



México Summit 2026

Innovación con **propósito**



De las Tendencias de Fraude a la Confianza Digital: El Futuro de la Prevención de Fraude

Miguel Rivera

Director Senior, Soluciones de Fraude e Identidad
TransUnion LATAM

Oscar Ariza

Gerente Senior, Soluciones de Fraude e Identidad
TransUnion LATAM

Agenda

01

Contexto LATAM

- El fraude evoluciona hacia la identidad
- LATAM enfrenta una presión superior a la del promedio global
- La batalla es desigual
- La respuesta es inteligencia conectada

02

Profundización en México

- ¿Qué hace distinto al mercado mexicano?
- TransUnion México + Buró de Crédito
- Cómo nuestras soluciones de fraude habilitan la inteligencia conectada

El fraude se desplaza de la transacción hacia la identidad

+83%

Crecimiento del robo de identidad, el mayor entre los tipos evaluados

+37%

Crecimiento de apropiación de cuentas

78.5%

Del volumen de fraude sospechoso en LATAM ocurrió en la etapa de login

Epidemia de suplantación

Phishing /
Vishing

Credenciales

Robo de
identidad

Apropiación de
cuentas

El fraude se desplaza hacia etapas tempranas y hacia riesgos de identidad cada vez más sofisticados y difíciles de detectar

La composición por tipología de fraude está cambiando

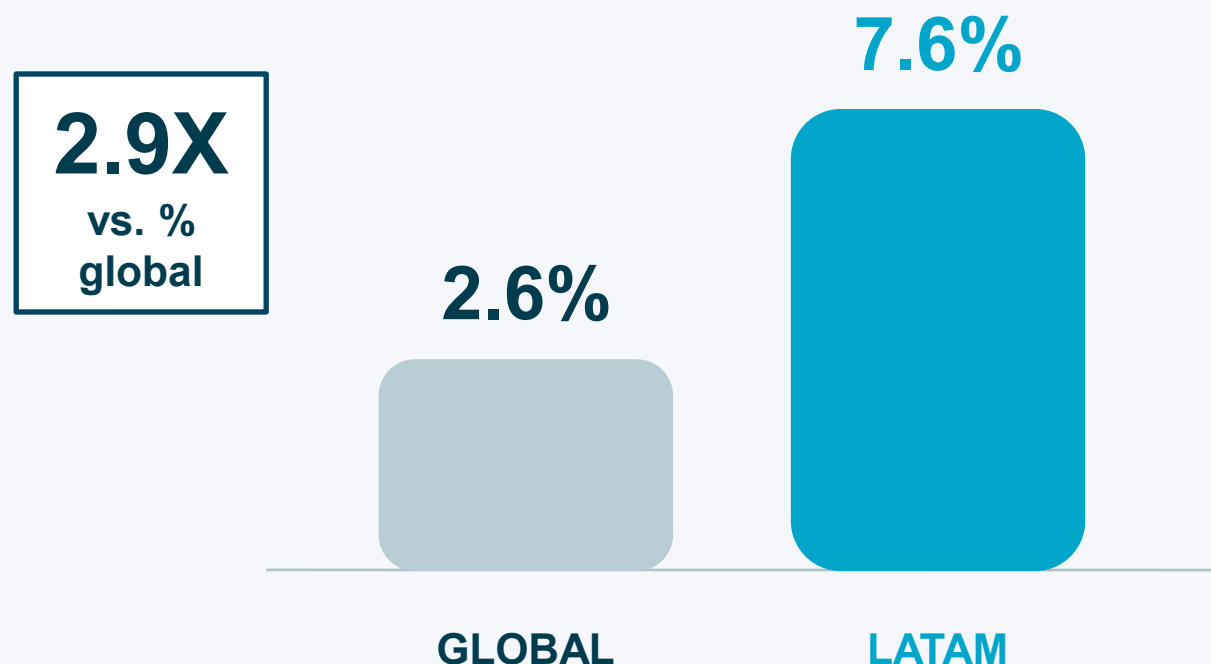
Datos globales | Participación de fraude digital sospechoso 2025 y Crecimiento anual en la participación contra 2025



Las modalidades asociadas con identidad y acceso son las que más rápido crecen, mientras las estafas siguen siendo las más prevalentes

LATAM enfrenta una presión de fraude significativamente superior al promedio global

Tasa de fraude digital sospechoso entre transacciones asociadas con suscriptores | H1 2026



¿DÓNDE SE MANIFIESTA?

- 78.5%** del volumen de fraude sospechoso en LATAM ocurrió en login
- 8.9%** de los intentos de login en LATAM fueron sospechosos
- 10.4%** Servicios Financieros, industria con mayor participación de fraude sospechoso en la región

LATAM no solo opera por encima del benchmark global—la presión se extiende a lo largo del ciclo de vida

La creación de cuentas concentra la mayor participación de sospecha de fraude global

Participación de fraude digital sospechoso por etapa del recorrido del cliente

Creación de cuentas

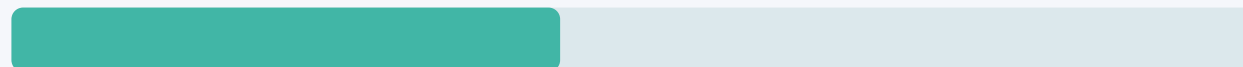
Registro, alta de cuentas y originación



8.3%

Inicio de sesión

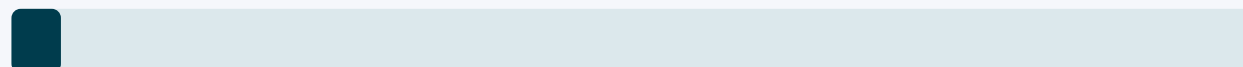
Accesos e intentos fallidos de login



4.3%

Transacciones financieras

Compras, retiros y depósitos



2.8%

La creación de nuevas cuentas fue la etapa con mayor crecimiento en sospechas de fraude digital, seguida por inicio de sesión

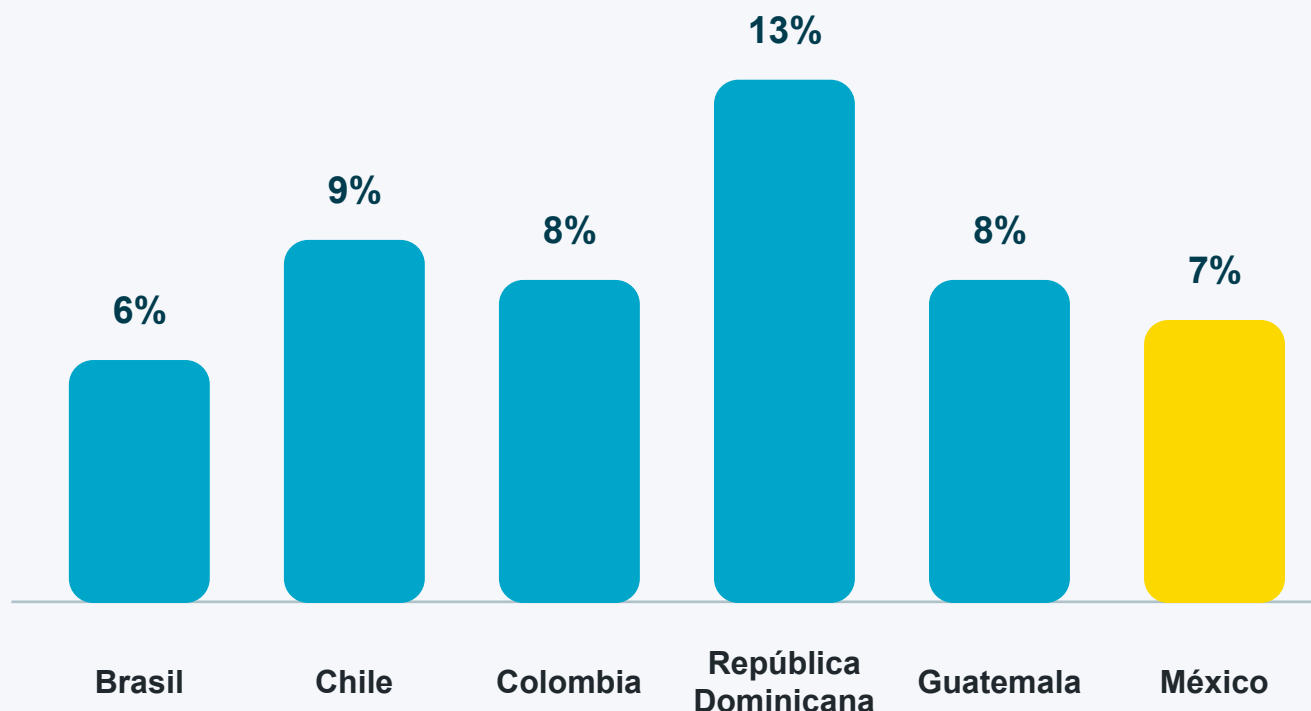
Las comunicaciones son el nuevo campo de batalla de la confianza

VISHING

Es el esquema más reportado por consumidores objeto de fraude en Brasil, Chile, Colombia y México

La confianza puede romperse antes del onboarding, a través de llamadas y otros canales de comunicación.

Consumidores que dijeron haber sido víctimas de fraude digital en los últimos tres meses



La lucha contra el fraude no es equitativa

DEFRAUDADORES

- Adoptan rápidamente nuevas tecnologías
- Automatizan y escalan ataques
- Combinan identidades, credenciales y canales
- No cargan con regulación ni fricción de cliente

EMPRESAS REGULADAS

- Deben cumplir regulación y privacidad
- Deben preservar la experiencia del cliente
- Operan con datos y controles fragmentados
- Asumen fraude y falsos positivos

26%

De los
consumidores
reportó pérdidas
por fraude

US\$1,671

Costo promedio de
pérdida



**Seguridad +
experiencia**

Para equilibrar la balanza: datos confiables + inteligencia compartida + visión integral del consumidor

La ventaja no es otro control - es la inteligencia conectada

¿Cómo verificar que una persona es real, legítima y consistente, en diferentes canales y a través del tiempo?



UNA VISIÓN DE RIESGO DE FRAUDE END-TO-END

Verificación de identidad unificada + IA + señales conectadas

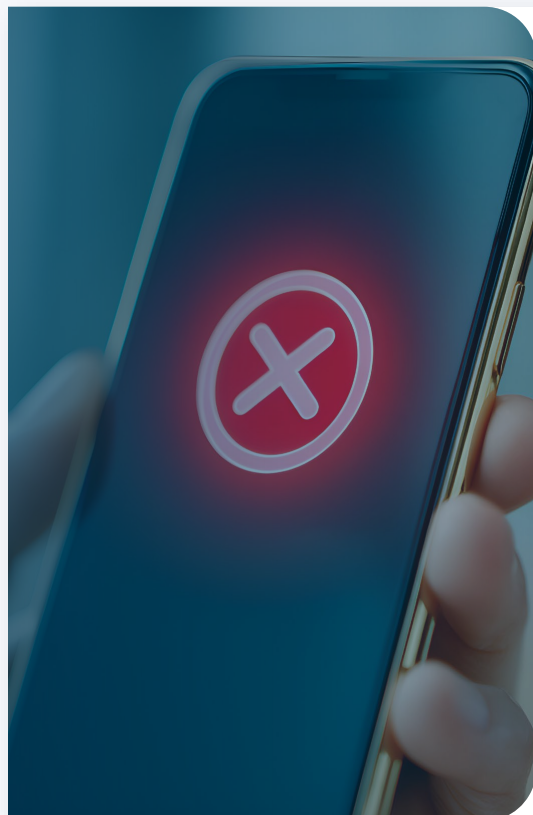
Detectar antes | Reducir fricción | Aprobar más clientes legítimos



**¿Qué significa este cambio
para México?**

Los canales digitales siguen siendo un entorno de riesgo...

Los defraudadores evolucionan y adaptan sus tácticas mejorando su sigilo y efectividad



- ! Los canales digitales ofrecen anonimato y escalabilidad a los atacantes
- ! La automatización multiplica el alcance de los ataques
- ! Los esquemas de fraude cada vez más sofisticados logran evadir los controles tradicionales

El tráfico automatizado ya supera al tráfico humano globalmente

El 51% del tráfico web global es generado por sistemas automatizados, y de este total, el 37% corresponde a bots maliciosos**

El 2.1% de las transacciones digitales en México exhibe señales asociadas a intentos de fraude*

...afectando al consumidor mexicano

Participación de Fraude Digital Sospechoso

6.3%

Creación de cuentas

Suplantación de identidad, identidades sintéticas, bots

5.8%

Inicio de sesión

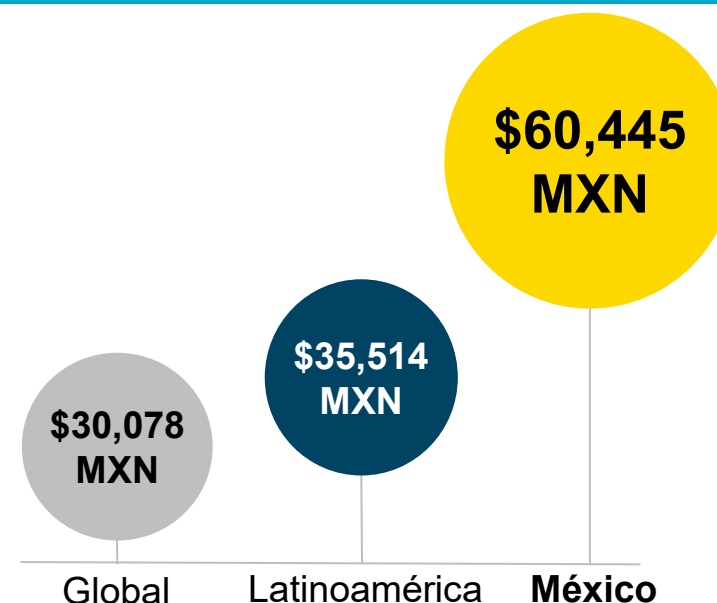
Robo de información (vishing, phishing), scams, brechas de información

1.4%

Transacciones financieras

Compras y pagos fraudulentos, medios de pago no autorizados

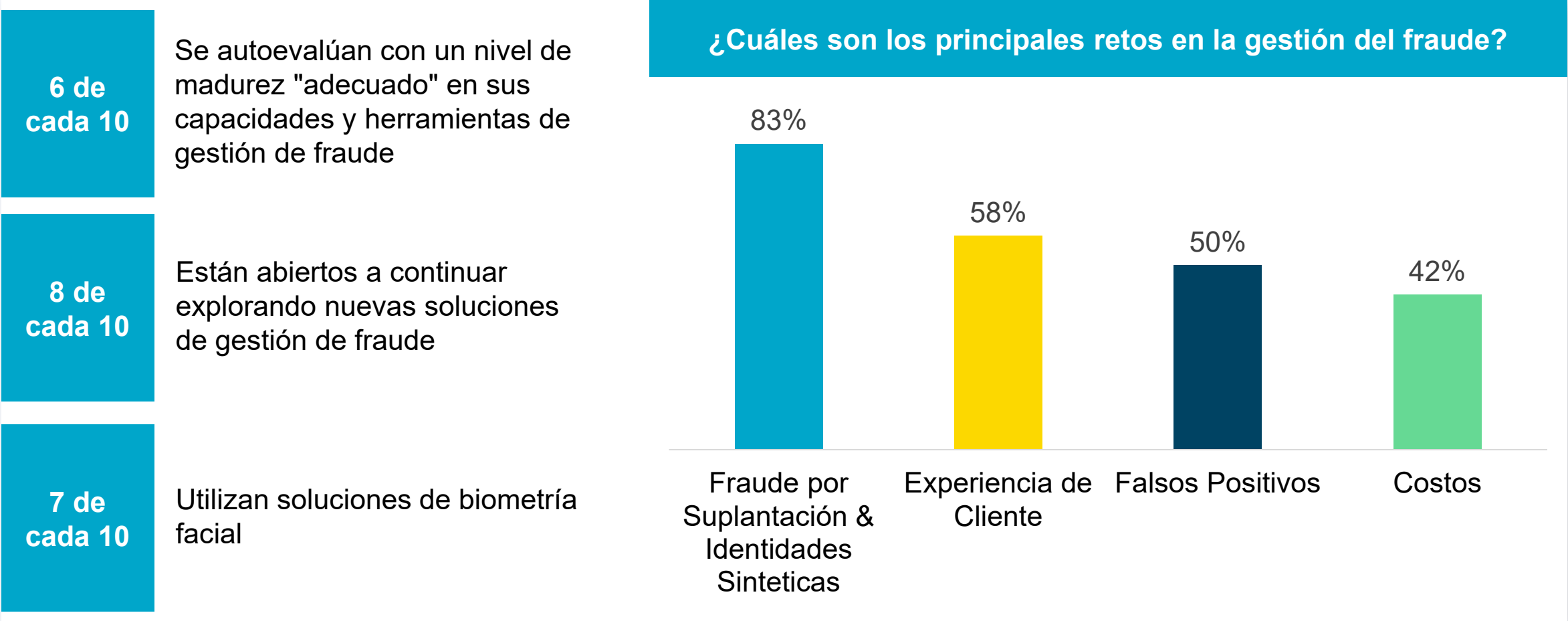
Impacto al Consumidor con Pérdidas Reales



Pérdida mediana por fraude reportada en pesos mexicanos entre los consumidores que indicaron haber perdido fondos a causa del fraude digital durante el último año

¿Dónde identifican los otorgantes los retos reales?

Resultado de encuestas realizadas a otorgantes de crédito en México – Abril 2026



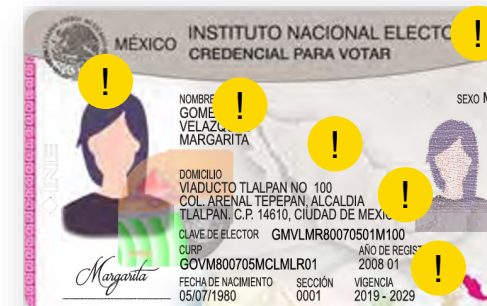
Los defraudadores utilizan esquemas más sofisticados...



**Tácticas de fraude
basadas en la identidad
impulsadas por IA**

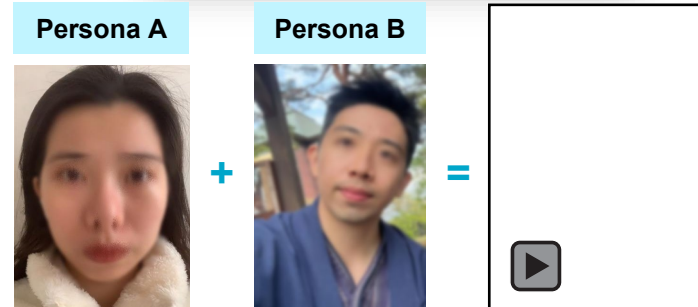
Manipulación de documentos

- Credenciales INE manipuladas
- Utilización de GenAI para crear réplicas hiper realísticas



Videos e imágenes deepfakes

- Rostros generados por IA, selfies animadas, face-swap en tiempo real
- Ataques de inyección y presentación



Construcción y uso de identidades sintéticas

- Datos reales y ficticios combinados en nuevas identidades
- GenAI para crear y validar identidades



...que nos retan a proteger las validaciones de identidad biométrica...

La identidad digital deja huellas más allá del rostro con una constante creación de historia



Identidad Estática

Verificación puntual

-  Credencial INE, CURP
-  Biometría Facial
-  Transacciones de un mismo sitio web
-  Contraseñas

Identidad 360°



Cada señal responde a una pregunta distinta. La verdadera ventaja aparece cuando todas cuentan la misma historia



Identidad Viva

Confianza Continua

-  Comportamiento y contexto del dispositivo utilizado
-  Reportes de intentos sospechosos de fraude
-  Reputación completa de identidad digital
-  Actividad conductual

...mediante el valor colectivo de millones de señales

Impulsadas por el ecosistema local y global de datos de TransUnion para reforzar validaciones de identidad



Mercado & Experiencia

- Profundo entendimiento de los servicios financieros en México y en el mundo.
- Experiencia mundial en la gestión de fraude en más de 45 mercados.



Datos & Señales Locales

- 131 millones de expedientes de personas físicas.
- Señales y alertas basadas en análisis de quebrantos e inconsistencias de datos.
- 750 mil transacciones mensuales en nuestras herramientas colaborativas de mitigación de fraude.

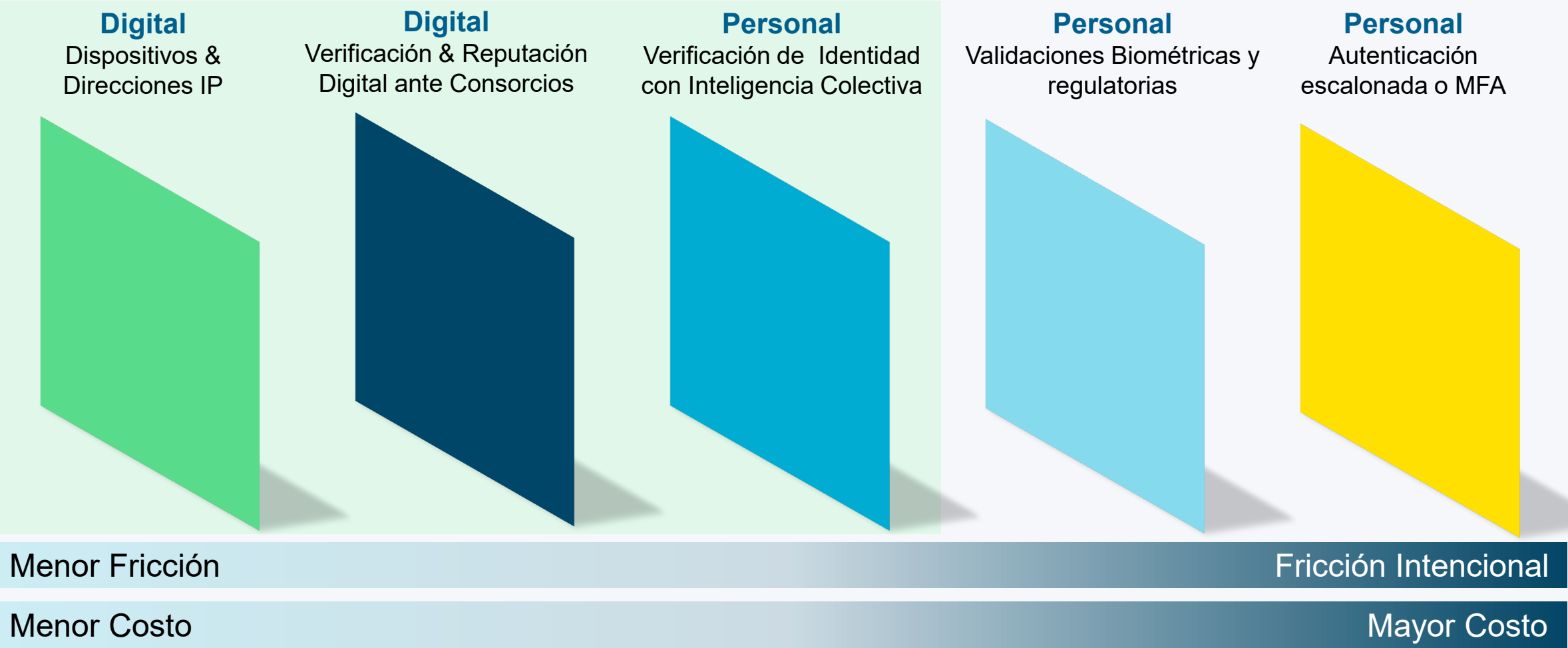


Datos & Señales Globales

- Red Global de Inteligencia mundial y multisectorial de información de dispositivos, protegiendo a más de 40 mil sitios webs y apps.
- Validaciones y reputación global de la identidad digital.
- Fuente de información de direcciones IP más confiable y reconocida a nivel mundial.

Habilitamos múltiples capas de confianza en cada interacción...

Reforzando validaciones de identidad biométricas y regulatorias con nuevas soluciones modulares



...que construyen confianza ante el fraude organizado...

Caso – Banca Digital realizando apertura de cuentas y tarjetas de crédito en canal web

Banca CO

Desafíos



Aumento en aplicaciones fraudulentas y pérdidas por suplantación



Control de Documento y Selfie en todas las solicitudes como medida de control con revisiones manuales



Solución



Análisis inteligente de la identidad digital en el canal web



Análisis de reputación del dispositivo mediante la Red Global de Inteligencia de TransUnion



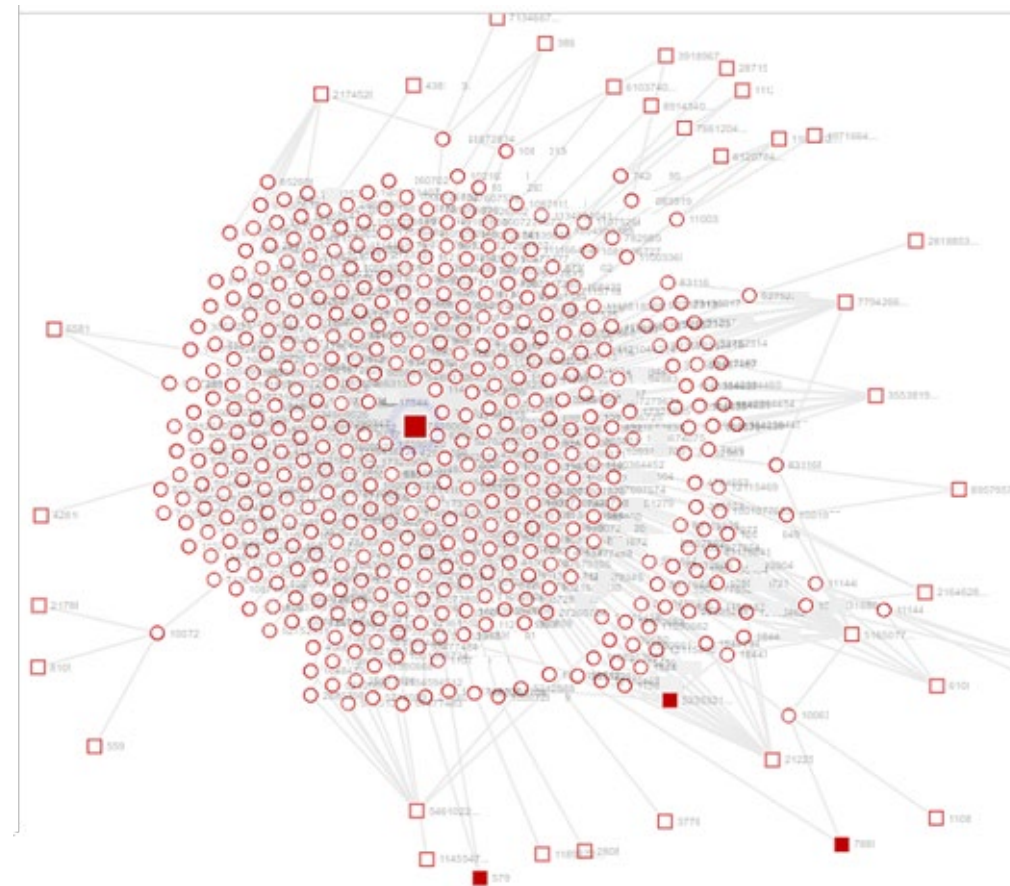
Resultados

- Reducción de la fricción en el 82% de las solicitudes
- Protección de 250K USD en 4 meses

Con un ticket promedio de 5.4K USD, se logró detectar y detener un total de 47 casos en los primeros 4 meses

+446 posibles casos de fraude en revisión

- Intento de 734 aperturas asociadas a 446 cédulas y 37 dispositivos vinculados a un dispositivo catalogado como fraudulento.



...permitiendo continuar innovando con propósito

Reconociendo que ninguna señal cuenta toda la historia por sí sola

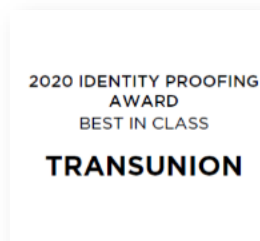


La confianza no proviene de una señal perfecta
Proviene de conectar todas las señales disponibles de la identidad estática e identidad viva

Apalancándonos en la inteligencia colectiva y la colaboración



Las organizaciones líderes ya no verifican únicamente identidades
Verifican y participan en ecosistemas completos de señales digitales para equilibrar crecimiento, fraude y experiencia.





¡Muchas gracias!



Queremos conocer su opinión.

Por favor escanee el Código QR y responda una breve encuesta