Supersalud

Superintendencia Nacional de Salud rechaza vehementemente ciberataques a la Entidad y anuncia que ya se adelantan acciones penales contra los implicados

Bogotá, marzo 31 de 2026.

En relación con los hechos informados a la opinión pública el día 27 de marzo relacionados con múltiples y masivos ciberataques detectados contra la seguridad de la Superintendencia Nacional de Salud, es preciso señalar a la opinión pública y usuarios del Sistema General de Seguridad Social en Salud que el evento identificado correspondió a un incidente de seguridad de alta criticidad.

El incidente de ciberseguridad se presentó contra el sistema de gestión documental SUPERARGO por accesos no autorizados que permitieron la descarga masiva de información que corresponde a un 1,6% de la base del total de la bodega documental de la plataforma tecnológica de la Superintendencia Nacional de Salud.

Cabe señalar que esta Superintedencia logró detectar el incidente en su fase inicial, mediante los sistemas de monitoreo, con el bloqueo de URLs, cierre de accesos y ajustes perimetrales, lo que permitió mitigar la explotación activa y la continuidad del ataque, y la protección de la información, de esta forma

poder restablecer la disponibilidad del servicio de manera inmediata en condiciones controladas.

La información comprometida corresponde a soportes documentales y archivos adjuntos asociados a peticiones, quejas, reclamos y denuncias (PQRD) en salud, interpuestas por la ciudadanía ante la Superintendencia Nacional de Salud.

En este contexto, se trata de información clasificada como dato personal y, eventualmente, dato sensible, en los términos de la Ley 1581 de 2012, por lo que la Superintendencia Nacional de Salud además de activar las acciones de mitigación de los riesgos, interpuso de manera inmediata la respectiva denuncia penal ante la Fiscalía General de la Nación, con el fin de que se adelanten las investigaciones y acciones penales a que haya lugar.

Es importante señalar que, una vez contenida la fase activa del incidente, la Superintedencia Nacional de Salud ha desplegado las acciones necesarias orientadas a fortalecer la postura de seguridad, teniendo monitoreo constante de las herramientas, implementando medidas robustas de autenticación sobre la plataforma tecnológica, con el fin de prevenir la recurrencia de eventos similares y evaluar el alcance de la afectación, dando cumplimiento a los marcos normativos aplicables en coordinación con el ColCERT (Centro de respuesta a emergencias cibernéticas de Colombia) y con el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática del sector salud en Colombia), para el análisis y acompañamiento técnico y responder de forma rápida y eficiente en el incidentes presentado.

Si bien las medidas implementadas por esta Superintedencia han permitido contener y mitigar la explotación activa del incidente, se informa a la

ciudadanía qué esta entidad continúa adelantando las acciones orientadas al fortalecimiento de sus controles de seguridad, así como al análisis detallado del impacto y alcance del evento.

Así mismo, y con las pruebas recaudadas se adelantarán todas las acciones legales correspondientes en la Fiscalía General de la Nación, la Policía Nacional, la Superintendencia de Industria y Comercio y demás organismos de seguridad, con el fin de garantizar la protección de la información y los datos y mitigar la afectación en los términos de ley.

SUPERINTENDENCIA NACIONAL DE SALUD

Página web Supersalud: www.supersalud.gov.co
Redes sociales Supersalud:
X: @Supersalud - https://x.com/Supersalud
Instagram: @Supersalud - https://www.instagram.com/supersalud
Facebook: Supersalud - https://www.facebook.com/supersalud
YouTube: @supersaludcomunica - https://youtube.com/@supersaludcomunica
TikTok: https://www.tiktok.com/@supersaludcol
Línea Gratuita Nacional: 018000 513 700

CP-OCEII-030