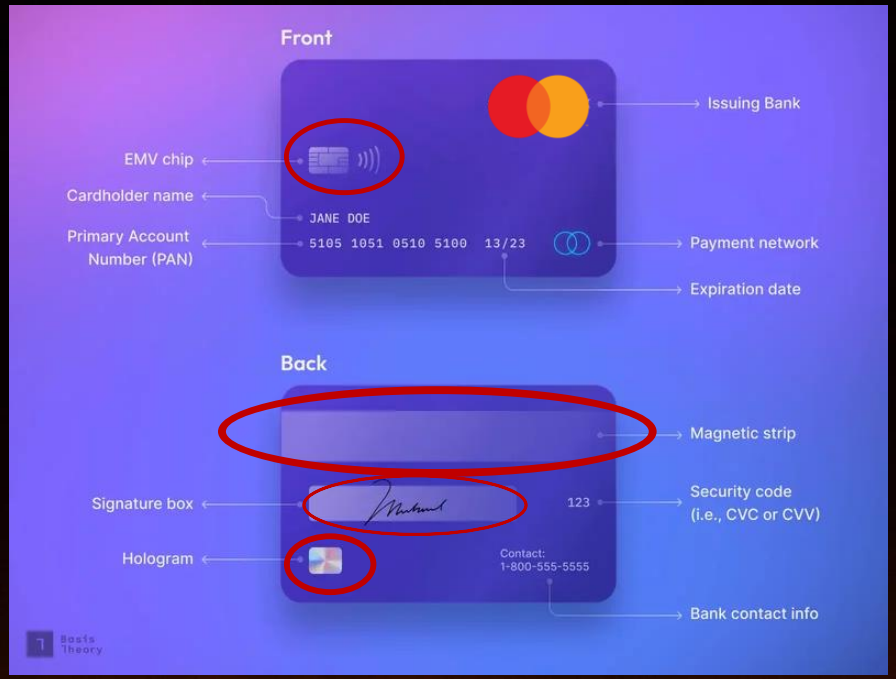
De la detección reactiva a la defensa proactiva del fraude

Nahuel Bello
Security Solutions

La evolución



Se estima que hasta un 20% del ecommerce en Latinoamerica podría ir a pérdida debido el fraude

Pérdidas brasileras por APP Scams

$247M

Las estafas por APP aumentarán a un ritmo del 21% 2025 y 2027, atacando a 1 de cada 10 brasileños.

Phising en Perú

2° puesto

En Latinoamerica, con 250.000 intentos diarios

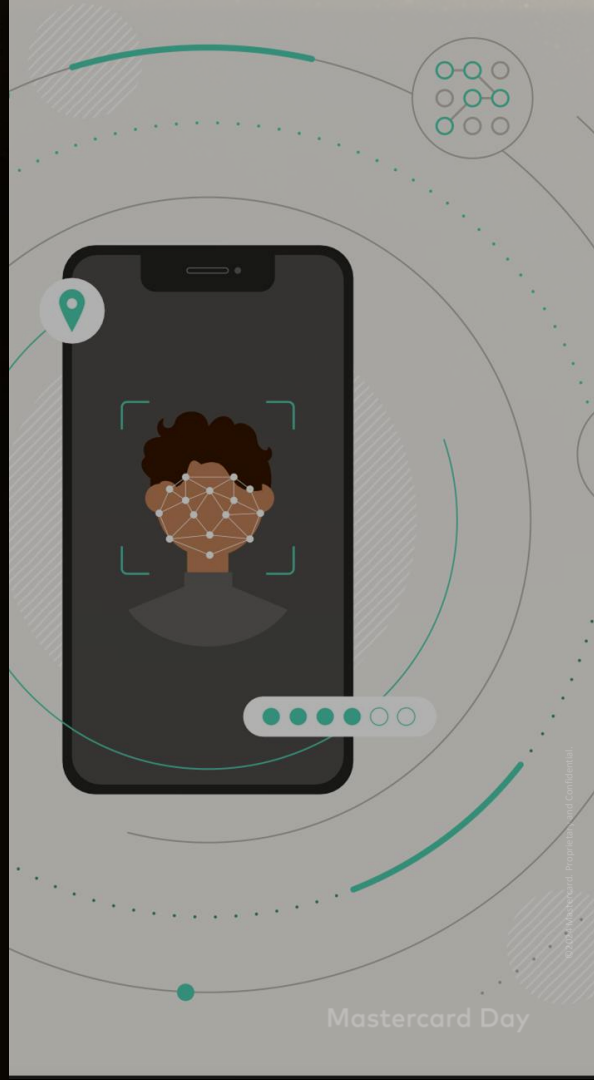
Población de Mexico que ha sido víctima de fraude

15%

Esto representa 1 de cada 5 usuarios, y en el 92% de los casos, el fraude se consuma con éxito.

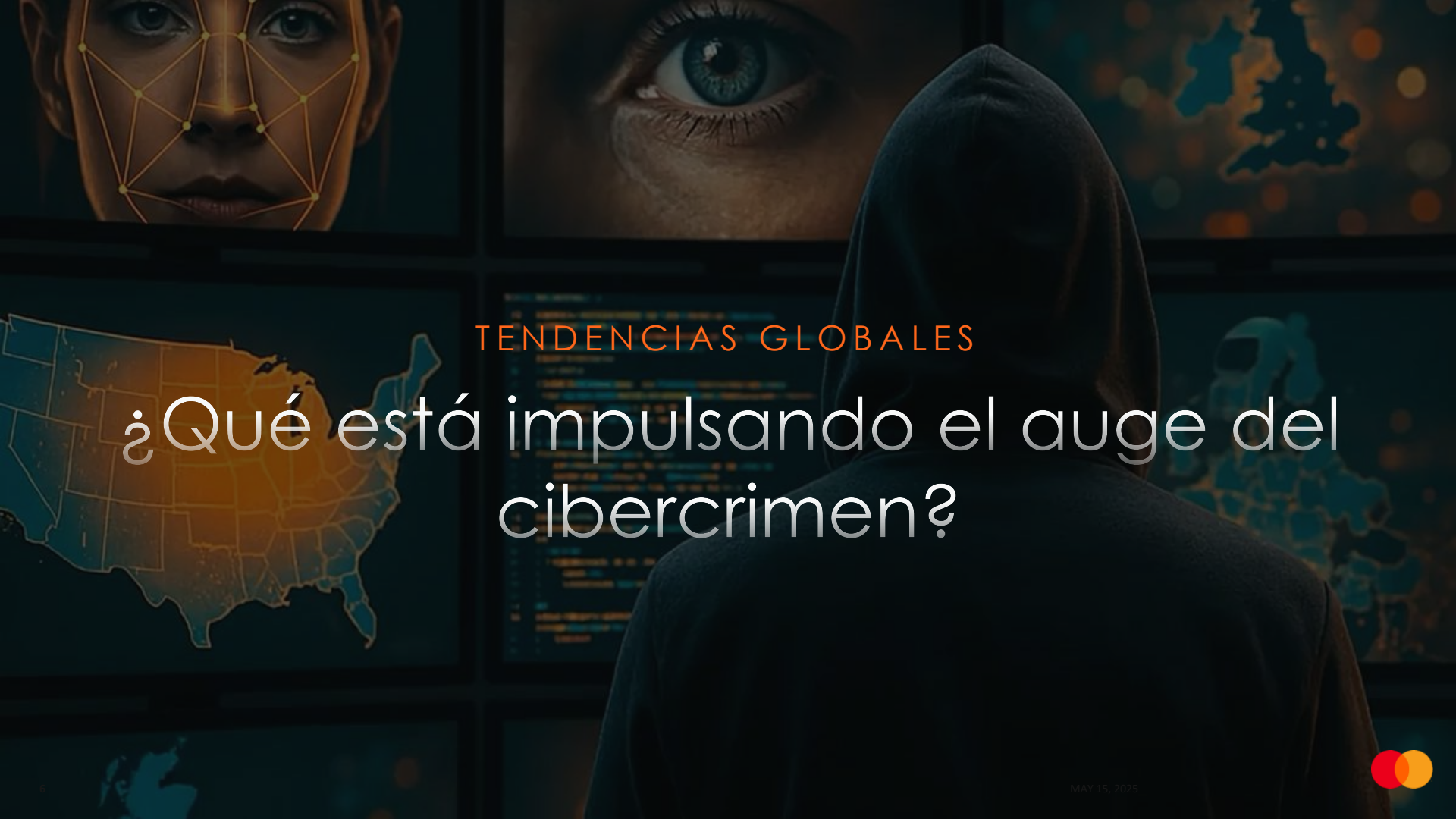
Fraude está en evolución

IA permite a los defraudaores volverse más creativos, sofisticados y asertivos en sus ataques



Cibercrimen: amenaza creciente, cambiando rápidamente

1 https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide



TENDENCIAS GLOBALES

¿Qué está impulsando el auge del cibercrimen?

¿QUÉ ESTÁ IMPULSANDO EL CRECIMIENTO?

1. Expansión de la superficie de ataque

Todo conectado, cada conexión es una amenaza potencial

NIST NATIONAL VULNERABILITY DATABASE NVD

280,000

vulnerabilidades cibernéticas documentadas en la base de datos nacional de vulnerabilidades de EE. UU.[2]

2 https://nvd.nist.gov/general/nvd-dashboard

2. Aumento de las amenazas geopolíticas

Ciber es armamento en un mundo incierto

X3

aumento en las filtraciones de datos motivado por espionaje 2023-4[3]

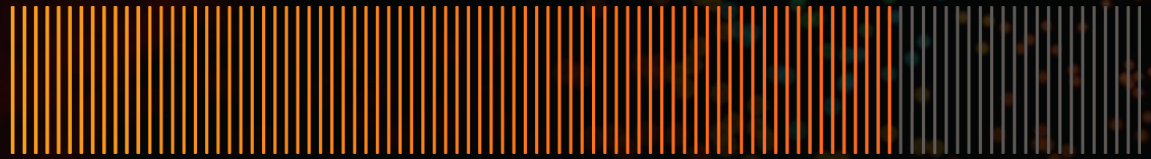
3 https://www.verizon.com/business/en-gb/resources/reports/dbir/

¿QUÉ ESTÁ IMPULSANDO EL CRECIMIENTO?

3. Aceleración de la escalabilidad de la IA

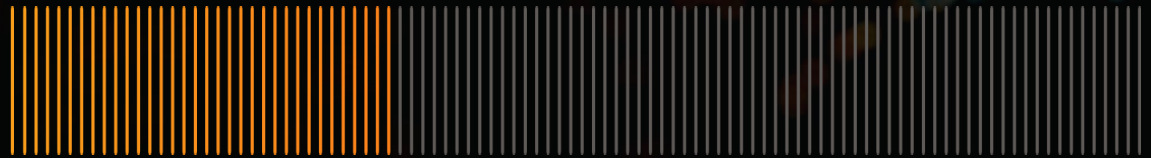
Herramientas más rápidas, inteligentes y autónomas

78%



de los directores de seguridad de la información están experimentando un "impacto significativo" de los delitos impulsados por la IA[4]

1/3



de todo el tráfico de Internet son "bots malos"[5]

4 Darktraces 2024 Annual Threat Report | 5 2024 Global Bot Security Report | DataDome

4. Democratizando el acceso de los ciberdelincuentes

Mayores rendimientos, menor riesgo, mayor alcance

57%

de las amenazas detectadas se deben al malware como servicio (MaaS), un aumento del 17% año tras año[6]

6 Darktrace's 2024 Annual Threat Report

OPORTUNIDADES EMERGENTES

Tres amenazas, tres respuestas

Amenazas aceleradas, Apuestas más altas

1. Agentes autónomos
2. Industrialización de estafas
3. Lavado de dinero sobrealimentado

Respuestas emergentes, Defensas en evolución

1. Seguridad proactiva
2. Defensa inteligente
3. Patrones y perfiles

AMENAZA 1: AGENTES AUTÓNOMOS

Bots agénticos: inteligentes y autónomos

La IA no duerme. Los motores argénticos sondearán sistemas de forma implacable, diseñaràn estrategias contra los objetivos y ejecutarán ataques. Estamos entrando en una nueva era de ciberdelincuencia autónoma diseñada por máquinas.

DE LA AUTOMATIZACIÓN A LA AUTONOMÍA

ENTONCES	PRÓXIMO
Configurar y olvidar bots automatizados	Bots autónomos y oportunistas
Mensajes de phishing basados en plantillas	Conversaciones de phishing sostenidas por IA
Ataques de fuerza bruta y relleno de credenciales	Segmentación inteligente y determinación de credenciales
Bots visibles	Bots invisibles y cambiantes
Tecnología compleja en manos de unos pocos	IA de generación al alcance de muchos

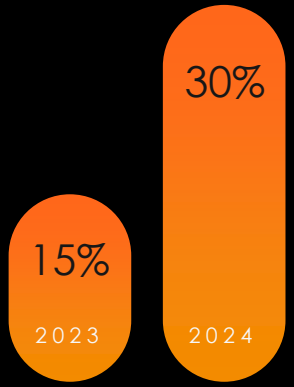
AMENAZA 1: AGENTES AUTÓNOMOS

Riesgo de terceros: un nuevo nivel de complejida

A medida que las herramientas de inteligencia artificial se integran en todos los sectores, gener
nuevas vulnerabilidades. Se espera un aumento en el riesgo asociado a terceros y a la cadena
de suministro.

de las reclamaciones de seguros cibernéticos ya se deben a vulnerabilidades de terceros[9]

de las organizaciones afirman no tener procesos para evaluar la seguridad de herramientas de IA antes[10]



de las filtraciones de datos están relacionadas con terceros[11]

9 Check Point Research |. 10 2024 Global Bot Security Report | DataDome |. 11 2025 Data Breach Investigations Report | Verizonq

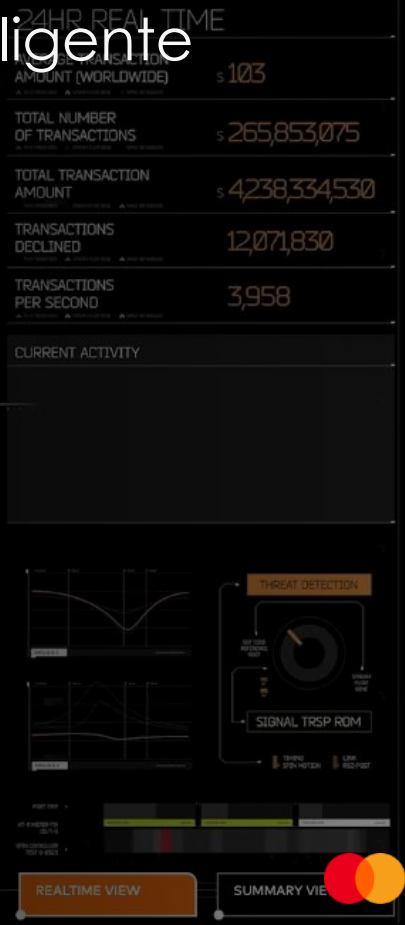
RESPUESTA

Seguridad proactiva

RESPUESTA 1: SEGURIDAD PROACTIVA

Defensas de autoaprendizaje: neutralización inteligente

Los sistemas proactivos están pasando de la mitigación reactiva de amenazas a los sistemas de defensa proactivos y autónomos. Predicen, detectan y neutralizan las amenazas antes del impacto.



ANÁLISIS EN TIEMPO REAL

Identificar anomalías y patrones sospechosos a medida que ocurren.

APRENDIZAJE ADAPTATIVO

Capacitación continua sobre nuevos datos, vectores de ataque y estrategias.

ANÁLISIS PREDICTIVO

Anticipar y mitigar futuros escenarios cibernéticos y de fraude.

Las herramientas *Decision Intelligence* y *Safety Net* de Mastercard monitorean signos de fraude en una red de 159 mil millones de transacciones cada año.[12]

12 One-click payments by 2030 with tokenization | Mastercard Newsroom

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

RESPUESTA 1: SEGURIDAD PROACTIVA

2

AMENAZA

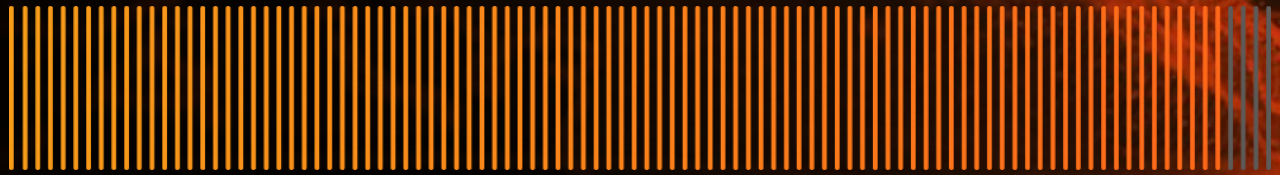
Industrialización de estafas

Una fuerza global

$1 trillón

pérdida por estafas cada año[15]

96%



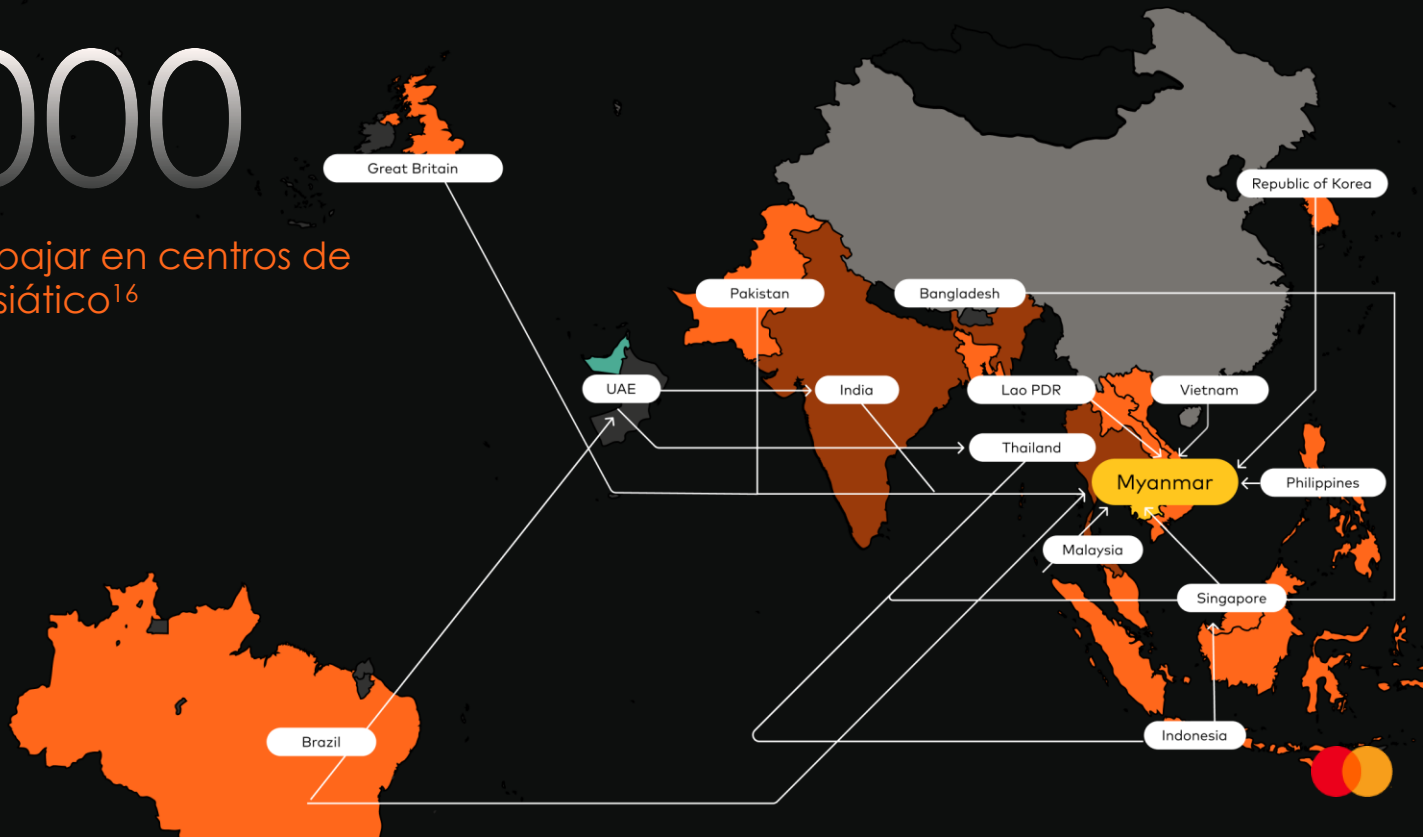
de las víctimas no recuperan su dinero[15]

15 Global Anti-Scam Alliance

Estafas organizadas y engaños emocionales

220,000

Personas forzada a trabajar en centros de fraude en el sudeste asiático[16]



16 United Nations Office on Drugs and Crime

Ningún país intacto

Países más afectados económicamente (%PIB)[17]

4.2%
Pakistán

3.6%
Kenia

3.4%
Sudáfrica

Países donde las estafas son más frecuentes (% de ciudadanos que se encuentran con estafas a diario) [17]

41%
Brasil

33%
Hong Kong

26%
Corea del Sur

17 Global Anti-Scam Alliance

AMENAZA 2: INDUSTRIALIZACIÓN DE ESTAFAS

Mercados clandestinos: dark web

La dark web es un centro de actividad cibercriminal, donde se intercambian consejos y conocimiento para estafas, herramientas de hacking y ransomware

270 millones

de las credenciales de pago robadas y que se publicaron a la venta en la Dark Web en 2024[18]

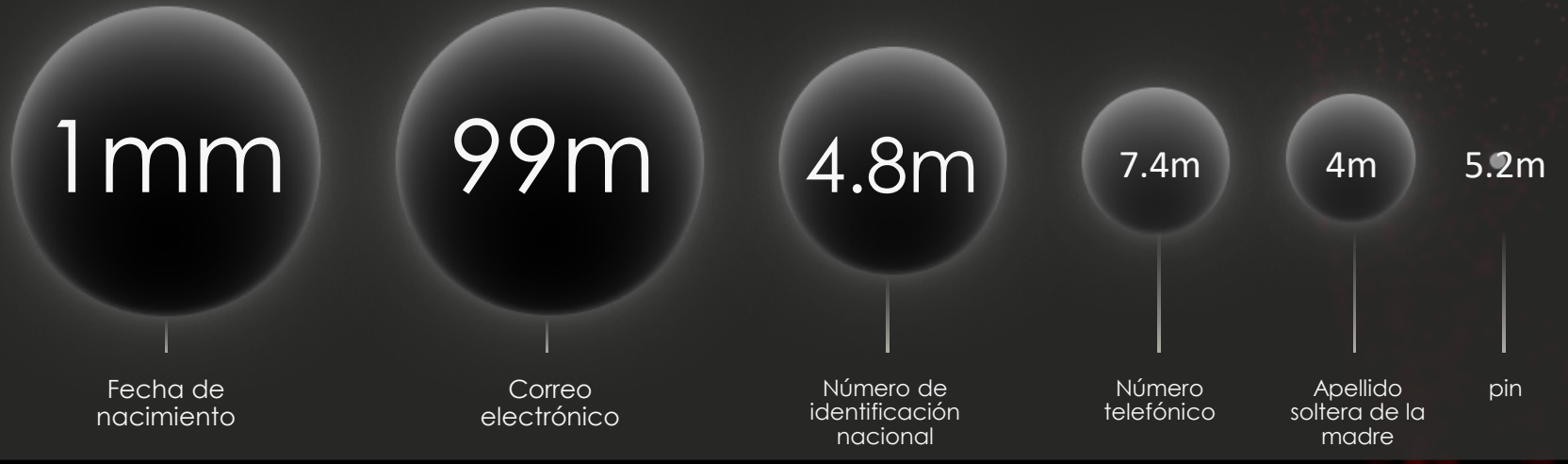
18 Recorded Future 2024 Payment Fraud Report: Trends, Insights, and Predictions for 2025

AMENAZA 2: INDUSTRIALIZACIÓN DE ESTAFAS

Infostealers: recolección de datos personales

El robo de identidad compienza con los datos personales. Los *infostealers* son programas maliciosos diseñados para infiltrarse en sistemas y dispositivos con el fin de extraer información personal valiosa.

ELEMENTOS DE INFORMACIÓN PERSONAL IDENTIFICABLE OFRECIDOS JUNTO CON DATOS DE TARJETAS ROBADAS EN 2024[19]



19 Recorded Future 2024 Payment Fraud Report: Trends, Insights, and Predictions for 2025

AMENAZA 2: INDUSTRIALIZACIÓN DE ESTAFAS

Ataque de identidades sintéticas: *deepfakes* autónomos

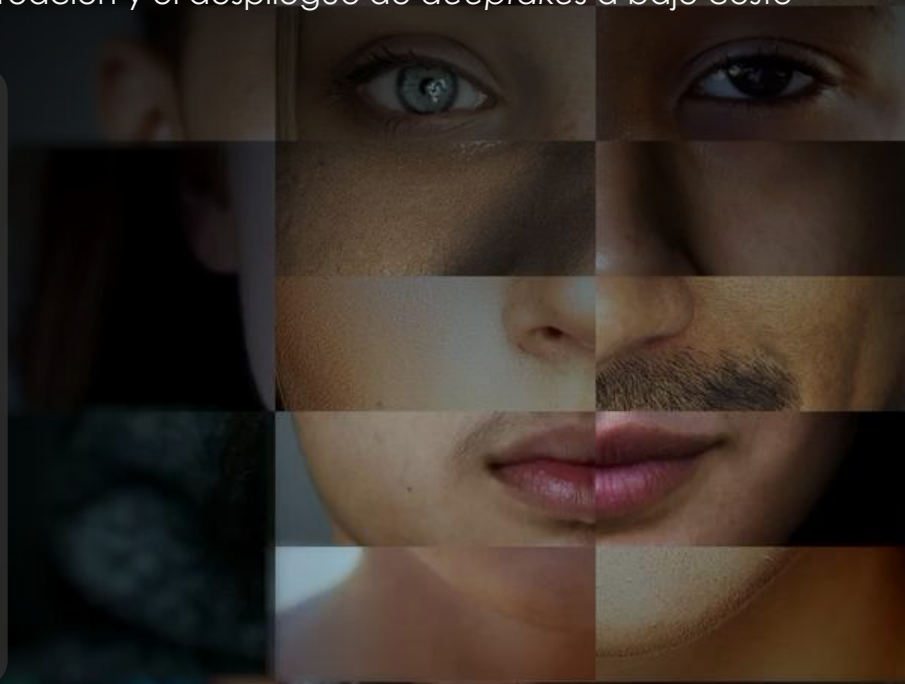
La tecnología está potenciando las estafas, facilitando la creación y el despliegue de *deepfakes* a bajo costo

4x

crecimiento en incidentes fraudulentos de *deepfakes* en 2023[20]

FUTURO PROBABLE

Bots con inteligencia artificial rastrean redes sociales en busca de imágenes, videos y voces, crean identidades sintéticas y ejecutan múltiples estafas en tiempo real.



20 Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes Circulated in 2024

2

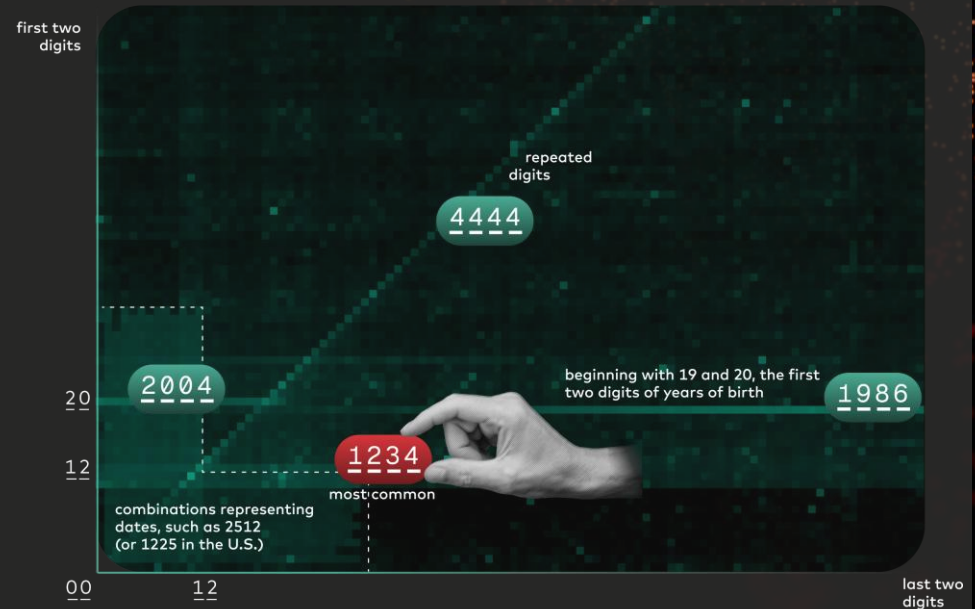
RESPUESTA

Defensa inteligente

Evolucionando mas allá de contraseñas y PIN

ABC NEWS

Un análisis de 29 millones de PIN expuestos realizado por ABC News de Australia reveló que los números consecutivos, fechas y años de nacimiento son los PIN más comunes elegidos por los usuarios. En este gráfico, los PIN más populares se representan con píxeles más brillantes.[21]



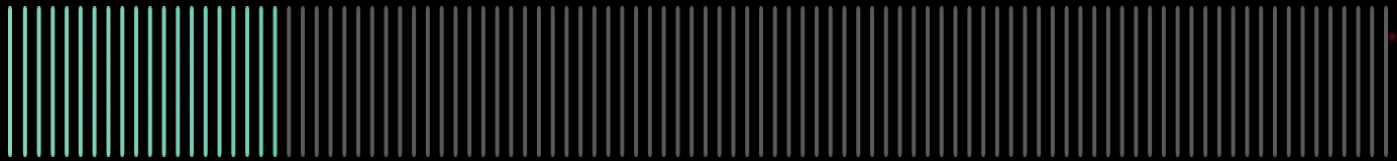
21 www.abc.net.au

RESPUESTA 2: DEFENSA INTELIGENTE

Tokenización y passkeys: doble motor contra el fraude

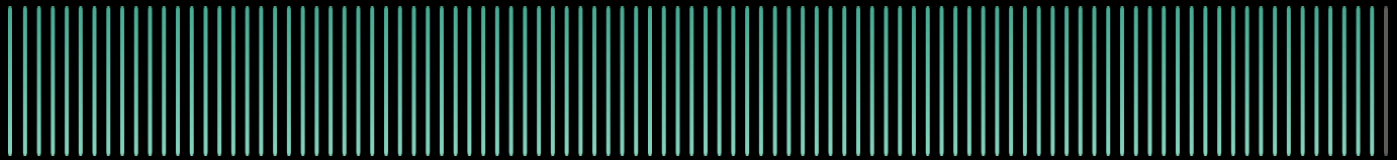
La tokenización se está convirtiendo en el mecanismo silencioso que protege la identidad, los datos, los pagos y las interacciones en el comercio digital. Los passkeys eliminan la necesidad de contraseñas y PIN, marcando el fin de métodos tradicionales de autenticación.

% de los 100 principales servicios y sitios web del mundo que ya han adoptado passkeys[22]



20%

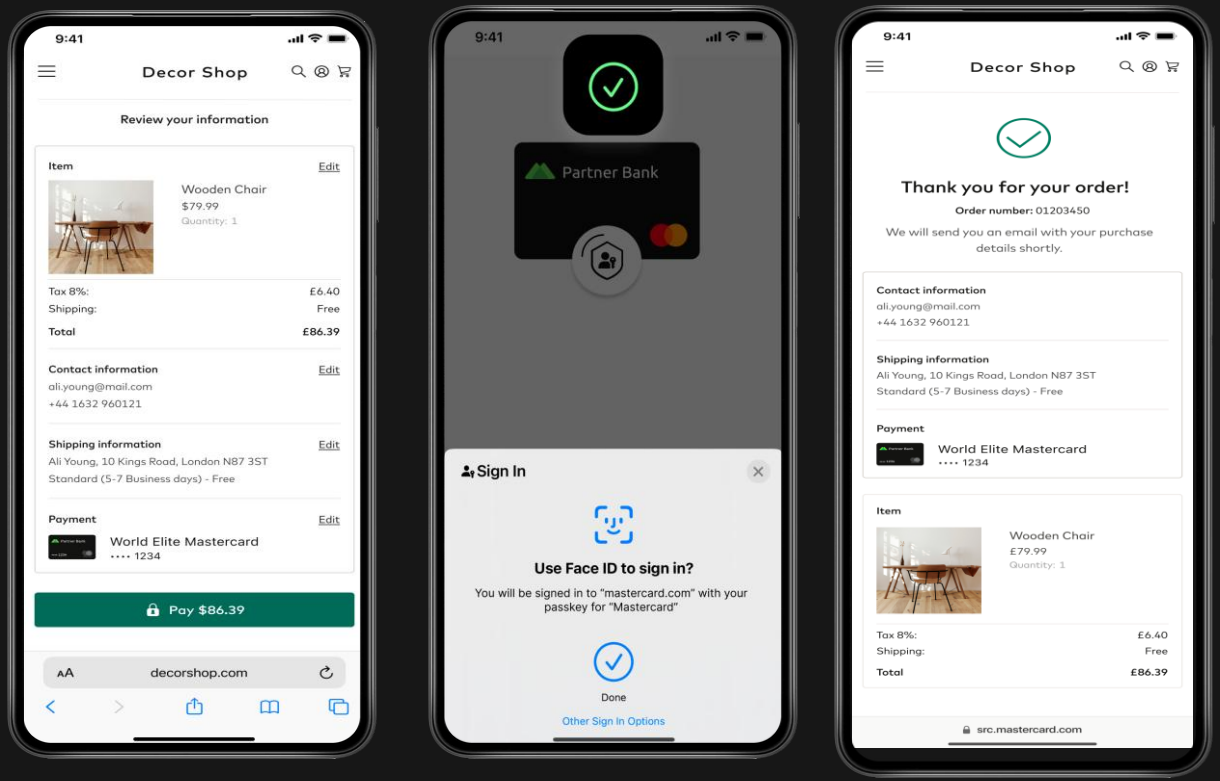
Objetivo de Mastercard para la tokenización de transacciones de comercio electrónico para 2030[23]



90%

22 www.fraud.net | 23 www.pwc.com

Tokenización y passkeys: doble motor contra el fraude



RESPUESTA 2: DEFENSA INTELIGENTE

Autenticación continua: seguridad siempre activa

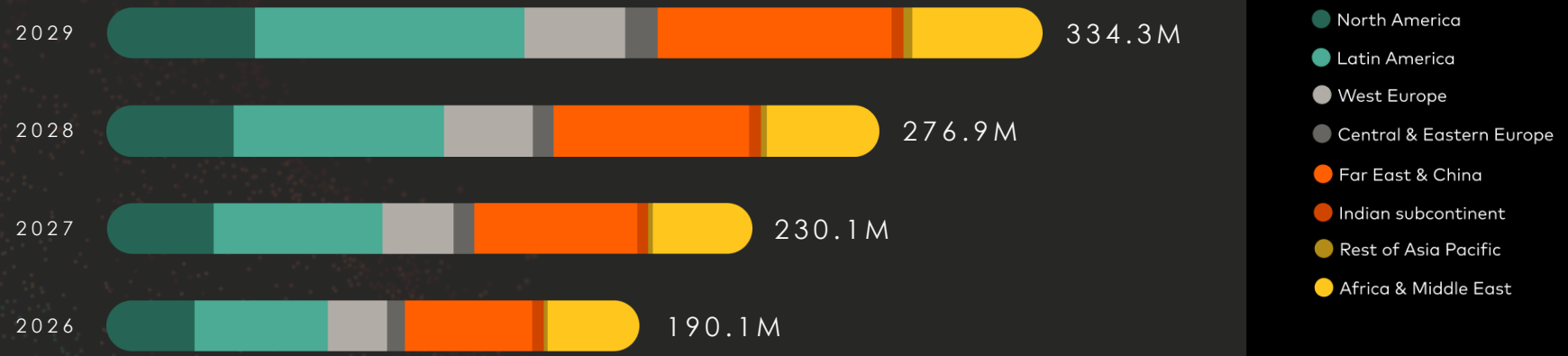
Los próximos cinco años verán un cambio decisivo hacia la autenticación continua, en tiempo real y basada en el riesgo, basada en análisis de comportamiento, biometría y redes de identidad

RESPUESTA 2: DEFENSA INTELIGENTE

Protección contra estafas: comportamientos y anomalías

Las tecnologías emergentes pueden detectar si la manipulación y el engaño están afectando el juicio de las víctimas. La inteligencia artificial mapea relaciones entre cuentas sospechosas en redes de pagos en tiempo real.

AUMENTO PREVISTO EN EL NÚMERO DE TRANSACCIONES FRAUDULENTAS MEDIANTE PAGOS PUSH[24]



24 Global Fraud Detection and Prevention in Banking Market: 2024-29 - Juniper

Huella de identidad digital.

Personal

Análisis de información personal dinámica a medida que avanza a lo largo del ciclo de vida digital

Pago

Comprender la identidad de la cuenta de pago de una persona para crear un análisis basado en riesgos

Comportamiento

Comprender cómo los usuarios ingresan su información y cómo se usan elementos de identidad en línea para distinguir comportamientos riesgosos de seguros

Dispositivo

Usamos inteligencia del dispositivo y biometría para identificar personas y vincularlas a sus dispositivos

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

Hacia un futuro más seguro

La IA agéntica, los datos en tiempo real, la inteligencia de comportamiento y las tecnologías de identidad avanzadas crearán una seguridad más inteligente, rápida y resistente.

Las amenazas autónomas serán contrarrestadas por la defensa proactiva, el fraude de identidad por un razonamiento más inteligente y el lavado de dinero por
Inteligencia exigente.

La colaboración global es clave. Las estrategias coordinadas, el intercambio de conocimientos y las redes de confianza son peldaños hacia una ciberseguridad más eficaz.

Nahuel Bello, Security

linkedin.com/in/nahuel-bello