# smartid

# Prevención de fraude inteligente

## Cero fricción

Plataforma AI para banca digital

+125 mil millones de transacciones · +12 mil millones de sesiones protegidas

# El Fraude Financiero en LATAM

Causa pérdidas millonarias en LATAM.

Las soluciones tradicionales ya no bastan.

Nuestra Suite ha logrado cero fraudes en canales electrónicos para nuestros clientes.

SmartID es un servicio de seguridad en la nube impulsado por Inteligencia Artificial que identifica usuarios, dispositivos y transacciones, permitiendo la prevención en tiempo real del fraude cibernético

smartid

# El fraude digital en LATAM
# CRECE EXPONENCIALMENTE

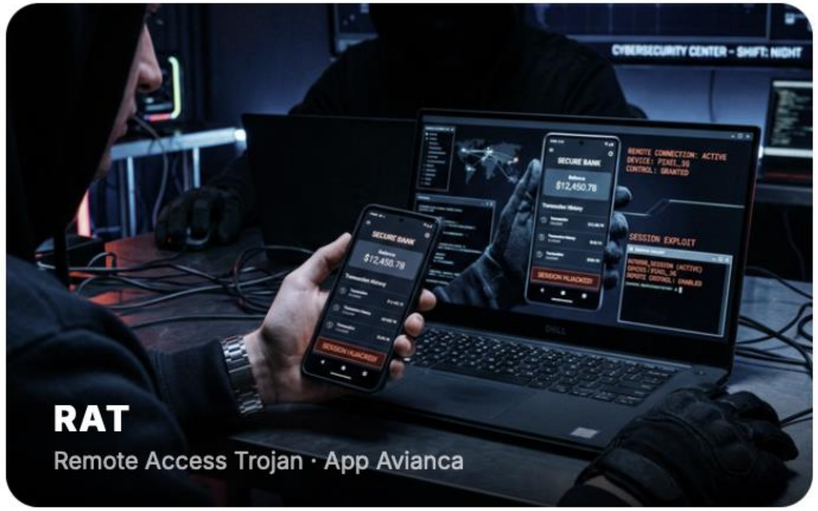
## Aumento Alarmante
83% de aumento en reporte de fraudes por parte de las organizaciones financieras en LATAM — Kaspersky 2025

## 4X Malware Móvil
Troyanos bancarios en smartphones se cuadruplicaron en 2025 vs 2024. — Kaspersky 2025

## 3x Robo Dispositivos
Casos de fraude por dispositivos robados o comprometidos se triplicaron en la región. — BioCatch 2025

# Casos reales de fraude en LATAM

## ULTIMOS 3 MESES

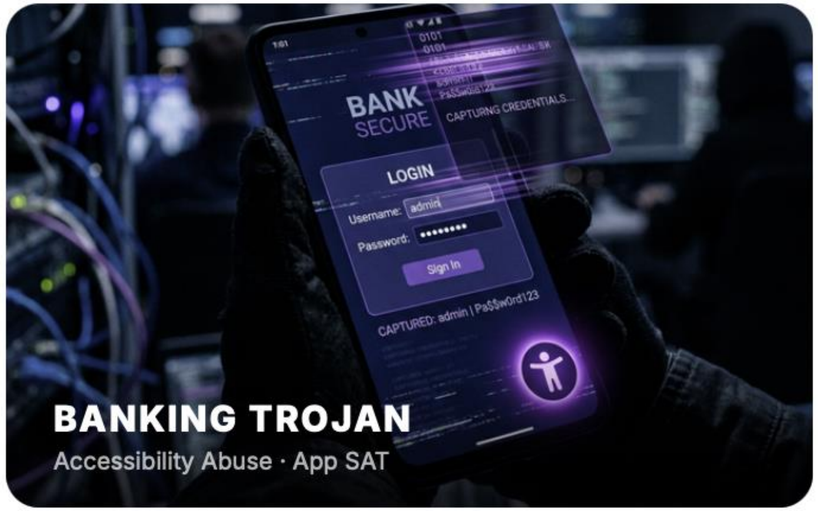



**RAT**

Remote Access Trojan · App Avianca


**SPYWARE**

Info-Stealer




**BANKING TROJAN**

Accessibility Abuse · App SAT


**INJECTION ATTACK**

Bypass biométrico · Deepfake / Video

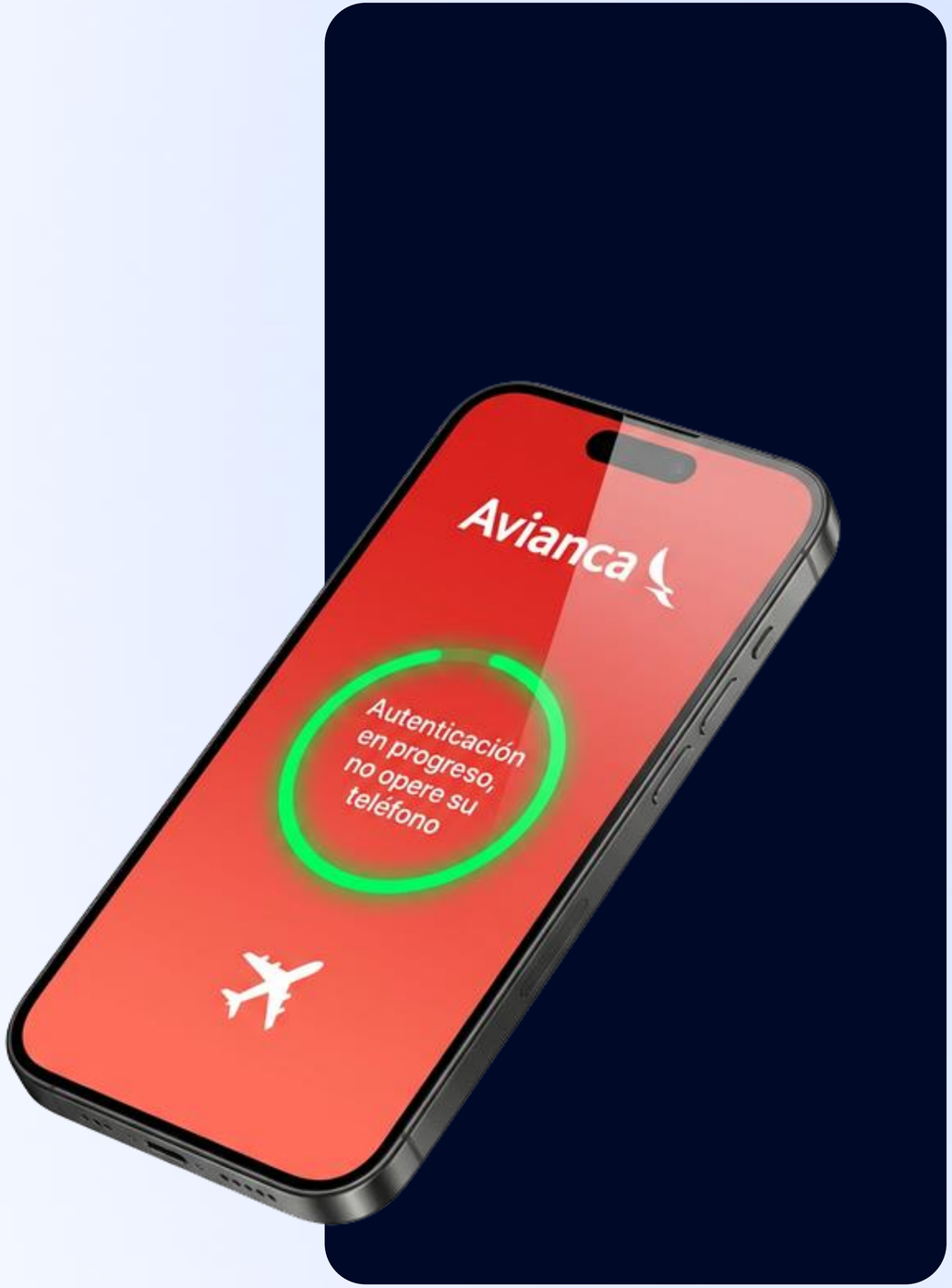
smartid

## RAT – Diciembre 2025

# APP AVIANCA

El usuario descarga una app falsa de Avianca que contiene un RAT (Remote Access Trojan). Una vez instalada, el atacante toma **control remoto del dispositivo en tiempo real**: habilita screen sharing, y despliega una pantalla falsa (overlay) que cubre la app bancaria. Mientras el usuario cree ver su banca normal, el atacante opera la cuenta por detrás — transfiriendo fondos, cambiando contraseñas o registrando nuevos beneficiarios.

- **Identificación de herramienta de acceso remoto.**
- **Detección de pantalla del dispositivo transmitida a un tercero.**




smartid


## SPYWARE – Diciembre 2025

# APP PUNTOS

El usuario recibe un enlace de una app falsa que simula un programa de recompensas del banco. **Este malware opera de forma completamente silenciosa en segundo plano**.

Leer SMS silenciosamente para interceptar códigos 2FA
Grabar cámara y micrófono capturando conversaciones y rostros
Extraer la lista de contactos para propagar el ataque a más víctimas

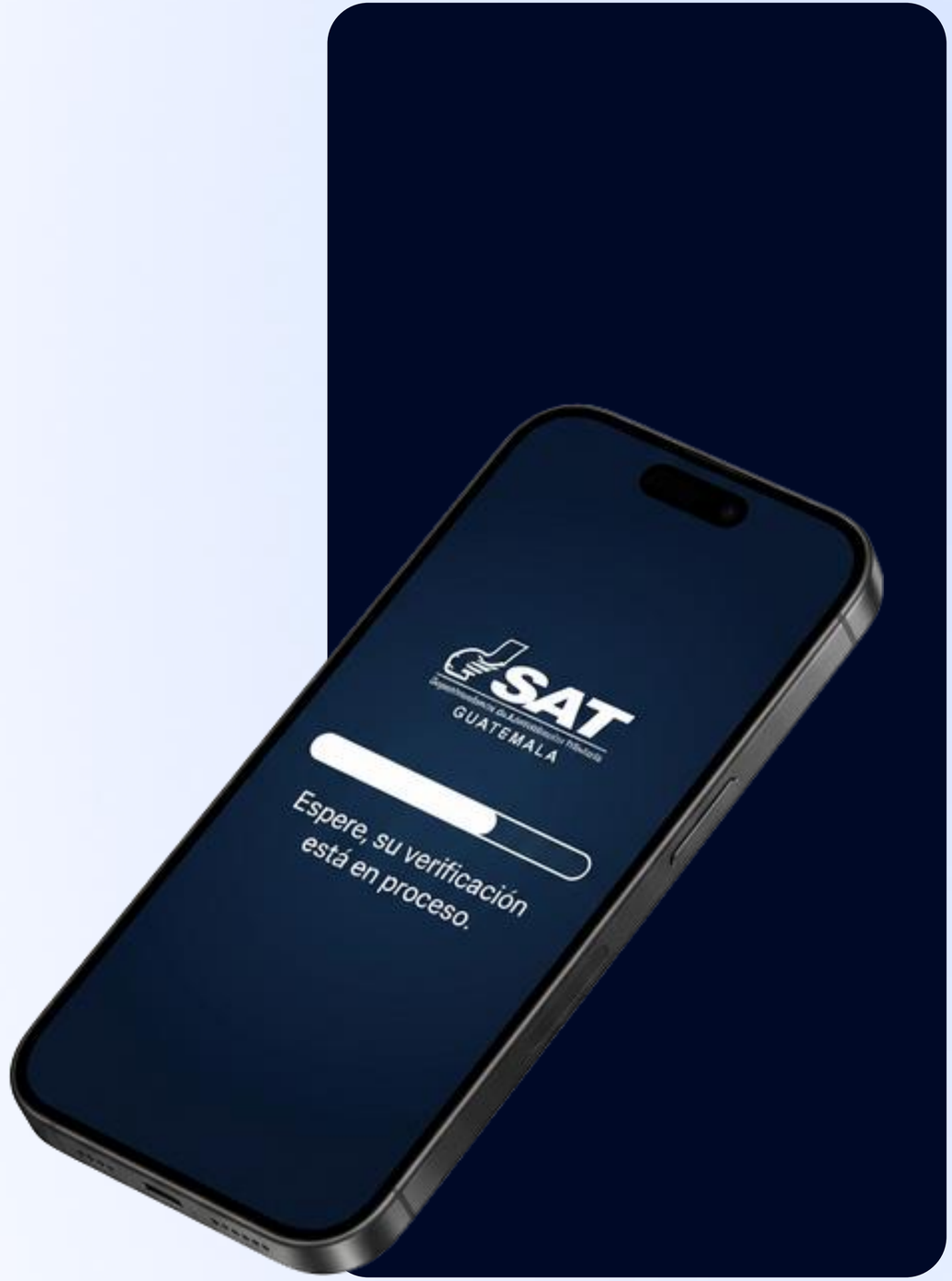
- **Verificamos la integridad del dispositivo a nivel de Google**
- **Device binding**
- **Velocicity Checks + Geo-Anomaly Detection**

## BANKING TROJAN – Enero 2026

# APP SAT

El usuario descarga una app falsa de la SAT que solicita habilitar el **Servicio de Accesibilidad** de Android. Una vez activo, el troyano monitorea la pantalla en tiempo real, detecta cuándo se abre la app bancaria, captura credenciales automáticamente y ejecuta transferencias sin intervención humana. Es el mismo vector que usan Grandoreiro y BrasDex — las familias de malware bancario más peligrosas de Latinoamérica.

- **Detección de aplicaciones no autorizadas con servicios de accesibilidad**




smartid


## INJECTION ATACK – Febrero 2026

# VIRTUAL CAMERA

El atacante utiliza una cámara virtual para alimentar un deepfake o grabación pregrabada directamente al proceso de verificación biométrica del banco. El sistema cree que la persona está presente físicamente cuando en realidad recibe una identidad sintética generada con IA. No requiere malware ni acceso al dispositivo — es un ataque directo contra la prueba de vida.

- **Detección de camaras virtuales**
- **Stream inyectado.**
- **Prueba de vida activa/pasiva**
- **Deepfake Score**

smartid

# Solución integral

MONITOREO DE OPERACIONES Y TRANSACCIONES

VERIFICACIÓN DE IDENTIDAD

AI Y MACHINE LEARNING

RECONOCIMIENTO DE DISPOSITIVO

MULTIPLE FACTOR DE AUTENTICACIÓN

smartid

# ¿Cómo funciona?

Estrategia de seguridad cibernética integrada y cumplimiento normativo


ANTES DEL LOGIN

### Spoofing Prevention

Evaluamos el dispositivo antes de permitir el acceso: root, jailbreak, emuladores, VPN, apps maliciosas, cámaras virtuales, liveness y deepfake detection.

**52+ señales en <100ms**

DURANTE LA SESIÓN

### Session Intelligence

Perfilamos el comportamiento de cada usuario. Detectamos anomalías: ubicación imposible, dispositivo nuevo, ritmo de interacción inusual, acceso remoto.

**Monitoreo continuo 24/7**

EN CADA TRANSACCIÓN

### Transaction Risk Scoring

Un score de riesgo 0-100 por operación, combinando señales de dispositivo, historial del usuario y contexto. Decisiones automáticas e inteligentes.

**Motor de reglas configurable**

smartid

# Resultados comprobados
# en la región

**+95%**
**Precisión en detección de fraude**

**+125MMM**
**Transacciones protegidas**

**+12MMM**
**Sesiones protegidas**

Cero fricción – el usuario legítimo no nota la protección

No reemplaza – se agrega a su stack de seguridad actual

Consola 360° - Visibilidad total de dispositivos, sesiones y transacciones

SDK ligero – Integración en días, < 200kb

Experiencia con bancos en la región

Certificación ISO27001 en segurdad de la información

smartid

# Piloto de 30 días

## sin costo de integración

En 30 días verá exactamente cuántos ataques no detecta hoy
y cuántos falsos positivos puede eliminar.

https://smartidsuite.ai  sales@smartidsuite.ai  ISO 270001 Certified