

Alerta ID:	114
Fecha del reporte:	24/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Campaña Activa: Ataques A Firewalls Y Vpn (Fortinet / Palo Alto / Cisco)
Herramienta de detección	N/A
Activo involucrado:	Mozilla Firefox y Thunderbird
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una campaña activa de ataques dirigida a dispositivos de seguridad perimetral, incluyendo firewalls y servicios VPN de fabricantes como Fortinet, Palo Alto Networks y Cisco, en la cual actores de amenaza están ejecutando actividades automatizadas de acceso no autorizado mediante el uso de credenciales comprometidas, ataques de fuerza bruta y técnicas de credential stuffing.

El propósito de esta alerta es que las entidades del sector salud validen la exposición y configuración de sus sistemas de acceso remoto y seguridad perimetral, tanto en infraestructura local como en entornos híbridos o administrados por terceros, identificando



posibles servicios VPN expuestos a Internet, credenciales reutilizadas o filtradas y ausencia de mecanismos de autenticación multifactorial.

Esta validación debe incluir la revisión de sus inventarios tecnológicos de seguridad de red, sistemas de acceso remoto, portales administrativos de firewalls, infraestructura de conectividad entre sedes hospitalarias y cualquier componente que funcione como punto de entrada a la red institucional, con el fin de prevenir accesos no autorizados, compromiso de datos sensibles y afectación de la continuidad operativa de los servicios de salud.

Descripción:

Se ha identificado una campaña activa de ataques dirigida a dispositivos de seguridad perimetral, específicamente firewalls y servicios VPN de fabricantes como Fortinet, Palo Alto Networks y Cisco, en la cual actores de amenaza están realizando intentos sistemáticos de acceso no autorizado a interfaces de administración y servicios de acceso remoto expuestos a Internet.

Esta campaña no se encuentra asociada a una vulnerabilidad única de tipo zero-day, sino al abuso combinado de credenciales comprometidas previamente filtradas, junto con técnicas automatizadas de ataque como credential stuffing, password spraying y fuerza bruta distribuida, orientadas a validar accesos válidos en servicios VPN corporativos y portales administrativos de firewalls.



Los atacantes aprovechan la exposición de servicios de acceso remoto en Internet, así como la ausencia o debilidad de controles de autenticación robusta (como MFA), para obtener acceso inicial legítimo a la infraestructura perimetral. Una vez autenticados, pueden interactuar con los dispositivos de seguridad como usuarios válidos, lo que dificulta la detección mediante controles tradicionales basados en firmas o reputación.

El acceso exitoso a estos sistemas permite la modificación de políticas de seguridad, la creación de túneles VPN no autorizados, la manipulación de reglas de filtrado de tráfico y la posible desactivación de controles de inspección, facilitando la exposición de la red interna.

En el contexto del sector salud, esta amenaza es especialmente crítica debido a que los dispositivos comprometidos actúan como punto de entrada a redes clínicas, sistemas de historia clínica electrónica, plataformas de telemedicina y servicios administrativos, lo que podría derivar en accesos no autorizados, interrupción de servicios esenciales o exfiltración de información sensible de pacientes.

Consecuencias de la explotación



La explotación exitosa de esta campaña activa dirigida a dispositivos de seguridad perimetral (firewalls y VPN) puede generar impactos críticos tanto a nivel técnico como operativo en las organizaciones del sector salud, debido al papel central que estos dispositivos cumplen como puerta de entrada a la infraestructura institucional.

1. Acceso no autorizado a la red interna

El compromiso de credenciales VPN o de administración de firewalls permite al atacante establecer accesos válidos hacia la red interna, eludiendo controles perimetrales tradicionales.



Esto puede derivar en el acceso a sistemas clínicos, administrativos y plataformas de gestión hospitalaria.

2. Movimiento lateral dentro de la infraestructura hospitalaria

Una vez dentro de la red, el atacante puede desplazarse lateralmente hacia activos críticos como:

- Historia clínica electrónica (HCE)
- Sistemas de laboratorio clínico
- Plataformas de imágenes diagnósticas (PACS)
- Servidores de aplicaciones hospitalarias
- Sistemas financieros y administrativos

3. Interrupción de la continuidad operativa

El acceso a dispositivos de red permite la modificación de reglas de firewall, políticas de VPN y segmentación de tráfico, lo que puede generar:

- Caída de conectividad entre sedes hospitalarias
- Interrupción de servicios clínicos digitales
- Indisponibilidad de sistemas de atención al paciente

4. Exposición de información sensible

El atacante puede acceder y potencialmente extraer información crítica como:

- Historias clínicas electrónicas
- Datos personales de pacientes



- Credenciales institucionales
- Información administrativa y financiera

5. Incremento del riesgo de ransomware

El compromiso de la infraestructura perimetral puede ser utilizado como punto de entrada para despliegue de ransomware, incluyendo:

- Desactivación de backups
- Cifrado de servidores críticos
- Interrupción de servicios hospitalarios esenciales

6. Compromiso del control de seguridad perimetral

El atacante puede modificar configuraciones del firewall o VPN, tales como:

- Reglas de filtrado de tráfico
- Políticas de acceso remoto
- Túneles VPN no autorizados
- Excepciones de seguridad persistentes

7. Impacto regulatorio y reputacional

El acceso no autorizado a información sensible puede generar:

- Incumplimiento de la Ley 1581 de 2012 (protección de datos personales en Colombia)



- Sanciones regulatorias
- Pérdida de confianza institucional
- Afectación reputacional del prestador de salud

8. Persistencia del atacante

El uso de credenciales válidas permite a los atacantes mantener acceso prolongado en el tiempo sin detección inmediata, incrementando el riesgo de exfiltración continua y escalamiento del ataque

apropiadas

Modo de explotación del ataque

La campaña activa dirigida a dispositivos de seguridad perimetral (firewalls y VPN) sigue una cadena de ataque estructurada, basada principalmente en el abuso de credenciales válidas y el acceso a servicios expuestos a Internet. A continuación, se describe su desarrollo en fases:

Fase 1 – Reconocimiento de superficie de ataque

Los actores de amenaza realizan escaneos masivos en Internet para identificar:

- Firewalls expuestos públicamente
- Portales VPN corporativos accesibles desde Internet
- Interfaces de administración mal configuradas
- Servicios de autenticación sin restricciones geográficas o de IP



Objetivo: mapear organizaciones vulnerables dentro del sector salud y otros sectores críticos

Fase 2 – Recolección y uso de credenciales comprometidas

Se emplean bases de datos filtradas provenientes de brechas previas para:

- Credential stuffing (reutilización masiva de credenciales)
- Password spraying (contraseñas comunes sobre múltiples cuentas)
- Validación de accesos mediante autenticación automatizada

MITRE ATT&CK: T1078 – Valid Accounts / T1110 – Brute Force

Fase 3 – Acceso inicial a servicios VPN o firewall

Cuando las credenciales son válidas, el atacante obtiene acceso legítimo a:

- VPN corporativa
- Consola de administración del firewall
- Portales de gestión remota

Este acceso simula comportamiento autorizado, dificultando la detección por sistemas tradicionales.

Fase 4 – Abuso de acceso privilegiado

Con acceso autenticado, el atacante puede:

- Modificar políticas de firewall
- Alterar reglas de filtrado de tráfico



- Crear o modificar túneles VPN
- Deshabilitar controles de inspección o monitoreo

MITRE ATT&CK: T1562 – Impair Defenses

Fase 5 – Movimiento lateral en la red interna

Una vez comprometido el perímetro, el atacante puede pivotar hacia sistemas internos críticos:

- Historia clínica electrónica (HCE)
- Servidores clínicos y administrativos
- Sistemas de laboratorio e imágenes diagnósticas
- Infraestructura de bases de datos

MITRE ATT&CK: T1021 – Remote Services

Fase 6 – Persistencia y mantenimiento del acceso

El atacante busca mantener acceso a largo plazo mediante:

- Reutilización de credenciales válidas
- Creación de cuentas administrativas ocultas
- Configuración de accesos VPN alternos
- Modificación de reglas de acceso persistente

MITRE ATT&CK: T1078 – Valid Accounts

Fase 7 – Preparación de impacto (post-explotación)

En etapas avanzadas, los atacantes pueden:



- Desactivar backups
- Preparar cifrado de información (ransomware)
- Exfiltrar datos sensibles
- Interrumpir servicios críticos

MITRE ATT&CK: T1486 – Data Encrypted for Impact.

Vulnerabilidades asociadas



La campaña activa contra dispositivos de seguridad perimetral no se basa en una vulnerabilidad única de software, sino en la combinación de técnicas de ataque del framework **MITRE ATT&CK** y debilidades frecuentes de configuración en infraestructuras VPN y firewalls utilizadas en organizaciones del sector salud.

1. Uso de credenciales válidas comprometidas

MITRE ATT&CK: T1078 – Valid Accounts

Descripción

Los atacantes utilizan credenciales previamente filtradas en brechas de seguridad, repositorios de leaks o malware tipo infostealer.

Debilidad asociada

- Reutilización de contraseñas entre sistemas



- Falta de rotación de credenciales
- Ausencia de monitoreo de credenciales filtradas

2. Ataques de fuerza bruta y password spraying

MITRE ATT&CK: T1110 – Brute Force

Descripción

Intentos automatizados de autenticación masiva sobre VPNs y portales firewall.

Debilidad asociada

- Falta de bloqueo por intentos fallidos
- Ausencia de rate limiting
- No implementación de CAPTCHA o mecanismos anti-bot en portales VPN

3. Exposición de servicios VPN y paneles de administración

MITRE ATT&CK: T1133 – External Remote Services

Descripción

Servicios de acceso remoto expuestos directamente a Internet sin restricciones adecuadas.

Debilidad asociada

- Consolas de firewall accesibles públicamente
- VPN sin restricción por IP o geolocalización
- Interfaces administrativas sin segmentación

4. Falta de autenticación multifactor (MFA)



Debilidad crítica de configuración

Descripción

Acceso a VPN o firewalls protegido únicamente con usuario y contraseña.

Impacto

Permite que credenciales filtradas sean suficientes para acceso completo.

5. Segmentación de red deficiente

MITRE ATT&CK: T1021 – Remote Services

Descripción

Red hospitalaria sin separación clara entre:

- red administrativa
- red clínica
- infraestructura de servidores
- zona de gestión de red

Impacto

Facilita movimiento lateral una vez comprometido el perímetro.

6. Falta de monitoreo de autenticación y comportamiento

MITRE ATT&CK: T1040 – Network Sniffing / T1071 – Application Layer Protocol

Descripción



Ausencia de correlación de eventos en SIEM sobre accesos VPN.

Debilidad asociada

- No detección de accesos desde ASN sospechosos
- No correlación de login + cambio de configuración
- Logs no centralizados o no analizados en tiempo real

7. Configuración débil de reglas en firewall**Debilidad operacional crítica****Descripción**

Reglas permisivas que permiten acceso excesivo a servicios internos.

Impacto

- Exposición de servicios clínicos internos
- Acceso indirecto a bases de datos hospitalarias
- Apertura de rutas innecesarias desde VPN

8. Falta de control de sesiones y acceso persistente

MITRE ATT&CK: T1078 – Valid Accounts (Persistence abuse)

Descripción

Sesiones VPN que permanecen activas sin control o sin reautenticación.

Debilidad asociada

- Sesiones largas sin timeout



- Ausencia de revalidación MFA
- Falta de monitoreo de sesiones concurrentes

El riesgo no proviene de una vulnerabilidad de software específica, sino de un **modelo de seguridad débil en la gestión de accesos remotos**, donde la autenticación se convierte en el principal punto de falla del perímetro hospitalario.

Recomendaciones de detección y mitigación

Para reducir el riesgo asociado a la campaña activa de compromiso de dispositivos de seguridad perimetral (firewalls y VPN), se recomienda implementar un enfoque integral basado en detección conductual, correlación avanzada de eventos y endurecimiento de infraestructura crítica.

1. DETECCIÓN EN SOC / SIEM

Detección de intentos de acceso no autorizados

Configurar alertas para identificar:

- Múltiples intentos fallidos de autenticación VPN en corto tiempo
- Incremento súbito de autenticaciones desde una misma IP
- Intentos de acceso desde países o ASN no habituales
- Autenticaciones fuera de horario laboral institucional

1.2 Detección de credential stuffing y password spraying

Implementar correlación para detectar:



- múltiples usuarios autenticados desde una misma IP
- uso de patrones repetitivos de login
- accesos secuenciales a múltiples cuentas
- incremento de fallos seguidos de éxito de autenticación

1.3 Detección de anomalías en sesiones VPN

Alertar sobre:

- sesiones VPN activas simultáneas en múltiples ubicaciones
- cambios de comportamiento inmediatamente después del login
- conexiones VPN con alta duración sin actividad
- accesos a segmentos internos no habituales

1.4 Detección de actividad administrativa sospechosa

Monitorear eventos como:

- cambios en reglas de firewall
- modificación de políticas VPN
- creación de usuarios administrativos
- deshabilitación de MFA o controles de seguridad

2. CORRELACIÓN AVANZADA EN SIEM

Reglas recomendadas

- LOGIN EXITOSO + cambio de firewall en menos de 10 min → CRÍTICO
- múltiples intentos fallidos + login exitoso → ALTO
- VPN login + escaneo interno posterior → CRÍTICO
- creación de usuario admin + acceso VPN reciente → CRÍTICO



Logs a centralizar

- VPN authentication logs
- Firewall administration logs
- Radius / LDAP / AD logs
- Network flow logs (NetFlow / IPFIX)
- Logs de cambios de configuración

3. THREAT HUNTING (BÚSQUEDA PROACTIVA)

Se recomienda búsqueda continua de:

- accesos VPN desde IPs residenciales o TOR
- autenticaciones repetidas fallidas seguidas de éxito
- uso de cuentas administrativas en horarios inusuales
- conexiones VPN sin actividad posterior
- cambios de configuración no programados

4. HARDENING DE FIREWALL Y VPN

4.1 Control de acceso

- Implementar MFA obligatorio en VPN y firewalls
- restringir acceso por IP allowlist
- bloquear acceso administrativo desde Internet
- segmentar consola de administración en red interna aislada

4.2 Reducción de superficie de ataque

- deshabilitar servicios no utilizados en firewall
- cerrar puertos de administración expuestos
- evitar interfaces web públicas de administración



- usar redes separadas para gestión y usuarios

4.3 Fortalecimiento de credenciales

- políticas de contraseñas robustas y únicas
- rotación periódica de credenciales administrativas
- eliminación de cuentas inactivas o heredadas
- prohibición de reutilización de contraseñas

4.4 Segmentación de red

Separar estrictamente:

- red de administración (firewall/VPN)
- red clínica (HCE / laboratorios)
- red de usuarios finales
- red de invitados

4.5 Seguridad operativa

- auditorías periódicas de configuración de firewall
- revisión de reglas de acceso remoto
- validación de políticas VPN activas
- control de cambios con aprobación formal

5. RESPUESTA AUTOMATIZADA (SIEM + SOAR)

Se recomienda automatizar:

- bloqueo de IP tras múltiples intentos fallidos
- cierre de sesiones VPN sospechosas
- desactivación de cuentas con comportamiento anómalo



- generación automática de alertas críticas al SOC

El principal vector de riesgo en esta campaña no es técnico, sino **organizacional y de configuración**, donde la ausencia de MFA, la exposición de servicios VPN y la reutilización de credenciales convierten el perímetro en el punto más crítico de compromiso en las redes del sector salud.

Recomendaciones de prevención y mitigación

Para reducir la superficie de exposición frente a la campaña activa de ataques dirigidos a dispositivos de seguridad perimetral (firewalls y VPN), se recomienda implementar controles preventivos orientados a la **reducción del riesgo de acceso no autorizado, fortalecimiento de la autenticación y endurecimiento de la infraestructura de red.**

1. Gestión de identidades y control de acceso

- Implementar **autenticación multifactor (MFA) obligatoria** para todo acceso VPN y administración de firewalls.
- Aplicar el principio de **mínimo privilegio** en cuentas administrativas.
- Eliminar usuarios inactivos, genéricos o compartidos.
- Establecer políticas de **rotación periódica de credenciales críticas**.
- Prohibir reutilización de contraseñas entre sistemas internos y externos.

2. Reducción de exposición de servicios

- Evitar la exposición directa de VPN y paneles de administración a Internet.
- Restringir el acceso mediante **listas blancas de IP (IP allowlist)**.
- Segmentar redes administrativas del tráfico general.
- Deshabilitar servicios de administración remota no utilizados.



- Limitar interfaces web administrativas a redes internas seguras.

3. Fortalecimiento de la infraestructura perimetral

- Mantener firewalls y VPN actualizados con los últimos parches de seguridad.
- Revisar y optimizar reglas de firewall eliminando configuraciones permisivas innecesarias.
- Implementar inspección de tráfico y control de sesiones activas.
- Separar el plano de gestión del plano de usuario en la arquitectura de red.

4. Seguridad en autenticación

- Aplicar políticas de contraseñas robustas (longitud + complejidad).
- Bloqueo automático tras múltiples intentos fallidos.
- Implementar detección de autenticación desde ubicaciones anómalas.
- Integrar autenticación con sistemas centralizados (LDAP / AD con MFA).

5. Segmentación de red hospitalaria

- Separar estrictamente:
 - red clínica (HCE, laboratorios, PACS)
 - red administrativa
 - red de usuarios finales
 - red de gestión de infraestructura
- Implementar microsegmentación para limitar movimiento lateral.

6. Monitoreo continuo y auditoría

- Habilitar registro detallado de accesos VPN y administración de firewall.
- Integrar logs en un **SIEM centralizado**.
- Realizar auditorías periódicas de configuración de red.
- Detectar cambios no autorizados en reglas de firewall o políticas VPN.



7. Gestión de vulnerabilidades y exposición

- Evaluar periódicamente la exposición de servicios perimetrales en Internet.
- Realizar escaneos de superficie de ataque (attack surface management).
- Mantener inventario actualizado de dispositivos de red expuestos.
- Aplicar parches de seguridad de forma prioritaria en infraestructura crítica.

8. Concienciación y factores humanos

- Capacitar al personal en:
 - riesgos de reutilización de contraseñas
 - phishing dirigido a credenciales VPN
 - buenas prácticas de acceso remoto seguro
- Promover cultura de reporte temprano de incidentes.

El principal factor de riesgo en este tipo de ataques no es una vulnerabilidad técnica específica, sino la **combinación de exposición de servicios VPN/firewall y debilidades en la gestión de identidades**, lo que convierte la seguridad de accesos remotos en un punto crítico para la continuidad operativa del sector salud.

Recomendaciones de respuesta ante compromiso

En caso de sospecha o confirmación de compromiso asociado a la campaña activa de ataques contra dispositivos de seguridad perimetral (firewalls y VPN), se deben ejecutar de manera inmediata acciones de contención, análisis y erradicación con el objetivo de limitar la propagación del incidente y preservar la integridad de la infraestructura del sector salud:

1. Contención inmediata del incidente



- Aislar el dispositivo comprometido (firewall, VPN o consola administrativa) de la red de producción.
- Suspender temporalmente las conexiones VPN activas hasta validar el alcance del incidente.
- Bloquear direcciones IP sospechosas asociadas a intentos de autenticación o acceso no autorizado.
- Deshabilitar cuentas administrativas potencialmente comprometidas.

2. Preservación de evidencia

- Evitar el reinicio inmediato de los dispositivos afectados.
- Capturar logs de autenticación VPN, firewall y administración.
- Exportar configuraciones actuales del dispositivo comprometido.
- Conservar registros de SIEM, NetFlow y syslogs para análisis forense.

3. Análisis del compromiso

- Identificar cuentas utilizadas en accesos no autorizados.
- Revisar cambios recientes en reglas de firewall y políticas VPN.
- Validar creación de túneles VPN o accesos persistentes no autorizados.
- Correlacionar eventos de autenticación con actividades administrativas posteriores.

4. Erradicación de la amenaza



- Revocar todas las credenciales sospechosas o comprometidas.
- Forzar el restablecimiento de contraseñas en cuentas administrativas.
- Eliminar accesos VPN no autorizados o configuraciones desconocidas.
- Restaurar configuraciones de firewall desde respaldos confiables.

5. Recuperación del entorno

- Reintegrar el dispositivo a la red únicamente después de validación de integridad.
- Verificar que no existan sesiones activas no autorizadas.
- Aplicar actualizaciones de seguridad y parches del fabricante.
- Reestablecer servicios VPN de forma controlada y monitoreada.

6. Notificación del incidente

- Informar al equipo de seguridad (SOC / CSIRT interno).
- Notificar a la dirección de TI y responsables de infraestructura.
- En caso de afectación de datos sensibles, reportar conforme a la Ley 1581 de 2012 en Colombia.
- Escalar a entidades externas (CSIRT nacional o regulador) si aplica impacto crítico.

7. Fortalecimiento post-incidente

- Implementar MFA obligatorio en todos los accesos VPN y administrativos.



- Revisar y reforzar segmentación de red.
- Incrementar monitoreo en SIEM para detección de comportamientos anómalos.
- Realizar auditoría completa de la infraestructura perimetral.
- Aplicar políticas de mínimo privilegio en cuentas de administración.

El éxito en la respuesta a este tipo de ataques depende de la velocidad de contención, la visibilidad sobre los accesos VPN/firewall y la capacidad de correlación de eventos en tiempo real, evitando la persistencia del atacante dentro de la infraestructura hospitalaria.

Conclusiones



La campaña activa de ataques dirigida a dispositivos de seguridad perimetral, incluyendo firewalls y servicios VPN de fabricantes como Fortinet, Palo Alto Networks y Cisco, representa una amenaza crítica para las organizaciones del sector salud, debido a su impacto directo sobre los mecanismos de acceso remoto y control de la infraestructura de red.

Esta actividad no se encuentra asociada a una vulnerabilidad técnica específica, sino al abuso sistemático de credenciales comprometidas, la reutilización de contraseñas filtradas y la explotación de servicios de autenticación expuestos a Internet, lo que incrementa significativamente la superficie de ataque en entornos hospitalarios.

El compromiso exitoso de estos dispositivos puede derivar en el acceso no autorizado a la red interna, facilitando el movimiento lateral hacia sistemas críticos como historia clínica electrónica, plataformas de laboratorio, sistemas administrativos y servicios de telemedicina, afectando directamente la continuidad operativa de los servicios de salud.



Adicionalmente, la falta de mecanismos robustos de autenticación multifactor, la exposición de interfaces administrativas y la segmentación insuficiente de redes corporativas incrementan el riesgo de persistencia del atacante y dificultan su detección oportuna dentro del entorno institucional.

En este contexto, la seguridad del perímetro de red se convierte en un componente crítico para la protección de la infraestructura tecnológica del sector salud, siendo indispensable la implementación de controles de acceso estrictos, monitoreo continuo y capacidades de respuesta automatizada ante eventos sospechosos.

Finalmente, se concluye que la mitigación efectiva de esta amenaza depende principalmente de la gestión adecuada de identidades, la reducción de la exposición de servicios de administración y la capacidad de detección basada en comportamiento, más que en la existencia de vulnerabilidades de software específicas.

Fuentes:



- Fortinet Security Advisories (FortiGuard PSIRT) – Publicaciones oficiales de Fortinet sobre incidentes de seguridad, campañas activas de credenciales comprometidas y vulnerabilidades en firewalls y VPN FortiGate. o <https://www.fortiguard.com/psirt>
- Palo Alto Networks Security Advisories – Reportes oficiales sobre seguridad en GlobalProtect, VPN corporativa y hardening de plataformas de acceso remoto. o <https://security.paloaltonetworks.com/>



- Cisco Security Advisories – Publicaciones oficiales de Cisco sobre vulnerabilidades y recomendaciones de seguridad en dispositivos de red, VPN y SD-WAN.
o <https://sec.cloudapps.cisco.com/security/center/publicationListing.x>
- CISA Cybersecurity Advisories – Alertas oficiales sobre campañas activas contra infraestructura crítica, incluyendo ataques a VPN y servicios de acceso remoto.
o <https://www.cisa.gov/>
- MITRE ATT&CK Framework – Base de conocimiento de técnicas de ataque utilizadas en campañas de compromiso de accesos remotos y abuso de credenciales.

o	T1078	–	Valid	Accounts
o	T1110	–	Brute	Force
o	T1133	–	External	Remote
o	T1021	–	Remote	Services

o <https://attack.mitre.org/>
- ENISA Threat Landscape – Informes de inteligencia de amenazas sobre ataques a infraestructura crítica, VPN corporativas y exposición de servicios perimetrales.
o <https://www.enisa.europa.eu/publications>
- Shodan Internet Exposure Platform – Motor de búsqueda de dispositivos expuestos a Internet utilizado para identificación de firewalls y VPN accesibles públicamente.
o <https://www.shodan.io>
- Censys Attack Surface Intelligence – Plataforma de análisis de superficie de ataque para detección de servicios expuestos en Internet.
o <https://censys.io>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico





Alerta Vulnerabilidad
ATAQUES A FIREWALLS Y VPN
(Fortinet / Palo Alto / Cisco)

CSIRTSALUD-AL-20260624-114

TLP: CLEAR

csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

