



En el cuarto informe se documentaron **102 casos de ciberviolencia en Guatemala**.

Aunque los ataques verbales y discursos de odio siguen vigentes, el informe revela una **alarmante evolución y complejidad respecto a las agresiones virtuales** que se han diversificado hacia el engaño, fraudes económicos, control digital y acceso no autorizado. Estas conductas, fuertemente potenciadas por el anonimato y dinámicas colectivas, no solo reproducen desigualdades sociales preexistentes afectando a ciudadanos individuales, sino que **ahora escalan de forma alarmante mediante el uso de inteligencia artificial y ciberataques** dirigidos a la infraestructura de instituciones públicas y privadas.

01 PRINCIPALES HALLAZGOS DEL CUARTO INFORME



Se reportó un notable incremento de casos intrusivos y utilitarios orientados a la obtención de dinero, datos sensibles o el control de cuentas digitales mediante el engaño, fraude y la manipulación virtual.



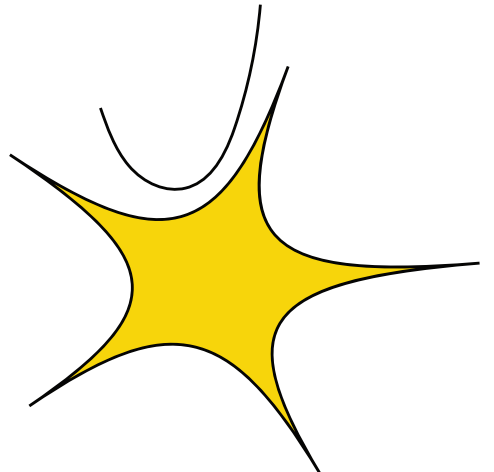
El fenómeno mantiene una fuerte naturaleza colectiva: el 44% de los agresores actúa en grupos de individuos y en el 33% de los casos la identidad es desconocida. El anonimato que propician las redes sociales y el ciberespacio son clave para amplificar y coordinar estos ataques.



Se consolidó el uso ilícito de nuevas tecnologías como la inteligencia artificial para crear contenido falso, difamatorio y suplantar identidades. Además, la violencia trascendió los ataques individuales, registrándose hackeos masivos a bases de datos de instituciones públicas y empresas privadas en Guatemala.



El entorno digital reproduce la discriminación social y agudiza la violencia de género. Las mujeres sufren ataques orientados principalmente a su sexo o género, apariencia física y rol profesional; mientras que los perfiles masculinos son agredidos por su actividad profesional, capacidad intelectual, origen étnico u orientación sexual.



02 DATOS DESTACADOS

41% de los casos **correspondieron de forma aislada** a ataques verbales y discursos de odio.

40% de las acciones violentas se concentraron en **tácticas de engaño, fraude y manipulación**.

28% de los afectados **manifestaron consecuencias directas** comprobadas como daños reputacionales, pérdidas económicas o crisis emocionales.

51% de las víctimas afectadas fueron **personas individuales**.

56% **Facebook** se mantienen como las **principales plataformas** donde se perpetran los incidentes.
19% **WhatsApp**



03 CASOS E HISTORIAS



CASO DE DIFAMACIÓN Y ENGAÑO

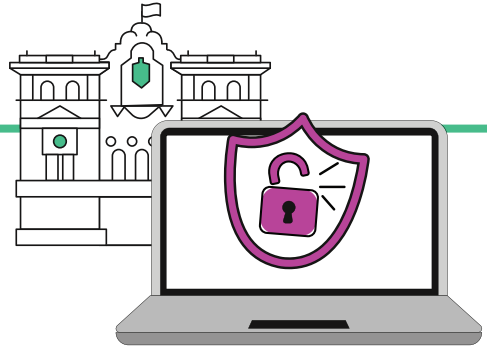
El 15 de abril de 2026, la página Noticias de Impacto Guatemala difundió una **noticia falsa** sobre la supuesta captura de una extorsionista apodada "la reina". Utilizaron una imagen sugerente **generada con inteligencia artificial para engañar**, atraer al público masculino y **aumentar de forma fraudulenta las interacciones y vistas en la plataforma**.

CASOS DE ACCESO NO AUTORIZADO, VULNERACIÓN DE SISTEMAS Y ATAQUES INFORMÁTICOS



CIBERATAQUE MASIVO A UNIVERSIDADES

El hacker "MrGoblinciano" vulneró los sistemas de la Universidad de San Carlos (Usac) y la Universidad Rafael Landívar (URL). **Comprometió información financiera y nóminas** de la Usac, y filtró **datos personales** junto a 84,620 fotografías de estudiantes y docentes de la URL.



HACKEO A PORTALES GUBERNAMENTALES

El atacante "NemorisHacking" (vinculado al grupo "JXLLTEAM") **ejecutó una serie de ofensivas cibernéticas** dirigidas contra los portales institucionales de la Procuraduría General de la Nación (PGN) y la Superintendencia de telecomunicaciones (SIT), **comprometiendo la seguridad informática del Estado**.

