Ciberseguridad

Peligran los datos de millones de mexicanos: advierten hackeo masivo en IMSS y SAT que podrían arruinar la economía de todos

Recientemente, se filtraron datos de más de 36 millones de mexicanos. Los expertos advierten que esto se debió a fallas estructurales en ciberseguridad.

Hackeo de datos en internet

Actualizado el 12 de Febrero de 2026 • 16:36

Un **ciberataque nacional** derivó en la **filtración de información** perteneciente a instituciones públicas y partidos políticos en México. Esta situación evidencia las **deficiencias estructurales** en la estrategia del Gobierno respecto a la **ciberseguridad**.

El contexto, marcado por escasa legislación, limitada inversión tecnológica y una alta rotación de proyectos y administraciones, amplificó el impacto del incidente, de acuerdo con la firma **Salles Sainz Grant Thornton**.

Alerta por hackeo masivo de información personal en México

La consultora explicó que el ataque fue atribuido a un grupo de ciberdelincuentes identificado como Chronus o Cronus, responsable de obtener y difundir datos de dependencias federales, estatales y municipales, así como de institutos políticos.

¿Qué datos se filtraron en México?

Entre las instituciones comprometidas se encuentran:

- Servicio de Administración Tributaria (SAT)
- IMSS
- IMSS Bienestar
- Secretaría de Educación Pública (SEP)
- Secretaría de Salud

Además de distintas instancias del Gobierno Federal y administraciones locales, incluido el DIF Sonora. También resultaron afectados partidos políticos, entre ellos Morena, cuyo padrón de afiliados quedó expuesto.

A este panorama se sumó la **Comisión Nacional de Seguros y Fianzas** (CNSF), que reconoció una vulneración en los sistemas. Según informó, se expusieron cédulas de intermediarios con información mayoritariamente de carácter público.

¿Por qué se filtraron datos personales en México?

Para Salles Sainz Grant Thornton, el ataque ocurrió en un entorno de **debilidad institucional en materia digital**, lo que incrementó la exposición de datos sensibles de millones de personas.

Por su parte, Fidel Delgado -especialista en tecnología y ciberseguridad de la firma- advirtió que la intrusión coincidió con el arranque del Mundial, un momento de alta actividad online en el que aparecen sitios y aplicaciones falsas. Este escenario eleva el riesgo de robo de datos, suplantación de identidad y fraudes cibernéticos, tanto para ciudadanos como para instituciones.

¿Qué datos se hackearon en México?

Entre los datos comprometidos se encuentran:

- Nombres completos
- Domicilios
- CURP
- RFC
- Números de seguridad social
- Teléfonos
- Correos institucionales

También se filtraron expedientes médicos, registros de programas sociales, bases administrativas completas, el padrón del Sistema de Protección Social en Salud -con un peso aproximado de 1.8 terabytes- y bases de carácter político, como el padrón de afiliados de Morena, integrado por 26,899 militantes.

[...] del Gobierno respecto a la ciberseguridad.
El contexto, marcado por escasa legislación, limitada inversión tecnológica y una alta rotación de proyectos y administraciones, amplificó el impacto del incidente, de acuerdo con la firma Salles Sainz Grant Thornton.
Alerta por hackeo masivo de información personal en México
La consultora explicó que el ataque fue atribuido a un grupo de ciberdelincuentes identificado como Chronus o Cronus, responsable de obtener y difundir datos de depend [...]

Recientemente, se filtraron datos de más de 36 millones de mexicanos. Los expertos advierten que esto se debió a fallas estructurales en ciberseguridad. Hackeo de datos en internet

Un ciberataque nacional derivó en la filtración de información perteneciente a instituciones públicas y partidos políticos en México. Esta situación evidencia las deficiencias estructurales en la estrategia del Gobierno respecto a la ciberseguridad.

El contexto, marcado por escasa legislación, limitada inversión tecnológica y una alta rotación de proyectos y administraciones, amplificó el impacto del incidente, de acuerdo con la firma Salles Sainz Grant Thornton.

Alerta por hackeo masivo de información personal en México

La consultora explicó que el ataque fue atribuido a un grupo de ciberdelincuentes identificado como Chronus o Cronus, responsable de obtener y difundir datos de dependencias federales, estatales y municipales, así como de institutos políticos.

Entre las instituciones comprometidas se encuentran:

Además de distintas instancias del Gobierno Federal y administraciones locales, incluido el DIF Sonora. También resultaron afectados partidos políticos, entre ellos Morena, cuyo padrón de afiliados quedó expuesto.

A este panorama se sumó la Comisión Nacional de Seguros y Fianzas (CNSF), que reconoció una vulneración en los sistemas. Según informó, se expusieron cédulas de intermediarios con información mayoritariamente de carácter público.

Para Salles Sainz Grant Thornton, el ataque ocurrió en un entorno de debilidad institucional en materia digital, lo que incrementó la exposición de datos sensibles de millones de personas.

Por su parte, Fidel Delgado -especialista en tecnología y ciberseguridad de la firma- advirtió que la intrusión coincidió con el arranque del Mundial, un momento de alta actividad online en el que aparecen sitios y aplicaciones falsas. Este escenario eleva el riesgo de robo de datos, suplantación de identidad y fraudes cibernéticos, tanto para ciudadanos como para instituciones.

Entre los datos comprometidos se encuentran:

También se filtraron expedientes médicos, registros de programas sociales, bases administrativas completas, el padrón del Sistema de Protección Social en Salud -con un peso aproximado de 1.8 terabytes- y bases de carácter político, como el padrón de afiliados de Morena, integrado por 26,899 militantes.