

// informe • ciberseguridad de las instituciones públicas

Después de La brecha.

Lo que la conversación pública revela sobre la ciberseguridad de las instituciones públicas de México • ene 2024 – sep 2026



Cada punto es un incidente contra una institución pública (ene 2024 – sep 2026): 40 en total, 25 después de la extinción del INAI.

// licencia y créditos

Licencia y créditos.

CC BY-NC-ND
4.0 INTERNACIONAL

© 2026 CyberCats Academy A.C. Esta obra está bajo una licencia **Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)**. Puede compartirse con fines no comerciales, sin modificaciones y siempre con atribución.

creativecommons.org/licenses/by-nc-nd/4.0/deed.es

Puedes

- **Compartir:** copiar y redistribuir este documento completo y sin cambios, en cualquier medio o formato.
- **Citar:** retomar datos y fragmentos breves, con la referencia a esta nota.

Siempre que

- **Atribución:** des crédito a CyberCats Academy A.C. y enlaces la licencia.
- **No comercial:** no lo uses con fines comerciales.
- **Sin derivadas:** no distribuyas versiones modificadas, traducciones ni adaptaciones. Para eso, escríbenos.

Las citas de declaraciones oficiales y de notas de prensa se reproducen con fines de análisis y se atribuyen a su fuente; no forman parte de esta licencia.

Cómo citar

CyberCats Academy A.C. (2026). *Después de la brecha: lo que la conversación pública revela sobre la ciberseguridad de las instituciones públicas de México (2024–2026)*. Nota de investigación, octubre de 2026.

Créditos

- **Investigación, análisis y edición:** CyberCats Academy A.C.
- **Edición:** primera, octubre de 2026 · Ciudad de México.
- **Documento complementario:** *Después de la brecha · Metodología*, con el método, la validación y los límites del análisis.
- **Contacto:** info@cyber-cats.org · cybercats-academy.org

Cuidado con los datos. Este documento no reproduce datos filtrados, no enlaza a ellos y no incluye nombres de personas afectadas. Al compartirlo, mantén ese mismo cuidado.

// resumen

Lo que encontramos.

Analizamos unas 249 mil menciones públicas entre enero de 2024 y septiembre de 2026. Buscamos qué se sabe públicamente **después** de un incidente que afecta a una institución pública: qué se reconoce, a quién se avisa, quién responde y adónde van los datos.



01 • hallazgo

La conversación se desplazó hacia la identidad digital.

Tras la extinción del INAI, dentro de la conversación sobre incidentes, las menciones de CURP, del registro de líneas celulares y de datos biométricos se multiplicaron por 3 a 5, mientras las referencias a la transparencia cayeron cerca de 40 %.

02 • hallazgo

Primero se niega; el aviso no llega.

En los casos documentados a fondo, no encontramos información pública de que se avisara a las personas afectadas. En la conversación pública, los desmentidos duplican a los reconocimientos, antes y después de la extinción del INAI.

03 • hallazgo

El daño llega a la ciudadanía, con impactos aún desconocidos.

Datos de una institución pública terminaron a la venta y, después, en extorsiones a derechohabientes.

04 • hallazgo

El robo y la venta de datos se ofrecen en abierto.

Unas 270 mil ofertas en español para robar cuentas y vender datos, en redes sociales accesibles desde México.

CyberCats Academy A.C. • Ciudad de México • Octubre de 2026.

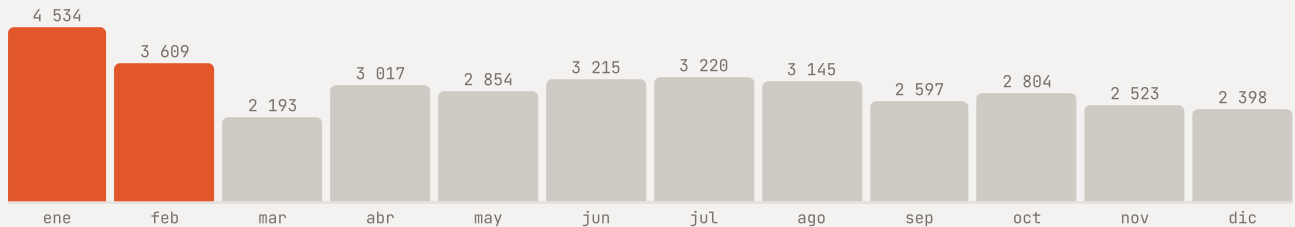
Nota de investigación. Las cifras provienen de clasificación automática con validación humana por muestras; el método y sus límites están en el documento de metodología.

// contexto · volumen mensual

El año, mes a mes.

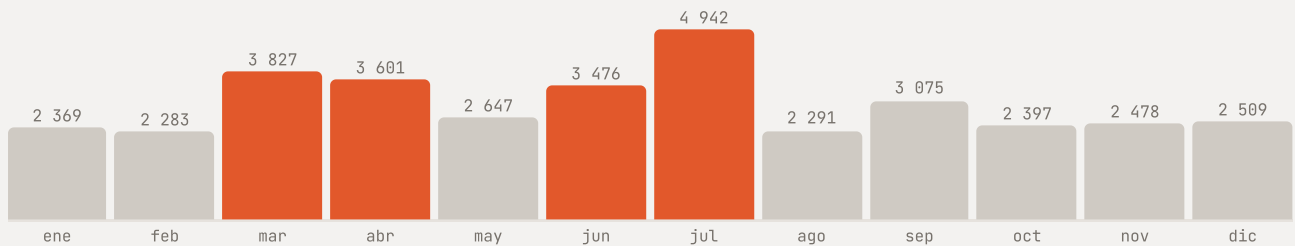
Publicaciones mexicanas por mes, un panel por año · misma escala en los tres

2024 · 36 109 publicaciones · promedio 3 009 al mes



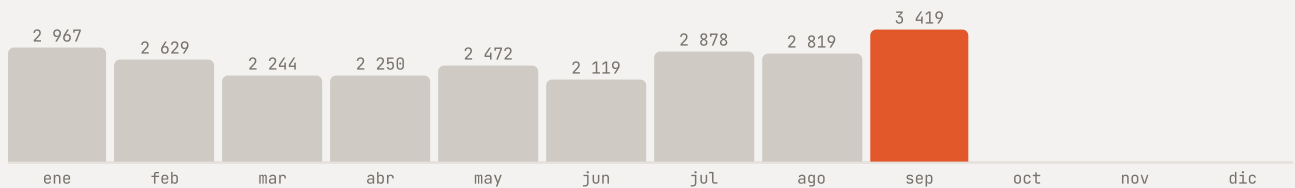
Pico en enero: exposición de datos de periodistas acreditados a la conferencia matutina.

2025 · 35 895 publicaciones · promedio 2 991 al mes



Picos en marzo y abril (extinción del INAI el 21 de marzo; debate sobre datos biométricos) y en julio (investigación de la FGR por Pegasus).

2026 (ene-sep) · 23 797 publicaciones · promedio 2 644 al mes



Pico en septiembre, impulsado por las ofertas de bases de datos robadas (el mes con más menciones de venta de datos en 2026) y por Pegasus.

Resaltados: los meses por encima de 3 400 publicaciones. 2024 y 2025 tienen un volumen casi idéntico (~36 mil publicaciones cada uno); 2026 va algo por debajo. La atención pública es estable; lo que cambia es el tema (hallazgo uno).

// cronología · 2024

40 incidentes contra instituciones públicas.

FECHA	INSTITUCIÓN	NIVEL	QUÉ PASÓ	DATOS Y ALCANCE	RESPUESTA INICIAL
ene 2024	Presidencia ♦ periodistas	Federal	Acceso desde España con la clave de un extrabajador	263 periodistas acreditados a la mañanera: credenciales de elector, pasaportes, domicilios	• renombra el incidente «No fue hackeado»
ene 2024	Congreso de Hidalgo	Estatal	Comprometen el correo institucional de Comunicación Social	Cuenta institucional	✓ reconocido Denuncia ante la Procuraduría estatal
mar 2024	Gobierno de Oaxaca	Estatal	Un grupo afirma haber robado información de 2007 a 2024; tras el desmentido, altera el sitio oficial (abr)	~2,9 millones de registros (~800 MB), según el grupo	• desmentido Niega el robo de información
abr 2024	Gobierno de la CDMX	Estatal	Venta de correos por una falla del servidor conocida desde 2019	~1,3 TB (unos 2,1 millones de correos)	ⓘ reconocimiento parcial «No se almacena información crítica»
may 2024	Gobierno de Yucatán	Estatal	Un grupo de ransomware lo lista como víctima, con 14 días para pagar; atribución dudosa	No reportado	o sin respuesta localizada
may 2024	Llave CDMX (Agencia Digital de Innovación Pública)	Estatal	Filtran accesos y contraseñas de la principal plataforma de trámites de la capital	Hasta 6,3 millones de usuarios en riesgo; acceso a documentos personales	• renombra el incidente Dice no tener evidencia de hackeo; activa la doble autenticación
may 2024	Secretaría de Seguridad Ciudadana de la CDMX	Estatal	Difunden datos de policías de una plataforma de capacitación y, en junio, accesos a la intranet de inteligencia policial	Accesos de más de 30.000 policías; credenciales de un sistema de inteligencia en tiempo real	o sin respuesta localizada
jun 2024	Instituto Electoral de la CDMX	Estatal	Cae el portal del conteo preliminar la noche de la elección; un consejero habla de ciberataque	Sitio del conteo preliminar; sin datos reportados	• desmentido El Consejo lo atribuye a una «demanda atípica»
ago 2024	Poder Judicial de la CDMX	Estatal	Un grupo de hackers deja el sitio fuera de línea y, tras exigir un pago, publica datos de su sistema	Accesos y correos de ~162.000 usuarios, en su mayoría abogados	o sin respuesta localizada
sep 2024	Gobierno de Sinaloa	Estatal	Hackean los portales del SAT estatal y del COBAES con amenazas al gobernador	Sitios web; sin datos reportados	✓ reconocido Control recuperado en ~10 minutos
nov 2024	Consejería Jurídica, Presidencia	Federal	Ransomware; descrito como el primer hackeo al nuevo gobierno federal	~313 GB sustraídos (contratos, datos de funcionarios); ~210 GB publicados	o en documentación
nov 2024	SEP de Hidalgo ♦ niñez	Estatal	Un atacante afirma tener acceso total al expediente digital y publica archivos	~873.000 estudiantes, docentes y personal, según el atacante	ⓘ verificación interna Investiga; dice que la vulneración no se confirmó en su totalidad
dic 2024	Fiscalía de Nuevo León ♦ víctimas	Estatal	Sustracción de carpetas de investigación; la actividad se detectó en febrero de 2024	~960 carpetas de investigación	ⓘ reconocido tarde ~10 meses después de detectarlo

respuesta: • renombra el incidente • desmentido ⓘ parcial o tardía ✓ reconocido
o sin respuesta o en documentación ♦ mujeres o grupos vulnerables

Todo según lo reportado públicamente. La última columna resume la respuesta pública inicial de la institución. ♦ Marca los 12 incidentes (de 40) que, según lo reportado, afectan en particular a mujeres, niñez, personas mayores, víctimas, denunciantes o informantes, o periodistas; 9 ocurrieron después de la extinción del INAI. Continúa en la página siguiente.

// cronología · 2025

2025: se extingue el INAI.

FECHA	INSTITUCIÓN	NIVEL	QUÉ PASÓ	DATOS Y ALCANCE	RESPUESTA INICIAL
ene 2025	Ayuntamiento de Pachuca	Municipal	Acceso no autorizado al sistema municipal; filtran más de cien archivos internos en un foro	Archivos internos (cartillas militares, DIF municipal)	● reconocimiento parcial Confirma el acceso, niega un «saqueo»; sospecha de personal interno
feb 2025	Secretaría de Gobierno de Hidalgo	Estatal	Toman el control de su cuenta oficial en redes sociales	Cuenta institucional	○ en documentación
21 de marzo de 2025 · Se extingue el INAI. Los 25 episodios siguientes ocurren sin una autoridad autónoma de protección de datos.					
abr 2025	Municipio de Chicoloapan	Municipal	Toman el control de sus cuentas oficiales en redes sociales	Cuentas institucionales	○ en documentación
may 2025	Ayuntamiento de Tepotzotlán (Edomex)	Municipal	Hackean la página web y la cuenta oficial de Facebook; publican imágenes de un colectivo de hackers	Página web y cuenta institucional	✓ reconocido Confirma la intrusión y anuncia acciones legales
jun 2025	C5 de la CDMX ◆ informantes	Estatal	Según el Departamento de Justicia de EE. UU., un hacker al servicio de un cártel accedió a las cámaras para rastrear informantes	Cámaras de videovigilancia	● desmentido
jul 2025	Secretaría de Educación y Cultura de Sonora ◆ niñez	Estatal	Con las credenciales robadas de una cuenta de usuario, un atacante descarga y publica expedientes de una primaria de Nogales	366 alumnos: CURP, calificaciones, tipo de sangre, alergias y datos de madres, padres o tutores	● renombra el incidente Habla de «acceso no autorizado»; afirma que el portal «no fue vulnerado»; presenta denuncia
ago 2025	Congreso de Morelos	Estatal	Hackeo y uso no autorizado de sus plataformas digitales	No reportado	✓ reportado por la institución
sep 2025	IMSS ◆ personas mayores	Federal	Se vende la base de pensionados en 50 mil pesos	~20 millones de pensionados	● desmentido Atribuye la fuga a un «uso indebido» de accesos del personal
oct 2025	INE	Federal	Denuncias de hackeo durante el proceso electoral de 2024	No reportado	● desmentido
oct 2025	SEP ◆ niñez	Federal	Circulan reportes de una filtración de datos de alumnos en Campeche y Puebla	Datos de alumnos, según los reportes	● desmentido «No se ha detectado vulneración»
nov 2025	Fiscalía de Guanajuato	Estatal	Filtración tras un ciberataque	~10 GB	○ en documentación
nov 2025	Secretaría de Turismo	Federal	Hackean la página oficial	Sitio web	✓ seguimiento judicial Una persona vinculada a proceso

respuesta: ● renombra el incidente ● desmentido ○ parcial o tardía ✓ reconocido

○ sin respuesta ○ en documentación ◆ mujeres o grupos vulnerables

Todo según lo reportado públicamente. Continúa en la página siguiente.

// cronología · 2026

2026: el año con más incidentes.

FECHA	INSTITUCIÓN	NIVEL	QUÉ PASÓ	DATOS Y ALCANCE	RESPUESTA INICIAL
ene 2026	UNAM	Federal	Hackeo de cinco sistemas informáticos en vacaciones	Según la UNAM, los datos sensibles siguen seguros	✓ reconocido Confirma el hackeo; refuerza sus lineamientos
ene 2026	25 instituciones (SAT, IMSS- Bienestar...)	Federal y estatal	Publicación masiva de información	~2,3 TB	• desplaza responsabilidad La ATDT culpa a «sistemas obsoletos» de proveedores
feb 2026	SAT	Federal	Según una firma de seguridad, un atacante usó chatbots de IA contra dependencias; las empresas de IA bloquearon las cuentas	~195 millones de registros de identidad	• desmentido «No se identificó acceso ilegítimo»
feb 2026	Fiscalía de Guanajuato ♦ mujeres · víctimas	Estatal	Exposición del banco de datos de violencia contra las mujeres	Más de 336 mil expedientes (2014–2025), con nombres de víctimas y agresores	• desmentido Culpa a otra dependencia con acceso; después reconoce mal uso de credenciales
abr 2026	SAT	Federal	El grupo que vendió los datos del IMSS difunde gratis registros extraídos en 2024	~6,5 millones de registros fiscales (RFC, CURP, domicilios)	🕒 verificación interna Activa protocolos
abr 2026	Seguridad y Paz, Guanajuato ♦ mujeres · víctimas	Estatal	Filtración de expedientes	Policías estatales, víctimas de violencia de género y pacientes	🕒 en documentación
abr 2026	Secretaría de Marina (Sistema Portuario Nacional)	Federal	Se expone un archivo de ~39,7 GB y, después, el sistema Puerto Inteligente Seguro	Más de 640.000 trabajadores portuarios y aduanales	🕒 reconocimiento parcial Una administración portuaria admite un «posible» robo; la Marina no se pronuncia
may 2026	Secretaría de Bienestar ♦ mujeres	Federal	Acceso no autorizado con credenciales vigentes	Datos de personas beneficiarias; habría incluido la Pensión Mujeres Bienestar	🕒 reconocimiento parcial «Acceso no autorizado», no «hackeo»
jun 2026	911 de León (C4) ♦ víctimas	Municipal y estatal	Extracción interna; los atacantes amenazan con acosar a las víctimas	~179 mil registros prehospitales con nombres, domicilios y diagnósticos	✓ reconocido Extracción interna; persona sospechosa identificada
jul 2026	Gobierno de Sinaloa	Estatal	Presunto hackeo	~1 millón de registros fiscales, bancarios y médicos	🕒 en documentación
jul 2026	Municipio de León	Municipal	Segundo hackeo en un mes; datos difundidos gratis	~250 mil personas: CURP, domicilio, teléfono y coordenadas de sus casas	✓ reconocido Denuncia ante la fiscalía estatal
jul 2026	Presidencia (SIDAC) ♦ denunciantes	Federal	Exposición del sistema que canaliza denuncias ciudadanas a 59 dependencias	Más de 400 mil denuncias con nombres, domicilios y texto íntegro (homicidio, extorsión, corrupción)	🕒 sin respuesta localizada
ago 2026	Ayuntamiento de San Luis Potosí	Municipal	Hackeo y filtración	Datos de servidores públicos	✓ reconocido Anuncia denuncia
ago 2026	INAH	Federal	Detecta actividad irregular	No reportado	✓ reconocido Denuncia ante la FGR
sep 2026	Secretaría Anticorrupción (autoridad de datos)	Federal	Detecta la venta de datos atribuidos a centros de llamadas	~12,9 millones de registros (RFC, domicilios, datos bancarios)	✓ la autoridad actúa Abre una investigación de oficio

respuesta: • renombra el incidente • desmentido 🕒 parcial o tardía ✓ reconocido

🕒 sin respuesta o en documentación ♦ mujeres o grupos vulnerables

Los 40 episodios identificados hasta ahora, cada uno con cobertura de al menos dos medios; la lista no es exhaustiva. Alcances según lo reportado, no cifras validadas por la autoridad. Las etiquetas describen la respuesta pública inicial. Fuera del conteo: el ataque a la Cumbre Latinoamericana de Defensoras Digitales (feb-2025), interrumpida con imágenes sexuales explícitas en el panel de la Ley Olimpia.

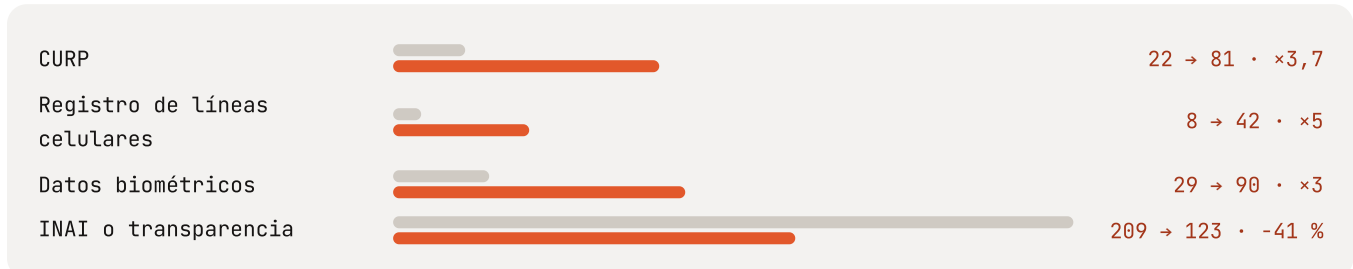
// 01 · hallazgo

La conversación se desplazó hacia la identidad digital.

La atención total sobre ciberseguridad se mantuvo estable: unas 2 800 publicaciones al mes, antes y después de la extinción del INAI. Lo que cambió fue **de qué se habla**.

Promedio mensual de publicaciones sobre incidentes de ciberseguridad que mencionan cada tema (sin comentarios)

■ 2024 (INAI ya sin quórum) ■ Después (abr 2025 - sep 2026)



Se excluye la transición entre la reforma constitucional (publicada el 20-dic-2024, vigente desde el 21-dic) y la extinción efectiva del INAI (21-mar-2025). El patrón se mantiene con cualquiera de los dos cortes. Las cifras miden el cruce de cada tema con la conversación sobre incidentes, no el debate total sobre el tema, que es mucho mayor.

La publicación con más reacciones de todo el periodo trata sobre el **registro obligatorio de líneas telefónicas**. En ese debate se repiten dos ideas: que la medida es ineficaz y que esas bases de datos también podrían ser hackeadas.

Una parte del aumento sigue la agenda legislativa (la CURP biométrica, el padrón de telefonía), no necesariamente los incidentes. Pero el patrón es claro: **la ciudadanía discute cada vez más los datos que el Estado le pide, en el mismo periodo en que se debilitó la supervisión independiente de esos datos**.

// 02 · hallazgo

Silencio tras la brecha, antes y después del INAI.

Después de un incidente, la ley obliga a avisar **«sin dilación alguna»** a las personas cuyos datos quedaron expuestos (arts. 34 y 35 de la ley de datos personales del sector público). En los casos que documentamos a fondo, **no hemos encontrado información pública sobre si se avisó a las personas afectadas**. Lo que sí encontramos, una y otra vez, es una primera respuesta que niega o minimiza.

// antes de la extinción del INAI

- **ene 2024 · Presidencia**. Los datos de periodistas «no fueron hackeados», sino extraídos con la clave de un extrabajador.
- **mar 2024 · Oaxaca**. Niega el robo; el grupo responde alterando el sitio oficial.
- **may 2024 · Llave CDMX**. Sin evidencia de hackeo, dice la agencia digital; pero activa la doble autenticación.

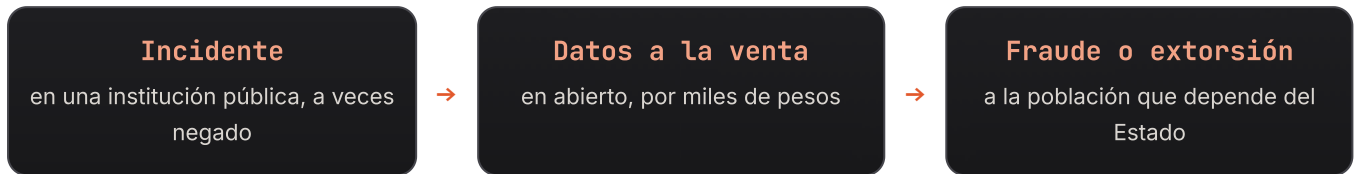
// después

- **jul 2025 · Sonora**. «Acceso no autorizado»; el portal «no fue vulnerado». Eran expedientes de niñas y niños.
- **sep 2025 · IMSS**. Atribuye una «posible filtración» al «uso indebido de accesos» de su personal.
- **may 2026 · Bienestar**. «No se trata de un hackeo», sino de un «acceso no autorizado».

El patrón **no empezó con la extinción del INAI**. En la conversación pública, los desmentidos son **aproximadamente el doble** que los reconocimientos, antes y después (ver la metodología). La cronología coincide: de los **27 incidentes en que los datos salieron de la institución**, 9 empezaron con un desmentido o con otro nombre para el incidente, 7 con un reconocimiento parcial o tardío y solo 4 con un reconocimiento claro; de los otros 13 (sitios alterados, cuentas secuestradas, caídas), 7 se reconocieron. **Se reconoce el sitio alterado; se niega la fuga de datos**. Y negar no elimina la obligación de avisar.

// 03 · hallazgo

El daño llega a la ciudadanía, con impactos aún desconocidos.



En junio de 2026, un medio local de Aguascalientes reportó que 26 personas fueron extorsionadas por quienes se hacían pasar por servidores públicos, con datos que el medio atribuye a un hackeo de la base del IMSS; la Policía Cibernética estatal investiga. No está confirmado que se trate de la misma base puesta a la venta en 2025. Lo mismo se repite con el registro de líneas celulares: el plazo oficial para registrarse se usó como gancho de fraude. El caso más grave para las mujeres: en febrero de 2026 se habrían expuesto más de 336 mil expedientes de violencia contra las mujeres de la Fiscalía de Guanajuato, con nombres de víctimas y agresores.

El costo de un incidente no lo paga solo la institución. Lo pagan sobre todo las personas que entregaron sus datos porque no tenían alternativa. Este daño casi no aparece en los informes de ciberseguridad, que miden sistemas y no personas.

// 04 · hallazgo

El robo y la venta de datos se ofrecen en abierto.

Buscamos en español ofertas para robar cuentas, espiar conversaciones y vender bases de datos, sin filtrar por país: **unas 270 mil menciones** en redes sociales abiertas, no solo en la *dark web*. Aunque en nueve de cada diez no se detecta un país, **circulan en redes accesibles desde México**, y unas 38 mil provienen de perfiles ubicados en México.



Clasificación por contenido (teléfonos +52, instituciones, lugares, moneda y comercios mexicanos), no por la ubicación que asigna la herramienta. Regla descrita en la metodología.

- Muchas ofertas siguen la misma plantilla: «contacta al hacker correcto», «disponible 24/7», «me ayudó a recuperar mi cuenta». Muchas son a su vez **estafas**.
- La ubicación que asignan las herramientas no es confiable: de las menciones ubicadas en México, solo ~9 % habla de México en el texto.
- **Con perspectiva de género:** abundan las ofertas para **espiar a la pareja**. La vigilancia en la intimidad es una forma documentada de violencia digital contra las mujeres, y este mercado la ofrece abiertamente.

// hallazgos · año por año

Tres años, tres momentos.

Promedios mensuales de publicaciones sobre incidentes de ciberseguridad que mencionan cada tema (sin comentarios); no es el debate total sobre cada tema. 2026 cubre enero a septiembre. Indicadores léxicos (ver la metodología).

INDICADOR (PROMEDIO MENSUAL)	2024	2025	2026
Publicaciones totales	3 009	2 991	2 644
CURP	22	64	91
Registro de líneas celulares	9	22	61
Datos biométricos	30	94	76
INAI o transparencia	212	141	106
Procesos electorales	452	246	274
Pegasus	170	230	113
Fiscalías	210	272	159
SAT	36	56	80
Desmentidos : reconocimientos	~2 : 1	~1,7 : 1	~2,8 : 1

2024 · El año electoral y de los grandes robos de información

- La conversación gira en torno a las **elecciones** (el mayor nivel del periodo) y a la **transparencia**, cuando el INAI todavía existe, aunque sin quórum desde abril de 2023.
- Robos de información a **instituciones centrales**: periodistas acreditados a la conferencia matutina, correos del gobierno capitalino, Consejería Jurídica de la Presidencia, carpetas de investigación de la Fiscalía de Nuevo León.
- El desmentido ya está presente («no fue hackeado») y aparece el **reconocimiento tardío**: una fiscalía hizo público en diciembre lo que detectó en febrero.

2025 · El año de la transición institucional

- Se extingue el INAI (marzo) y **se triplica la conversación sobre datos biométricos**, impulsada por la propuesta de acceso gubernamental a esos datos.
- Es el año con más menciones de **Pegasus** (investigación de la FGR) y de **fiscalías**, y con la acusación de EE. UU. sobre el C5 de la Ciudad de México.
- La venta de datos de **20 millones de pensionados del IMSS** lleva el problema de los sistemas a las personas. Las ofertas de robo y venta de datos desde perfiles ubicados en México se multiplican respecto a 2024, sobre todo en comentarios.

2026 · El año de la identidad digital y las filtraciones masivas

- Dentro de la conversación sobre incidentes, el **registro de líneas celulares** gana peso: su promedio mensual es unas 7 veces el de 2024. La CURP y el SAT alcanzan sus niveles más altos.
- Filtraciones de gran escala: **25 instituciones** en enero, **Programas del Bienestar** en mayo, sistemas de atención ciudadana en julio. La responsabilidad se traslada a **proveedores** y a **credenciales comprometidas**.
- Es el año con menos reconocimientos: **casi 3 desmentidos por cada reconocimiento** (año incompleto).

// preguntas abiertas

Lo que todavía no sabemos.

- **¿Se notifica a las personas afectadas?** No encontramos evidencia pública en ninguno de los casos documentados a fondo.
- **¿Qué hace el nuevo supervisor?** La filtración del IMSS se describió como el «primer gran reto» de la nueva unidad de protección de datos. No hemos localizado resoluciones públicas.
- **¿Cuáles son los 14 incidentes que reconoce el gobierno?** El Primer Informe de Gobierno (septiembre de 2025) reporta 14 incidentes relevantes de ciberseguridad en instituciones públicas en 11 meses, sin nombrarlos. En esos meses, nuestra cronología solo registra uno en una dependencia federal.
- **¿Hay recursos para prevenir?** Un análisis del IMCO y El Universal (abril de 2026) encontró que al menos cinco instituciones con incidentes recortaron su gasto en informática entre 2018 y 2025, hasta 85 % en términos reales. Falta saber cuánto de ese gasto va a seguridad.
- **¿Quién responde por los proveedores?** Si el incidente ocurre en el sistema de un contratista, ¿qué dice el contrato y quién rinde cuentas?
- **¿Cómo responden las instituciones sin un supervisor autónomo?** La supervisión se erosionó durante años (sin quórum en 2023, recorte en 2024, extinción en 2025). Para responder hay que documentar casos posteriores a la extinción, con codificación humana.

Responder estas preguntas es el objetivo de **After the Breach / Después de la brecha**, un monitoreo ciudadano que proponemos desarrollar en 2026–2027.

// método

Método.

El método, las fuentes de datos, la validación y los límites de este análisis se describen en el documento complementario **Después de la brecha · Metodología**.

// fuentes

Fuentes de los casos.

Diario Oficial de la Federación, 20-dic-2024 (reforma constitucional en materia de simplificación orgánica); nueva Ley General de Transparencia, vigente desde el 21-mar-2025. 2024: Expansión, La Jornada, Proceso e Infobae (periodistas, ene); R3D, Expansión y El Financiero (CDMX, abr); AMECI (Yucatán, may); Infobae y RíoDoce (Sinaloa, sep); El Financiero y R3D (Consejería, nov); Infobae, UnoTV y Latinus (Nuevo León, dic). IMSS: El Universal (sep-2025); Infobae (24-sep-2025 y 08-oct-2025); BI Noticias Aguascalientes (jun-2026). Filtración de 25 instituciones: El Financiero, Latinus e Infobae (30–31-ene-2026). Bienestar: Infobae, Aristegui Noticias y Político MX (29–30-may-2026). León: La Silla Rota y Periódico Correo (1–2-jul-2026). SIDAC: Infobae (29-ago-2026) y XEU. UNAM: Latinus (29-ene-2026) y El Universal (11-abr-2026). Primer Informe de Gobierno: IT Masters Mag (4-sep-2025). Gasto en informática: El Universal (11-abr-2026) e IMCO (13-abr-2026), con datos de la Cuenta Pública. Cronología: cobertura de prensa (≥2 medios por episodio).

Comentarios bienvenidos. Si tienes información sobre alguno de estos casos, sobre notificaciones a personas afectadas o sobre errores en este documento, escríbenos a info@cyber-cats.org.