Ciberataque filtró datos de instituciones federales, estatales y partidistas en México

- **El ciberataque de Chronus afectó a más de 36 millones de personas en México.**
- **El ataque afectó a dependencias como SAT, IMSS, SEP, Secretaría de Salud, gobiernos estatales y municipales, así como a partidos políticos.**

Ciudad de México, febrero de 2026.- **A finales de enero de 2026, un grupo de ciberdelincuentes identificado como Chronus (o Cronus) hackeó y filtró 2.3 terabytes de información de instituciones federales, estatales y partidistas en México**.

El ataque, ocurrido en un contexto marcado por una baja legislación en materia de ciberseguridad, cambios constantes de gobierno y de proyectos, así como una limitada inversión en infraestructura tecnológica y protección digital (ciberseguridad), dejó al descubierto las vulnerabilidades estructurales del país en materia de ciberseguridad.

"Esta vulneración se da en un momento sensible para México, con el inicio del Mundial, cuando aumenta la actividad digital y la proliferación de sitios y aplicaciones falsas, elevando los riesgos de robo de información, suplantación de identidad y fraude cibernéticos", comentó Fidel Delgado, experto en tecnología y ciberseguridad de Salles Sainz Grant Thornton.

La filtración afectó a múltiples instituciones públicas de distintos niveles de gobierno, como el SAT, el IMSS e IMSS Bienestar, la SEP, Secretaría de Salud, así como el Gobierno Federal, gobiernos estatales y municipales, incluido el DIF Sonora. También se vieron afectados partidos políticos, entre ellos Morena, cuyo padrón de afiliados fue expuesto.

La magnitud del incidente se conoció luego de que el propio grupo de ciberdelincuentes filtrara en la deep web información correspondiente a entre 36 y 36.5 millones de mexicanos, lo que equivale a los 2.3 terabytes de datos sustraídos.

La **información comprometida incluye datos personales como nombres completos, domicilios, CURP, RFC, números de seguridad social, teléfonos y correos institucionales**; también datos médicos del IMSS, registros de programas sociales del DIF, bases de datos administrativas completas, el padrón del Sistema de Protección Social en Salud con 1.8 terabytes, así como información política, como el padrón de afiliados de Morena, integrado por 26,899 militantes.

Una de las preguntas centrales tras el suceso es cómo fue posible la filtración de este volumen de información. Hasta ahora, **no existe un informe técnico oficial que detalle paso a paso la intrusión**. La información pública disponible proviene de declaraciones del gobierno, publicaciones del propio grupo **Chronus**, investigaciones periodísticas, análisis de empresas de ciberseguridad y notas basadas en filtraciones. Aun así, los datos conocidos permiten identificar pistas claras sobre los vectores de acceso utilizados.

De acuerdo con la información confirmada, el ataque no se explica por una sola vulnerabilidad. **La Agencia de Transformación Digital y Telecomunicaciones (ATDT) reconoció que parte del acceso fue posible mediante el uso indebido de usuarios y contraseñas válidas**, es decir, credenciales reales que se encontraban activas en los sistemas y que posteriormente tuvieron que ser deshabilitadas.

Otro de los factores para la filtración de información se debió a la infraestructura digital obsoleta, con la que operaban las dependencias, en algunos casos con sistemas de más de 20 años de antigüedad, así como plataformas heredadas administradas por terceros privados, con deficiencias en mantenimiento, aplicación de parches y supervisión.

En conjunto, **la información disponible apunta a que el hackeo fue resultado de una combinación de factores**:

- Credenciales comprometidas confirmadas oficialmente
- Sistemas vulnerables sin mantenimiento adecuado
- Infraestructura fragmentada y delegada a terceros sin controles modernos
- Protocolos ineficientes, según el propio grupo Chronus
- Falta de cultura de ciberseguridad en México

Hasta el momento, **no se han revelado exploits técnicos concretos**, **pero sí han quedado expuestas las condiciones que hicieron posible la exposición de información.** El caso subraya que la protección digital ya no puede limitarse al uso de soluciones básicas, y más aún hablando del ámbito gubernamental.

Frente al volumen y la sensibilidad de la información que manejan las instituciones públicas, resulta indispensable contar con **infraestructura de ciberseguridad robusta y equipos especializados**, como **Centros de Operaciones de Seguridad (SOC)**. Dar prioridad a la ciberseguridad implica asignar presupuesto, establecer políticas y procedimientos claros, así como desarrollar marcos legales específicos, especialmente ante los proyectos y compromisos digitales que enfrenta el país.

--- Fin ---

Notas