración

Propiedades: Bloquear Puerto 137 TCP

Opciones avanzadas Entidades de seguridad locales Usuarios remotos

General Programas y servicios Equipos remotos Protocolos y puertos **Ámbito**

General

Nombre: Bloquear Puerto 137 TCP

Descripción:

☒ Habilitado

Acción:

☐ Permitir la conexión

☐ Permitir la conexión si es segura

☒ Bloquear la conexión

Propiedades: Bloquear puerto 137 y 138 UDP

Opciones avanzadas Entidades de seguridad locales Usuarios remotos

General Programas y servicios Equipos remotos Protocolos y puertos **Ámbito**

General

Nombre: Bloquear puerto 137 y 138 UDP

Descripción:

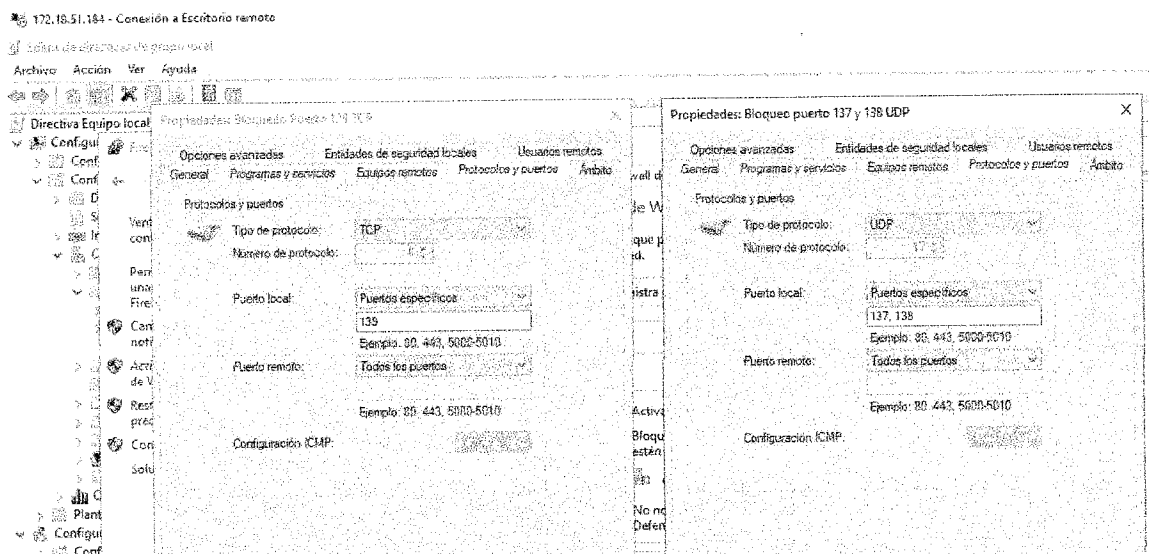
☒ Habilitado

Acción:

☐ Permitir la conexión

☐ Permitir la conexión si es segura

☒ Bloquear la conexión



Actividades adicionales de fortalecimiento de seguridad perimetral

En atención a la **Alerta de Ciberseguridad por Data Leak** emitida por el Ministerio de Defensa y conforme a lo informado mediante comunicación oficial del **19 de enero**, se realizaron actividades adicionales de **endurecimiento de la seguridad perimetral** sobre la infraestructura institucional. Estas acciones se implementaron con el fin de mitigar riesgos asociados a accesos no autorizados y amenazas externas, complementando las labores de remediación por host.

Como parte de estas actividades, se realizó la **configuración manual de políticas de firewall** en el equipo **FortiGate 600E**, creando reglas específicas por **segmento de red, VLAN e interfaz**, de acuerdo con los flujos de tráfico requeridos. Estas políticas fueron definidas de manera individual para los distintos orígenes y destinos (auditorios, aulas, redes cableadas, servidores, impresoras y salida a WAN), permitiendo aplicar los controles de seguridad de forma precisa y funcional. Esta implementación garantizó el bloqueo y filtrado del tráfico conforme a los lineamientos establecidos, asegurando la correcta operación de los servicios sin depender de agrupaciones lógicas que no resultaron efectivas en este escenario.

Adicionalmente, se habilitó el **control de tráfico por geolocalización**, definiendo un grupo de países considerados de riesgo según el informe de seguridad, incluyendo **Rusia, China y Venezuela**, y se configuró una **política de firewall** para bloquear el tráfico de entrada y salida asociado a dicho grupo de países.

Asimismo, se creó y configuró un **conector de seguridad tipo Threat Feed**, enlazado a un servidor local institucional, desde el cual se cargaron **964 direcciones IP públicas** relacionadas en el informe de seguridad. Este Threat Feed fue integrado a las políticas del firewall, permitiendo el bloqueo automático del tráfico proveniente de dichas direcciones IP, fortaleciendo los mecanismos de prevención y control frente a intentos de intrusión.

2	1	AUTHORIO(AUTHORIO)	1	VLAD SERVED	3
3	1	AUTHORIO(AUTHORIO)	1	WAN	4
4	1	AUDAS(MAN AUDAS)	1	RIC OCCPI	5
5	1	AUDAS(MAN AUDAS)	1	VLAD SERVED	6
6	1	AUDAS(MAN AUDAS)	1	WAN	7
7	1	CABLE(MAN CABLE)	1	Imociano(Man Imociano)	8
8	1	CABLE(MAN CABLE)	1	RIC OCCPI	9
9	1	CABLE(MAN CABLE)	1	SALA ESDEG(SALA ESDEG)	10
10	1	CABLE(MAN CABLE)	1	WAN SERVED	11
11	1	CABLE(MAN CABLE)	1	WAN	12

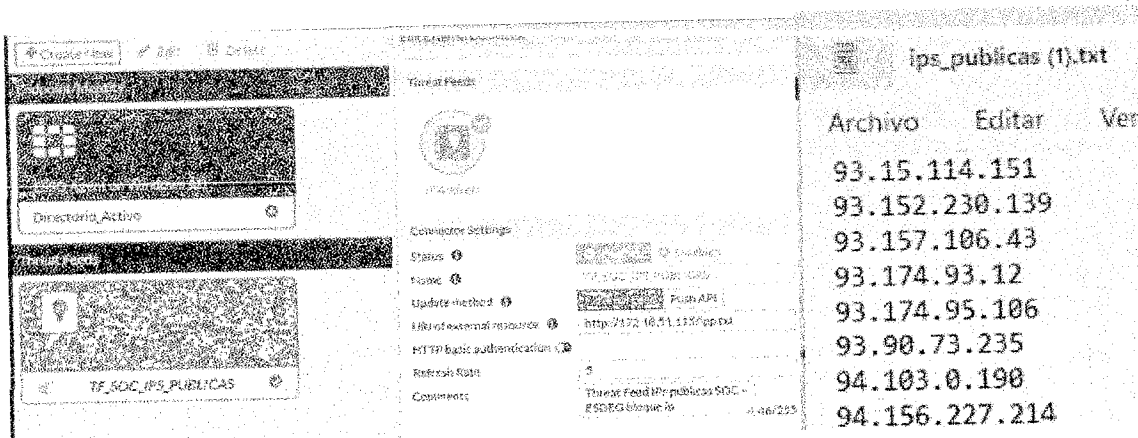
Name	Details	Interface	Type	Ref
Port				
Address Group	<ul style="list-style-type: none"> 10.10.10.10 10.10.10.11 10.10.10.12 10.10.10.13 10.10.10.14 10.10.10.15 		Address Group	10
Address Group	<ul style="list-style-type: none"> China Europe North America 		Address Group	3

[+ Create New](#)
[Edit](#)
[Set in CU](#)
[Create](#)
[Q Policy Group](#)
[Search](#)

Name	Source	Destination	Schedule	Service	Action
FW Filter Server WAN					
Bloqueo_IP	all	Bloqueados IPV4	always	ALL	DENY
SERVER WAN	all	all	always	ALL	ACCEPT

WAN -> VLAN_SERVER					
WAN_WAF	all	WAF WAF SSL CL5MA	always	HTTP HTTPS Puerto 8080 SMTP SMTPS	ACCEPT

Zona Bloqueada		Zona Bloqueada		Zona Bloqueada	
Bloqueo_Rusia_informe1	all	Bloqueados IPV4 Países Bloqueado	always	ALL	DENY
Bloqueo_Rusia_informe2	Bloque Países	all	always	ALL	DENY
IpsinformeRusia	TF_SO	all	always	ALL	DENY



Las actividades descritas hacen parte de un proceso de remediación y fortalecimiento de seguridad que se encuentra actualmente **en ejecución**. A la fecha, se han implementado controles técnicos que permiten reducir de manera significativa la superficie de ataque y mitigar los riesgos identificados. El proceso continuará desarrollándose de forma progresiva, y una vez se completen la totalidad de las acciones previstas, se presentará el cierre definitivo con los resultados finales.

PS. YESSID ARAMIS CÁCERES VÁSQUEZ
Ingeniero de Infraestructura y Seguridad
Departamento TIC ESDEG

PAGADO 14/01/2026

I. DATOS DEL APORTANTE

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

II. DETALLE DEL APORTANTE

Datos del Afiliado				Novedades												Pensiones			Salud			Riesgos			Cajas				Parafiscales				Total			
Identificación	Apellidos y Nombres	Tipo Cotizante	Sitio Cotizante	ING	RET	PRE	OTR	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA	Administradores	IBC Pension	Aporte Pension	Administradores	IBC Salud	Aporte Salud	Tarifa	IBC Riesgos	Aporte Riesgos	Administradores	IBC Caja	Aporte Caja	Aporte SENA	Aporte ICBF	ESAP	Aporte Ministerio	Total
CC 72342326	YESSID ARAMIS CACERES VASQUEZ	59	00																	(231001) COLFONDOS	\$ 3.560.000	\$ 569.600	(EPS005) EPS SANITAS	\$ 3.560.000	\$ 446.000	0.522	\$ 3.560.000	\$ 16.600	(NIN-CC) NINGUNA CCF	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0	\$ 1.033.200

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, Salidas a Favor) EPS	Incapacidades ARP	SUBTOTAL SIN INTERESES DE MORA	TOTAL INTERESES DE MORA	TOTAL FINAL
\$ 3.560.000	\$ 3.560.000	\$ 3.560.000	\$ 0	\$ 569.600	\$ 445.000	\$ 18.600	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0	\$ 0	\$ 1.033.200	\$ 3.900	\$ 1.037.100