iQSEC®
AI-DRIVEN CYBERSECURITY AND DIGITAL IDENTITY PROTECTION

Tendencias de **Ransomware**

2024–2025

La información presentada en este reporte es resultado del monitoreo continuo de amenazas que realiza IQSEC. Los datos aquí mostrados se basan en publicaciones realizadas por grupos de ransomware en sus sitios de filtración, donde suelen exhibir a las organizaciones que presuntamente han sido comprometidas. Es importante aclarar que estas publicaciones no equivalen necesariamente a incidentes confirmados de manera oficial, sino que representan indicios relevantes dentro del ecosistema de amenazas digitales.

¿Qué es el ransomware y por qué importa?

El ransomware es una de las **amenazas digitales más comunes y dañinas** en la actualidad. Opera como un **esquema de extorsión**, en el que los atacantes acceden a los sistemas de una organización, **cifran o bloquean información crítica** y exigen un pago para permitir su recuperación o evitar su divulgación pública.

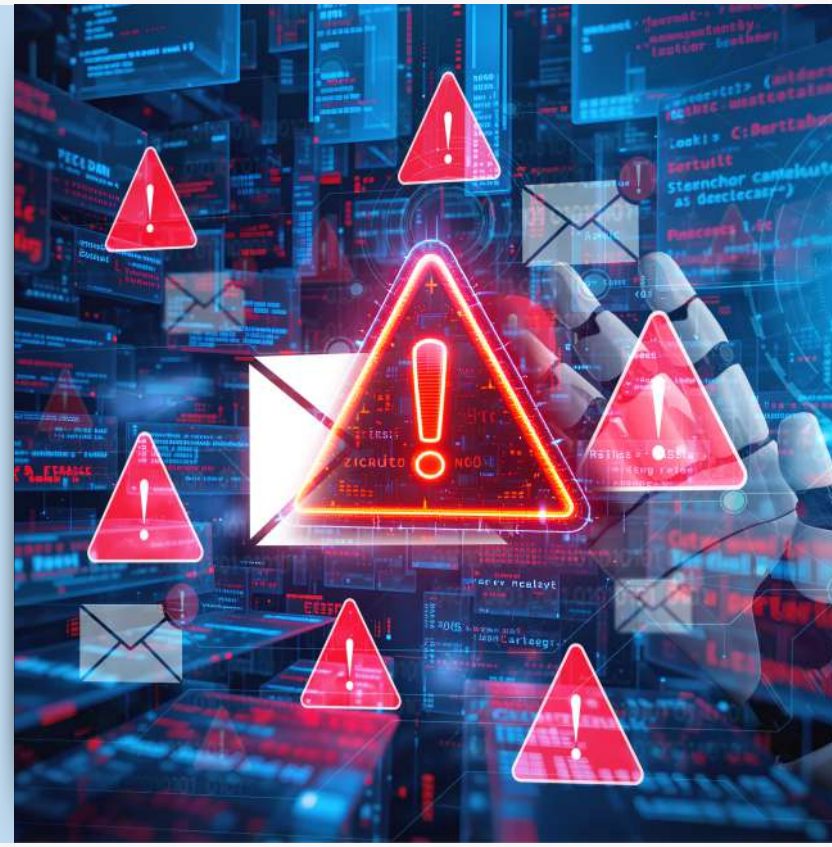
Más allá del componente técnico, su impacto real se refleja en:

- **Interrupción operativa**
- **Daño reputacional**
- **Presión directa sobre los equipos directivos**
- **Decisiones críticas bajo escenarios de crisis**

Vector de ataque más frecuente

La mayoría de los incidentes **no inician con exploits avanzados**, sino con:

- *Credenciales legítimas comprometidas*
- *Campañas de phishing dirigidas*
- *Malware para robo de contraseñas*
- *Falta de preparación organizacional*
- *Gobernanza de seguridad débil*



Hallazgos clave (global)

El panorama global del ransomware muestra una **tendencia clara y sostenida de crecimiento.**
Durante **2024** se registraron **5,319 presuntas víctimas**, mientras que en **2025** la cifra ascendió a **7,146 casos** (corte al 17 de diciembre de 2025), lo que representa un **incremento interanual aproximado del 34.5%**.

Lectura estratégica

El ransomware **no solo crece en volumen**, sino en **frecuencia, alcance sectorial y velocidad de ejecución**.
Estados Unidos se mantiene como el país más afectado a nivel global. En 2024 se reportaron **2,553 presuntas víctimas**, cifra que aumentó a **3,703 en 2025**, reflejando un crecimiento cercano al **45%** y un alto nivel de exposición digital.

Ecosistema criminal en expansión

103	146	+41.7%
grupos activos en 2024	grupos activos en 2025	de crecimiento

El ransomware se consolida como un modelo criminal profesionalizado, más que como eventos aislados.

México en el contexto global

En el caso de México, la evolución del ransomware es particularmente relevante. Durante **2024** se registraron **37 presuntas víctimas**, mientras que en **2025** la cifra aumentó a **74 casos**, lo que representa prácticamente el doble en un solo año.

Este crecimiento se refleja también en el ranking global:

Alerta país

México pasó del lugar **16 en 2024** al **lugar 11 en 2025**, **quedando a las puertas del Top 10 mundial.**

Este comportamiento confirma un **incremento del interés de los actores de amenaza** sobre el país.

Distribución geográfica

Top 10 países con más presuntas víctimas (publicaciones de grupos)

La concentración de ataques y víctimas en Estados Unidos es consistente con su poder económico y superficie digital, su volumen representa más del 50% de los casos del Top 10 en el 2025. México sube posiciones de forma relevante: el cambio de 2024 a 2025 lo acerca a los países con mayor exposición dentro del conjunto analizado.

2024		
Rank	País	Víctimas
1	United States	(2553)
2	Canada	(261)
3	United Kingdom	(240)
4	Germany	(154)
5	Italy	(128)
6	France	(128)
7	India	(114)
8	Spain	(104)
9	Brazil	(103)
10	Australia	(91)
16	México	(37)

2025		
Rank	País	Víctimas
1	United States	(3703)
2	Canada	(389)
3	Germany	(258)
4	United Kingdom	(231)
5	France	(161)
6	Italy	(155)
7	Spain	(137)
8	Brazil	(118)
9	Australia	(110)
10	India	(103)
11	México	(74)

Tabla 1. Top 10 países con más presuntas víctimas

Top 10 sectores más afectados

A nivel global, el patrón sectorial cambia de 2024 a 2025: el sector Salud (Healthcare) encabezó en 2024, mientras que los sectores de la Construcción (Construction) y Legal (Law) encabezan el primer lugar en 2025 (corte al 17 de diciembre de 2025), el sector de Bienes raíces (Real Estate) muestra un crecimiento particularmente marcado entre ambos periodos.

Rank	2024 (Sector)	2025 (Sector)
1	Salud	Construcción
2	Construcción	Salud
3	Manufactura	Legal
4	Educación	Manufactura
5	Legal	Educación
6	Finanzas	Bienes raíces
7	Equipamiento industrial	Finanzas
8	Servicios	Logística
9	Bienes raíces	Alimentos y bebidas
10	Software	Tecnologías de la información

Tabla 2. Sectores más afectados por ransomware en el 2024 y 2025.

En México, se observa un cambio relevante entre 2024 y 2025: en 2024 predominó el sector Manufactura, mientras que en 2025 el sector con mayor exposición pasa a ser Gobierno, seguido por Educación. Además, Tecnologías de la información y Manufactura se mantienen entre los sectores más afectados.

Rank	México 2024	México 2025
1	*Manufactura*	*Gobierno*
2	*Tecnologías de la información*	*Educación*
3	*Automotriz*	*Manufactura*
4	*Gobierno*	*Tecnologías de la información*
5	*Medios y entretenimiento*	*Bienes de consumo*

Tabla 3. Sectores más afectados en México 2024-2025.

Grupos de ransomware más activos (Top 10)

A nivel global, el comportamiento de los grupos de ransomware muestra cambios constantes en su liderazgo. Entre 2024 y 2025 se observa un relevo claro entre los actores más activos. Durante 2024, los grupos que encabezaron la actividad fueron RansomHub, LockBit y Play; sin embargo, en 2025 el primer lugar es ocupado por Qilin (Agenda), seguido por Akira y CL0P.

Este cambio refleja la naturaleza dinámica del ecosistema del ransomware, donde algunos grupos pierden protagonismo mientras otros emergen o se consolidan rápidamente. La

Rank	2024: Grupo	2025: Grupo
1	*Ransom Hub Ransomware Group*	*Qilin (Agenda) Ransomware Group*
2	*LockBit Gang*	*Akira Ransomware Group*
3	*Play Ransomware Group*	*CLOP Ransomware Group*
4	*Hunters International*	*Play Ransomware Group*
5	*Akira Ransomware Group*	*INC RANSOM*
6	*BlackBasta Ransomware Group*	*Safepay Ransomware Group*
7	*Medusa Ransomware Group*	*Lynx Ransomware Group*
8	*BianLian Ransomware Group*	*Ransom Hub Ransomware Group*
9	*Qilin (Agenda) Ransomware Group*	*Dragon Force Group*
10	*KillSecurity Ransomware Group*	*Medusa Ransomware Group*

Tabla 4. Grupos de ransowmare más activos a nivel mundial 2024-2025.

En el caso de México, el comportamiento de los grupos de ransomware también presenta cambios relevantes entre 2024 y 2025. Durante 2024, los grupos con mayor presencia fueron LockBit y RansomHub, concentrando la mayor parte de los casos publicados.

Sin embargo, en 2025 el liderazgo cambia de forma notable. Qilin (Agenda) pasa a ocupar el primer lugar, seguido por Kazu y CL0P, mientras que LockBit pierde protagonismo frente a estos nuevos actores. Este cambio confirma que el panorama de amenazas en México no es estático y que los grupos criminales se adaptan rápidamente, buscando nuevas oportunidades y ajustando sus operaciones para mantener su impacto.

Rank	2024: Grupo	Casos
1	*LockBit Gang*	10
2	*Ransom Hub Ransomware Group*	5
3	*Akira Ransomware Group*	2
4	*Cactus Ransomware Group*	2
5	*DarkVault Ransomware Group*	2

Rank	2024: Grupo	Casos
1	*Qilin (Agenda) Ransomware Group*	11
2	*Kazu Ransomware Group*	10
3	*CLOP Ransomware Group*	8
4	*LockBit Gang*	5
5	*Safepay Ransomware Group*	5

Tabla 5. Grupos de ransomware más activos en México 2024-2025.

Proyección de IQSEC hacia 2026

- México tiene alta probabilidad de ingresar al **Top 10 global**
- **Gobierno y Educación** seguirán concentrando incidentes
- Aumentarán los accesos iniciales vía **credenciales válidas**
- **Más phishing**, automatización y presión pública
- **Ataques más rápidos**, coordinados y competitivos

Hablemos de IQSEC

IQSEC es una empresa 100% mexicana con amplia trayectoria en ciberseguridad, criptografía, identidad digital e inteligencia artificial. Integramos capacidades propias de investigación, desarrollo y enfoque cyberlegal para anticipar riesgos mediante análisis continuo y soluciones tecnológicas diseñadas internamente.

Con implementaciones exitosas a nivel nacional, arquitecturas avanzadas como cybersecurity mesh y una visión consultiva independiente, acompañamos a organizaciones públicas y privadas en el fortalecimiento de su gestión de riesgo. **Nuestro Cyber Risk Operation Center (CROC)**, junto con **programas de formación y semilleros de talento**, refleja un compromiso activo con la resiliencia digital y el impacto social.

Para más información:
www.IQSEC.com.mx