Revelan descuido de personal en sistemas

Estiman aumenten hackeos a Gobierno

Especialistas señalan carencias normativas y técnicas que frenan defensa institucional

LUIS PABLO SEGUNDO

Los constantes ataques cibernéticos contra el Gobierno federal podrían cerrar el año con un alza de 260 por ciento en comparación con el año anterior; en el que los empleados serán los principales responsables.

"La amenaza más inquietante no proviene de los hackers externos, sino de los llamados insiders: empleados activos, ex colaboradores con credenciales no revocadas o personal negligente", dijo Víctor Ruiz, CEO y fundador de SILIKN.

El especialista señaló que este tipo de personal está implicado en aproximadamente 70 por ciento de las brechas de seguridad, filtraciones de datos y ciberataques en instituciones gubernamentales.

De acuerdo con Ruiz, este fenómeno refleja una vulnerabilidad estructural, debido a que a nivel global, el 68 por ciento de las brechas están relacionadas con el factor humano, y México no es la excepción.

En entrevista señaló que en México, 60 por ciento de las violaciones de datos provienen de errores humanos y 22 por ciento involucra directamente a empleados internos.

"En el sector gubernamental, la tendencia es más crítica, debido a que más de la mitad de las instituciones mexicanas sufrieron al menos un incidente en 2024, concentrándose los casos más graves en los sectores gubernamental, de salud y financiero", externó.

Ruiz resaltó que entre los ataques más recientes este año destacan uno contra el Gobierno de Pachuca, Hidalgo, el cual sufrió la filtración de más de 100 archivos sensibles de su área de sistemas. En octubre de 2025, presuntos hackers afirmaron haber accedido a la red del Instituto Nacional Electoral (INE).

Uno que tuvo mucho impacto fue el de la Secretaría de la Defensa Nacional (Sedena), que fue víctima en 2022 del conocido Guacamaya Leaks, que expuso 6 terabytes de datos confidenciales. En 2019, el ISSSTE dejó al descubierto datos médicos de millones de derechohabientes debido a fallos en sus protocolos internos.

"Estos episodios sólo evidencian deficiencias normativas, técnicas y culturales en la gestión de la ciberseguridad. Aunque México cuenta con leyes como la Ley Federal de Protección de Datos Personales, su aplicación es limitada", acusó.

Mientras el Gobierno continúa haciendo pequeñas inversiones en infraestructura perimetral, ignora que el 95 por ciento de los ciberataques a nivel mundial inician con ingeniería social, explotando el eslabón más débil que son las personas, añadió el especialista.

Ruiz recomendó fortalecer los programas de concientización y capacitación digital entre servidores públicos, además de establecer auditorías continuas que permitan identificar vulnerabilidades internas antes de que sean explotadas por atacantes externos.

Dependencias expuestas

En México, la mayoría de las dependencias gubernamentales serán objetivo de nuevos ataques cibernéticos debido a errores humanos.

63%
De dependencias de Gobierno fueron atacadas cibernéticamente el año pasado.

12%
De las organizaciones públicas están preparadas para enfrentar amenazas internas.

60%
De los ataques ocurren por errores humanos.

22%
De los hackeos provienen de colaboradores internos.

Fuente: SILIKN