

Tendencias de fraude en la actualidad

El consumidor/usuario de hoy



Necesidad de información constante



Búsqueda de experiencias exclusivas y personalizadas



Plataformas disponibles sin ninguna interrupción



Las redes sociales son el medio predilecto de interacción (tareas, grupos, comentarios)



Entornos fáciles de controlar y que estén interconectados



Exigencia de garantías en la protección de datos



Conexión a múltiples dispositivos (Nube)





Estamos hablando hoy de ciber seguridad,
y qué tan seguras son las contraseñas de la gente.

Panorama actual en la era digital

Cada persona tiene
múltiples

Cuentas + Dispositivos + Ubicaciones



Acciones del usuario

- Revisar el email.
- Compras online.
- Revisión de las RRSS.
- Pagar obligaciones.
- Hacer reservas...

83% de las personas prefieren el correo electrónico para recibir información corporativa comercial.

En promedio, una persona revisa su correo electrónico **15 veces** al día.

Las personas tienen aproximadamente **2 cuentas** por usuario.

51% conserva su correo por más de 10 años y el **89%** revisa su correo a diario.

130 es el número de cuentas que en promedio se asocian a un correo.

Se envían más de **3 millones** de correos electrónicos cada segundo.

Tendencias globales



Fuente: Lexisnexis

TIPOS DE FRAUDE



HUMAN-INITIATED ATTACKS

Attack rates on individual online transactions that typically return full digital identity data have seen a significant rise in 2022, outpacing the growth in good customer transactions, with attacks continuing to shift to the mobile channels.

ATTACK VOLUME

905M

Growth YOY
+56% ▲



AUTOMATED BOT ATTACKS

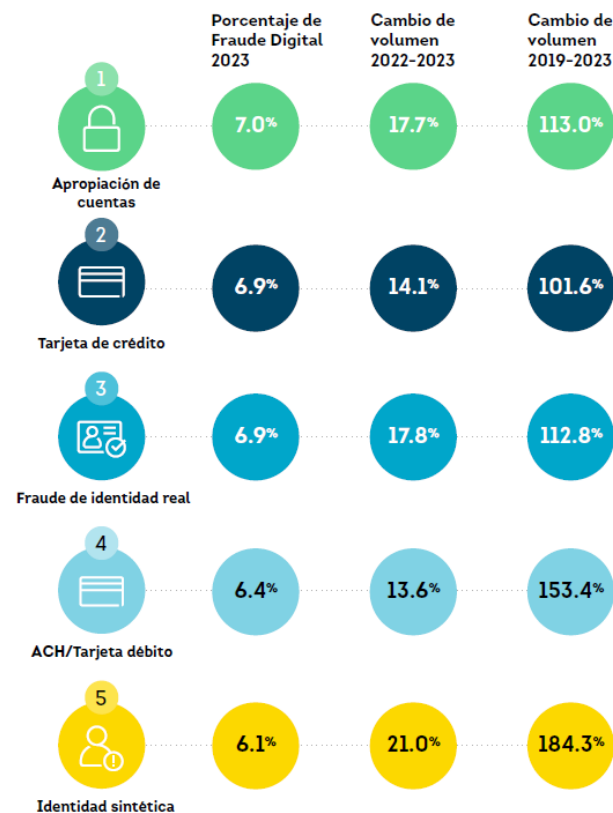
Automated bot attacks (typically used to credential test stolen identities at high volume) have shifted focus away from the communications, mobile and media (CMM) industry in 2022, focusing now predominantly on the ecommerce sector.

ATTACK VOLUME

3.5B

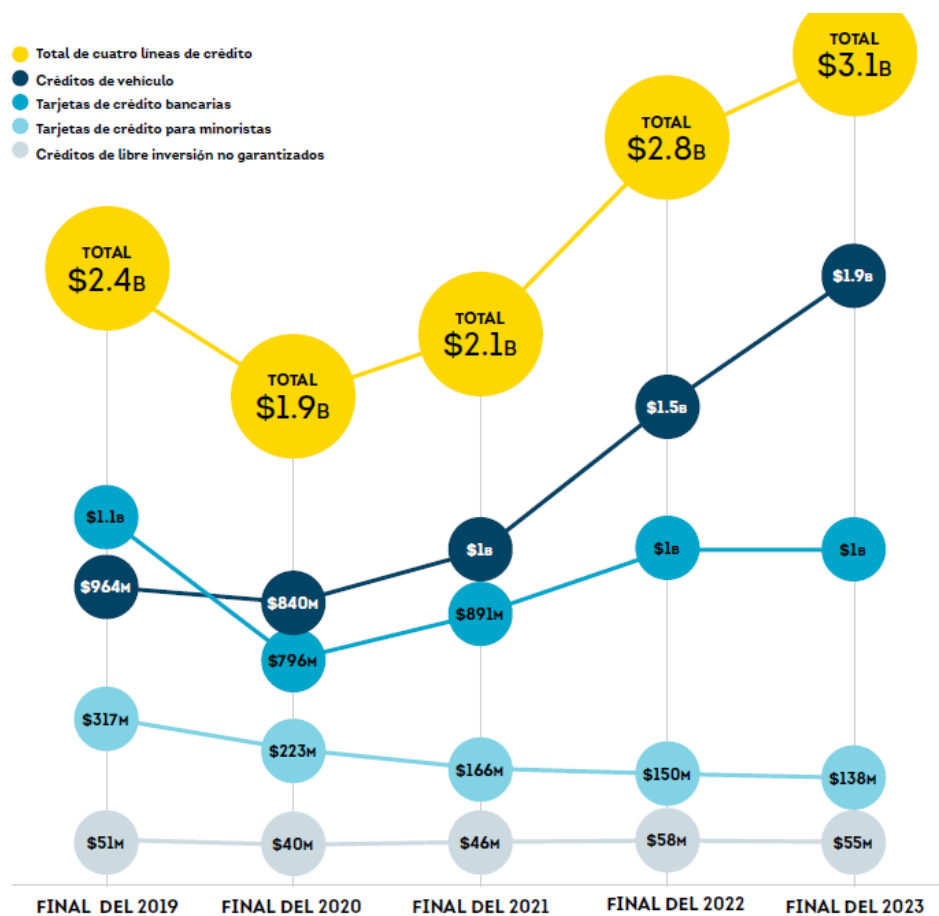
Growth YOY
+27% ▲

Tipos de fraude principales y su crecimiento



Fuente: Transunion

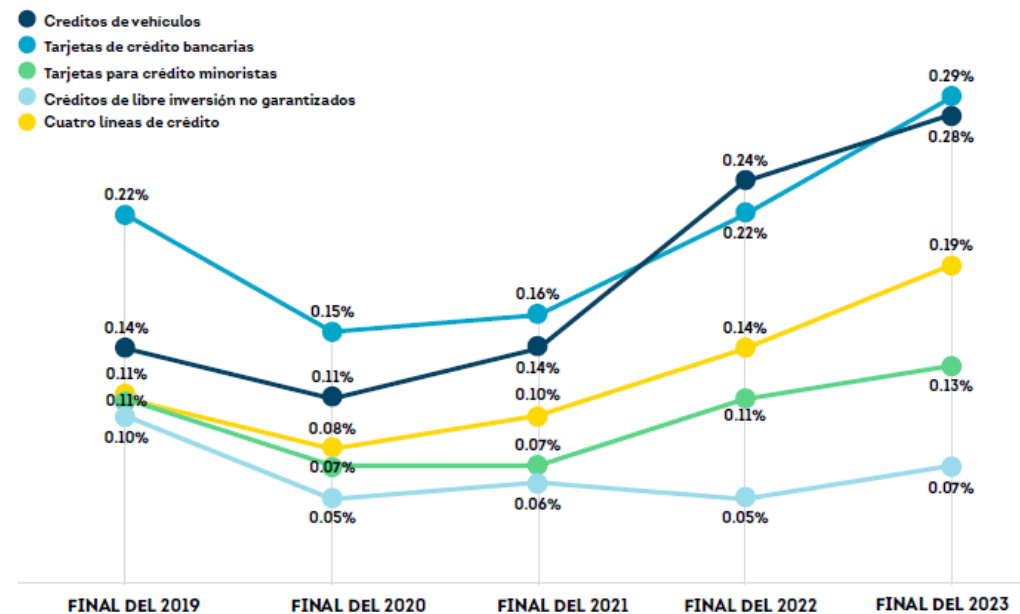
Tendencias globales



Fuente: Transunion

Identidades sintéticas en la apertura de cuentas

Porcentaje de cuentas recién abiertas en Estados Unidos asociadas con identidades sintéticas



¿Y en Colombia?

68%

De los profesionales indicó que la mayoría de las amenazas se producían por “accidentes de empleados” ⁽¹⁾

Modalidades

Phishing, fraude amistoso pruebas de tarjetas y robo de identidad ⁽³⁾

24.206

Casos de hurto por medios informáticos ⁽²⁾

7.203

Violaciones de datos personales ⁽²⁾

9.317

Accesos abusivos a sistemas informáticos ⁽²⁾

85%

De los delitos informáticos tienen un fin lucrativo ⁽⁴⁾

Tendencias de fraude

Los fraudes no son estáticos, se adaptan a medida que avanza la tecnología, cambian los modelos de negocio y surgen nuevas oportunidades.

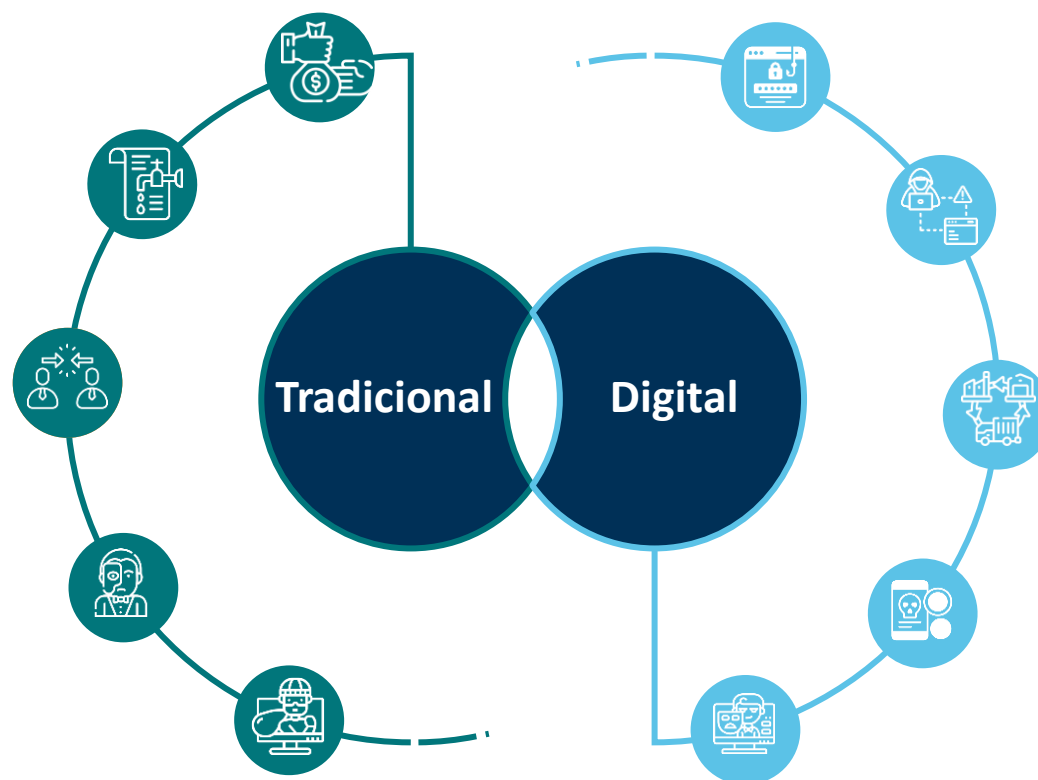
Corrupción, soborno y malversación de activos.

Abuso de información privilegiada.

Conflictos de interés.

Hurto de activos físicos.

Emisión de pólizas falsas.



Phishing avanzado e ingeniería social.

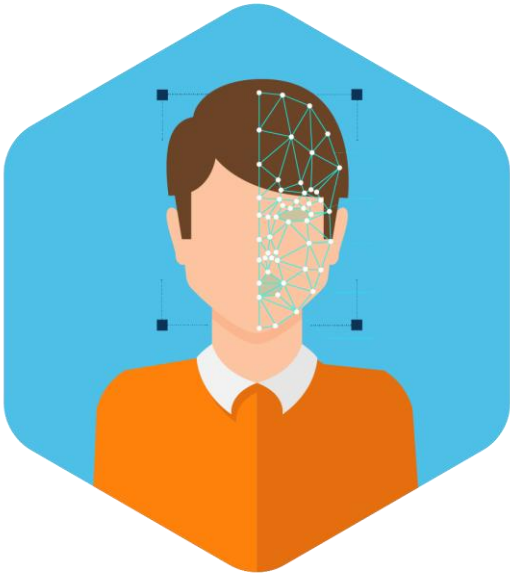
Sim Swap

Ransomware (secuestro de datos).

Robo de información.

Suplantación de identidad (identidades sintéticas).

IA: ¿Amiga o Enemiga?



VS



Reconocimiento facial

IA generativa en tiempo real

Fuente: <https://www.forbes.com.mx/como-la-ia-esta-potenciando-el-fraude-financiero-y-haciendolo-mas-dificil-de-detectar/>

Perfil del defraudador

Convencional

- 30-45 años.
- Manipulación de documentos o procesos físicos.
- Motivación: principalmente económica o deseos de venganza.
- Alcance: local o regional.
- Formación académica.
- Habilidades sociales, se muestran encantadores y son manipuladores.



Ciberdelincuente

- Desde los 15 años.
- Habilidades técnicas en informática.
- Motivación: búsqueda de experiencias, reconocimiento en el ciberespacio, política y económica.
- Alcance: global.
- Aprendizaje empírico.
- Introversión social en persona, ocultan su identidad, manipulación psicológica en el entorno digital.



Para más información consulte en: <https://inif.com.co/sin-enganos/>



Negocios inteligentes: el rol de la IA en la gestión antifraude

Contextualización

54%

Empresas habían utilizado IA generativa en sus negocios en noviembre de 2023, justo un año después de la publicación de ChatGPT (Pwc)

79%

De los estrategas corporativos afirmaron que tecnologías como la inteligencia artificial serían fundamentales para su éxito en los próximos dos años (Gartner, 2023)

34%

De todas las tareas relacionadas con la empresa son realizadas por máquinas (Foro Económico Mundial, 2023)

82%

De las grandes empresas colombianas incrementarán su presupuesto de IA en los próximos dos años (Microsoft, 2024)



IA en la gestión antifraude

PREVENCIÓN

- Reducción del **80%** en los fraudes de pago – identificación de transacciones sospechosas. ⁽¹⁾
- Ahorro de **\$1.000 millones** anuales en la industria de la salud gracias a la detección temprana de fraudes y errores médicos. ⁽²⁾
- Reducción del **50%** en los fraudes de identidad en la industria financiera. ⁽³⁾
- INIF mejoró su alertamiento de riesgo de fraude alto en un **55%** gracias al uso de técnicas analíticas. ⁽⁴⁾



DETECCIÓN

- Identificación de **85%** de los fraudes de seguro mediante la analiza de datos y patrones con IA ⁽⁵⁾
- Detección de **90%** de los fraudes de pago en línea: analizar patrones de comportamiento ⁽⁶⁾
- Reducción del **70%** en el tiempo de detección de fraudes en la industria financiera ⁽⁷⁾
 - **3.7 millones USD:** Ahorro generado por INIF a sus clientes por la gestión efectiva antifraude ⁽⁸⁾

IA + ética + capacitación + supervisión =
estrategia de negocios inteligentes



*En un mundo donde el fraude evoluciona constantemente, el verdadero enemigo no es la IA, sino la decisión de ignorarla y no **aprovechar su potencial en la optimización y defensa de nuestros negocios.***

Gracias



@inifsocial



inifsocial



inif



atencionalcliente@inif.com



www.inif.com