

Alerta ID:	115
Fecha del reporte:	24/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Panorama de amenazas dirigidas al sector salud en América Latina
Herramienta de detección	N/A
Activo involucrado:	Infraestructuras críticas del sector Salud
Tipo de alerta:	Alerta
Nivel de riesgo:	Critico

Descripción:

Durante el primer semestre de 2026 el sector salud se consolidó como uno de los tres objetivos más golpeados por el cibercrimen a nivel global, junto con manufactura y tecnología. América Latina dejó de ser un blanco oportunista para convertirse en un objetivo activo y sostenido: la combinación de una digitalización acelerada con niveles desiguales de madurez en ciberseguridad ofrece a los atacantes organizaciones de alto valor y baja resistencia. El sector salud es particularmente atractivo porque concentra datos clínicos, financieros y personales sensibles, opera bajo una presión crítica por restablecer servicios y, en muchos casos, dispone de presupuestos de seguridad limitados frente al valor de la información que custodia.

El ecosistema de ransomware del trimestre estuvo dominado por tres operaciones que, en conjunto, concentraron cerca del 30 % de las víctimas globales: Qilin (también conocido como Agenda), The Gentlemen (rastreado por Microsoft como Storm-2697) y Akira. Las tres operan bajo el modelo de ransomware como servicio (RaaS) y aplican doble extorsión —cifrado más exfiltración con amenaza de publicación—. En paralelo, el robo de credenciales mediante



infostealers se afianzó como el habilitador silencioso de la mayoría de las intrusiones: en la región, Lumma Stealer fue la familia más detectada y las credenciales robadas alimentan posteriormente accesos iniciales de ransomware y fraude.

En Colombia, el sector experimentó de forma directa esta presión con el incidente de alta criticidad contra la Superintendencia Nacional de Salud en marzo de 2026. Los vectores de acceso inicial más recurrentes observados en la región se concentran en dispositivos de borde expuestos (VPN y firewalls de Fortinet, SonicWall, Cisco y Check Point), credenciales válidas robadas o por fuerza bruta, y campañas de phishing. Este informe detalla los actores, los indicadores de compromiso, los métodos predominantes y un conjunto priorizado de medidas de prevención aplicables a las entidades monitoreadas.

Hallazgos clave

- Tres operaciones RaaS dominan el panorama —**Qilin, The Gentlemen (Storm-2697) y Akira**— y todas han impactado al sector salud y a la región latinoamericana.
- El acceso inicial se obtiene mayoritariamente por **explotación de dispositivos de borde y credenciales válidas**, desplazando la dependencia exclusiva del phishing.
- Los **infostealers** (Lumma a la cabeza en la región) son el principal habilitador de robo de credenciales y antesala del ransomware.
- La **doble extorsión** es el modelo estándar: el cifrado se combina con exfiltración de historias clínicas y datos sensibles para maximizar la presión.
- **Colombia, Argentina, México, Brasil y Chile** registraron incidentes documentados contra entidades y proveedores del sector salud en lo corrido de 2026.



Alcance

Este informe especial recopila y analiza la actividad de actores de amenaza dirigida al sector salud en América Latina, con énfasis en el periodo enero-junio de 2026 y referencias a antecedentes relevantes de 2023 a 2025. Su objetivo es ofrecer a las entidades monitoreadas por CSIRT Salud una visión consolidada de quién ataca, cómo lo hace, con qué indicadores puede detectarse la actividad y qué medidas reducen la exposición.

La información proviene de fuentes abiertas de inteligencia (OSINT): avisos de organismos oficiales (CISA, FBI, INCIBE), investigaciones de proveedores de seguridad (Microsoft Threat Intelligence, Trend Micro, Group-IB, Huntress, Rapid7, Arctic Wolf, ESET y Lumu, entre otros), portales de seguimiento de víctimas de ransomware y reportería especializada.

El análisis tiene carácter preventivo y se centra en patrones y tendencias. La atribución de operaciones a actores específicos refleja la evaluación pública de la comunidad de inteligencia al cierre del periodo y puede evolucionar conforme avancen las investigaciones.

Por qué el sector salud es un objetivo prioritario

El sector salud reúne una combinación de factores que lo vuelven especialmente rentable para los atacantes. En primer lugar, custodia datos de altísimo valor: las historias clínicas contienen diagnósticos, medicación, estudios, antecedentes y coberturas, información que en el mercado clandestino puede valer significativamente más que un dato financiero porque no caduca y habilita extorsión, fraude de identidad y estafas dirigidas. En segundo lugar, la criticidad operativa es extrema: un cifrado puede detener diagnósticos, cirugías y atención de urgencias, lo que reduce el margen de negociación y eleva la probabilidad de pago del rescate.

A esto se suman condiciones estructurales propias de la región: equipamiento médico y sistemas que operan con software sin soporte, inversiones de ciberseguridad inferiores al valor de los activos protegidos, escasez de talento especializado y una superficie de exposición



creciente por la digitalización acelerada de servicios (telemedicina, historia clínica electrónica, portales de afiliados). Estudios del sector sitúan a la salud como la industria con el mayor costo medio por brecha de datos durante más de una década, y reportan que una proporción mayoritaria de los dispositivos de imagenología opera con sistemas no soportados, lo que facilita la explotación de vulnerabilidades conocidas y el movimiento lateral.

En el ámbito regional, durante el primer trimestre de 2026 se contabilizaron a escala global más de 200 ataques de ransomware en el sector salud, de los cuales la mayoría golpeó directamente a hospitales, clínicas y prestadores, y el resto a negocios vinculados (proveedores de facturación, fabricantes médicos y empresas healthtech). Esta cadena de suministro ampliada es un punto ciego frecuente: el compromiso de un proveedor tecnológico puede impactar simultáneamente a múltiples entidades, como ya se observó en precedentes históricos en Colombia.

Panorama regional 2026

El primer trimestre de 2026 confirmó que el ransomware es un fenómeno consolidado y en expansión: se superaron las 2.000 víctimas a escala global, con manufactura, tecnología y salud como sectores más afectados. Tres operaciones marcaron el pulso del trimestre y, en conjunto, sumaron cerca de 900 víctimas, equivalentes a más del 30 % del total global.

Concentración del ecosistema de ransomware (1T 2026)

Operación	Víctimas aprox.	Rasgos distintivos
Qilin (Agenda)	+400	Líder del trimestre; profesionalización extrema del RaaS, incluida asesoría a sus afiliados.
The Gentlemen (Storm-2697)	~250	Operación emergente; campañas dirigidas, adaptativas y de marca cuidada; reparto 90/10 a afiliados.
Akira	+200	Fuerte presencia en Latinoamérica; alertas de organismos internacionales como el FBI.



En el plano geográfico latinoamericano, Brasil y México encabezaron el número de ataques, seguidos por incidentes documentados en Argentina, Chile, Perú, Paraguay, Ecuador, Venezuela, Colombia, Guatemala, Panamá y República Dominicana. Colombia y Argentina, además, mantienen una presencia constante en los mapas de detección de infostealers.

El habilitador silencioso: infostealers y robo de credenciales

De acuerdo con el Compromise Report 2026 de Lumu, las campañas de infostealers dominaron buena parte de la actividad maliciosa en la región, con Lumma Stealer como la familia más detectada tanto en Suramérica (alrededor del 43 %) como en Centroamérica y el Caribe (cerca del 29 %), pese a las acciones de desmantelamiento contra su infraestructura. En el frente de ransomware regional, DeathRansom se consolidó como una de las familias más prevalentes en Latinoamérica. Por su parte, la telemetría de ESET ubica a Formbook como la familia más detectada a nivel global al cierre de 2025 y documenta hitos regionales como la campaña masiva de Lumma en México y el fraude vía NFC en Brasil.

La relevancia operativa es directa: un equipo comprometido por un infostealer expone contraseñas guardadas, cookies de sesión y tokens. Las **cookies de sesión** permiten suplantar al usuario aun sin descifrar su contraseña, por lo que un simple cambio de credencial puede no invalidar el acceso del atacante. Estas credenciales se comercializan y se convierten, semanas después, en el acceso inicial de una intrusión de ransomware ejecutada por un actor distinto.

Actores de amenaza relevantes

A continuación se perfilan los actores con mayor incidencia sobre el sector salud y la región. Por tratarse de operaciones de tipo RaaS, las cadenas de ataque varían entre afiliados; por ello el análisis prioriza tácticas, técnicas y procedimientos (TTP) y patrones por encima de firmas puntuales.



Qilin (Agenda)

Qilin es una operación de ransomware como servicio de habla rusa, activa desde 2022, inicialmente conocida como Agenda. Tras la disolución de RansomHub a comienzos de 2025 absorbió a numerosos afiliados y se posicionó como el grupo más prolífico del periodo, con más de mil víctimas publicadas en su sitio de filtraciones. Sus afiliados reciben una proporción elevada del rescate (en torno al 80–85 %), y la operación ha llevado la profesionalización a niveles inéditos, incluida la oferta de asesoría a sus afiliados para incrementar la presión en las negociaciones.

El sector salud es uno de sus objetivos más consistentes, junto con manufactura, servicios profesionales y educación. Su ataque más notorio fue el dirigido contra Synnovis, proveedor de servicios de patología asociado a hospitales del NHS en Londres en 2024, que obligó a cancelar miles de procedimientos. En la región, su sitio de filtraciones ha listado centros médicos latinoamericanos durante 2026.

TTP y comportamiento

- **Acceso inicial:** cuentas válidas obtenidas de volcados de credenciales o páginas de phishing, explotación de aplicaciones expuestas (Citrix, RDP, VPN) y, recientemente, explotación de CVE-2026-50751 en Check Point Remote Access VPN.
- **Cifradores en Go y Rust**, multiplataforma (Windows, Linux y VMware ESXi); el binario suele nombrarse con un identificador único y sufijo de cifrado.
- **Movimiento lateral y robo de credenciales con PsExec, Mimikatz y WinSCP;** exfiltración con Rclone y balizamiento C2 (se ha observado tráfico periódico a dominios maliciosos cada ~10 minutos).



- **Técnicas antianálisis** (detección de máquinas virtuales y entornos de sandbox), borrado de registros de eventos y eliminación de instantáneas de volumen (VSS) para impedir la recuperación.
- **Doble extorsión** con filtración pública en su blog en la red Tor si no se paga.

The Gentlemen (Storm-2697)

The Gentlemen es una operación RaaS emergente que surgió a mediados de 2025 y que Microsoft rastrea como Storm-2697. Pese a su corta trayectoria, escaló con rapidez hasta concentrar alrededor del 10 % de la actividad de ransomware observada en abril de 2026, solo por detrás de Qilin, y al cierre del periodo declaraba cientos de víctimas en decenas de países. Se distingue por una identidad de marca cuidada, un ciclo de desarrollo muy reactivo (incluso publicó un parche el mismo día en que se difundió un descifrador) y un modelo de reparto agresivo del 90 % para los afiliados, lo que le ha permitido atraer operadores cualificados. Sus objetivos incluyen salud, manufactura, seguros, construcción y servicios profesionales, con concentración notable en el Sudeste Asiático y América Latina.

Una característica de alto interés para el sector y para las entidades monitoreadas es su dependencia de dispositivos de borde de Fortinet. La investigación pública asocia la operación con la explotación de CVE-2024-55591 (omisión de autenticación en FortiOS/FortiProxy) y reporta el mantenimiento de una base de miles de dispositivos FortiGate ya comprometidos, así como cientos de credenciales VPN validadas por fuerza bruta y listas para usar. Esto conecta de forma directa con la exposición de credenciales Fortinet que CSIRT Salud monitorea en su portafolio.



TTP y comportamiento

- **Acceso inicial:** servicios expuestos a Internet (VPN y firewalls de Fortinet y Cisco) y credenciales robadas o por fuerza bruta.
- **Cifrador escrito en Go** (ofuscado con Garble), con cifrado híbrido (Curve25519 + XChaCha20) y versiones para Windows, Linux, ESXi y NAS.
- **Propagación tipo gusano:** con el argumento de propagación intenta desplegarse en cada sistema alcanzable de la red; con el argumento de borrado elimina artefactos recuperables tras el cifrado.
- **Evasión y abuso de defensas:** manipulación de GPO para ataques a nivel de dominio, uso de controladores vulnerables (BYOVD) para deshabilitar soluciones de seguridad, desactivación de Microsoft Defender por PowerShell, adición de exclusiones de antivirus y borrado de registros de eventos.
- **Herramientas de post-explotación:** NetExec, RelayKing, TaskHound, PrivHound, CertiHound, Advanced IP Scanner, PsExec, WinSCP y persistencia mediante software de acceso remoto (AnyDesk).
- **Extorsión multicanal:** combina cifrado con presión por correo y por teléfono, además de la filtración en su DLS.

Akira

Akira es una operación RaaS activa desde comienzos de 2023, con vínculos atribuidos al extinto grupo Conti y rastreada también como Storm-1567, Howling Scorpious y Gold Sahara. Acumula más de 1.400 víctimas y un volumen de rescates estimado en cientos de millones de dólares. Es capaz de pasar del acceso inicial al cifrado completo de la red en menos de cuatro horas, y mantuvo una actividad muy elevada en lo corrido de 2026, ubicándose como la segunda



operación más activa a nivel global. Su presencia en América Latina ha sido especialmente significativa y motivó alertas de organismos internacionales. Entre sus víctimas se cuentan hospitales en Norteamérica, con impacto directo en la atención al paciente.

El rasgo más relevante de su actividad reciente es la explotación sistemática de dispositivos SonicWall como vector repetible de acceso inicial, aprovechando CVE-2024-40766 y configuraciones inseguras de SSL VPN, con casos en los que se eludió la autenticación multifactor. También explota VPN de Cisco sin MFA y servidores Veeam sin parche.

TTP y comportamiento

- **Acceso inicial:** explotación de SonicWall (CVE-2024-40766) y de VPN de Cisco sin MFA, RDP expuesto, phishing y credenciales válidas; rociado de contraseñas con herramientas como SharpDomainSpray.
- **Variantes:** cifrador original en C++ (extensión .akira) y variante Megazord en Rust (extensión .powerranges); existe además Akira_v2 para ESXi.
- **Mando y control / túnel:** uso de utilidades de tunelización como Ngrok y cloudflared para abrir sesiones cifradas que evaden el monitoreo perimetral; negociación vía Tor.
- **Impacto:** eliminación de instantáneas de volumen con vssadmin, deshabilitación de servicios mediante PowerShell y WMIC, exfiltración previa al cifrado y doble extorsión.

Ecosistema de infostealers y robo de credenciales

Más allá de los grandes grupos de ransomware, la mayor parte del riesgo silencioso para el sector salud proviene de los infostealers, malware diseñado para robar de forma encubierta contraseñas, cookies de sesión, datos de autocompletado y monederos. Tras las acciones de las fuerzas del orden contra Lumma y RedLine, el ecosistema se reconfiguró con rapidez: Vidar, StealC, Acreed, Rhadamanthys, SnakeStealer y Formbook figuran como familias activas o en



ascenso, y el modelo de malware como servicio garantiza que la interrupción de una familia acelere la adopción de sus sucesoras.

En la región, los vectores de distribución predominantes son el phishing y el spam localizado con señuelos en español (facturas o pedidos falsos), la publicidad maliciosa, el software pirata y la técnica ClickFix —páginas con CAPTCHA falsos que inducen a la víctima a ejecutar comandos mediante el cuadro Ejecutar de Windows o PowerShell—. Algunas variantes incorporan inteligencia artificial para localizar y exfiltrar secretos, y otras combinan robo de credenciales con acceso remoto y fraude vía NFC en plataformas financieras.

Para una entidad de salud, la cadena de daño es clara: el equipo de un funcionario o de un contratista se infecta, se roban credenciales y cookies de portales clínicos, de VPN o de correo, y esas credenciales se venden. Semanas después, un operador de ransomware las utiliza como acceso inicial. Por ello, la detección temprana de infecciones por infostealer y la **rotación inmediata de credenciales e invalidación de sesiones** ante cualquier compromiso son medidas de primer orden.

Actores de filtración, extorsión y hacktivismo en la región

Junto a las operaciones de cifrado, la región registra una actividad creciente de actores centrados en la exfiltración y venta de datos, así como de grupos hacktivistas que combinan filtraciones con desfiguraciones y denegación de servicio. Estos actores suelen anunciar sus operaciones en foros clandestinos y canales de mensajería, y con frecuencia mezclan datos auténticos con material fabricado o reempaquetado, lo que exige una verificación rigurosa antes de validar cualquier filtración. En el sector salud, su objetivo predilecto son los proveedores que concentran datos de múltiples entidades (laboratorios, sistemas de imágenes y plataformas de gestión clínica), porque un solo compromiso multiplica el impacto. La sección 9 detalla casos concretos observados en Colombia, Argentina y México.



Métodos y vectores de ataque más recurrentes

Del análisis transversal de los actores anteriores se desprende un patrón claro que se repite en la mayoría de las intrusiones contra el sector salud en la región. Comprenderlo permite priorizar las defensas donde más impacto tienen.

- **Acceso inicial: el borde de la red y las credenciales**

El vector dominante ya no es exclusivamente el phishing, sino la explotación de dispositivos de borde expuestos a Internet —VPN y firewalls— y el uso de credenciales válidas. Qilin, The Gentlemen y Akira coinciden en aprovechar appliances de Fortinet, SonicWall, Cisco y Check Point, ya sea por vulnerabilidades conocidas sin parchear o por credenciales robadas y validadas por fuerza bruta. Las credenciales provienen, en buena medida, de infecciones previas por infostealer. El phishing y la ingeniería social siguen vigentes como puerta de entrada complementaria, especialmente para la distribución de malware de robo de información.

- **Evasión de defensas e impacto**

Una vez dentro, los atacantes priorizan desactivar las defensas antes de cifrar: deshabilitan el antivirus o el EDR mediante PowerShell, agregan exclusiones, abusan de controladores vulnerables (BYOVD), manipulan políticas de grupo (GPO) para extender el ataque a todo el dominio y borran los registros de eventos para dificultar la respuesta forense. La fase de impacto incluye, de forma casi sistemática, la eliminación de instantáneas de volumen y copias de seguridad accesibles para forzar el pago, y cada vez más operaciones incorporan capacidades de autopropagación tipo gusano que cifran toda la red en minutos.



- **Doble (y triple) extorsión**

El estándar actual es la doble extorsión: antes de cifrar, los operadores exfiltran historias clínicas y datos sensibles y amenazan con publicarlos en sus sitios de filtración. Algunas operaciones suman presión multicanal por correo y teléfono dirigida a directivos y, en ocasiones, a pacientes. Para el sector salud, la sola exfiltración de datos clínicos constituye ya un incidente de alto impacto regulatorio y reputacional, con independencia de si se logra restaurar los sistemas cifrados.

- **Living-off-the-land y herramientas legítimas**

Los atacantes abusan de herramientas administrativas legítimas (PsExec, PowerShell, WMIC, WinSCP, PuTTY, AnyDesk, Advanced IP Scanner) para mezclarse con la actividad normal y dificultar la detección basada en firmas. Esto refuerza la necesidad de detección basada en comportamiento y de inventarios estrictos de software y de cuentas privilegiadas.

Mapeo MITRE ATT&CK

La siguiente tabla resume las técnicas más representativas observadas de forma consistente entre los actores analizados. Es una guía de priorización para detección e ingeniería de reglas, no un listado exhaustivo de cada operación.

Táctica	Técnica (ID)	Uso observado
Acceso inicial	Explotación de servicio expuesto (T1190)	Explotación de VPN/firewalls de Fortinet, SonicWall, Cisco y Check Point.
Acceso inicial	Servicios remotos externos (T1133)	Acceso por SSL VPN y RDP expuestos.
Acceso inicial	Cuentas válidas (T1078)	Credenciales robadas por infostealer o validadas por fuerza bruta.



Táctica	Técnica (ID)	Uso observado
Acceso inicial	Phishing (T1566.001/.002)	Adjuntos y enlaces maliciosos; distribución de infostealers.
Persistencia	Inicio automático en arranque/sesión (T1547.001)	Persistencia vía claves de ejecución; scripts VBScript suplantando componentes del sistema.
Escalada / Evasión	Modificación de políticas de dominio – GPO (T1484.001)	Manipulación de GPO para despliegue a nivel de dominio.
Evasión	Deshabilitar/modificar herramientas (T1562.001)	Desactivación de Defender/EDR y exclusiones de AV; BYOVD.
Evasión	Borrado de indicadores – logs (T1070.001)	Limpieza de registros de eventos de Windows.
Acceso a credenciales	Volcado de credenciales LSASS (T1003.001)	Uso de Mimikatz y utilidades equivalentes.
Descubrimiento	Escaneo de red (T1046)	Advanced IP Scanner y utilidades de enumeración de AD.
Movimiento lateral	SMB / recursos administrativos (T1021.002)	Distribución del cifrador con PsExec.
Movimiento lateral	Transferencia lateral de herramientas (T1570)	Despliegue de utilidades y cifradores en la red.
Mando y control	Tunelización de protocolos (T1572)	Ngrok y cloudflared para evadir el perímetro.
Exfiltración	Exfiltración a almacenamiento en la nube (T1567)	Uso de Rclone para extraer datos antes del cifrado.
Impacto	Datos cifrados para impacto (T1486)	Cifrado de archivos y sistemas; extensiones específicas por familia.
Impacto	Inhibir recuperación del sistema (T1490)	Eliminación de instantáneas de volumen (vssadmin).



Indicadores de compromiso (IOCs)

Importante: estos indicadores deben verificarse en el contexto de cada entidad antes de aplicar bloqueos. Las direcciones IP y dominios pueden corresponder a infraestructura compartida o reutilizada, y los hashes pueden variar entre muestras.

Hashes de archivo (SHA-256)

Tipo	Indicador	Atribución
SHA-256	22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67	The Gentlemen
SHA-256	1848fa2af5371d00bc4f0346ae1f5afd843677ca87de377a3f7b2433c0b7b187	The Gentlemen
SHA-256	e0ba5641d4ebc6292c44b817c7cc0f74aa8fcf416006bbe27b194d2cc773bef5	The Gentlemen
SHA-256	f4ae346deaf87ffdbba0086a29c00819df99cfb380bd08f1da60e45e76b1b63	The Gentlemen
SHA-256	eb3bc08e16d1e7c048aef7ffe3298186f452ce57c6301463d9cdab55af2b4f83	The Gentlemen
SHA-256	d080f553c9b1276317441894ec6861573fa64fb1fae46165a55302e782b1614d	Akira (w.exe)

Indicadores de red

Tipo	Indicador	Atribución / uso
IPv4	176.120.22.127	The Gentlemen — IP histórica reportada por la comunidad.



Tipo	Indicador	Atribución / uso
IPv4	66.165.243.39	Akira — endpoint de exfiltración (AS29802 HVC-AS).
Dominio	cloudflariz[.]com	Qilin — C2 con balizamiento periódico (~10 min).

Artefactos en disco (extensiones, notas y herramientas)

Tipo	Indicador	Atribución
Extensión	.7mtzhh / .ojuopo / .fjn1jw	The Gentlemen (variables por afiliado).
Nota de rescate	README-GENTLEMEN.txt	The Gentlemen.
Extensión	.akira / .powerranges	Akira / Megazord.
Binario	[ID]_crypt.exe	Qilin (nombre con identificador único).
Herramientas	Allpatch2.exe, NetExec, RelayKing, TaskHound, PrivHound, CertiHound	The Gentlemen (post-explotación).
Herramientas	Mimikatz, PsExec, Rclone, WinSCP, AnyDesk, Advanced IP Scanner	Uso compartido (LotL / abuso de utilidades).
Detección AV	Ransom:Win64/Gentlemen.SH!M TB	The Gentlemen (Microsoft Defender).



Vulnerabilidades explotadas (CVE)

CVE	Producto / descripción	Atribución
CVE-2024-55591	FortiOS / FortiProxy — omisión de autenticación.	The Gentlemen
CVE-2024-40766	SonicWall — control de acceso inadecuado en SSL VPN.	Akira
CVE-2026-50751	Check Point Remote Access VPN — omisión de autenticación.	Qilin
CVE-2020-3259 / CVE-2023-20269	Cisco — VPN sin MFA.	Akira
CVE-2023-27532	Veeam Backup & Replication — servidores sin parche.	Akira

Casos relevantes en la región

- Colombia — Superintendencia Nacional de Salud (marzo de 2026)**

A finales de marzo de 2026, la Superintendencia Nacional de Salud confirmó un incidente de seguridad de alta criticidad contra su sistema de gestión documental SUPERARGO, que permitió la descarga masiva no autorizada de información equivalente a cerca del 1,6 % de su bodega documental. La entidad reportó haber identificado y contenido más de 23 millones de intentos de ciberataque en el último mes y detectó el ataque en su fase inicial, lo que permitió bloquear accesos y restablecer el servicio de forma controlada. La información comprometida correspondía a soportes de peticiones, quejas, reclamos y denuncias, con datos personales y eventualmente sensibles en los términos de la Ley 1581 de 2012; reportes posteriores mencionaron también exposición de datos de EPS, IPS, afiliados y credenciales institucionales. El análisis técnico se adelantó en coordinación con ColCERT y CSIRT Salud, y la entidad interpuso denuncia penal.



Lectura para el portafolio: este caso confirma que las entidades del sector salud colombiano son blanco activo de campañas de exfiltración y extorsión, y subraya el valor de la detección temprana y de la contención coordinada. Constituye, además, un antecedente directo para las entidades monitoreadas por CSIRT Salud.

- **Argentina — proveedores y organismos de salud**

Argentina ha concentrado varios incidentes de alto volumen que ilustran el riesgo de la cadena de suministro. Un precedente relevante de 2025 fue la venta, por parte del actor D0T CUM, de más de 665.000 estudios médicos extraídos de un proveedor de sistemas de imágenes que daba servicio a decenas de clínicas y sanatorios. En octubre de 2025, el grupo Nova Ransomware afirmó haber obtenido información de cerca de dos millones de pacientes. Ya en 2026, entre marzo y mayo, el país sufrió grandes filtraciones de organismos estatales — incluidas referencias a registros sanitarios— atribuidas a actores como Chronus Team y Skull1172, con bases que, según las publicaciones, alcanzaban decenas de millones de registros.

- **México — infraestructura crítica y dispositivos obsoletos**

En México, el sector salud arrastra una deuda tecnológica que amplifica el riesgo: reportes del sector señalan un incremento cercano al 35 % en los ataques a la industria médica y advierten que una proporción mayoritaria de los dispositivos de imagenología opera con sistemas no soportados. A los antecedentes de incidentes de ransomware y filtraciones de bases de afiliados en años previos se suma el alto costo de la inactividad, que en salud es el más elevado entre todas las industrias. México fue, además, epicentro de una campaña masiva de Lumma Stealer durante 2025.



- **Operaciones de ransomware con víctimas de salud en la región**

Los portales de seguimiento de víctimas registraron durante 2026 listados de centros médicos latinoamericanos en sitios de filtración de las principales operaciones, incluida Qilin. Estos listados confirman que las clínicas y los centros médicos de la región —y no solo las grandes instituciones— forman parte del conjunto de objetivos de las operaciones RaaS dominantes, en línea con el patrón global de presión sobre el sector.

- **Antecedente estructural — proveedores compartidos**

El precedente histórico del ataque de ransomware al proveedor IFX Networks en septiembre de 2023, que afectó simultáneamente a decenas de portales del Estado colombiano —incluidos sistemas del Ministerio de Salud y de la Superintendencia Nacional de Salud— sigue siendo la mejor ilustración del riesgo de concentración en proveedores. Refuerza la necesidad de exigir y verificar la postura de seguridad de terceros y de contar con planes de continuidad que contemplen la indisponibilidad de un proveedor crítico.

Histórico de ataques al sector salud con nombre propio



La siguiente cronología recopila incidentes de ciberseguridad con afectación documentada al sector salud, identificando con nombre propio a las organizaciones y a los actores cuando la atribución es pública. Incluye una línea de tiempo regional y un conjunto de referentes internacionales que han marcado el panorama. Varias cifras —volúmenes de datos, número de afectados o montos de rescate— corresponden a reclamos de los propios atacantes o a estimaciones de medios y no siempre han sido confirmadas oficialmente; deben tomarse como indicativas.



Línea de tiempo — sector salud en América Latina

Fecha	Organización / objetivo	País	Actor / amenaza	Impacto reportado
Oct 2022	INVIMA	Colombia	Ransomware (sin atribución pública)	Secuestro de información (~700 GB en tres ataques entre 2022 y 2023); plataformas fuera de línea durante semanas.
Nov 2022	Keralty — EPS Sanitas, Colsanitas, Medisanitas	Colombia	RansomHouse	~0,7 TB exfiltrados; ~242.000 afiliados con datos comprometidos; ~5,5 M de usuarios afectados; rescate exigido ~USD 3 M; 45 días de contingencia.
2022	Procaps, Red de Salud de Ladera, Clínica Laura, Comfacundi	Colombia	Ransomware (varias familias)	Cifrado y exposición de datos en entidades y prestadores del sector (reporte ACHC).
Ene 2023	Audifarma	Colombia	Sin atribución pública	Infraestructura tecnológica paralizada; afectación de servicios en ~600 centros de dispensación.
2023	PAMI (obra social)	Argentina	Ransomware	Gestión manual de recetas y derivación de pacientes; datos de millones de afiliados expuestos.
Sep 2023	IFX Networks (proveedor) → MinSalud (MIPRES), Supersalud	Colombia	Ransomware	Más de 50 portales estatales afectados; contingencia prolongada en MIPRES.
Ene 2024	Salud Total	Colombia	Sin atribución pública	Alteraciones de sistemas con afectación a ~4,6 M de usuarios.



Fecha	Organización / objetivo	País	Actor / amenaza	Impacto reportado
Abr 2025	DaVita (diálisis)	Brasil	Ransomware	Sistemas internos cifrados; datos de pacientes en hemodiálisis potencialmente expuestos.
Abr 2025	Informe Médico (proveedor de imágenes, 30+ clínicas)	Argentina	DOT CUM	Más de 665.000 estudios médicos expuestos y puestos a la venta.
2025	Hospital pediátrico	Perú	Nightspire	Reclamo de 30 GB de información crítica exfiltrada.
Oct 2025	Bases de pacientes (no nombradas)	Argentina	Nova Ransomware	Reclamo de datos de ~2 M de pacientes con amenaza de publicación.
Dic 2025	Clínica Dávila	Chile	Devman	~250 GB exfiltrados (fichas clínicas, diagnósticos, resultados de VIH, cédulas); requerimiento del SERNAC.
Mar 2026	Organismos estatales con datos sanitarios	Argentina	Chronus Team	Publicación de más de 1 TB de información de ciudadanos.
Mar 2026	Dos organizaciones (salud y medios)	Colombia	The Gentlemen	Listadas en el sitio de filtración (DLS) del grupo.
Mar 2026	Superintendencia Nacional de Salud — SUPERARGO	Colombia	Actor «delitospenales»	Incidente de alta criticidad; ~1,6 % de la bodega documental; reclamo de exfiltración de 2 TB («Paquete N.º 1»).
May 2026	Ministerio de Salud y organismos	Argentina	Skull1172	Reclamo de compromiso de 900+ dominios; referencias a registros sanitarios.



Referentes internacionales

Aunque ocurrieron fuera de la región, estos incidentes son referencia obligada por su escala y por ilustrar el impacto potencial sobre la continuidad asistencial y la privacidad de los pacientes.

Fecha	Organización / objetivo	País	Actor / amenaza	Impacto reportado
May 2021	HSE — Health Service Executive	Irlanda	Conti	Parálisis del sistema de salud nacional; cancelación masiva de citas y servicios.
Mar 2023	Hospital Clínic de Barcelona	España	RansomHouse	Más de una semana de parálisis; solo urgencias; filtraciones de datos posteriores.
Feb 2024	Change Healthcare	EE. UU.	ALPHV/Black Cat	Disrupción sistémica del procesamiento de pagos de salud en EE. UU.
Jun 2024	Synnovis (proveedor del NHS)	Reino Unido	Qilin	~400 GB de datos de pacientes publicados; miles de procedimientos cancelados en Londres.
2026	Rajagiri Hospital	India	Qilin	Exfiltración de más de 800 GB de datos de pacientes y administrativos.

Del histórico anterior se desprenden tres patrones consistentes para el sector salud: primero, la recurrencia de ataques a proveedores tecnológicos compartidos —sistemas de imágenes, dispensación de medicamentos y gestión documental—, cuyo compromiso afecta simultáneamente a múltiples entidades; segundo, la reincidencia de operaciones como RansomHouse y Qilin sobre objetivos de la región; y tercero, el desplazamiento hacia la extorsión por exfiltración y filtración de datos clínicos, que constituye un incidente grave incluso cuando no hay cifrado o este se contiene a tiempo. La participación de CSIRT Salud en la



respuesta coordinada de varios de estos casos en Colombia refuerza el valor de la detección temprana y del intercambio de inteligencia entre entidades.

Medidas de prevención y recomendaciones

Las siguientes medidas se presentan priorizadas según su impacto frente a los métodos predominantes descritos. Están alineadas con las capacidades del portafolio tecnológico de las entidades monitoreadas y con la operación de CSIRT Salud.

Prioridad crítica

1. **Asegurar el borde de la red.** Parchear con prioridad VPN, firewalls y servicios expuestos (Fortinet, SonicWall, Cisco, Check Point). Donde sea posible, restringir el acceso de administración por IP y deshabilitar servicios SSL VPN que no sean estrictamente necesarios. Atender de inmediato las CVE listadas.
2. **Imponer MFA resistente a phishing.** Aplicar autenticación multifactor en todos los accesos remotos y cuentas privilegiadas, priorizando métodos resistentes a phishing. Considerar que algunas campañas han eludido el MFA por TOTP cuando existe exposición previa de credenciales o portales mal configurados.
3. **Gestionar credenciales expuestas.** Monitorear de forma continua la exposición de credenciales e infecciones por infostealer (FortiRecon, Lumu). Ante cualquier compromiso, rotar credenciales e invalidar sesiones y tokens activos, no solo cambiar contraseñas.
4. **Proteger y aislar las copias de seguridad.** Mantener respaldos cifrados, fuera de línea o inmutables, segregados de la red de producción y probados periódicamente. Es la defensa más eficaz frente al cifrado y la eliminación de instantáneas (VSS).



Prioridad alta

5. **Reglas de reducción de superficie de ataque.** Habilitar reglas ASR y controles que bloqueen actividad típica de ransomware y robo de credenciales, así como el uso de controladores vulnerables (BYOVD).
6. **Segmentación de red y mínimo privilegio.** Segmentar la red para limitar el movimiento lateral y el radio de impacto de la autopropagación; aplicar mínimo privilegio y revisar cuentas privilegiadas y de servicio.
7. **Endurecer el acceso remoto y los protocolos.** Restringir RDP, deshabilitar protocolos obsoletos (NTLMv1, logon anónimo SMB) y auditar cuentas locales en appliances de borde, eliminando las inactivas.
8. **Gestión de vulnerabilidades continua.** Sostener el ciclo de escaneo y remediación (Tenable VM/WAS) con foco en activos expuestos y en dispositivos médicos y de imagenología con sistemas sin soporte.

Prioridad media

9. **Concientización dirigida.** Capacitar al personal frente a phishing y a la técnica ClickFix (CAPTCHA falsos que piden ejecutar comandos), y reforzar la cultura de reporte temprano.
10. **Seguridad de la cadena de suministro.** Evaluar y verificar la postura de seguridad de proveedores tecnológicos críticos e incluir su indisponibilidad en los planes de continuidad.
11. **Plan de respuesta y simulacros.** Actualizar el plan de respuesta a incidentes con escenarios de ransomware y exfiltración, y ejecutar simulacros que validen roles y tiempos de contención.



Conclusiones



El sector salud latinoamericano enfrenta en 2026 un escenario de amenaza maduro y sostenido, impulsado por operaciones de ransomware altamente profesionalizadas —Qilin, The Gentlemen y Akira— y por un ecosistema de infostealers que actúa como su habilitador silencioso. El acceso inicial se ha desplazado hacia el borde de la red y el uso de credenciales válidas, lo que sitúa la gestión de dispositivos expuestos y de credenciales comprometidas en el centro de la estrategia defensiva.

Para Colombia, el incidente de la Superintendencia Nacional de Salud y los antecedentes de afectación a proveedores compartidos confirman que el riesgo es presente y material. La defensa eficaz no depende de una sola herramienta, sino de la combinación de higiene de credenciales, aseguramiento del perímetro, detección basada en comportamiento, copias de seguridad resilientes y una respuesta coordinada. CSIRT Salud mantendrá el seguimiento de estos actores y emitirá las alertas y boletines correspondientes ante nuevos desarrollos que afecten al portafolio de entidades monitoreadas.

Fuentes:



- Microsoft Threat Intelligence — The Gentlemen ransomware (Storm-2697), análisis técnico (mayo 2026).
- CISA / FBI — #StopRansomware: Akira Ransomware (actualización noviembre 2025).
- Group-IB — Hastalamuerte / The Gentlemen RaaS TTPs (2026).
- Trend Micro — Unmasking The Gentlemen Ransomware (2025).
- Huntress — Qilin, Akira y The Gentlemen, perfiles y TTPs (2026).
- Rapid7 / Arctic Wolf / Darktrace — campañas Akira sobre SonicWall SSL VPN (2025–2026).



- ESET / WeLiveSecurity — actividad de ransomware e infostealers en Latinoamérica (1T 2026).
- Lumu Technologies — Compromise Report 2026.
- SOCRadar / ThreatLocker / Qualys / CloudSEK — perfiles de Qilin y The Gentlemen (2025–2026).
- Comparitech — estadísticas de ransomware en salud (1T 2026).
- El Colombiano / Infobae / Consultorsalud — incidente Superintendencia Nacional de Salud (marzo 2026).
- INCIBE-CERT / Defonline / Expansión — incidentes en Argentina y México (2025–2026).
- La República / Semana / El Tiempo — ciberataques al sector salud en Colombia (2022–2024).
- ACHC – Revista Hospitalaria / Latinpyme — recuento de afectaciones del sector salud colombiano.
- WeLiveSecurity (ESET) — Gobierno y Salud, sectores golpeados en Latinoamérica (1.º semestre 2025).
- SERNAC (Chile) — incidente de ciberseguridad de Clínica Dávila (diciembre 2025).
- Segu-Info / Ransomware Help / Infobae — incidentes y tendencias de ransomware en la región (2025–2026).

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

