SEGURIDAD Y FRAUDE

Mitos o Realidad

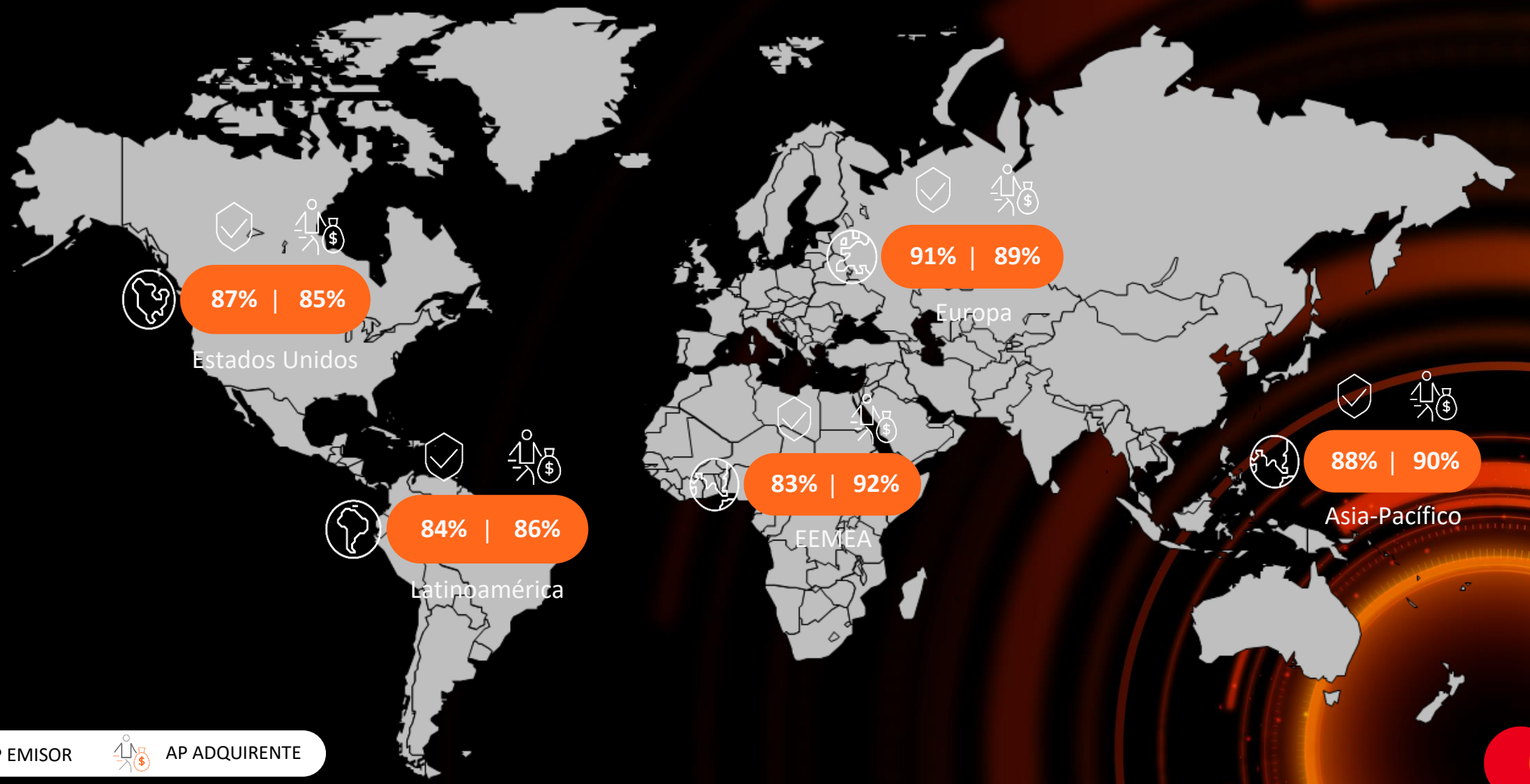
JAVIER GIACONE

Director

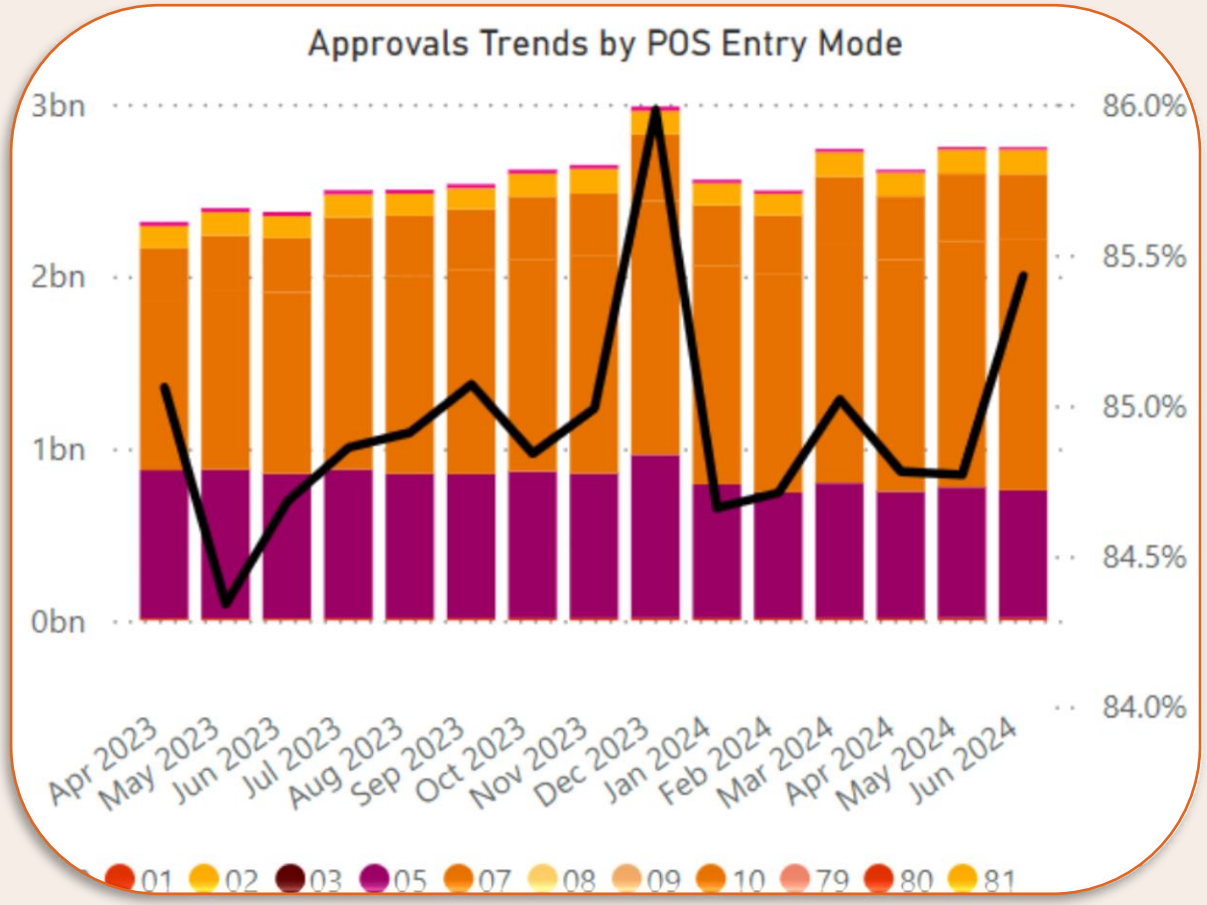
Customer Compliance & Fraud

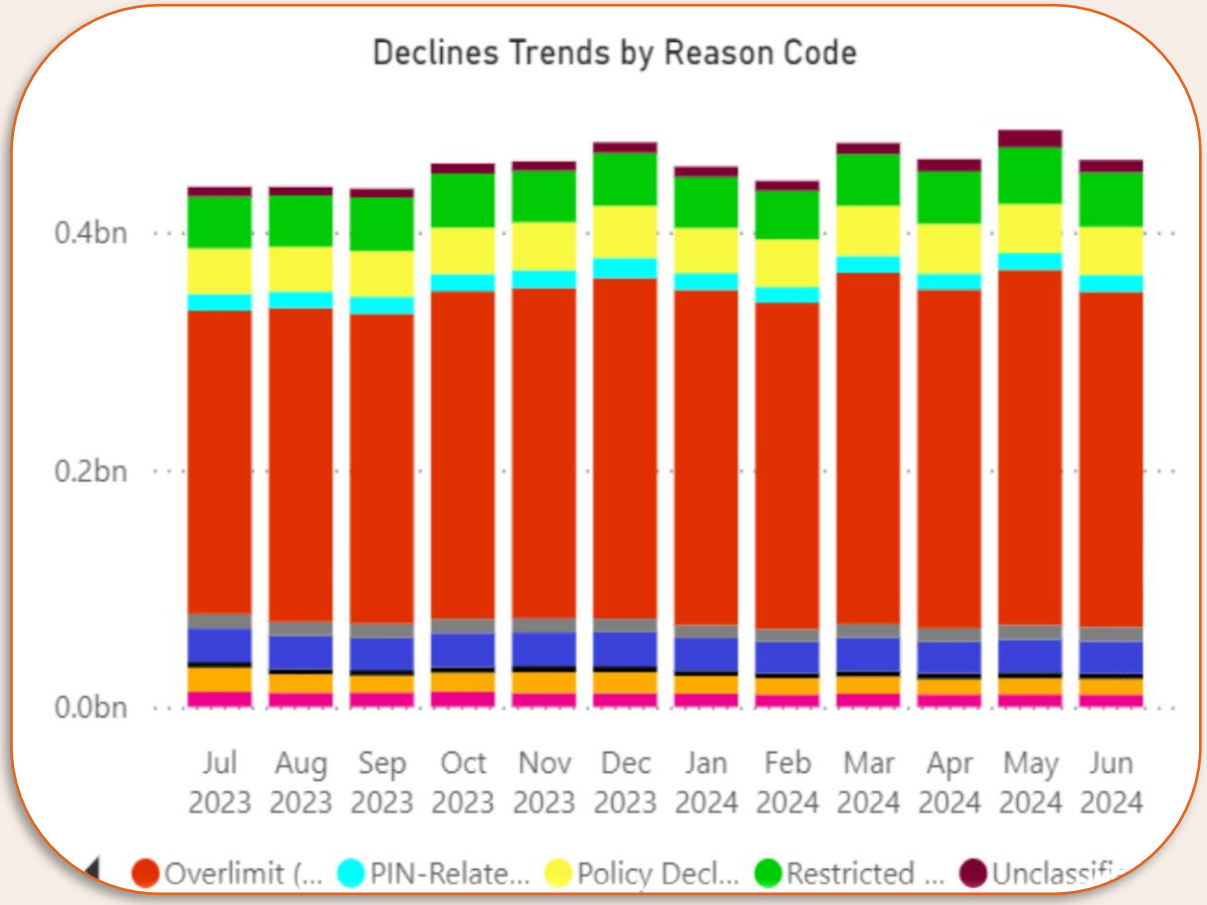
Agosto 2024

Tasas de Aprobación por Región – Emisor y Adquirente



Tasa de Aprobación y Motivos de Rechazo

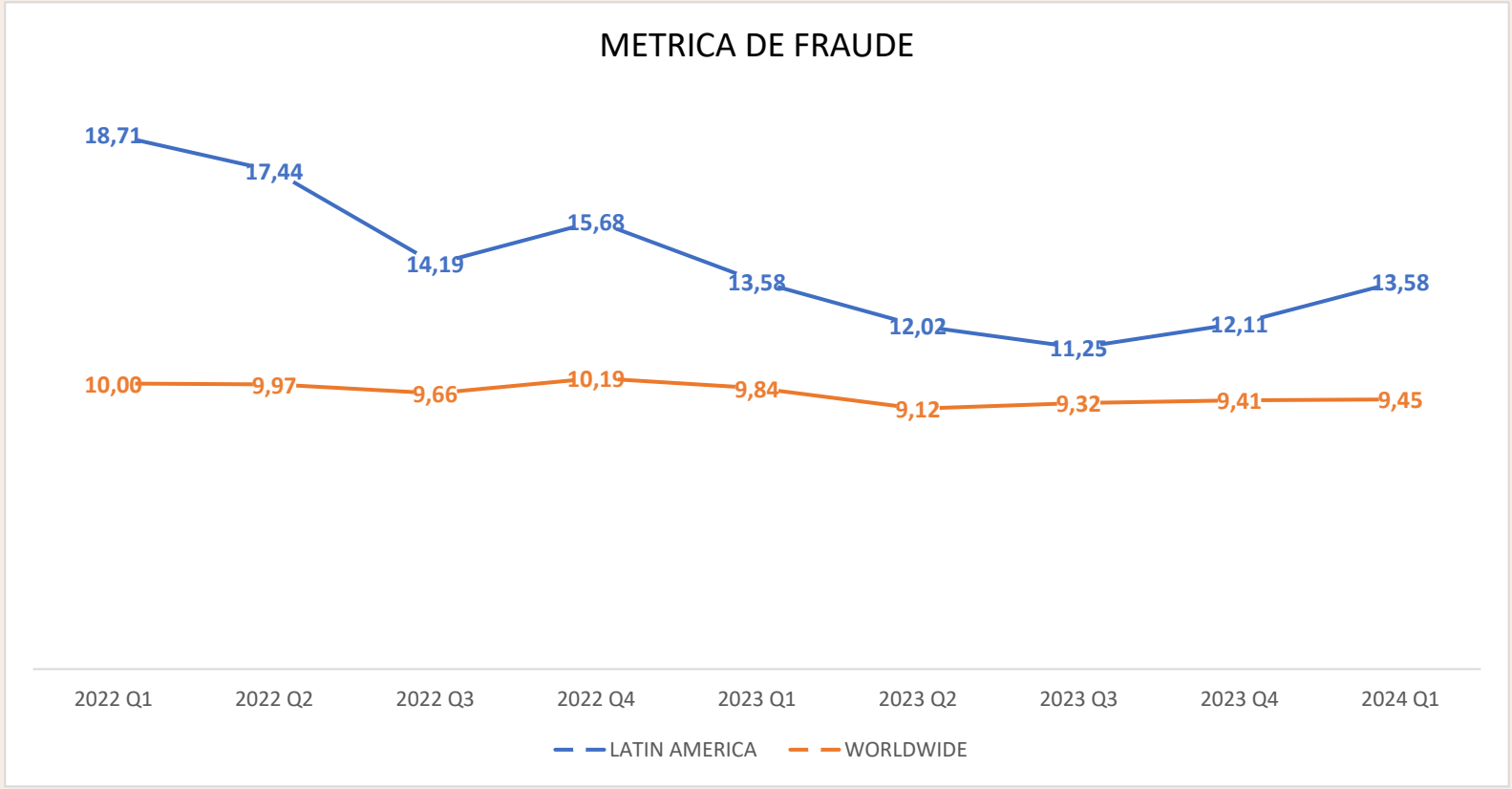




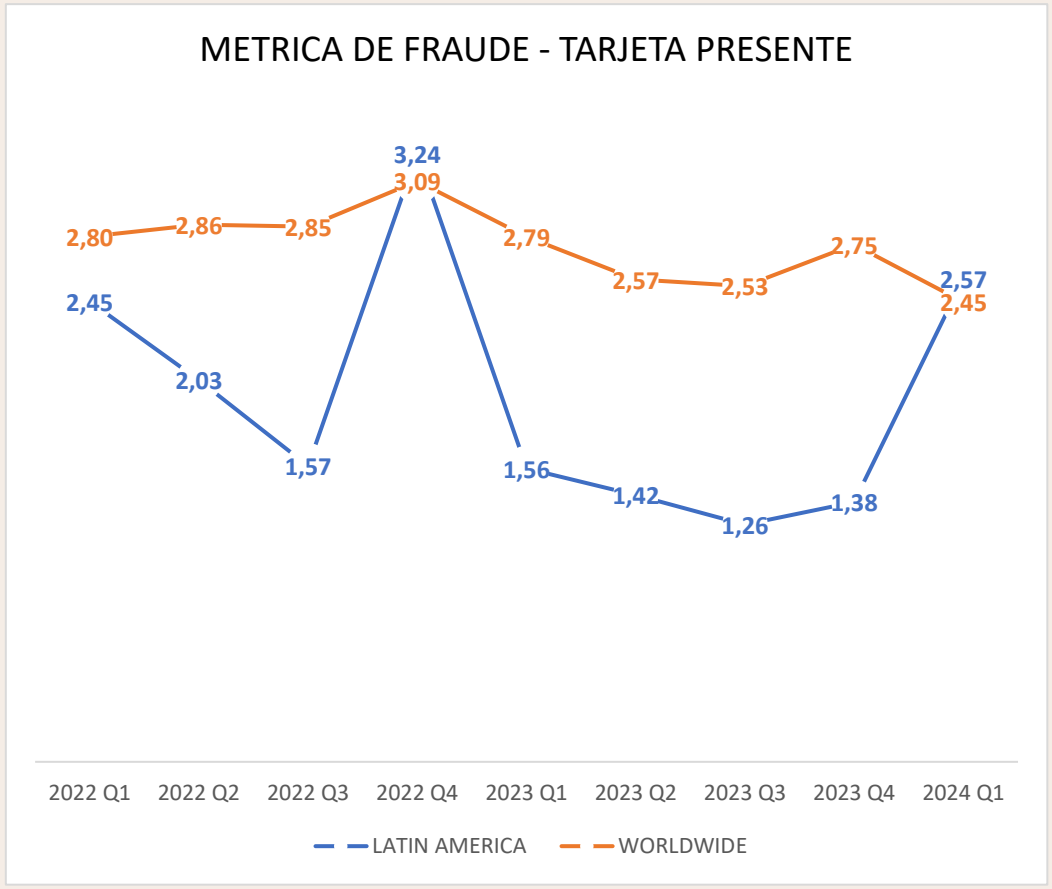
Índice general del fraude: Latino América vs. Resto del Mundo

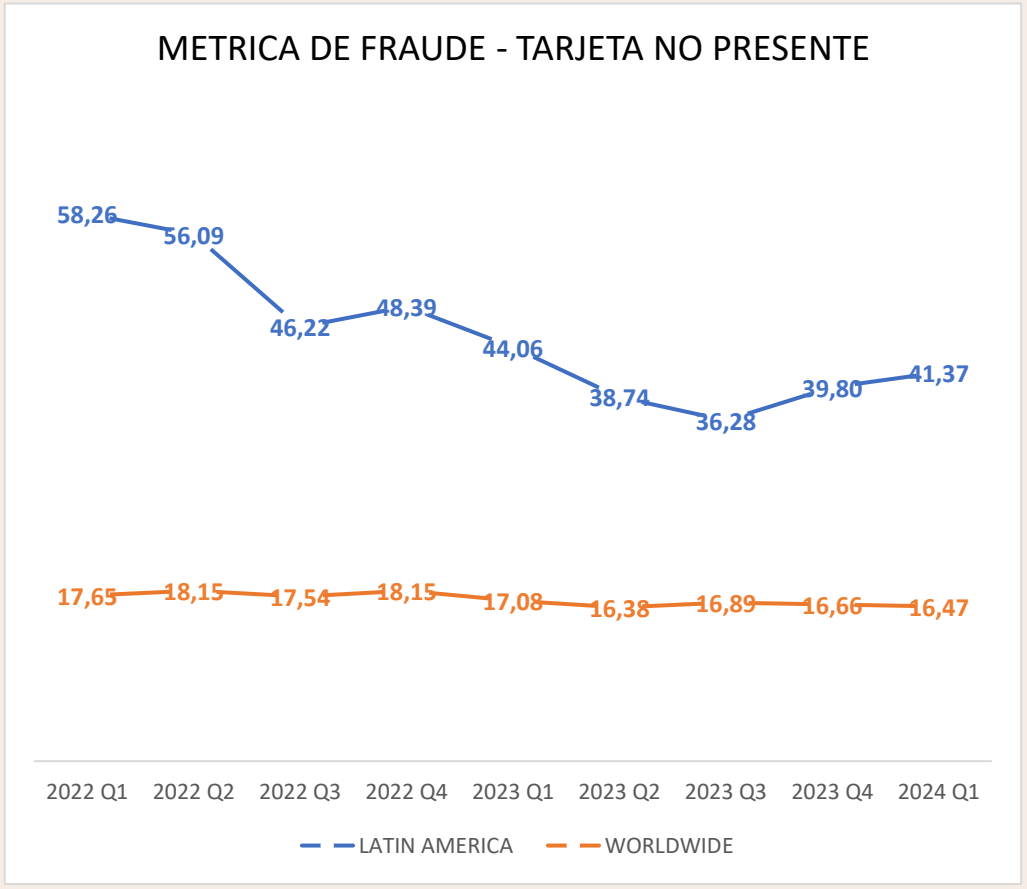
Mejora sostenida desde principios del 2022 , obteniendo una baja del 37% en Puntos Base de fraude a fin del 2023

Un gap de **4 PB's** con el mundo, un camino te mejoras tecnológicas que hay que recorrer.

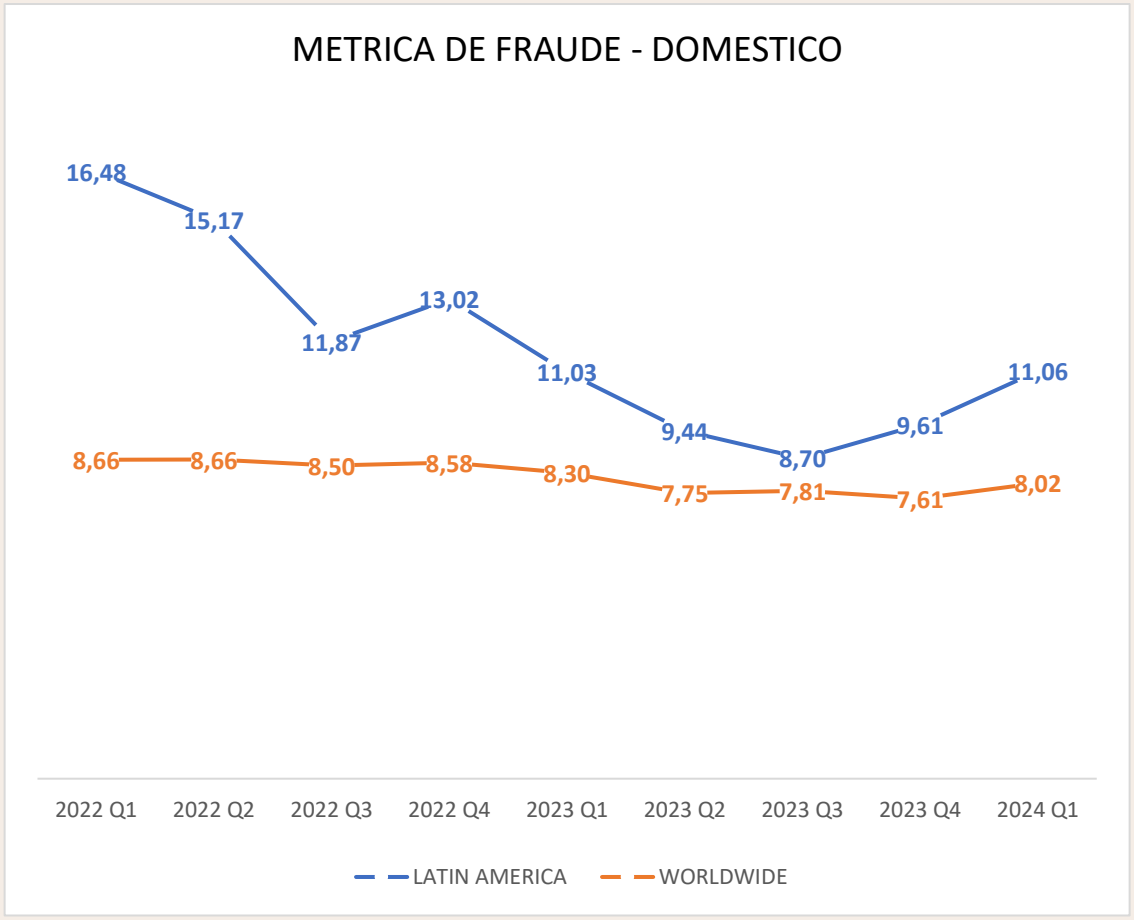


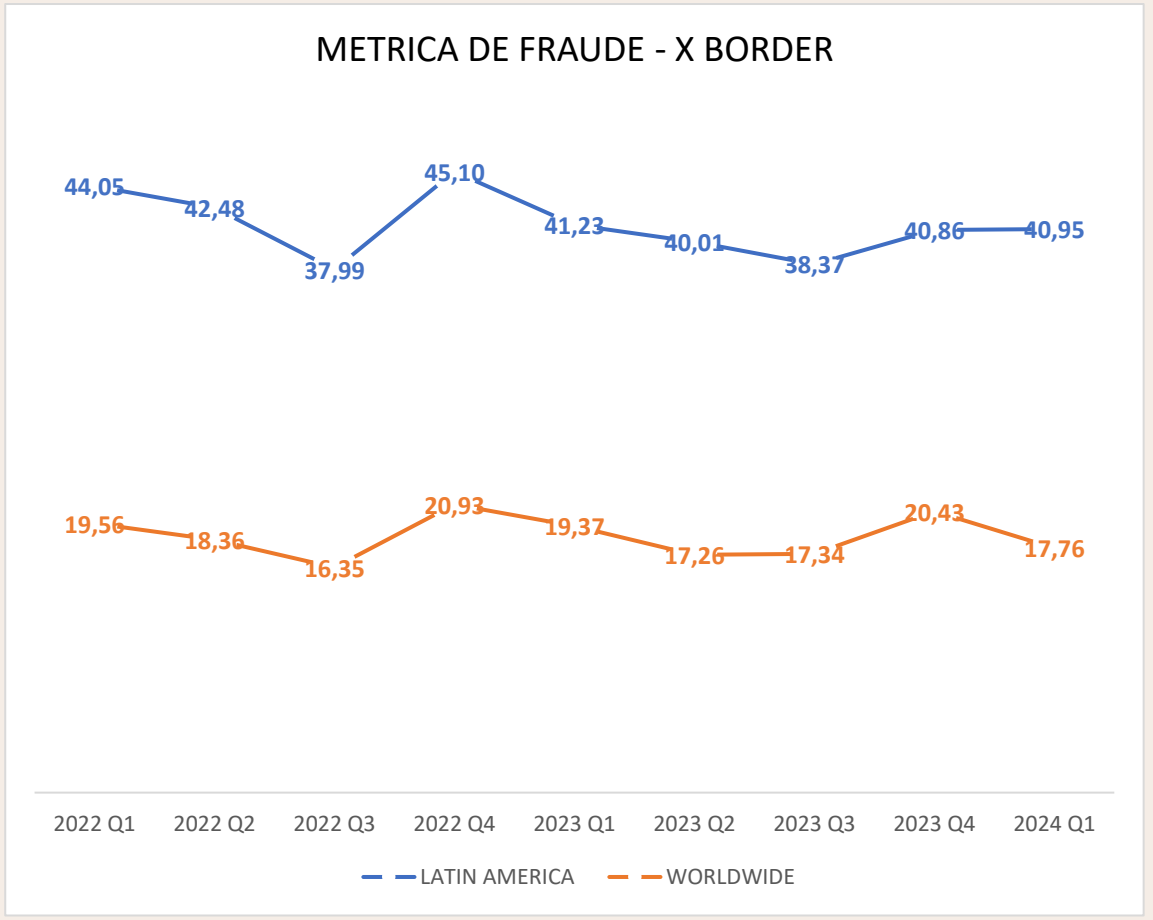
Índice general del fraude: vista Tarjeta Presente / Tarjeta No Presente





Índice general del fraude: vista Domestica & Exterior





Últimas tendencias de Fraude en la región:

- Ataques de BINES – Fuerza Bruta
- Fraude por transacciones de devolución (refund)
- Falsas Biometrías en sistemas de poca seguridad
- Cuentas “Mula” – impacto en emisores y adquirentes

• Scams (estafas)

01 ESTAFA DE SUPLANTACION DE IDENTIDAD BANCARIA

Estafas de suplantación de identidad bancaria: los estafadores se hacen pasar por empleados del banco y la víctima cree que están enviando dinero a una “cuenta segura”

02 ESTAFA DE COMPRA

Estafas de compra: se estafa a la víctima para que pague por bienes inexistentes, o sus compras nunca llegan a su destino.

03 ESTAFA DE SERVICIOS

Estafas de suplantación de servicios: los delincuentes afirman representar a una empresa de servicios públicos/ privados, afirman que la víctima debe pagar una multa ficticia o pagar un impuesto vencido

04 ESTAFA DE SECUESTRO VIRTUAL

Estafas de secuestro virtual: un secuestrador falso convence a un familiar en pánico para que pague un rescate en el acto

Otras : Estafas de cripto-romance, estafas de préstamos de día de pago, estafas de tarifas avanzadas, estafas de romance, estafas de descuentos/compras, etc.

Desafíos de la “tokenización” de billeteras en dispositivos

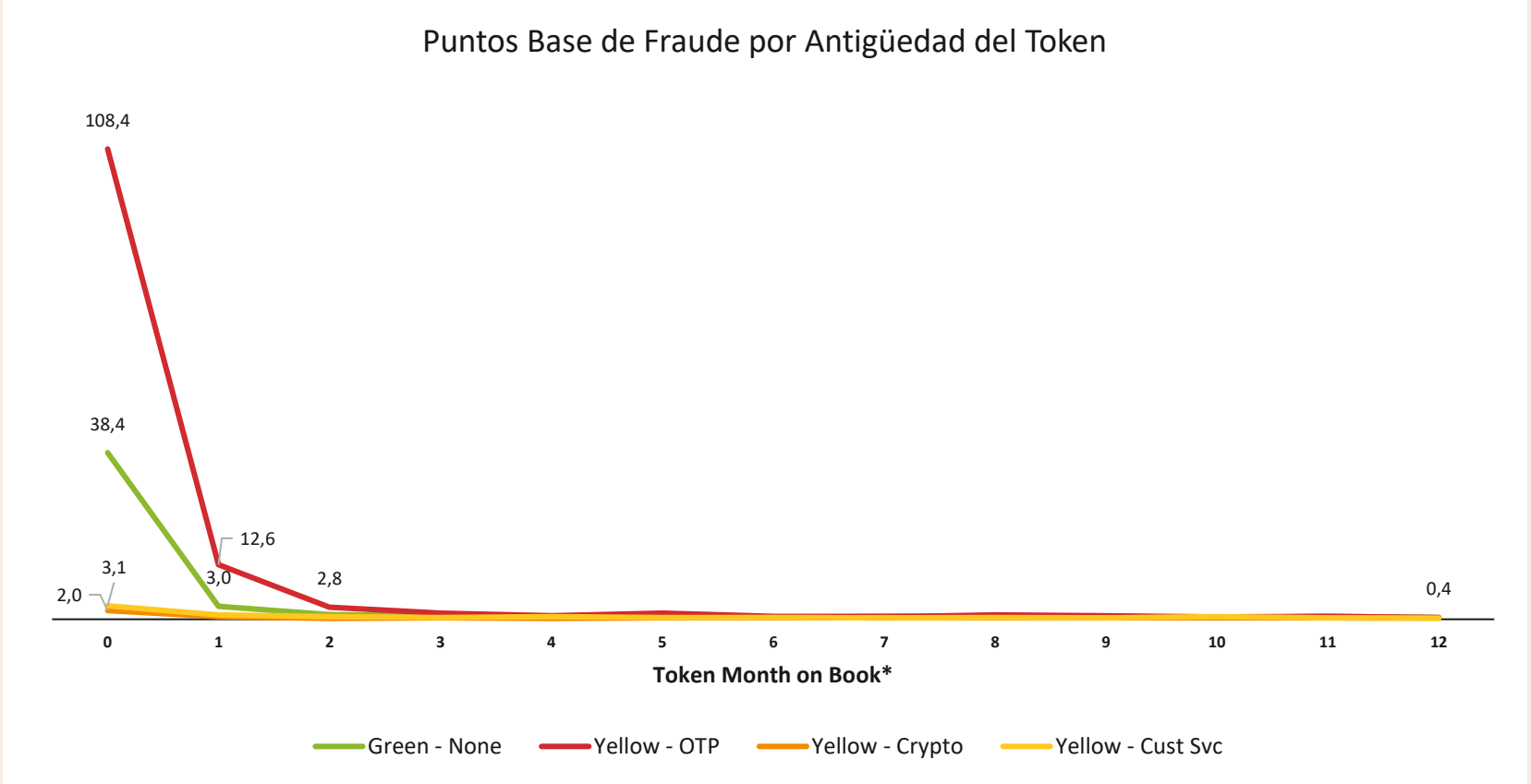
El fraude en Billeteras electrónicas ocurre en 99% durante los primeros días desde el ingreso de las credenciales.

Es importante que los clientes se sientan seguros de utilizar estos métodos de pagos, para ello el emisor tiene que implementar distintos monitoreos:

» Controlar los tokens ya otorgados.

» Validar el enrrollment de los clientes mediante diferentes métodos. Utilización de la biometría de los celulares

» Aviso y validación de las compras “obligatorio” que realice el cliente con tokens nuevos.



IA, Experiencias y Biometría
Conectando Inteligencia

La seguridad de un ecosistema en evolución va mas allá de proteger transacciones

Ecosistema inicial

Ecosistema en expansión

Ecosistema en evolución

DATOS RELEVANTES

200 ZETTABYTES

de datos globales se proyecta que se almacenarán para 2025[1]

MAS INTERACCIONES

5.3 MIL MILLONES

usuarios activos de Internet en todo el mundo a partir de enero de 2024[2]

ATAQUES POR MINUTO

33

Argentina es el 5to país con más ataques por minuto en la región y 45ª global6

TENDENCIAS DEL ECOSISTEMA

AUGE DEL COMERCIO ELECTRÓNICO

$8 TRILLONES

Valor estimado ecommerce para 2026[3]

AUMENTO DE LA BANCA DIGITAL

54%

del mundo usara billeteras digitales para 2026[4]

CRECIMIENTO EN IOT

33 MIL MILLONES

De dispositivos IoT estimados para 2030[4]

1. CYBERCRIME MAGAZINE. 2024.2. STATISTA. 2024. 3. FORBES. ECOMMERCE STATISTICS OF 2023. 4. FIS, THE GLOBAL PAYMENTS REPORT, 2023. 5. TRANSFORMA INSIGHTS' GLOBAL FORECAST REPORT. 2023.

La inversion global en seguridad y gestion de riesgo se estima que crecera un 14% y alcanzará $215B este 2024 – siendo Generative AI el factor clave[1]

- Herramientas maliciosas de AI están fácilmente disponibles en la web – habilitando a los delincuentes menos sofisticados a generar amenzas más sofisticadas

- Los Modelos de AI que funcionan similar a Chat GPT (como WormGPT) pueden simplemente proporcionar información sobre como realizar cualquier actividad ilegal

- Este uso no ético de AI está provocando un incremento en malware, phishing attacks and fraudes basado en AI– aumentando el fraude en pagos

1. GARTNER. GARTNER FORECASTS GLOBAL SECURITY AND RISK MANAGAMENT SPENDING TOO GORW 14% IN 2024. SEPTEMBER 2023.

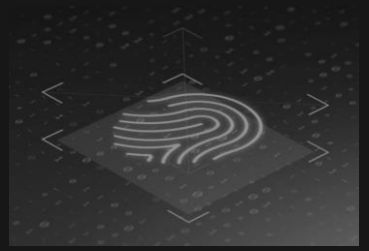
Mitigar el cibercrimen: Utilizando el monitoreo global de la red de fraude, nos permite identificar anomalías desde ataques a BINes generados por AI

SECURE THE PAYMENT ECOSYSTEM

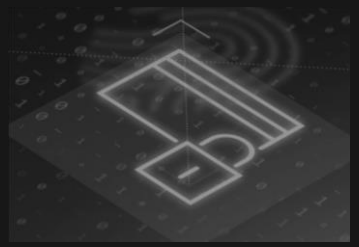
- Sólo el año pasado, Mastercard evitó 20.000 millones de dólares en intentos de autorización sospechosos en todo el mundo
- En América Latina, Mastercard ha rechazado 1.350 millones de dólares en intentos de autorización sospechosos, en su mayoría ataques BIN.

Muchos datos disponibles requieren de una robusta autenticación para asegurar al ecosistema de las nuevas manipulaciones de identidad

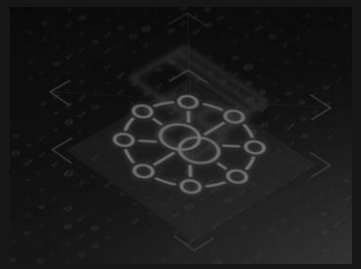
IDENTIDAD EN DISPOSITIVOS
Identificar a las personas y sus dispositivos



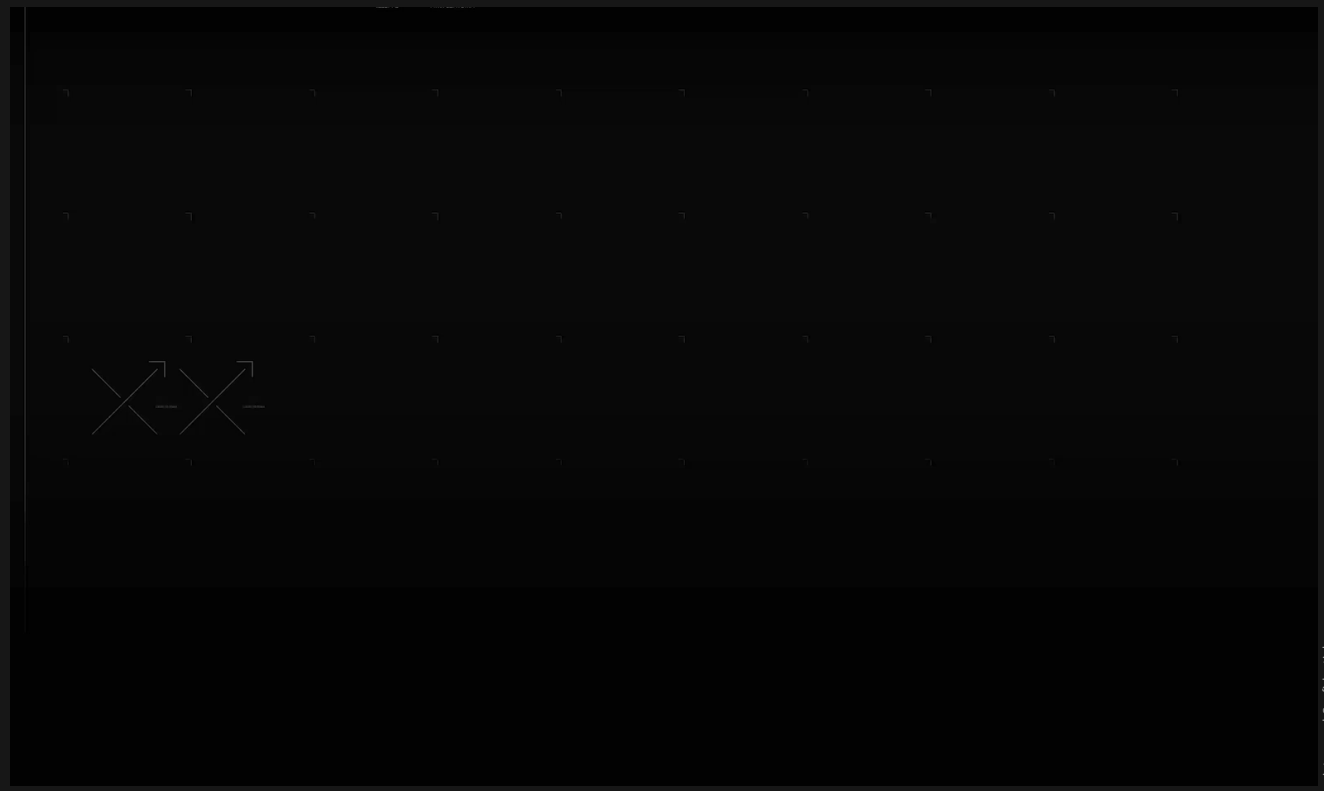
IDENTIFICACIÓN DE CUENTAS
Realizar análisis de riesgos en función a las cuentas



BIOMETRÍAS FÍSICAS Y COMPORTAMENTALES
Patrones para identificar a las personas indicadas



IDENTIDAD INDIVIDUAL
Analizar información personal dinámica en todo el ciclo de vida para proteger a las personas



Utilizar **IA** en todo el ciclo de vida de pago de las personas mejorando sus **experiencias digitales**

Una coordinación de soluciones basadas en IA en milisegundos, facilitando **decisiones inteligentes**

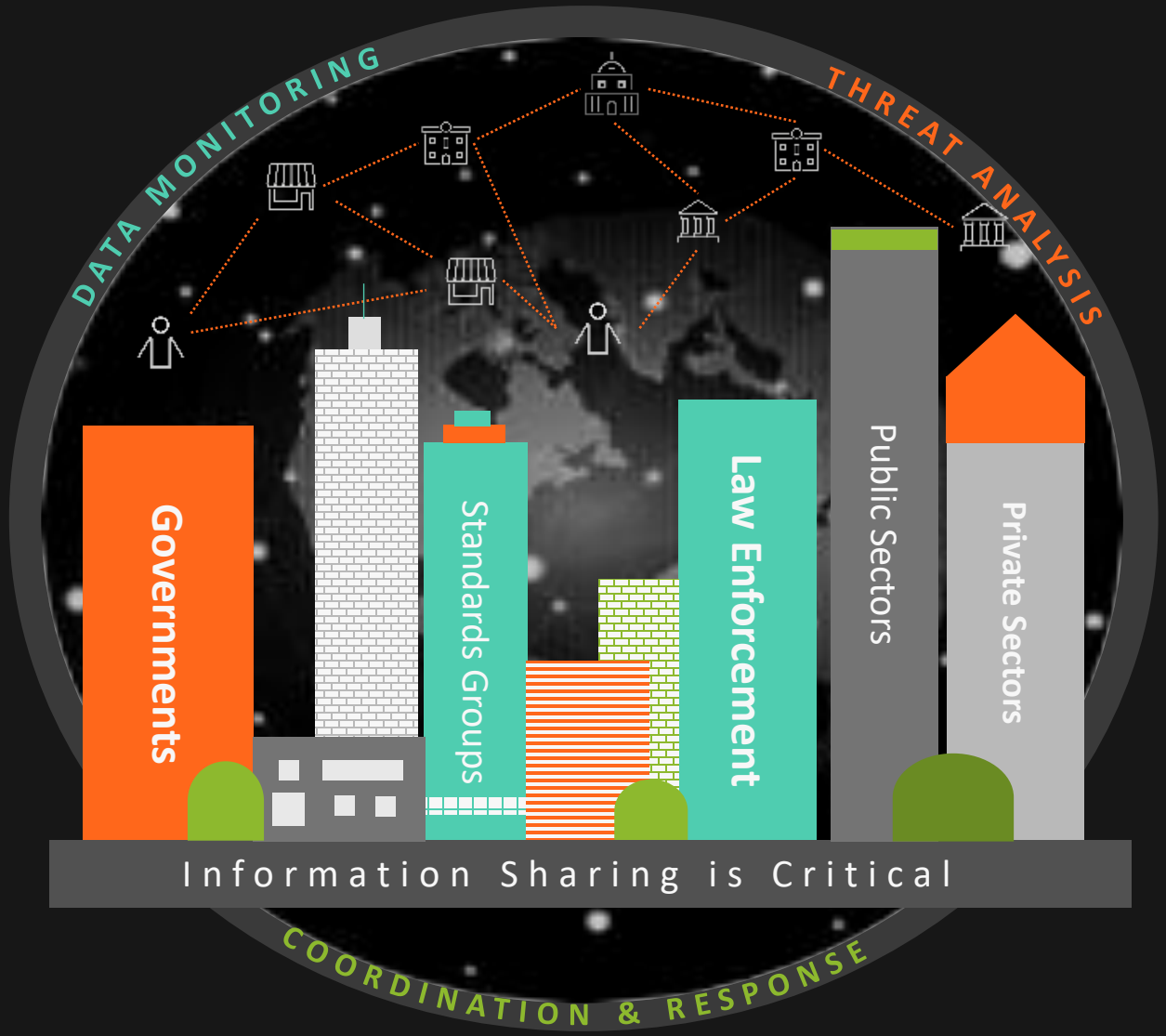
Most Common Passwords

Is yours here?

select a category below to filter

alphanumeric · animal · fluffy · food · macho · names · nerdy · rebellious · security · sports

La colaboración cross industrias compartiendo inteligencia es la clave para construir el futuro de la Cyber Seguridad e Innovación



GRACIAS