

SECCURACY
Certeza en seguridad de la información

ESTADÍSTICAS DE FRAUDE EN BILLETERAS VIRTUALES

Reporte de Situación Argentina 2026

* Un análisis integral basado en UFECI, BCRA y consultoras líderes.

CRECIMIENTO DEL FRAUDE GENERAL

34.468 denuncias por delitos informáticos en 2024

Incremento del 21,1% respecto al año anterior.

Fuente: [Chequeado](#).

SECCURACY
Certeza en seguridad de la información

ACCESO ILEGÍTIMO Y VULNERABILIDAD



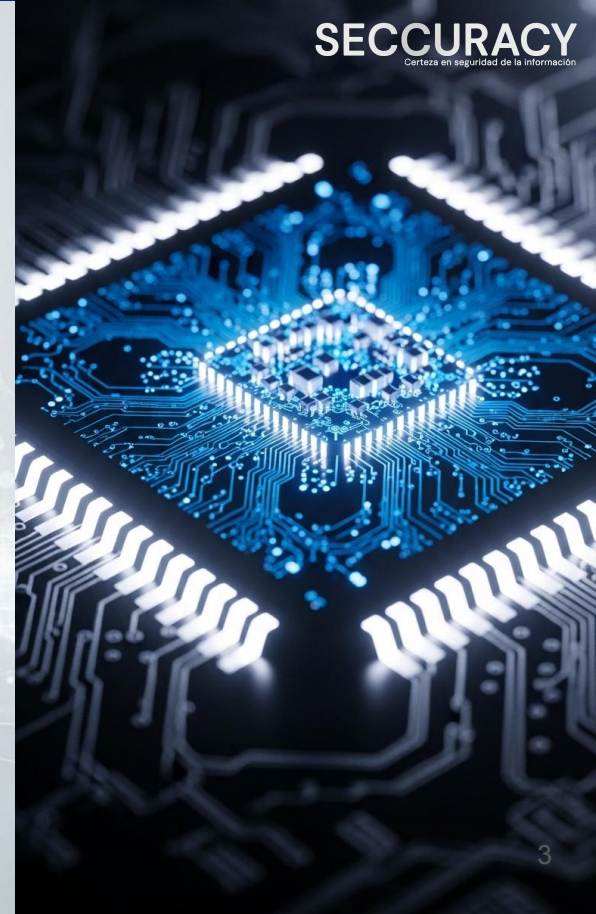
Mercado Pago (26%): segunda plataforma más atacada después de WhatsApp (30%)

Impacto: El 20% de los usuarios y el 18% de los comerciantes sufrieron hackeos de cuenta.

Exposición: 60% de las personas reportó robo de tarjetas o datos bancarios.

Fuente: [Chequeado](#).

SECCURACY
Certeza en seguridad de la información



¿QUÉ PASA DESPUÉS DEL FRAUDE?

43% Logró devolución total.

35% Resolución parcial (con pérdida de dinero).

22% Sin solución alguna.

Reclamos: Defensa al Consumidor CABA registró un aumento del 43% en reclamos (672 casos en 2024).

Fuente: [100% SEGURO](#), [La Nación](#).

SECCURACY
Certeza en seguridad de la información

METODOLOGÍAS: DEL ENGAÑO AL CONTROL



Phishing: 75,5% de las amenazas generales.
100% de los casos en el sector Fintech.



Smishing: Estafas vía SMS/Mensajería (Caso Payoneer).



Ingeniería Social: Robo de código de verificación de WhatsApp para suplantación.



Software de Acceso Remoto (RAT): Enlaces que permiten el control total del dispositivo y toma de préstamos.

Fuente: [La Nación](#), [infobae](#), [Chequeado](#).



NUEVAS FRONTERAS DEL DELITO



SIM Swapping: Duplicación de SIM para saltar la seguridad bancaria.



Compra ilegal de CVU/CBU: Mercado negro en redes sociales para lavado de dinero.



Spoofing: Suplantación de IP, correos o dispositivos.



Perfiles Falsos: Identidades falsas de entidades financieras en redes sociales.

Fuente: [Chequeado](#), [100% Seguro](#), [infobae](#), [La Nación](#).

SECURACY
Certeza en seguridad de la información



BUENAS PRÁCTICAS Y ACCIONES

Estrategias de prevención y respuesta inmediata

SECCURACY
Certeza en seguridad de la información

BUENAS PRÁCTICAS Y PREVENCIÓN

SECURACY
Certeza en seguridad de la información

Dispositivo: Contraseña robusta/biometría y PIN en la tarjeta SIM.

Cuenta: Activar 2FA independiente del SMS (Google Authenticator). Jamás compartir copias de DNI o PIN.

Contactos: Las entidades nunca piden datos por teléfono. Desconfiar de "actualizaciones de datos".

¿CÓMO REACCIONAR?

SECURACY
Certeza en seguridad de la información



Reportar a la billetera/banco de inmediato.



Denunciar en UFECI, Policía Federal y Defensa al Consumidor.



Preservar evidencia: Capturas de pantalla y mensajes originales.

Fuentes principales

Fuentes	Tipo
UFECI (Ministerio Público Fiscal)	Oficial estatal
BCRA	Oficial regulatorio
Fiserv – “Números que hablan”	Consultoría privada
Consultora Kantar	Encuesta de mercado
Defensa al consumidor C.A.B.A.	Oficial municipal
La Nación / Chequeado / Infobae	Medios especializados

Certeza en seguridad de la información.

Informe desarrollado por **SECCURACY**

Febrero 2026



www.seccuracy.com.ar