Bogotá D.C. FECHA: julio 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. 06 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. 6 según forma y condiciones de pago y actividades del plan de trabajo descritas en el contrato.

## 1. DATOS DEL CONTRATO SUPERVISADO

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



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

| Recurso presupuestal | R10 |
|---|---|
| **Forma Y Condiciones De Pago** | El valor total del contrato se cancelará en forma parcial al CONTRATISTA de la siguiente forma (menos los descuentos de ley): ONCE (11) pagos cada uno por valor de CINCO MILLONES CUATROCIENTOS VEINTICINCO MIL PESOS (5.425.000,00) M/CTE sin IVA.<br>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.<br><br>PARÁGRAFO PRIMERO: Para el primer informe de supervisión se deberá allegar:<br>Acta de capacitación relacionada con: Sistema de Gestión de Seguridad y Salud en el Trabajo. Compromiso anticorrupción<br>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).<br>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).<br><br>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.<br><br>PARÁGRAFO TERCERO: De conformidad con lo establecido en la Directiva Presidencial No. 09 del 17 de Septiembre de 2020 "Lineamientos para el pago a los proveedores del Estado", en caso que el contratista este obligado a facturar electrónicamente, deberá presentar la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia, con lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020, y las normas que las modifiquen o sustituyan. Así mismo, el contratista deberá haber efectuado el proceso de Validación de la factura electrónica en el Sistema SECOP II, de |



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

<table>
<tr><td></td><td>conformidad con lo señalado sobre el particular por Colombia Compra Eficiente.<br><br>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.<br><br>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.<br><br>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.</td></tr>
<tr><td>Modificatorio</td><td>
<table>
<tr><th>TIPO DE MODIFICATORIO</th><th>MODIFICATORIO No.</th><th>FECHA</th><th>CLAUSULA MODIFICADA No.</th><th>RESUMEN DEL MODIFICATORIO</th></tr>
<tr><td>ADICIÓN-REDUCCIÓN-SUSPENSIÓN-OTROS</td><td>NO APLICA</td><td>NO APLICA</td><td>NO APLICA</td><td>NO APLICA</td></tr>
</table>
</td></tr>
<tr><td>Valor Final ( + modificatorio)</td><td>NO APLICA</td></tr>
<tr><td>Plazo De Ejecución Final ( + modificatorio)</td><td>NO APLICA</td></tr>
<tr><td>Nombre Del Supervisor</td><td>TE. RAMIREZ FLOR ENRIQUE</td></tr>
<tr><td>Número De Resolución De Nombramiento</td><td>001 DE 2026</td></tr>
<tr><td>Teléfono De Contacto</td><td>3135239402</td></tr>
<tr><td>Correo Electrónico</td><td>enrique.ramirez@esdeg.edu.co</td></tr>
</table>



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

## 1.1 CAMBIO DE SUPERVISOR

| | |
|---|---|
| **Nombre Del Supervisor** | |
| **Número De Resolución De Nombramiento** | |
| **Teléfono De Contacto** | |
| **Correo Electrónico** | |
| **Motivo del Cambio de supervisor** | |

## 2. GARANTÍAS

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

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

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

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

## 3. EJECUCIÓN CONTRACTUAL

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



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

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

## PLAN DE TRABAJO

| No | ACTIVIDADES DESARROLLADAS | ENTREGABLE |
|---|---|---|
| **1.** | Realizar un análisis de capacidad y rendimiento de la plataforma de servidores de virtualización y proponer mejoras para garantizar su escalabilidad si hace falta. | Anexo Informe |
| **2.** | Realizar un estudio de cobertura y calidad del servicio WIFI en áreas específicas de la ESDEG y tomar medidas correctivas según sea necesario. | Anexo Informe |
| **3.** | Verificar regularmente la ejecución exitosa de las copias de seguridad de los servidores. | Anexo Informe |
| **4.** | Monitorear continuamente la capacidad de almacenamiento utilizada para prever y mitigar problemas de espacio. Recomendar proactivamente la reorganización o eliminación de copias de seguridad antiguas, garantizando así la disponibilidad y la protección de datos esenciales cuando el almacenamiento alcanza su capacidad máxima si se llega a presentar. | Anexo Informe |
| **5.** | Monitorear continuamente los equipos perimetrales de seguridad y realizar ajustes según las necesidades detectadas y/u órdenes recibidas (Firewall Fortinet, Fortiswitch, Fortiap, Fortianalyzzer, Forti autenticador, Fortimanager, Veem Bk) | Anexo Informe |



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

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

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

| FECHA DE PAGO | NÚMERO DE PLANILLA | HONORARIOS MENSUALES | INGRESO BASE COTIZACIÓN (40%) | SISTEMA DE SALUD (12,5%) | SISTEMA DE PENSIÓN (16%) | ARL |
|---|---|---|---|---|---|---|
| NA | NA | NA | NA | NA | NA | SURA |
| 16/03/2026 | 84449480 | 9.929.000 | 3.971.600 | 496.500 | 635.500 | 20.800 |
| 16/04/2026 | 84457704 | 9.929.000 | 3.971.600 | 496.500 | 635.500 | 20.800 |
| 19/05/2026 | 85086490 | 9.929.000 | 3.971.600 | 496.500 | 635.500 | 20.800 |
| 16/06/2026 | 85755197 | 9.929.000 | 3.971.600 | 496.500 | 635.500 | 20.800 |
| 15/07/2026 | 86344465 | 9.929.000 | 3.971.600 | 496.500 | 635.500 | 20.800 |

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

## 5. CRITERIO DE EVALUACIÓN MENSUAL

Yo, TE. RAMIREZ FLOR ENRIQUE supervisor del contrato, verifiqué las actividades realizadas por EL CONTRATISTA y certifico que están acorde a las obligaciones específicas y al plan de trabajo pactadas en el **CONTRATO DE PRESTACIÓN DE SERVICIOS PROFESIONALES NO. 052-MDN-COGFM-ESDEG-2026**, por lo tanto, se recibe a satisfacción el cumplimiento de las obligaciones correspondientes al pago No. 06 según forma y condiciones de pago y actividades del plan de trabajo descritas en el contrato.

| CUMPLIMIENTO DE EJECUCIÓN PRESUPUESTAL |
|---|
| 54,55 % |

## 6. BALANCE

| BALANCE | |
|---|---|
| **DESCRIPCIÓN** | **VALORES** |
| VALOR INCIAL CONTRATO | $ 59. 675.000 |
| VALOR ADICIÓN | N/A |
| VALOR REDUCCIÓN | N/A |
| VALOR PAGADO. | $ 27.125.000 |
| PAGO PARA ESTE INFORME | $ 5.425.000 |
| PENDIENTE POR PAGAR | $ 27.125.000 |



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

## 7. ANEXOS

| ANEXO | HOJAS |
|---|---|
| Planilla 86344465 | 1 |
| Certificado de aplicación Retención en la Fuente (Decreto No. 2231 del 22 de diciembre del 2023) | 1 |
| Informe Incidente | 4 |
| Informe Infraestructura | 5 |
| Informe Ccoci | 4 |

Atentamente,

CONTRATISTA:

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

SUPERVISOR:

Grado y Nombre TE. RAMIREZ FLOR ENRIQUE
Tipo y No. Documento C.C. 1.061.743.430
Jefe del Departamento TIC

**Archivado en:** 15.103.12.5 Contrato de prestación de servicios 2026.



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

## 7. ANEXOS

| ANEXO | HOJAS |
|---|---|
| Informe Actividades | 4 |
| Planilla 86344465 | 1 |
| Certificado de aplicación Retención en la Fuente (Decreto No. 2231 del 22 de diciembre del 2023) | 1 |
| Informe Incidente | 4 |
| Informe Infraestrucutra | 5 |
| Informe_Ccoci | 4 |

Atentamente,

CONTRATISTA:

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

SUPERVISOR:

Grado y Nombre TE. RAMIREZ FLOR ENRIQUE
Tipo y No. Documento C.C. 1.061.743.430
Jefe del Departamento TIC

**Archivado en:** 15,103.42.5 Contrato de prestación de servicios 2026.



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

Bogotá D.C. junio de 2026
RADICADO No.0126109234 / MDN-COGFM-JEMCO-ESDEG-SBESG-VIADM-DETIC

**Señor Teniente**
**Enrique Ramírez Flor**
**Supervisor del Contrato**

**ASUNTO: INFORME DE INCIDENTE DE SEGURIDAD INFORMÁTICA**

Por medio del presente, me permito informar las actividades desarrolladas por el Departamento de Tecnologías de la Información y las Comunicaciones (DETIC) relacionadas en atención de un incidente de seguridad informática identificado el día 23 de junio de 2026, el cual ocasionó que múltiples cuentas institucionales del dominio @esdeg.edu.co se vieran comprometidas. Como parte de las acciones de respuesta, se realizó la auditoría de registros de autenticación en Microsoft Entra ID (Office 365), identificando intentos de acceso no autorizados desde diferentes ubicaciones geográficas, por lo que se ejecutaron medidas de contención, análisis y remediación orientadas a proteger la integridad de las cuentas institucionales, fortalecer los mecanismos de seguridad y mitigar cualquier riesgo asociado a la disponibilidad, confidencialidad e integridad de la información institucional.

**Análisis del Evento**

**Vector de Ataque:** El incidente se originó a partir del compromiso de credenciales institucionales mediante campañas de phishing. Una vez obtenidas dichas credenciales, los atacantes ejecutaron una campaña de password spraying, reutilizando las contraseñas comprometidas e intentando su autenticación sobre múltiples cuentas del dominio. Adicionalmente, emplearon patrones de contraseñas comunes y predecibles utilizados por los usuarios, tales como Colombia2026*, MesActual2026* y otras variantes similares, con el propósito de identificar cuentas adicionales vulnerables por reutilización de credenciales o por el uso de contraseñas débiles y fácilmente inferibles.

Estimado(a) usuario(a),

Por medio de la presente, le notificamos que su cuenta institucional ha sido seleccionada en nuestro sistema para un **proceso de revisión por falta de actividad y actualización de datos obligatoria.** De no registrarse movimiento, la cuenta será programada para su baja definitiva.

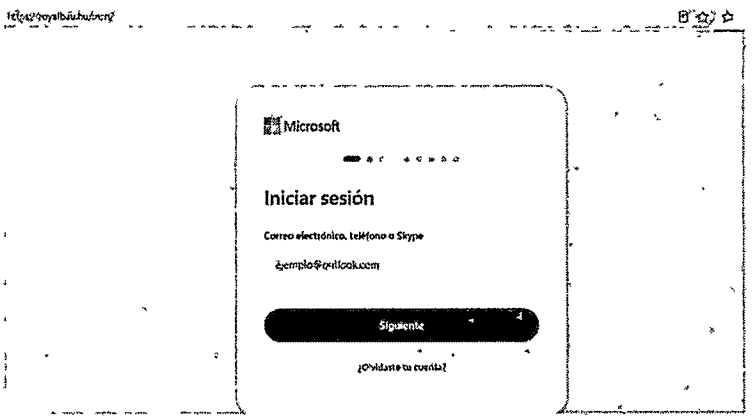
Para conservar sus accesos, correos y archivos almacenados, le solicitamos realizar la **validación de identidad obligatoria** a la brevedad posible a través de nuestros canales oficiales.

VALIDAR IDENTIDAD

Evite la pérdida irreversible de su información.

Atentamente,

**Soporte Técnico / Área de TI**




**Modo de Operación del Ataque**
El sitio fraudulento simulaba el proceso de autenticación institucional. Inicialmente solicitaba el usuario institucional, posteriormente la contraseña y, de manera sucesiva, presentaba pantallas simulando procesos de verificación de identidad, tales como reconocimiento facial y validación del número de teléfono celular. Finalmente inducía al usuario a ingresar el código de verificación (MFA) recibido mediante mensaje de texto. Mientras la víctima suministraba esta información, el atacante utilizaba las credenciales en tiempo real para autenticarse en Microsoft Outlook y completar el proceso de doble factor de autenticación, logrando el acceso únicamente cuando el usuario proporcionaba voluntariamente el código recibido y nuevamente se rep.

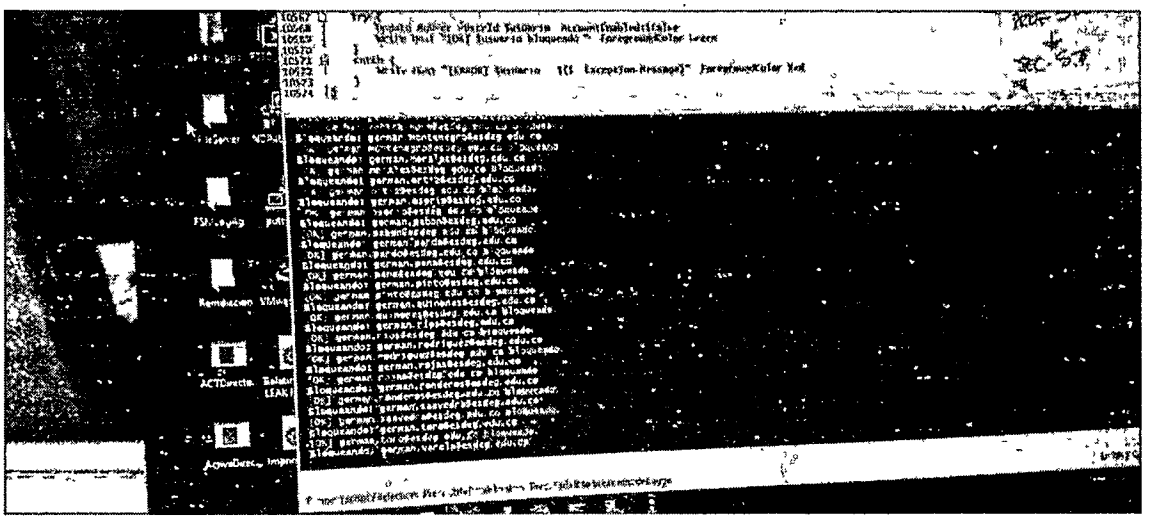
**Indicadores de Compromiso:** Durante el proceso de investigación se identificaron tres (3) URL maliciosas utilizadas por los atacantes como parte de la infraestructura empleada en la campaña de phishing. Estas direcciones incluían un servicio de acortamiento de URL y sitios intermedios utilizados para redirigir a las víctimas hacia la página fraudulenta de captura de credenciales:

- https://short.do/nPtzXE
- https://royalbau.hu/msn/
- https://planes.sapac.com.ar/caso-5121/

**Trazabilidad:** El incidente fue detectado tras los reportes de varios funcionarios que manifestaron anomalías relacionadas con el acceso a sus cuentas institucionales. Como parte del proceso de investigación, se analizaron los registros de autenticación de Microsoft Entra, identificándose múltiples eventos con el código de error **50126 (Error validando credenciales)** distribuidos entre diferentes cuentas del dominio, lo que confirmó que el incidente afectaba a varios usuarios institucionales.

**Contención**
Al confirmar el compromiso, el área de tecnología ejecutó protocolos de respuesta a incidentes en tiempo real:

**Bloqueo de acceso:** Como medida inmediata de respuesta al incidente, se bloqueó la capacidad de inicio de sesión de las cuentas que presentaban actividad anómala comprobada. De manera preventiva, la misma medida fue aplicada a las cuentas pertenecientes a alumnos y egresados, con el fin de reducir la superficie de exposición y evitar nuevos intentos de acceso no autorizado mientras se adelantaban las actividades de análisis, validación y recuperación de las cuentas afectadas.



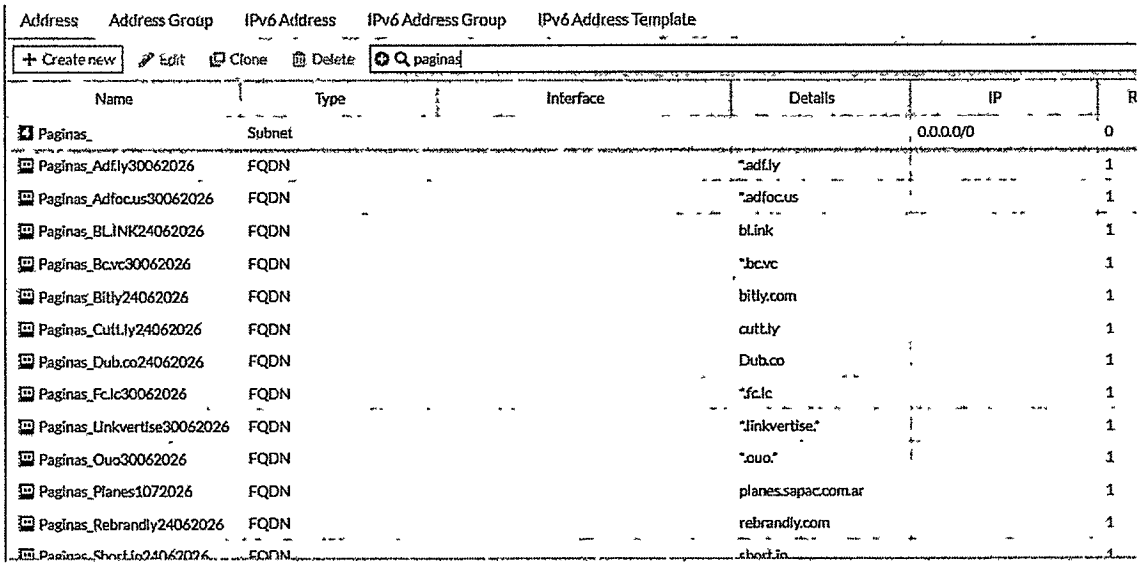
**Revocación de sesiones:** Se ejecutó el cierre forzado de todas las sesiones activas en la nube, invalidando cualquier token de acceso (OAuth) y expulsando inmediatamente a los actores maliciosos de los servicios de Microsoft (Exchange, Teams, etc.).

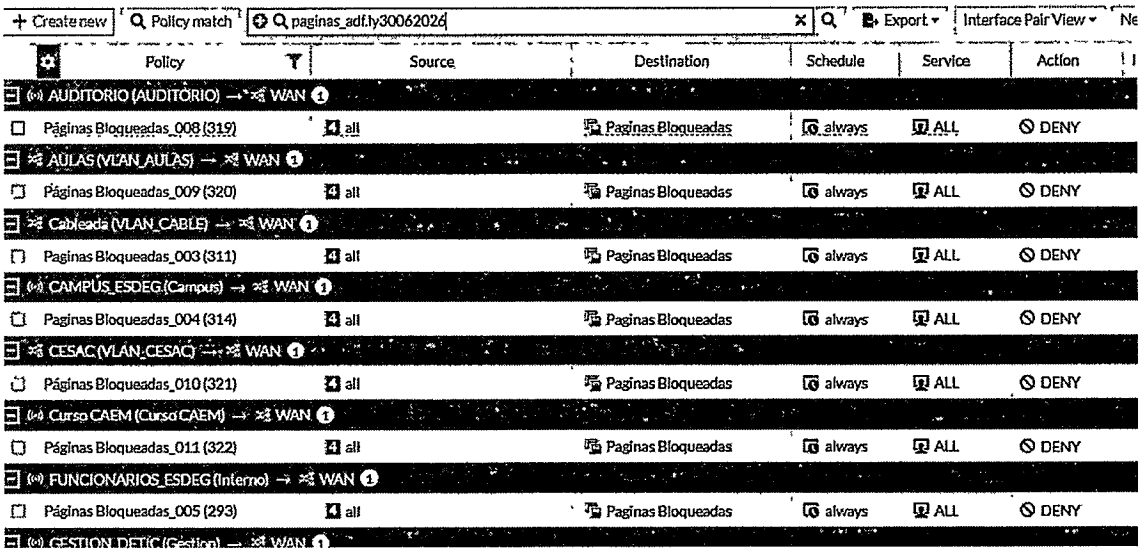
Untitled1.ps1*(Recovered) | Untitled2.ps1*(Recovered) | Untitled3.ps1*(Recovered)

```
4
5   $passwordTemporal = "************************"
6
7  foreach ($usuario in $UsuariosActivar) {
8      Write-Host "Activando: $usuario" -ForegroundColor Yellow
9      try {
10         # Activa la cuenta y asigna contraseña temporal
11         Update-MgUser -UserId $usuario `
12             -AccountEnabled:$true `
13             -PasswordProfile @{
14                 Password = $passwordTemporal
15                 ForceChangePasswordNextSignIn = $true
16                 ForceChangePasswordNextSignInWithMfa = $false
17             }
```

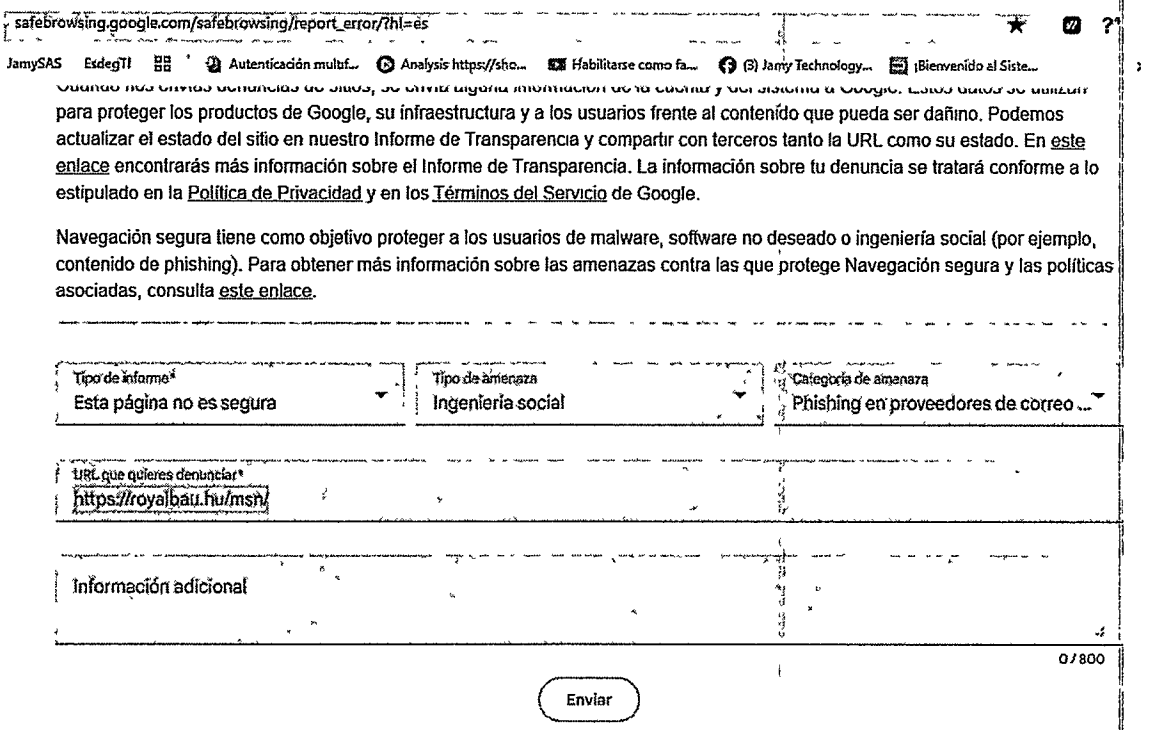
**Remediación y Erradicación**
Una vez contenido el ataque, se implementaron medidas correctivas a nivel de red y directivas de identidad:

**Bloqueo en el firewall perimetral:** Como medida inmediata de contención, las tres (3) URL identificadas durante la investigación fueron bloqueadas en las políticas del firewall perimetral institucional, impidiendo que los equipos de la **red interna** pudieran acceder a dichos sitios maliciosos. Adicionalmente, como medida preventiva, se incorporó el bloqueo de **veintiún (21)** de los servicios de acortamiento de URL más utilizados en Internet, reduciendo significativamente el riesgo de que enlaces de este tipo sean utilizados nuevamente como vector de ataque contra los usuarios de la institución.



**Reporte a Google Safe Browsing:** Como parte de las acciones de respuesta al incidente, las tres (3) URL maliciosas identificadas fueron reportadas ante el servicio Google Safe Browsing para su análisis y clasificación como sitios de phishing. Esta gestión tiene como finalidad contribuir a su inclusión en las listas de navegación segura de Google, protegiendo no solo a los usuarios institucionales, sino también a la comunidad de Internet que utilice navegadores y aplicaciones que consumen este servicio de reputación.




**Seguimiento y monitoreo de la infraestructura:** Como parte de las actividades posteriores a la contención y erradicación del incidente, se realizó un proceso de seguimiento continuo mediante las plataformas Tenable y Cisco, con el propósito de identificar posibles vulnerabilidades, verificar la ausencia de indicadores de compromiso adicionales y validar el estado de seguridad de la infraestructura tecnológica institucional. Las revisiones efectuadas permitieron confirmar que no se evidenciaron nuevos eventos asociados al incidente ni afectaciones adicionales sobre los activos monitoreados, manteniéndose un control permanente sobre la superficie de exposición y fortaleciendo la capacidad institucional para la detección temprana de amenazas.

**Recuperación Segura de Identidades**

**La rehabilitación de las cuentas afectadas**: se llevó a cabo mediante un proceso de control estricto y personalizado con cada usuario, el cual incluyó:

- **Restablecimiento de credenciales:** Asignación de nuevas contraseñas robustas.
- **Activación de MFA Forzado:** Configuración e imposición obligatoria del Doble Factor de Autenticación para blindar el acceso futuro.
- **Auditoría de buzones:** Revisión técnica de cada cuenta para garantizar que los atacantes no hayan creado reglas de reenvío automático de correos (Forwarding rules) hacia direcciones externas.
- **Validación de seguridad:** Confirmación y actualización de los datos de contacto y recuperación directamente con el usuario legítimo de la cuenta.

**Concientización y fortalecimiento del factor humano**

Como parte de las actividades posteriores al incidente, el Departamento de Tecnologías de la Información y las Comunicaciones (DETIC) realizó jornadas de sensibilización dirigidas a los funcionarios afectados, explicando detalladamente el funcionamiento de la campaña de phishing, el mecanismo utilizado por los atacantes para obtener las credenciales y la forma en que lograban eludir el proceso de autenticación multifactor mediante ingeniería social. Durante estas jornadas se reiteraron las recomendaciones institucionales para la identificación de correos fraudulentos y la protección de las credenciales de acceso.

**Campañas permanentes de sensibilización**

Es importante resaltar que, previo al presente incidente, la institución ya venía desarrollando campañas periódicas de concientización en ciberseguridad, incluyendo ejercicios controlados de simulación de phishing y actividades de sensibilización dirigidas al personal institucional. No obstante, este incidente evidencia que, pese a la implementación de controles técnicos y campañas de capacitación, el factor humano continúa representando uno de los principales vectores de riesgo en materia de seguridad de la información, razón por la cual estas actividades deberán mantenerse de manera permanente.

**Conclusión**

El incidente fue contenido y erradicado sin evidenciar afectaciones a la infraestructura tecnológica institucional ni pérdida de la disponibilidad de los servicios de Microsoft 365. La investigación determinó que el mecanismo de compromiso correspondió a una campaña de ingeniería social (phishing) orientada a obtener voluntariamente las credenciales de los usuarios y los códigos de autenticación multifactor, permitiendo a los atacantes autenticarse en tiempo real.

Las actividades de respuesta ejecutadas por el Departamento de Tecnologías de la Información y las Comunicaciones permitieron contener oportunamente el incidente, recuperar la totalidad de las cuentas comprometidas, fortalecer sus mecanismos de autenticación mediante MFA obligatorio y eliminar cualquier persistencia identificada en los buzones institucionales.

Es importante precisar que el mecanismo de autenticación multifactor (MFA) no presentó vulnerabilidades técnicas ni fue comprometido. El atacante logró superar este control exclusivamente porque el usuario, mediante engaño, suministró voluntariamente el código de verificación recibido en su dispositivo. En consecuencia, el incidente no obedeció a una falla de la plataforma tecnológica, sino al uso de técnicas avanzadas de ingeniería social dirigidas a manipular al usuario legítimo.

Finalmente, el incidente reafirma que el principal riesgo para este tipo de amenazas continúa siendo el factor humano. En consecuencia, además de los controles técnicos implementados, resulta indispensable mantener de forma permanente las campañas institucionales de concientización, capacitación y simulación de ataques de phishing, fortaleciendo la capacidad de los usuarios para identificar intentos de fraude y reducir la probabilidad de éxito de futuras campañas de ingeniería social.

Atentamente,

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

Bogotá D.C. julio de 2026

Señor Teniente
**Enrique Ramírez Flor**
Supervisor del Contrato

**ASUNTO: Infraestructura y Seguridad Informática del mes de Julio**

Por medio del presente, me permito presentar el informe correspondiente al mes de julio de 2026, en el cual se relacionan las actividades desarrolladas desde el Departamento de Tecnologías de la Información y las Comunicaciones (DETIC), en cumplimiento de las obligaciones contractuales y de los requerimientos técnicos propios de la operación institucional. Durante este periodo se ejecutaron las actividades programadas dentro del plan de trabajo, así como diversas acciones derivadas de necesidades operativas, solicitudes institucionales y eventos que requirieron atención y acompañamiento técnico especializado.

En desarrollo de las funciones asignadas, se realizaron actividades orientadas a la administración y fortalecimiento de la infraestructura tecnológica, monitoreo de plataformas y servicios institucionales, gestión de seguridad informática, respaldo y disponibilidad de la información, soporte a usuarios, administración de redes y equipos de seguridad perimetral, así como acompañamiento técnico en procesos administrativos, contractuales y de planeación tecnológica. Igualmente, se participó en reuniones de coordinación, mesas de trabajo y actividades de articulación con las diferentes dependencias de la Escuela Superior de Guerra, con el propósito de garantizar la continuidad y mejora de los servicios tecnológicos institucionales.

A continuación, se relacionan de manera detallada las actividades desarrolladas durante el periodo:

1. **Análisis de capacidad y rendimiento de la plataforma de servidores de virtualización.**

   Durante el periodo objeto del presente informe se realizó el análisis del comportamiento operativo de la plataforma institucional de virtualización, verificando el estado de los servidores físicos que soportan la infraestructura, la distribución de las máquinas virtuales, el consumo de recursos de procesamiento (CPU), memoria RAM, almacenamiento y utilización de la red.

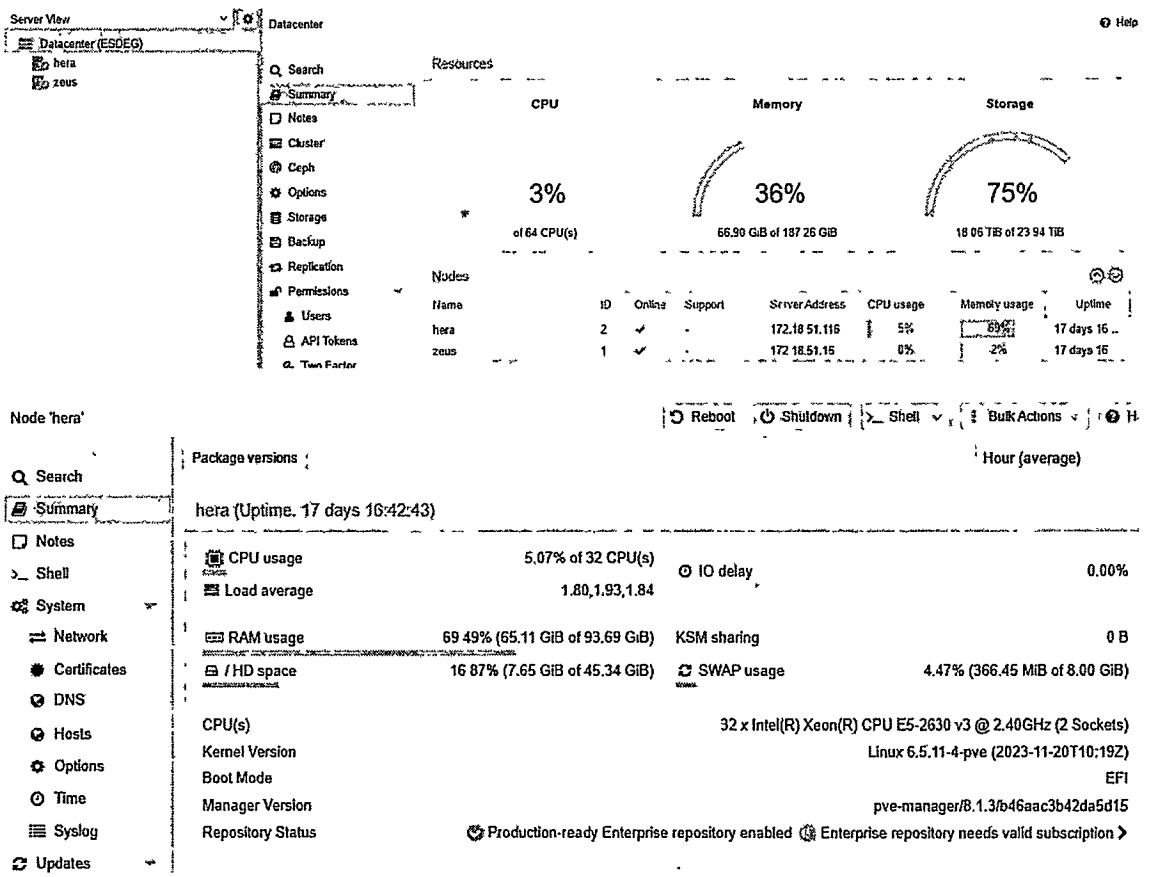
   Como parte de las actividades ejecutadas, se revisó la disponibilidad de los servicios alojados en la plataforma, identificando el comportamiento de la carga de trabajo sobre los nodos de



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

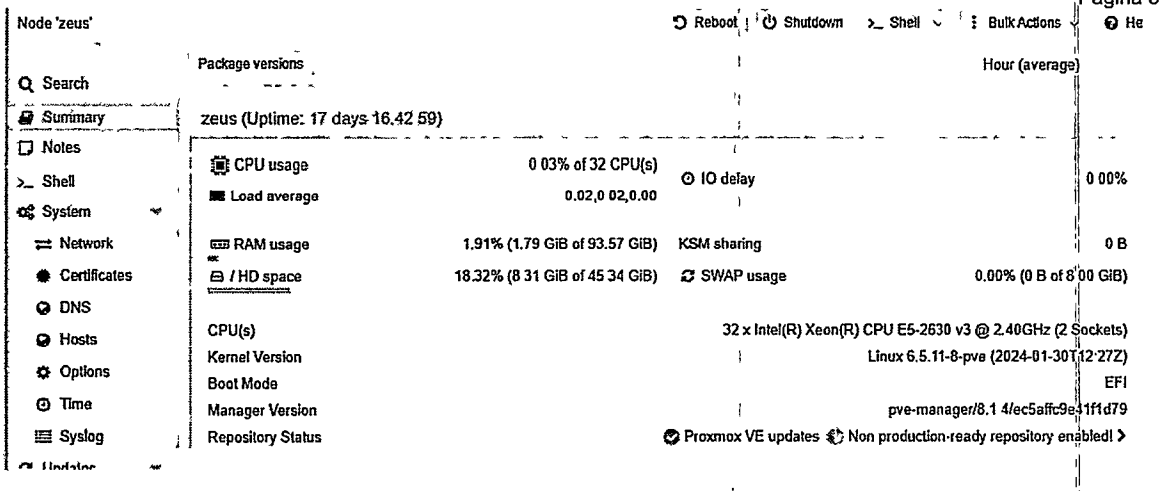
virtualización y evaluando la capacidad instalada frente al crecimiento de las necesidades institucionales. De igual manera, se verificó el desempeño de las máquinas virtuales críticas, validando la correcta asignación de recursos y la estabilidad de los servicios prestados.

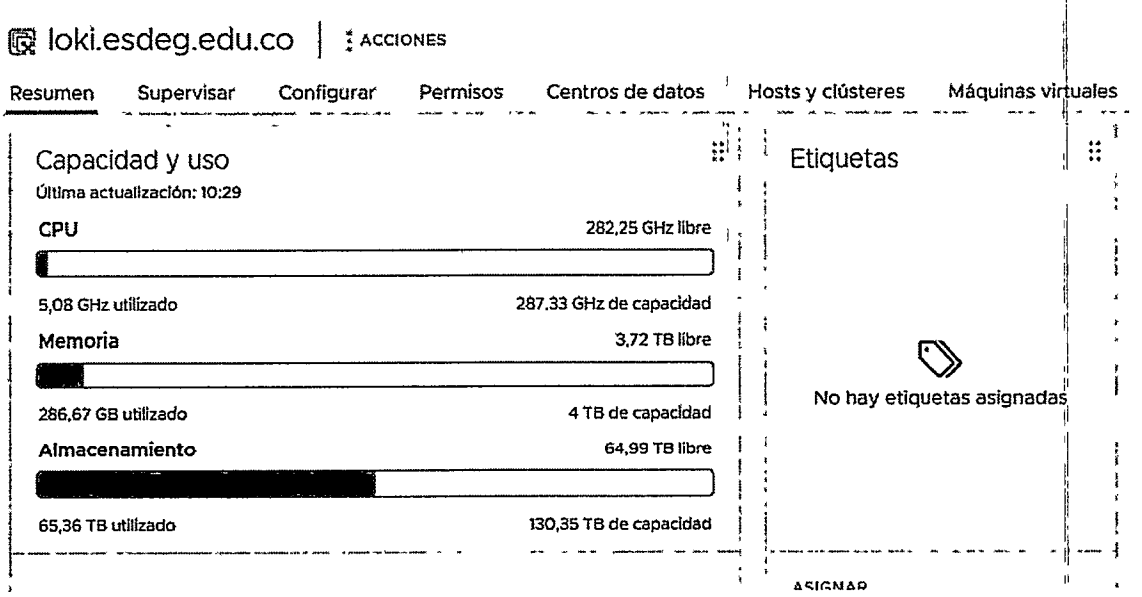
Como resultado del análisis efectuado, se evidenció que la plataforma de virtualización cuenta con capacidad suficiente para soportar la carga operativa actual, manteniendo niveles adecuados de utilización de los recursos de procesamiento, memoria y almacenamiento. Durante el periodo evaluado no se identificaron limitaciones de capacidad que comprometieran la disponibilidad o el rendimiento de los servicios institucionales, por lo que la infraestructura continúa operando dentro de parámetros estables y con disponibilidad de recursos para atender nuevos requerimientos tecnológicos, se propone para evitar inconvenientes eliminar las maquinas virtuales antiguas que se no se le están dando uso en la plataforma de Proxmox PVE.

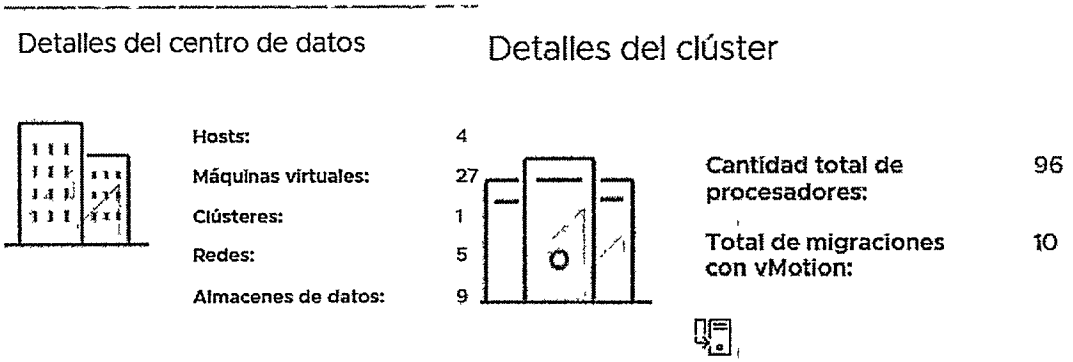





"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."



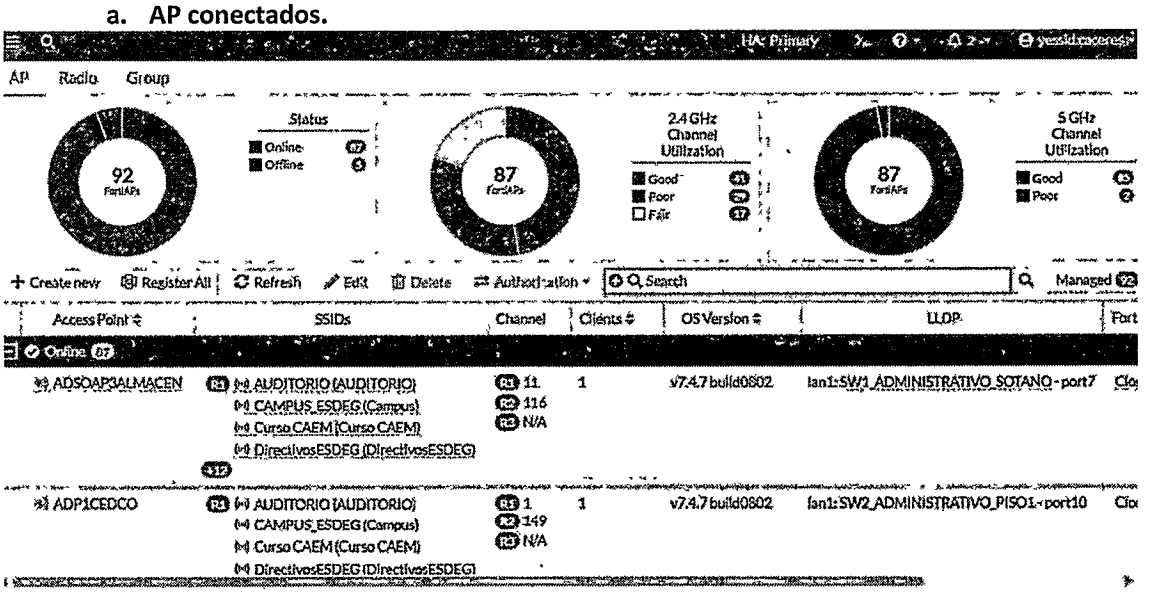



"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

## 2. Estudio de cobertura y calidad del servicio WIFI

Como parte de las actividades desarrolladas, se efectuó el estudio de cobertura y calidad del servicio de red inalámbrica (WiFi) en las áreas de la ESDEG que requirieron validación, verificando el estado operativo de los puntos de acceso FortiAP, la disponibilidad del servicio, la intensidad de la señal, la distribución de clientes y el desempeño general de la infraestructura inalámbrica. Como resultado de las verificaciones efectuadas, se evidenció un funcionamiento estable de la red WiFi, garantizando niveles adecuados de cobertura y disponibilidad para los usuarios institucionales. Así mismo, se realizó seguimiento permanente a las condiciones de operación de los puntos de acceso inalámbricos y, cuando fue requerido, se efectuaron ajustes de configuración orientados a optimizar el desempeño y la calidad del servicio. Como parte de estas actividades, se atendió un incidente presentado en el segundo piso del edificio administrativo, donde un punto de acceso (FortiAP) dejó de operar correctamente debido a la pérdida de comunicación con el FortiSwitch. Se efectuó el proceso de diagnóstico para identificar el equipo afectado, se realizaron las acciones correctivas correspondientes y se restableció la conectividad inalámbrica en el área afectada, garantizando nuevamente la disponibilidad del servicio para los usuarios, se pidió por parte del personal de técnicos la garantía del ap y revisión del switch.

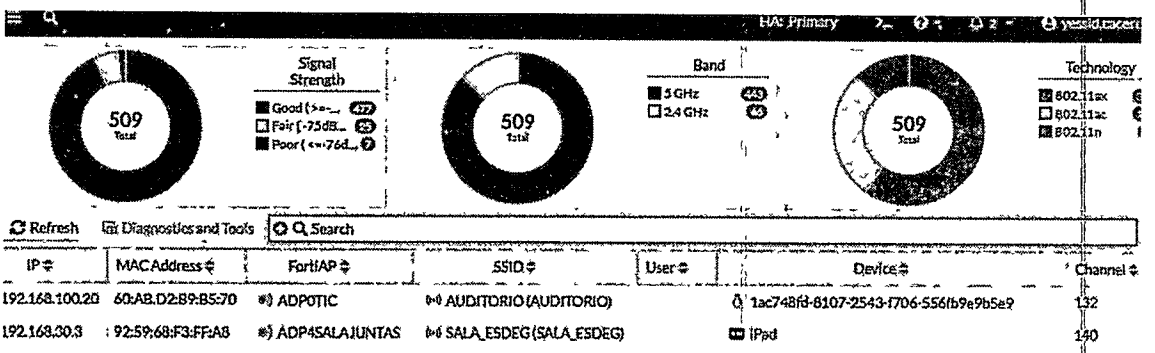
### a. AP conectados.





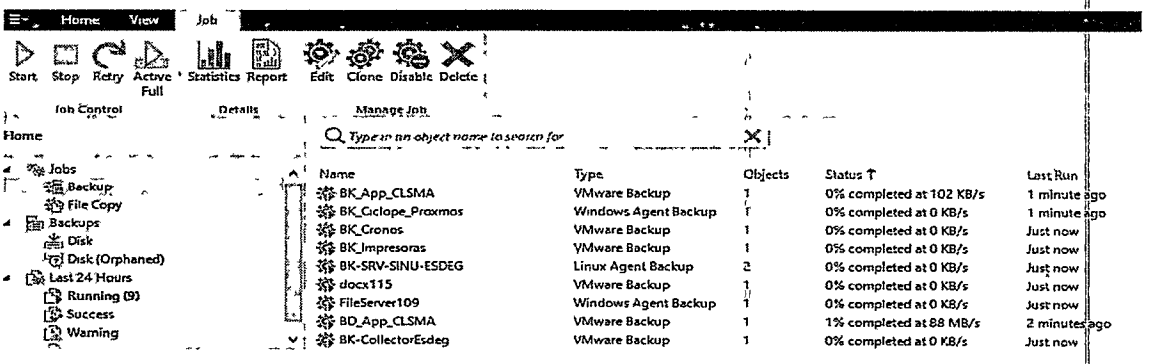

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

**b. Cantidad de clientes en los AP.**



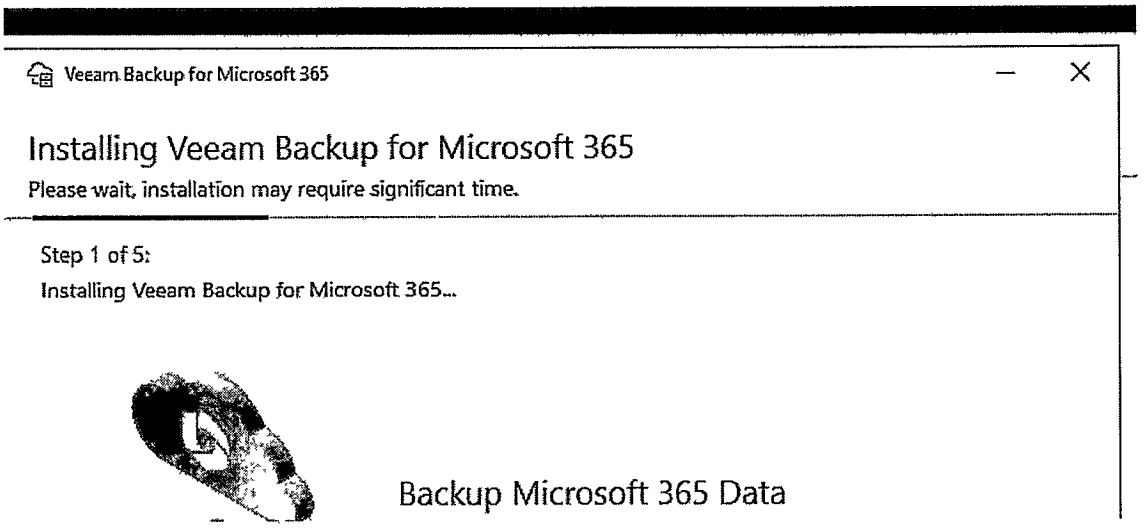

## 3. Verificación y control de copias de seguridad

Con el propósito de garantizar la disponibilidad y recuperación de la información institucional, se verificó periódicamente la correcta ejecución de las copias de seguridad de los servidores mediante la plataforma Veeam Backup & Replication. Durante las validaciones realizadas se revisó el estado de los trabajos programados, el resultado de las tareas de respaldo, la disponibilidad de los puntos de restauración y la integridad de las copias generadas, evidenciando el correcto funcionamiento del esquema de respaldo institucional. Así mismo, se identificó y corrigió una novedad de conectividad que impedía la ejecución normal de algunos procesos de respaldo, restableciendo satisfactoriamente la operación de la plataforma. Posteriormente, se realizó la actualización de **Veeam Backup for Microsoft 365** a la versión **8.4.0.1457**, incorporando las mejoras y correcciones publicadas por el fabricante. Durante la revisión también se evidenció que el consumo de licencias de **Veeam Backup for Microsoft 365** supera la capacidad licenciada en 80 usuarios, situación que fue informada para gestionar la ampliación del licenciamiento y garantizar la continuidad del servicio conforme a las condiciones establecidas por el fabricante.



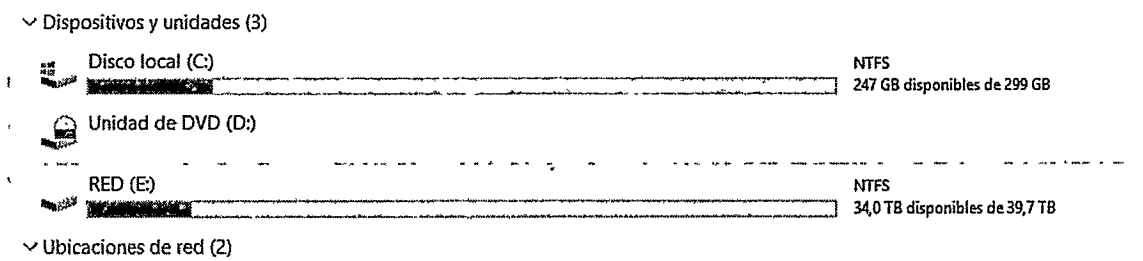



"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."



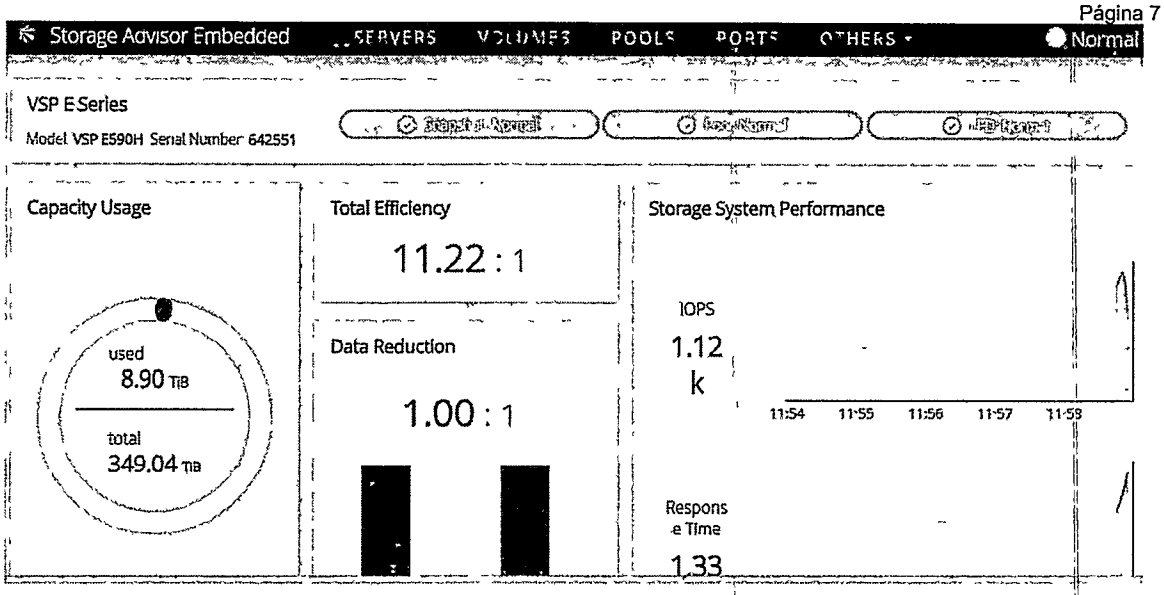

## 4. Administración del almacenamiento

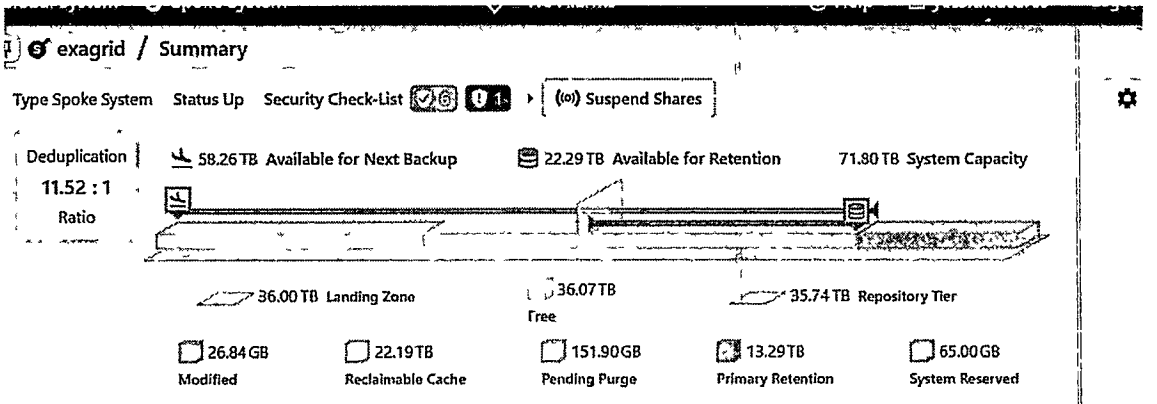
Con el fin de garantizar la disponibilidad de espacio para la ejecución de las copias de seguridad institucionales, se realizó el monitoreo periódico de la capacidad de almacenamiento utilizada por los repositorios de respaldo, verificando el crecimiento de la información almacenada, la disponibilidad de espacio y el comportamiento de la ocupación de los dispositivos destinados a la protección de datos. Como resultado de las verificaciones efectuadas, se evidenció que la infraestructura de almacenamiento dispone de capacidad suficiente para soportar el esquema actual de respaldos, sin presentarse condiciones que requirieran la reorganización o eliminación de copias de seguridad existentes. Así mismo, se mantuvo el seguimiento a las políticas de retención y crecimiento del almacenamiento, con el propósito de anticipar oportunamente posibles necesidades de expansión y garantizar la continuidad de la estrategia institucional de respaldo y recuperación de la información






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



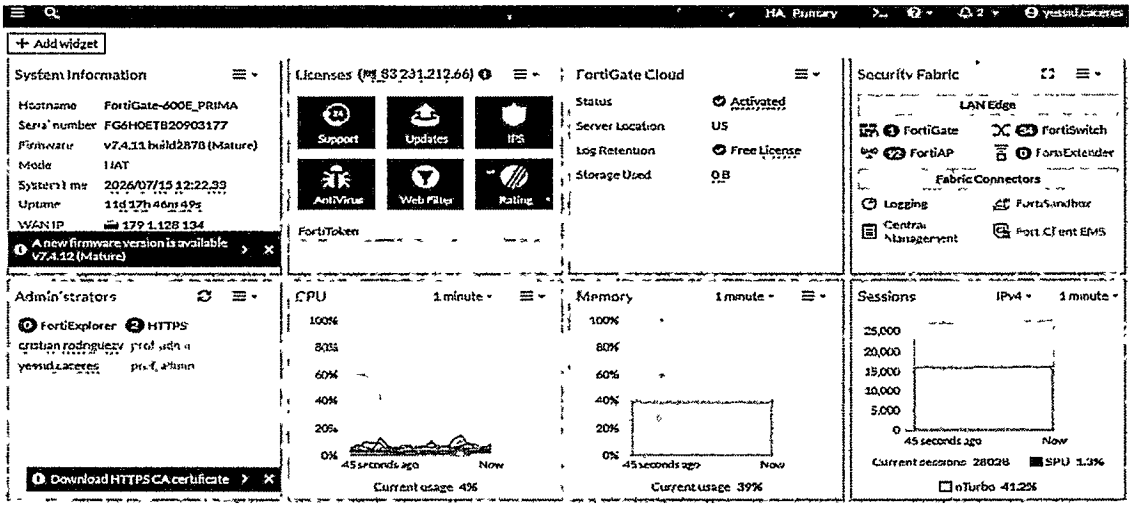

## 5. Monitoreo y administración de la plataforma de seguridad perimetral

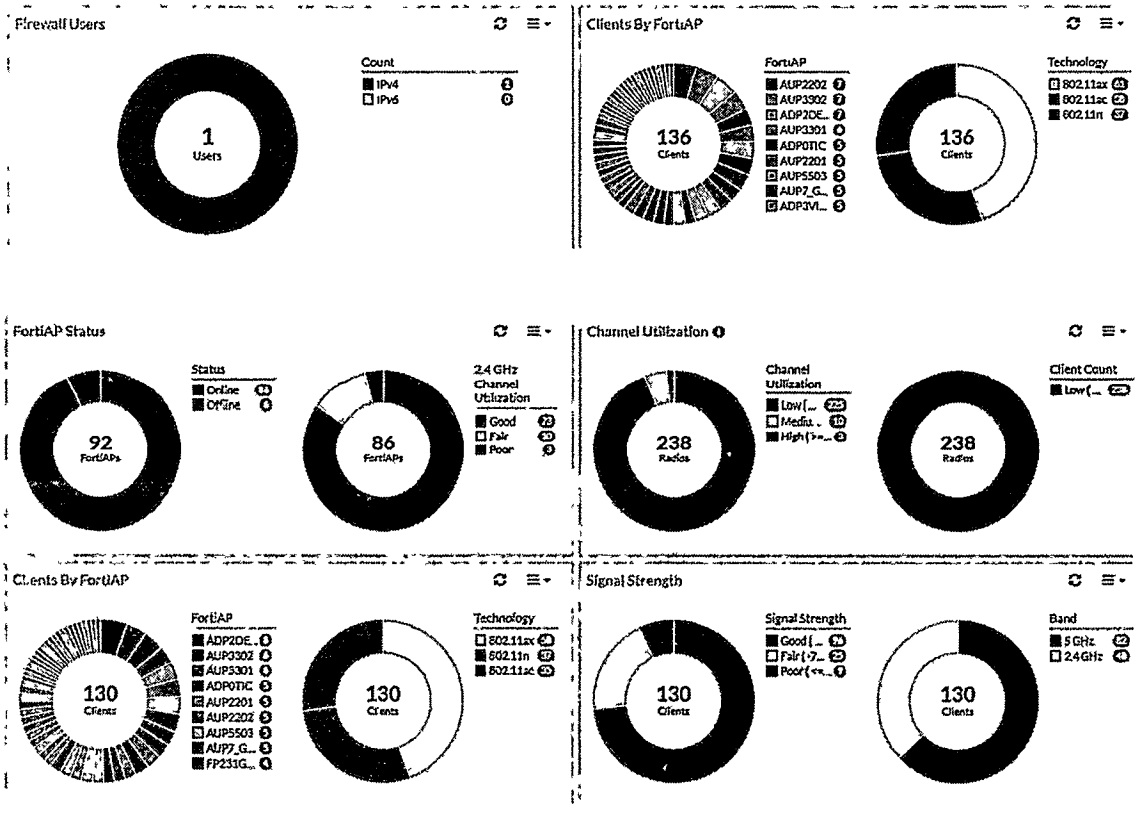
Con el propósito de garantizar la disponibilidad, seguridad y continuidad de los servicios tecnológicos institucionales, se realizó el monitoreo permanente de la plataforma de seguridad perimetral conformada por los equipos FortiGate, FortiSwitch, FortiAP, FortiAnalyzer, FortiAuthenticator, FortiManager y la plataforma Veeam Backup, verificando el estado operativo de los dispositivos, la generación de eventos, la disponibilidad de los servicios, el comportamiento de la infraestructura y el funcionamiento de las políticas de seguridad implementadas. Como parte de las actividades desarrolladas, se efectuaron revisiones de configuración, análisis de eventos de seguridad, validación de la conectividad entre los



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

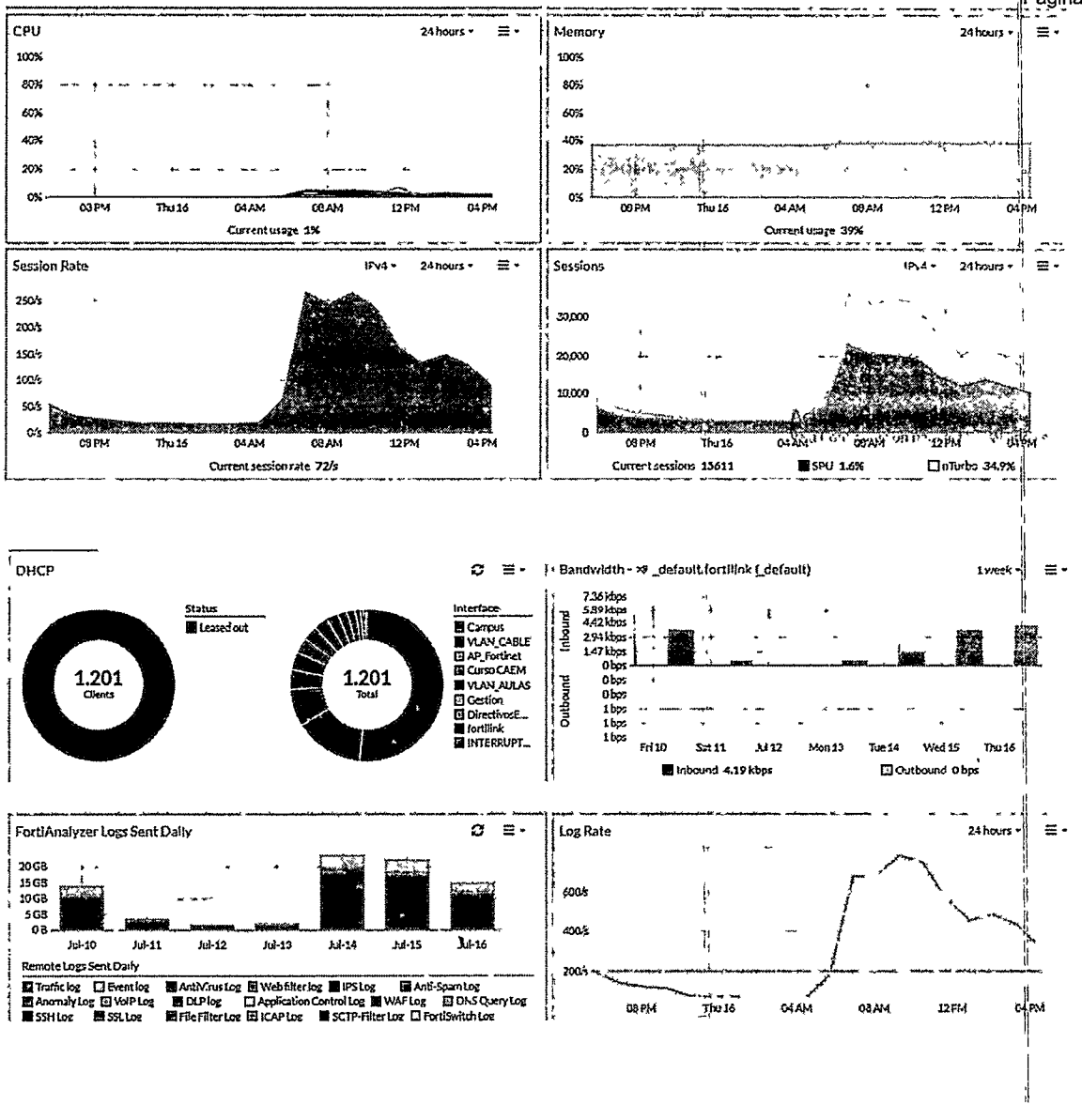
diferentes componentes de la infraestructura y atención de las novedades presentadas durante el periodo, implementando las acciones correctivas y ajustes técnicos requeridos para garantizar la estabilidad de la plataforma y la continuidad de los servicios institucionales.






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




## 6. Inicio Proceso de remediación informe

Se dio inicio al proceso de remediación de los hallazgos identificados en el informe de análisis de vulnerabilidades emitido por el CCOCI. Durante el periodo se efectuó el análisis técnico de las vulnerabilidades reportadas, la clasificación de los hallazgos de acuerdo con su aplicabilidad y criticidad, así como la implementación de las primeras acciones de remediación sobre los activos evaluados. Entre las actividades desarrolladas se encuentran la actualización de componentes de software, el fortalecimiento de configuraciones de seguridad en sistemas operativos Windows Server, la implementación de políticas de endurecimiento (hardening), la validación de servicios



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

de administración remota, el análisis de hallazgos no aplicables conforme a la arquitectura tecnológica institucional y la elaboración del informe técnico de avance con las respectivas evidencias de las acciones ejecutadas, el cual fue remitido a la supervisión para el seguimiento del plan de remediación institucional.

Cordialmente,

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



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

Bogotá D.C. FECHA: julio 17 de 2026

RADICADO No.0126107703 / MDN-COGFM-JEMCO-ESDEG-SBESG-VIADM-DETIC

Señora Mayor
**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. ***Ciclope– Windows Server 2019***

| IP | Vulnerabilidades |
|---|---|
| 172.18.51.6 | Este dispositivo se encuentra en el sitio ESDEG_51 y tiene una importancia muy alta.<br>Se descubrieron 108 vulnerabilidades críticas.<br>Se descubrieron 58 vulnerabilidades graves.<br>Se descubrieron 6 vulnerabilidades moderadas.<br>Se descubrieron 20 servicios <desconocidos>.<br>Se descubrieron 11 servicios DCE RPC.<br>Se detectaron 3 servicios HTTP.<br>Se detectaron 2 servicios LDAP.<br>Se descubrió un servicio LDAPS.<br>Se descubrió un servicio CIFS.<br>Se detectó un servicio de resolución de puntos finales de DCE.<br>Se detectó un servicio RDP.<br>Se ha detectado un servicio Kerberos.<br>Se descubrió un servicio DNS. |



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

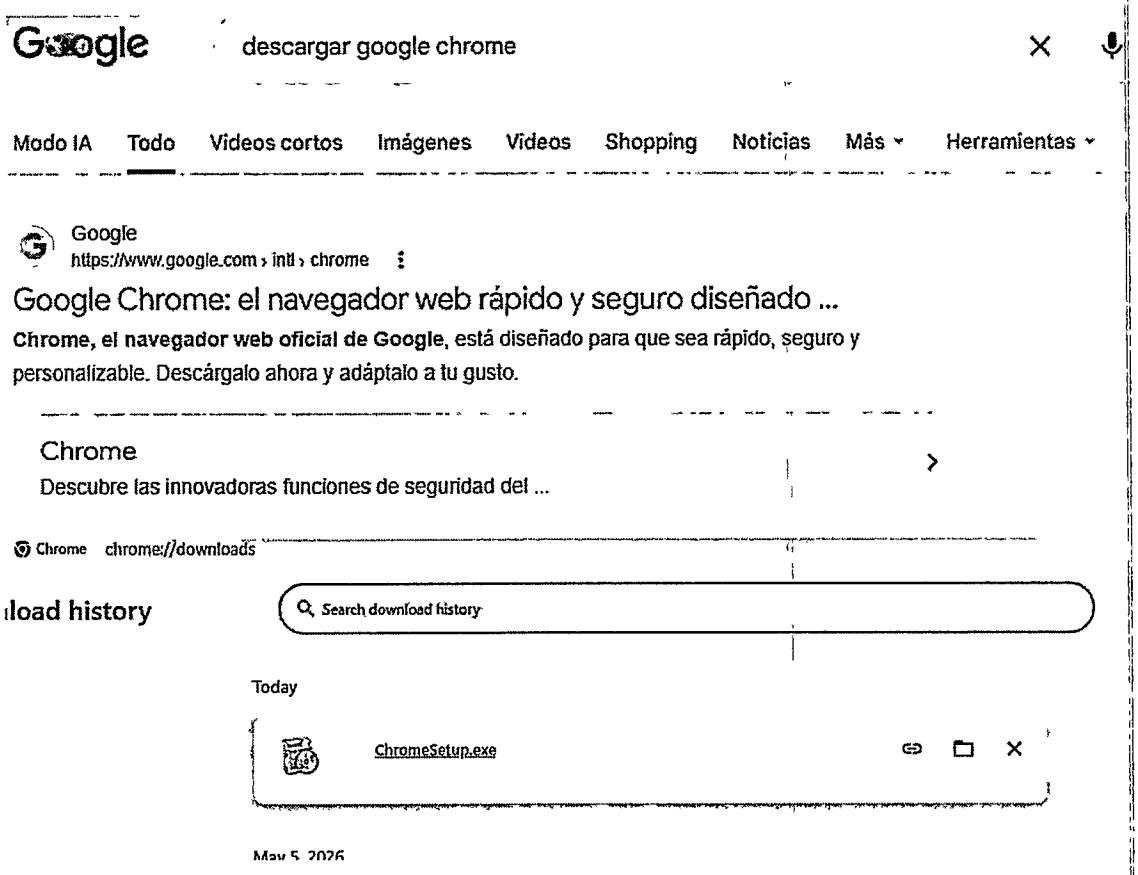
**Remediación:** La remediación de las vulnerabilidades identificadas en el presente host se realizó de manera satisfactoria mediante la actualización de Google Chrome a la versión más reciente disponible, conforme a las recomendaciones del fabricante. Con esta acción se corrigieron las vulnerabilidades asociadas a versiones desactualizadas del navegador, reduciendo la superficie de ataque del sistema y fortaleciendo su nivel de seguridad. De igual manera, se implementó la configuración de seguridad recomendada por Microsoft para mitigar la vulnerabilidad **CVE-2013-3900**, habilitando el mecanismo **EnableCertPaddingCheck** en el Registro del sistema. Esta medida refuerza la validación de certificados y firmas digitales **Authenticode**, evitando que archivos con firmas manipuladas puedan ser considerados válidos por el sistema operativo y reduciendo el riesgo de ejecución de código malicioso. **Adicionalmente, se ajustó la política de bloqueo de cuentas mediante la Directiva de Grupo del dominio, estableciendo un umbral máximo de tres (3) intentos fallidos de autenticación antes del bloqueo de la cuenta y una duración del bloqueo conforme a las recomendaciones de seguridad. Con esta configuración se mitiga el riesgo de ataques de fuerza bruta contra credenciales de acceso a través de servicios CIFS/SMB, fortaleciendo los mecanismos de autenticación y reduciendo la probabilidad de comprometer cuentas mediante intentos reiterados de inicio de sesión.** Asimismo, los hallazgos **"File system enumeration timed out"** y **"Configure your scanning credentials with required WinRM permissions"** fueron analizados y se determinó que corresponden a diagnósticos del proceso de escaneo generado por Rapid7, los cuales no representan vulnerabilidades del sistema operativo ni debilidades de seguridad del activo evaluado. En el primer caso, la condición obedece a un tiempo de espera excedido durante la enumeración del sistema de archivos por parte del motor de escaneo, por lo que su mitigación debe realizarse mediante el ajuste del parámetro de tiempo de espera en el **Scan Engine** de Rapid7 y la posterior ejecución de un nuevo análisis. En el segundo caso, el hallazgo se origina porque el motor de escaneo no pudo autenticarse correctamente mediante el servicio **WinRM**, debido a la configuración de las credenciales utilizadas, los permisos asignados a la cuenta de escaneo o la configuración del propio servicio. Su atención consiste en validar las credenciales configuradas en el **Scan Engine**, verificar que la cuenta utilizada disponga de privilegios administrativos o pertenezca a los grupos requeridos y confirmar que el servicio **WinRM** cuente con un *listener* habilitado para permitir la comunicación con el motor de escaneo. Asimismo, los hallazgos correspondientes a los boletines MS12-017, MS11-070, MS09-008 y MS09-039, a las actualizaciones KB2647170, KB2571621, KB961063, KB969883 y KB4018196, así como a las recomendaciones de configuración dirigidas a versiones anteriores de Microsoft Windows, entre ellas "Disable TCP timestamp responses on Windows versions before Vista", fueron revisados y se determinó que están destinados exclusivamente a sistemas operativos que no hacen parte del entorno evaluado, tales como Windows NT, Windows 2000, Windows XP, Windows Server 2003 y Windows Server 2008. Considerando que el host ejecuta Windows Server 2019 Standard, dichas actualizaciones y configuraciones no resultan aplicables a la versión ni a la arquitectura del sistema operativo instalado, por lo que no es posible ni necesario implementar las acciones referenciadas. temas operativos **Microsoft Windows 2000**, **Windows Server 2003** y **Windows Server 2008**, los cuales no hacen parte del entorno evaluado. Considerando que el host ejecuta **Windows Server 2019 Standard**, dichas actualizaciones no resultan aplicables a la versión ni a la arquitectura del sistema



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

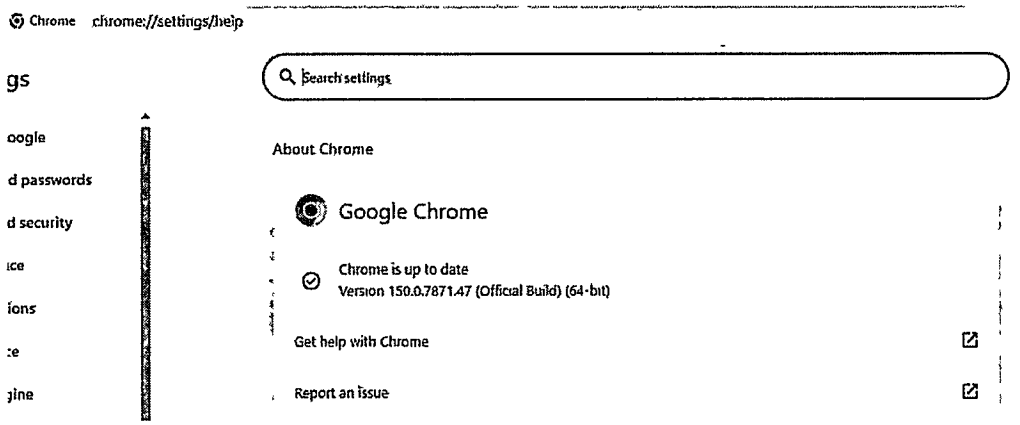
operativo instalado, por lo que no es posible ni necesario implementar los parches referenciados. En consecuencia, estos hallazgos se clasifican como **recomendaciones no aplicables** al activo evaluado, manteniéndose como medida de seguridad la instalación periódica de las actualizaciones acumulativas oficiales publicadas por Microsoft para la versión del sistema operativo en uso. A continuación, se presenta la evidencia del procedimiento ejecutado y las validaciones realizadas, las cuales confirman la correcta implementación de las actualizaciones y configuraciones aplicadas, así como la mitigación de las vulnerabilidades reportadas y la adecuada clasificación de los hallazgos de diagnóstico y de las recomendaciones no aplicables identificadas durante el proceso de escaneo.

### 1.1. Upgrade to the latest version of Google Chrome

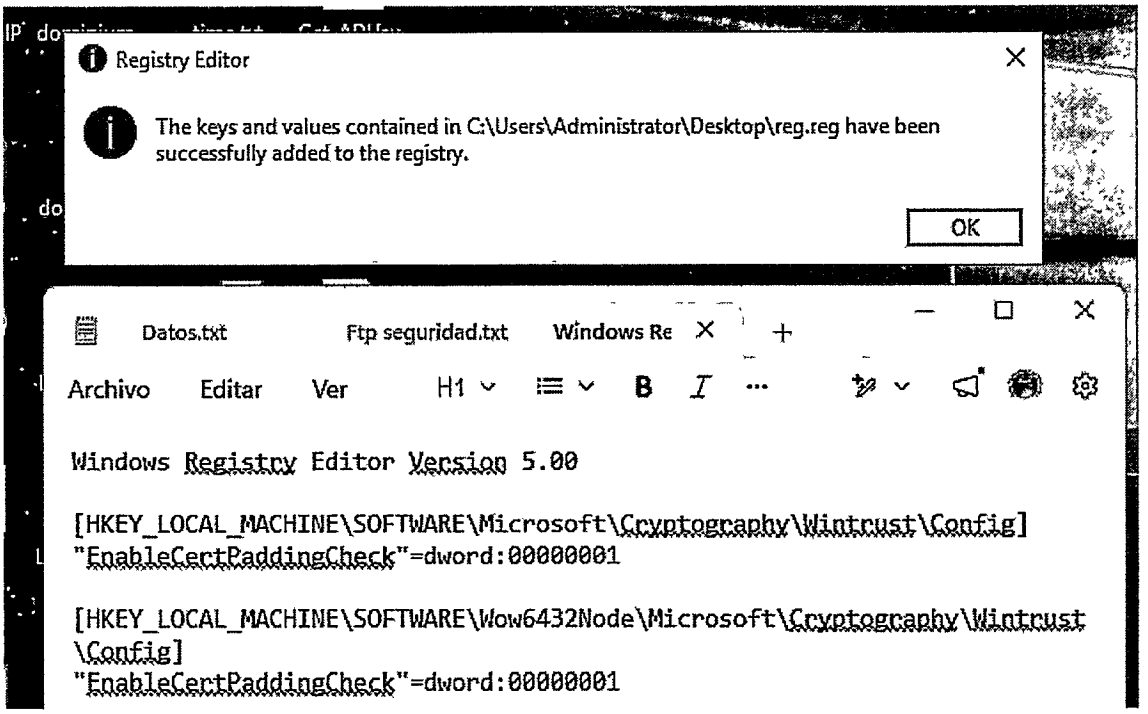





"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."




## 1.1. Enable Certificate Padding Check for Windows Systems






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

## 1.2. File system enumeration timed out

***3.1.1.3*** **File system enumeration timed out**

Estimated time: 10 minutes

The following information is for Scan Diagnostic purposes only, and is not indicative of a detected vulnerability.

In order to workaround file system enumeration timeouts, you may attempt to configure the file system enumeration timeout for Windows assets. This can be done using a custom property.

To set the 'com.rapid7.net.wmi.search.timeout' property on a local or distributed Scan Engine:

1. Access the host machine of the Scan Engine using your preferred method.
    1. If you want to set the property on the local Scan Engine, access the Security Console host itself.
2. Locate the 'CustomEnvironment.properties' file:
    1. On distributed scan engines the default location for this file is:
        1. Linux - '/opt/rapid7/nexpose/nse'
        2. Windows - 'C:\Program Files\Rapid7\NeXpose\nse'
    2. If using a local scan engine the default location for this file is:
        1. Linux - '/opt/rapid7/nexpose/nsc'
        2. Windows - 'C:\Program Files\Rapid7\NeXpose\nsc'
3. If the 'CustomEnvironment.properties' file does not exist, create it with a text editor.
4. Append the 'com.rapid7.net.wmi.search.timeout' property to the 'CustomEnvironment.properties' file as a new line according to this example:

```
com.rapid7.net.wmi.search.timeout=1800000
```

    1. NOTE: The units for the timeout value are in milliseconds
5. Save and close the 'CustomEnvironment.properties' file when finished.

## 1.3. Configure your scanning credentials with required WinRM permissions

***3.1.1.4*** **Configure your scanning credentials with required WinRM permissions**

Estimated time: 20 minutes

The following information is for Scan Diagnostic purposes only, and is not indicative of a detected vulnerability.

Ensure that the credentials provided are valid and correct.

If the credential provided is a local administrative account the "Apply UAC restrictions to local accounts on network logons" configuration must be disabled.

To better protect those users who are members of the local Administrators group, Microsoft implemented UAC restrictions on the network. This mechanism helps prevent against "loopback" attacks. This mechanism also helps prevent local malicious software from running remotely with administrative rights.

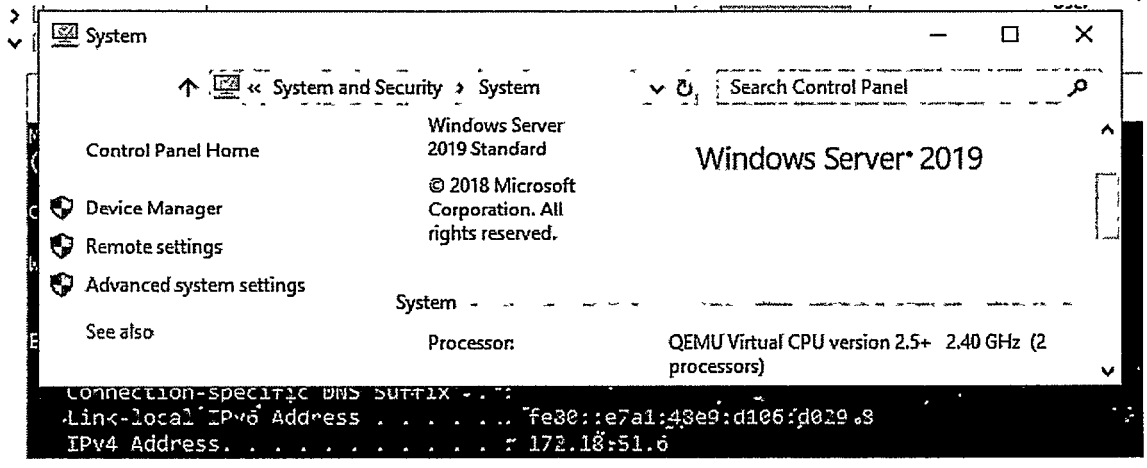
When a user who is a member of the local administrators group on the target remote computer establishes a remote administrative connection they will not connect as a full administrator. The user has no elevation potential on the remote computer, and the user cannot perform administrative tasks. If the user wants to administer the workstation with a Security Account Manager (SAM) account, the user must interactively log on to the computer that is to be administered.

These restrictions prevent InsightVM from making use of the Administrative access of local administrative account credentials, and therefore must be disabled.

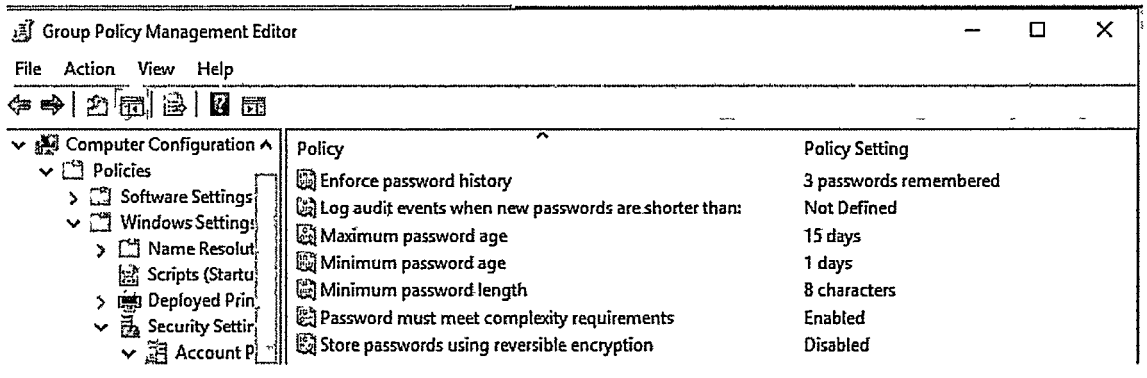
## 1.4. MS12-017: Security Update for Windows Server 2003 for Itanium-based Systems (KB2647170) - MS09-008: Security Update for Windows 2000 (KB961063) – MS 12-017: Security Update for Windows Server 2003 x64 Edition (KB2647170) - MS12-017: Security Update for Windows Server 2003 (KB2647170) - MS11-070: Security Update for Windows Server 2003 x64 Edition (KB2571621) – MS09-039: Security Update for Windows 2000 (KB969883) - MS11-070: Security Update for Windows Server 2003 for Itanium-based Systems (KB2571621) - Security Update for Windows Server 2008 for x64-based Systems (KB4018196) - MS11-070: Security Update for Windows Server 2003 (KB2571621) - Security Update for Windows Server 2008 (KB4018196)

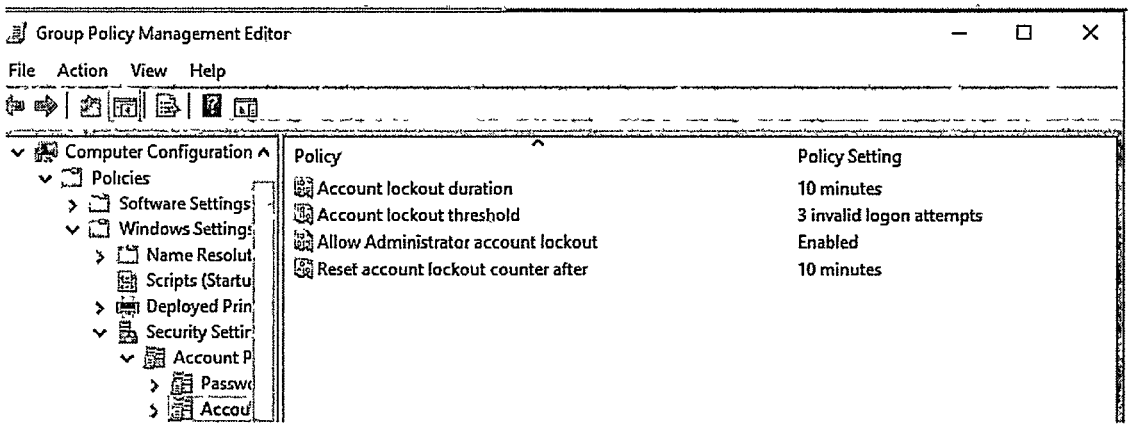


"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."




## 1.5. Set an account lockout threshold for Microsoft Windows






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

## 2. *Ciclope– Windows Server 2019*

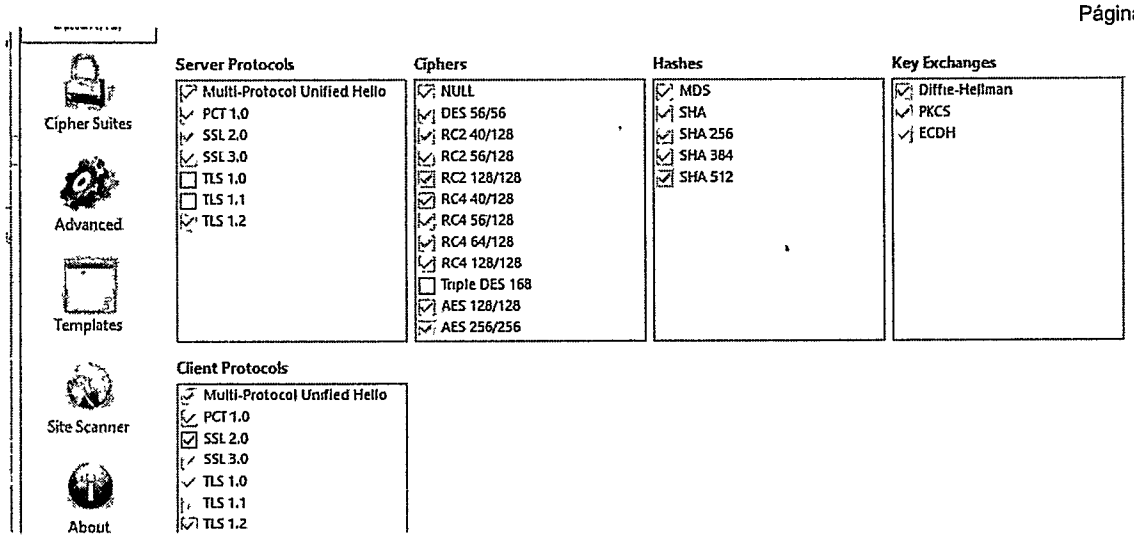
| IP | Vulnerabilidades |
|---|---|
| 172.18.51.6 | Este dispositivo se encuentra en el sitio ESDEG_51 y tiene una importancia muy alta.<br>Se descubrieron 108 vulnerabilidades críticas.<br>Se descubrieron 58 vulnerabilidades graves.<br>Se descubrieron 6 vulnerabilidades moderadas.<br>Se descubrieron 20 servicios <desconocidos>.<br>Se descubrieron 11 servicios DCE RPC.<br>Se detectaron 3 servicios HTTP.<br>Se detectaron 2 servicios LDAP.<br>Se descubrió un servicio LDAPS.<br>Se descubrió un servicio CIFS.<br>Se detectó un servicio de resolución de puntos finales de DCE.<br>Se detectó un servicio RDP.<br>Se ha detectado un servicio Kerberos.<br>Se descubrió un servicio DNS. |

**2.1. Remediación:** El hallazgo "Disable TCP timestamp responses on Windows versions before Vista" fue analizado conforme a las recomendaciones del fabricante y se determinó que la configuración propuesta aplica exclusivamente a versiones anteriores de Microsoft Windows, tales como Windows NT, Windows 2000, Windows XP y Windows Server 2003, las cuales no hacen parte del entorno evaluado. Considerando que el host ejecuta Windows Server 2019 Standard, la configuración del parámetro Tcp1323Opts no resulta aplicable al sistema operativo instalado, por lo que no es posible ni necesario implementar la acción recomendada. En consecuencia, el hallazgo se clasifica como una recomendación no aplicable al activo evaluado. A continuación, se presenta la evidencia correspondiente.

Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows 98SE, Microsoft Windows ME, Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows XP Tablet PC Edition, Microsoft Windows CE, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2003 R2, Standard Edition, Microsoft Windows Server 2003 R2, Enterprise Edition, Microsoft Windows Server 2003 R2, Datacenter Edition, Microsoft Windows Server 2003 R2, Web Edition, Microsoft Windows Small Business Server 2003 R2, Microsoft Windows Server 2003 R2, Express Edition, Microsoft Windows Server 2003 R2, Workgroup Edition



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




2.2. **Remediación: Se revisó la configuración de los certificados digitales utilizados por los servicios** publicados en el servidor, verificando la validez del Common Name (CN), la cadena de confianza y la entidad emisora de los certificados instalados. Como medida de remediación se sustituyeron los certificados autofirmados o emitidos por entidades no confiables por certificados emitidos por una Autoridad de Certificación (CA) reconocida, garantizando que el nombre común y, cuando aplica, los Subject Alternative Names (SAN) correspondan con los nombres de los servicios publicados. Con esta acción se fortalece la autenticidad de las comunicaciones cifradas, se elimina la dependencia de certificados no confiables y se reduce el riesgo de advertencias de seguridad o ataques de suplantación de identidad durante el establecimiento de conexiones TLS/SSL. A continuación, se presenta la evidencia correspondiente.

2.3. **Remediación:** Los hallazgos **"Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)"** y **"Self-signed TLS/SSL certificate (ssl-self-signed-certificate)"**, identificados sobre los servicios HTTPS/RDP del host evaluado, fueron analizados y se verificó que corresponden al uso de certificados digitales **autofirmados** implementados para servicios internos de la infraestructura. Se confirmó que dichos certificados proporcionan cifrado de las comunicaciones; sin embargo, al no ser emitidos por una Autoridad Certificadora (CA) de confianza, Rapid7 los clasifica como certificados no confiables y autofirmados. La remediación definitiva consiste en sustituir los certificados actuales por certificados emitidos por una Autoridad Certificadora pública o por la Autoridad Certificadora interna de la organización (AD CS), de acuerdo con la política institucional de gestión de certificados. Mientras dicha sustitución no sea implementada, el hallazgo corresponde a una condición derivada del esquema de certificación adoptado para los servicios internos del servidor.

Cordialmente,

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



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

**CERTIFICACIÓN APLICACIÓN**

**Decreto No. 2231 del 22 de diciembre del 2023**

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

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

| | |
|---|---|
| a. Se restará el 25% de renta exenta asociada a estas rentas en desarrollo de mi actividad **(numeral 10 del artículo 206 del estatuto tributario)** | X |
| b. Se tomarán costos o deducciones asociados a estas rentas en desarrollo de mi actividad. | |

Esta certificación se expide a los 16 días del mes de julio del año 2026

Firma: _____

Nombres y Apellidos: YESSID ARAMIS CÁCERES VASQUEZ

No. de Cédula: 72342326

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

enlace operativo

# SuAporte | AUTOLIQUIDACION CONSOLIDADA

**Fecha creación reporte:** 2026-07-15, 09:09:57 AM **Tipo Planilla:** I: PLANILLA INDEPENDIENTES **Numéro Planilla:** 86344465

**Periodo Cotización:** junio de 2026 **Periodo Servicio:** junio de 2026

**PAGADO 15/07/2026**

## I. DATOS DEL APORTANTE

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

## II. DETALLE DEL APORTANTE

| Datos del Afiliado | | | | Novedades | | | | | | | | | | | | | | | | Pensiones | | | Salud | | | Riesgos | | | Cajas | | | Parafiscales | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Identificación | Apellidos y Nombres | Tipo Cotizante | Subtipo Cotizante | ING | RET | RET P | TDE | TAE | TDP | TAP | VSP | COR | VST | SLN | IGE | LMA | VAC | AVP | VCT | IRP | Días ARP | Días EPS | Días ARP | Días CCF | Administradora | IBC Pensión | Aporte Pensión | Administradora | IBC Salud | Aporte Salud | Tarifa | IBC Riesgos | Aporte Riesgos | Administradora | IBC Caja | Aporte Caja | Aporte SENA | Aporte ICBF | ESAP | Aporte Ministerio | Total |
| CC 72342326 | YESSID ARAMIS CACERES VASQUEZ | 59 | 00 | | | | | | | | | | | | | | | | | 0 | 30 | 30 | 30 | 0 | (231001) COLFONDOS | $ 3.971.600 | $ 635.500 | (EPS005) EPS SANITAS | $ 3.971.600 | $ 496.500 | 0.522 | $ 3.971.600 | $ 20.800 | (NIN-CC) NINGUNA CCF | $ 0 | $ 0 | $ 0 | $ 0 | $ 0 | $ 0 | $ 1.152.800 |

## III.TOTALES

| IBC Pensión | IBC Salud | IBC Riesgos | IBC Cajas | Aportes Pensión | Aportes Salud | Aportes Riesgos | Aportes Cajas | Aportes Sena | Aportes ICBF | Aportes ESAP | Aportes Min Educación | Incapacidades, Licencias, Saldos a Favor) EPS | Incapacidades ARP | SUBTOTAL SIN INTERESES DE MORA | TOTAL INTERESES DE MORA | TOTAL FINAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ 3.971.600 | $ 3.971.600 | $ 3.971.600 | $ 0 | $ 635.500 | $ 496.500 | $ 20.800 | $ 0 | $ 0 | $ 0 | $ 0 | $ 0 | $ 0 | $ 0 | $ 1.152.800 | $ 7.000 | $ 1.159.800 |



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

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

EXPERTOS en PILA

## Transacción Aprobada

Su planilla ha sido enviada y pagada con éxito. Por favor imprima este comprobante como soporte del envío y pago de su planilla.

enlace operativo

| Información de la Planilla Pagada | |
|---|---|
| Nit de comercio Operador de Información | 900089104-5 |
| Razón Social del Operador de Información | Enlace Operativo |
| Descripción | Pago de SuAporte |
| Fecha | 2026-07-15, 09:07:57 AM |
| Periodo de Cotización Otros Riesgos | junio de 2026 |
| Periodo de Cotización Para Salud | junio de 2026 |
| Empresa | CACERES VASQUEZ YESSID ARAMIS |
| CEDULA CIUDADANIA | CC 72342326 |
| Código Sucursal (Nombre) | |
| Referencia de Pago/ Número Planilla | 86344465 |
| Tipo de Planilla | I |
| Número Transacción Bancaria/ CUS | 481143217 |
| Banco | (1051) - BANCO DAVIVIENDA |
| Valor | $ 1.159.800 |
| Estado de la Transacción | Aprobada |
| Dirección IP de Origen | www.suaporte.com.co |

| Nit | Código | Administradora | Número Afiliados | Valor sin Mora | Total Intéreses Mora |
|---|---|---|---|---|---|
| N800227940 | 231001 | FDO DE PENSIONES OBLIGATORIAS COLFONDOS | 1 | $ 635.500 | $ 3.800 |
| N800251440 | EPS005 | SANITAS EPS | 1 | $ 496.500 | $ 3.000 |
| N890903790 | 14-11 | ARL SURA | 1 | $ 20.800 | $ 200 |
| | | | SubTotales: | $ 1.152.800 | $ 7.000 |
| | | | Total a Pagar: | | $ 1.159.800 |



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

Enlace Operativo no se hace responsable de las planillas y pagos realizados a través de otros operadores de información dado que no tiene medios para corroborar

EXPERTOS en PILA

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