

Alerta ID:	127
Fecha del reporte:	28/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Presunta comercialización en foro clandestino de información clínica atribuida a la plataforma SaludTools
Herramienta de detección	N/A
Activos involucrados:	Historias clínicas electrónicas, documentos de identidad, consentimientos informados y material clínico custodiado en plataformas de terceros
Tipo de alerta:	Alerta
Nivel de riesgo:	Medio

Objetivo:

El CSIRT Salud informa a las entidades de su comunidad sobre la presunta comercialización, en un foro dedicado al tráfico de datos obtenidos ilícitamente, de un conjunto de información clínica que un actor de amenaza atribuye a SaludTools, plataforma colombiana de historia clínica electrónica utilizada por prestadores de servicios de salud y profesionales independientes en el país. El material ofrecido incluiría historias clínicas, documentos de identidad, consentimientos informados y material fotográfico de pacientes.

El presente boletín tiene carácter informativo y preventivo. Su propósito es documentar el estado de verificación del hecho reportado, advertir sobre el riesgo asociado a la custodia de datos sensibles de salud en plataformas de terceros y entregar recomendaciones para que cada entidad evalúe su exposición ante una eventual materialización de la filtración. Se advierte de manera expresa que, a la fecha de emisión de este documento, el hecho no ha sido confirmado por el proveedor señalado ni por fuentes oficiales, y que las cifras divulgadas corresponden únicamente a afirmaciones del actor de amenaza.

Descripción del hecho reportado:

El 23 de junio de 2026, el portal especializado en ciberseguridad MuchoHacker.lol publicó un reporte según el cual un actor malicioso puso a la venta, en un foro dedicado a la comercialización de datos robados, una presunta base de datos de información médica que atribuye a SaludTools. En la publicación, el actor afirmó poseer aproximadamente 2,3 terabytes de información y cerca de 4,5 millones de archivos, fijó un plazo y condicionó la no divulgación del material al cumplimiento de sus exigencias, patrón consistente con esquemas de extorsión basados en exfiltración de datos.

Para respaldar la oferta, el actor difundió una muestra compuesta por 433 archivos, que el medio citado revisó de manera directa. De acuerdo con ese análisis, la muestra estaría integrada por 345 archivos en formato PDF, 82 imágenes en formatos JPG, JPEG y PNG, y 2 archivos de video. Entre los documentos se habrían identificado historias clínicas, documentos de identidad y formularios de consentimiento informado.

El reporte señala que la muestra incluiría al menos once fotografías de pacientes, algunas asociadas a procedimientos estéticos, en las que las personas podrían resultar plenamente identificables, así como dos videos de un procedimiento quirúrgico. Este componente eleva de manera significativa la criticidad del caso, dado que se trata de material íntimo cuya exposición es irreversible y cuyo uso indebido puede derivar en extorsión dirigida contra las personas afectadas.

Adicionalmente, el medio extrajo de los documentos de la muestra los números de identificación tributaria (NIT) y las razones sociales referenciadas, y concluyó que el material alcanzaría a decenas de organizaciones distintas, entre ellas clínicas, instituciones prestadoras de servicios de salud (IPS), centros de estética, profesionales de cirugía plástica de Bogotá y Medellín, y empresas de diversos sectores. Varios de los documentos corresponderían a exámenes o certificados de medicina laboral, lo que extendería el impacto desde el paciente individual hacia los empleadores vinculados. El reporte menciona de manera específica el

hallazgo de documentos asociados a Profamilia y a la Clínica Portoazul de Barranquilla, entidades que fueron notificadas por el medio.

Se destaca que la muestra publicada representaría una fracción mínima del volumen total declarado por el actor y, aun así, ya involucraría a múltiples organizaciones. **SaludTools** es una compañía colombiana de tecnología para la salud que, según su propio sitio web, ofrece historia clínica electrónica, agenda, facturación electrónica, generación de RIPS y telemedicina, y es utilizada por más de 7.000 médicos en el país.

Estado de verificación y contraste de fuentes:

El CSIRT Salud adelantó una revisión de fuentes abiertas con corte al 28 de julio de 2026, orientada a establecer si el hecho contaba con confirmación independiente, pronunciamiento del proveedor señalado o divulgación posterior del material. Los resultados de esa verificación se resumen a continuación:

- **Fuente única.** La totalidad de la información pública disponible proviene del reporte de MuchoHacker.lol del 23 de junio de 2026. No se identificaron coberturas independientes en medios nacionales o internacionales, ni publicaciones de proveedores de inteligencia de amenazas que documenten el mismo evento.
- **Reserva del propio medio.** El portal que originó el reporte precisó que no pudo confirmar de forma independiente ni el volumen total declarado ni que la totalidad de los datos provenga efectivamente de SaludTools, y señaló que el actor tendría antecedentes de actividad maliciosa contra objetivos en Colombia.
- **Cifras no verificadas.** Los 2,3 terabytes y los 4,5 millones de archivos son afirmaciones del actor de amenaza y no han sido corroborados técnicamente por ninguna fuente. Lo único documentado por un tercero es el contenido de la muestra de 433 archivos.
- **Sin pronunciamiento del proveedor.** El medio informó haber notificado el hallazgo a la compañía señalada antes de la publicación, conforme a su protocolo de divulgación responsable, sin recibir respuesta al cierre de la edición. A la fecha de este boletín no se

ha identificado comunicado oficial, aviso a clientes ni declaración pública de SaludTools sobre el incidente en sus canales institucionales.

- **Sin evidencia de publicación posterior.** No se encontró evidencia pública de que el material haya sido liberado, vendido o divulgado más allá de la muestra inicial empleada como prueba de posesión.

En consecuencia, el CSIRT Salud clasifica el evento como NO CONFIRMADO Y EN VERIFICACIÓN. Lo que se encuentra documentado es la existencia de una oferta de venta acompañada de una muestra revisada por un tercero; la atribución del origen de los datos, su volumen real y el alcance de una eventual afectación permanecen sin establecer. Esta clasificación no reduce la pertinencia de las medidas preventivas descritas más adelante, toda vez que la muestra verificada por el medio contiene datos personales sensibles reales asociados a múltiples organizaciones del sector.

Análisis de riesgo para el sector salud:

El caso ilustra un escenario de riesgo de tercera parte que resulta especialmente relevante para la comunidad CSIRT Salud. La adopción de plataformas de historia clínica electrónica en modalidad de software como servicio (SaaS) traslada la operación técnica al proveedor, pero no traslada la responsabilidad legal de la entidad frente al titular del dato. En el marco de la Ley 1581 de 2012, la información relativa a la salud constituye dato sensible con protección reforzada, y la entidad prestadora conserva su condición de responsable del tratamiento aun cuando la custodia técnica recaiga sobre un encargado.

El avance de la interoperabilidad de la historia clínica electrónica, en desarrollo de la Ley 2015 de 2020 y de las resoluciones 866 de 2021 y 1888 de 2025, incrementa progresivamente la concentración de información clínica en un número reducido de plataformas tecnológicas. Esta concentración eleva el valor de dichos proveedores como objetivo y amplifica el impacto potencial de un único compromiso, que deja de ser un incidente aislado de una entidad para convertirse en un evento de alcance sectorial.

Riesgos derivados para pacientes y entidades

- **Extorsión dirigida a pacientes.** La combinación de historia clínica, documento de identidad y material fotográfico íntimo habilita esquemas de extorsión altamente efectivos contra personas identificadas de manera individual.
- **Ingeniería social de alta credibilidad.** Actores maliciosos pueden emplear datos clínicos reales como pretexto en campañas de phishing, vishing y smishing contra pacientes, personal asistencial y personal administrativo, elevando significativamente la tasa de éxito frente a campañas genéricas.
- **Suplantación de identidad y fraude.** Los documentos de identidad y los datos demográficos expuestos facilitan la apertura fraudulenta de servicios, la radicación de solicitudes ante el sistema de salud y el fraude a aseguradoras.
- **Exposición laboral indirecta.** La presencia de exámenes y certificados de medicina laboral vincula condiciones de salud con empleadores identificables, con riesgo de discriminación y de afectación a la reserva del acto médico.
- **Responsabilidad legal y reputacional.** Una eventual confirmación activaría deberes de notificación a titulares y de reporte a la autoridad de protección de datos, con exposición a investigaciones administrativas y a acciones judiciales.
- **Desinformación y atribución errónea.** La circulación de reportes no confirmados puede generar atribuciones incorrectas hacia entidades que aparecen referenciadas en documentos, sin que ello implique compromiso de su propia infraestructura.

Recomendaciones para las entidades:

El CSIRT Salud recomienda a las entidades de la comunidad adoptar, en la medida de sus capacidades y de acuerdo con su modelo de operación tecnológica, las siguientes acciones:

Gestión de proveedores y terceros

- **Verificar el uso de la plataforma.** Establecer si la entidad, sus sedes, sus prestadores contratados o los profesionales que operan en sus instalaciones utilizan SaludTools u

otras plataformas de historia clínica electrónica en modalidad de servicio, incluyendo contrataciones realizadas de manera descentralizada.

- **Requerir pronunciamiento formal del proveedor.** En caso de utilizar la plataforma, solicitar por escrito al proveedor un pronunciamiento sobre el estado del hecho reportado, el resultado de sus verificaciones internas, el alcance de una eventual afectación sobre la información de la entidad y las medidas de contención adoptadas.
- **Revisar las condiciones contractuales.** Verificar la existencia y suficiencia de cláusulas relativas a seguridad de la información, tratamiento de datos personales en calidad de encargado, plazos de notificación de incidentes, auditoría y devolución o supresión de información al terminar la relación contractual.
- **Actualizar el inventario de terceros.** Mantener un registro actualizado de proveedores que custodian o procesan datos clínicos, con clasificación por criticidad y volumen de información tratada.

Verificación técnica y control de accesos

- **Revisar registros de auditoría.** Solicitar y analizar los registros de acceso, consulta y exportación disponibles en las plataformas clínicas de terceros, buscando descargas masivas, accesos fuera de horario o desde direcciones IP no habituales.
- **Depurar cuentas y privilegios.** Identificar y desactivar cuentas de usuarios retirados o de terceros sin vinculación vigente, y restringir los perfiles con capacidad de exportación masiva de historias clínicas.
- **Reforzar la autenticación.** Confirmar la activación de autenticación multifactor en todos los accesos a plataformas clínicas y administrativas expuestas a Internet, y forzar el cambio de credenciales de cuentas privilegiadas.
- **Monitorear credenciales expuestas.** Verificar mediante las herramientas disponibles la presencia de credenciales corporativas asociadas a dominios de la entidad en repositorios de información filtrada o en registros de infecciones por malware de tipo stealer.

Referencias

- MuchoHacker.lol (23 de junio de 2026). Cuerpos desnudos e historias clínicas a la venta: filtración que expone a pacientes colombianos. Disponible en muchohacker.lol.
- SaludTools. Sitio web institucional. www.saludtools.com. Consultado el 28 de julio de 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.