7 tendencias que marcarán el panorama de fraude e identidad en 2024

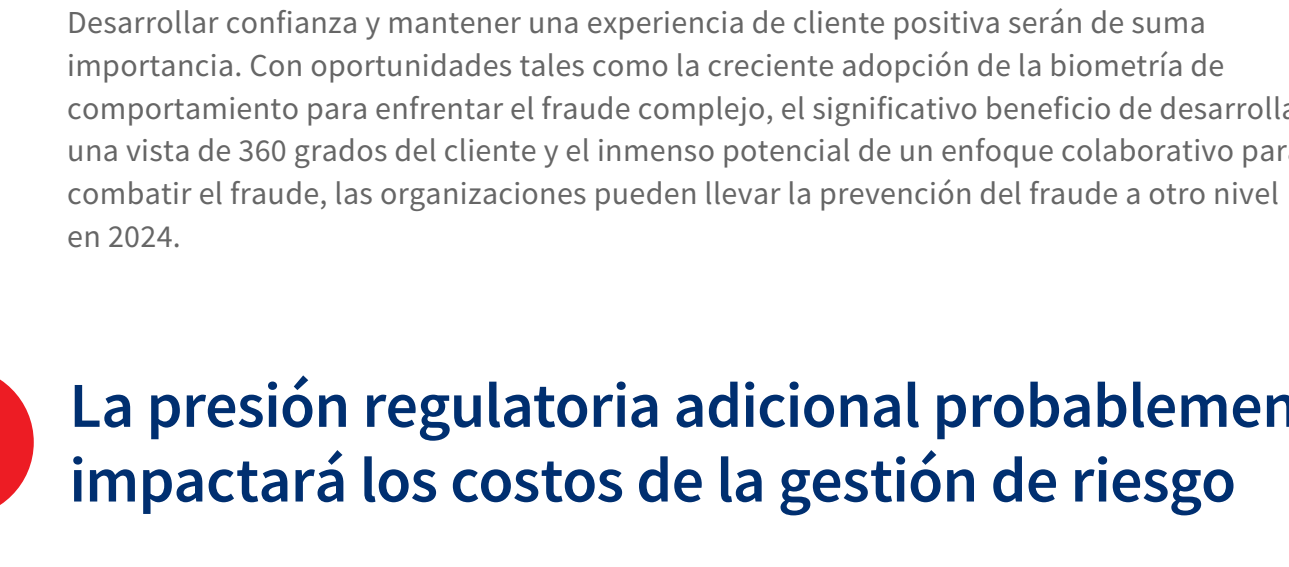
LexisNexis® RISK SOLUTIONS

Los profesionales de las áreas de fraude e identidad tendrán que enfrentar retos cada vez mayores tales como el impacto de la presión regulatoria creciente en muchas partes del mundo; el constante problema de fraude de identidad sintética; la utilización malintencionada de la inteligencia artificial con el carácter cada vez más interconectado y transfronterizo de los ataques de fraude.

Desarrollar confianza y mantener una experiencia de cliente positiva serán de suma importancia. Con oportunidades tales como la creciente adopción de la biometría de comportamiento para enfrentar el fraude complejo, el significativo beneficio de desarrollar una vista de 360 grados del cliente y el inmenso potencial de un enfoque colaborativo para combatir el fraude, las organizaciones pueden llevar la prevención del fraude a otro nivel en 2024.

1 La presión regulatoria adicional probablemente impactará los costos de la gestión de riesgo

En 2024 las organizaciones dedicarán aún más recursos a satisfacer exigencias regulatorias crecientes.



América Latina: Nuevas regulaciones para juegos y apuestas

El mercado regulado de apuestas en línea de América Latina se va a cuadruplicar y llegará a ingresos anuales de USD 6.750 millones a 2027, atrayendo jugadores tanto genuinos como malintencionados[8].

En Brasil una nueva ley de apuestas y juegos en línea que regula un mercado informal que genera más de **USD 30.000 millones** al año está a punto de ser aprobada[9].

El gobierno de Chile presentó recientemente un proyecto de ley que en la práctica legaliza las apuestas en línea. Se estima que un mercado legalizado podría generar ingresos de más de **USD 350 millones** al año[10].

En Perú, se han aprobado regulaciones para apuestas deportivas, creando mecanismos que protegen a los jugadores de fraudes o estafas potenciales.

EE.UU.: Persiste la incertidumbre sobre la responsabilidad por pérdidas debido a las estafas

La Electronic Fund Transfer Act [Ley de Transferencia Electrónica de Fondos] podría ampliarse para incluir las estafas con transferencias autorizadas. Las instituciones financieras están tomando medidas proactivas para detectar estafas y mitigar riesgos con visión a futuro.

82 % La mayoría de los líderes de servicios financieros que son responsables de las estrategias de riesgo y mitigación de fraude piensan que los consumidores esperan que los bancos los reembolsen por estafas exitosas que involucren a sus cuentas[1].

66 % Algunos consumidores estadounidenses dicen que probablemente cerrarían sus cuentas en una institución que no los reembolse por pérdidas debidas a estafas con transferencias autorizadas[2].

Reino Unido: Nuevos requisitos para pagos push autorizados [APP, por sus siglas en inglés]

El Regulador de Sistemas de Pagos del Reino Unido lanzó un nuevo sistema de reembolsos obligatorios para el fraude de APP, que en el último año le costó a los consumidores unos USD 630 millones[3].

Las nuevas normas exigen a bancos y otras compañías de pagos que reembolsen a víctimas de estafa a los pocos días, y el costo total debe ser compartido entre las organizaciones emisora y receptora.

A pesar de que los pagos resultantes del fraude de APP representaron menos de **0.1 %** del volumen general de pagos más rápidos en 2022, los pagos más rápidos se utilizan para **98 %** de los pagos de fraude de APP[4].

Los bancos más grandes del Reino Unido reportan hasta **USD 439** de pérdida por fraude de APP por cada USD 1,26 millones enviados en transacciones[5].

Los pagos push autorizados también son conocidos como 'estafas de transferencia autorizada' en EE.UU.

Europa: Propuesta de una nueva directiva de servicios de pagos y servicios de dinero electrónico (PSD3)

La legislación PSD3 desarrollará exigencias para priorizar intereses, seguridad y la confianza de los consumidores. Las propuestas incluyen:

- ampliación de los derechos de reembolso para víctimas de fraude;
- consolidación de las instituciones de dinero electrónico y de pagos bajo un régimen regulatorio unificado;
- garantía de que los consumidores tengan mejor protección y comprensión de sus derechos financieros.

Aunque ha sido eficaz en impulsar los pagos electrónicos y reducir el fraude, la PSD2 ha tenido costos de implementación (se estima en **USD 5.410 millones**) y mayores tasas de falla de transacciones, (se estima en **USD 36.200 millones**) que han sido sustanciales[6].

Las entidades que no cumplan con las exigencias de la PSD2 pueden ser multadas con hasta el **4 %** de sus ganancias anuales.

Hong Kong: Mayor seguridad para la banca electrónica

La Autoridad Monetaria de Hong Kong expidió medidas adicionales que aumentan la seguridad de la banca en línea y combaten el fraude digital. Los requisitos son obligatorios para todas las actividades de banca electrónica e incluyen:

autenticación adicional de clientes;

- revisión de límites de transferencias transfronterizas;
- controles de manejo de sesión que impiden intentos de inicio de sesión fraudulentos;
- una plataforma piloto de intercambio de información entre bancos que permite a estas instituciones compartir inteligencia de riesgo y tomar medidas de mitigación más ágiles.

India: Una nueva dirección en materia de ciberseguridad, controles de riesgo y gobernanza de TI

Las entidades bancarias y no bancarias reguladas deben cumplir con una nueva serie de normas expedidas por el Banco de la Reserva de la India, que incluyen un marco integral de gobernanza en TI para mitigar riesgos de ciberdelitos.

De los casi 53.000 casos de ciberdelincuencia que se registraron en 2021, **60 %** fueron de fraude[11].

Australia: Regulaciones para proveedores de pagos digitales

Las nuevas reglas propuestas por el gobierno de Australia buscan regular a los proveedores de billeteras digitales, permitiendo así al Banco de la Reserva de Australia monitorear transacciones de este tipo y de la misma manera en que lo hacen con redes de tarjetas de crédito.

Aumento de transacciones con billeteras digitales en Australia[12]

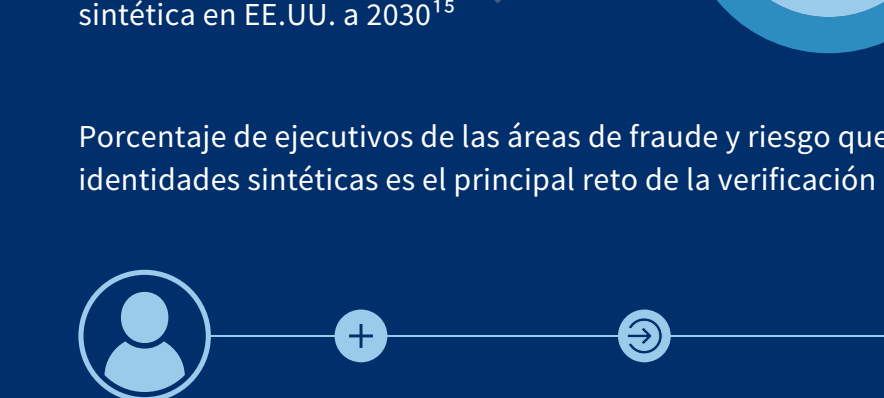
29,2 millones 2018 → **2.400 millones** 2022

2 Crecimiento explosivo del uso de identidades sintéticas

Los delincuentes explotan al auge de popularidad de la banca digital y el comercio electrónico para abrir cuentas fraudulentas nuevas con identidades sintéticas, las cuales combinan información real y ficticia. Enfrentar el fraude sintético será un complejo desafío de creciente prioridad en 2024.

El **48 %** de los minoristas y el **53 %** de las entidades financieras afirman que el auge de identidades sintéticas es el factor que más contribuye a dificultar la verificación de identidad en canales digitales[13]

Porcentaje de compañías que reportan un aumento de fraude de identidad sintética por región



52 % de compañías de todo el mundo reportan un aumento de fraude de identidad sintética en 2023[14]

USD 23.000 millones Valor esperado de pérdidas por fraude de identidad sintética en EE.UU. a 2030[15]

USD 81.000 - USD 98.000[16] Es la pérdida promedio por un fraude de identidad sintética no detectado

Porcentaje de ejecutivos de las áreas de fraude y riesgo que consideran que el auge de identidades sintéticas es el principal reto de la verificación de identidad durante:

- **55 %** Apertura de cuenta
- **55 %** Inicio de sesión
- **57 %** Transferencia / distribución de fondos[17]

3 El incremento en el uso de inteligencia artificial por parte de los delincuentes exigirá nuevas tácticas de mitigación de riesgo

La utilización malintencionada de inteligencia artificial (IA) está transformando el panorama de fraude y riesgo, aumentando la eficacia de los esfuerzos de los defraudadores y planteando nuevos retos al establecer y comprobar la identidad de una persona.

66 % De los profesionales de ciberseguridad detectaron ataques deepfake en sus organizaciones en 2022[18]

90 % Del contenido digital será generado en forma sintética a 2026, según estimativos[19]

4 Mayor utilización de inteligencia de comportamiento para enfrentar el fraude complejo

La biometría de comportamiento se está convirtiendo en una herramienta esencial para que las empresas y organizaciones desarrollen confianza con sus clientes y reduzcan el fraude, que es cada vez más sofisticado. Las empresas con visión a futuro que desean mejorar su estrategia de prevención de fraude y defenderse de estafas sofisticadas están acogiendo la biometría de comportamiento.

48 % de los ejecutivos del área de fraude clasificaron los ataques de estafas a consumidores entre sus principales preocupaciones en 2022[21].

USD 612 millones Pérdidas por estafas de pago push autorizado (APP) en el Reino Unido en 2022[23].

35 % de las organizaciones de servicios financieros de EE.UU. que respondieron habían implementado soluciones de biometría de comportamiento a septiembre de 2023[22].

A nivel global, **1/3** de las organizaciones están utilizado soluciones de biometría de comportamiento en toda la jornada del cliente[24].

Factores clave para la adopción de soluciones de biometría de comportamiento[25]

- Aceleración de la digitalización
- Fraude de apertura de cuenta nueva
- Fraude de apropiación de cuenta
- Fraudes/estafas de pago push autorizado (APP)
- Necesidades de autenticación fuerte de clientes [SCA, por sus siglas en inglés]
- Regulaciones KYC [conozca su cliente] y para la prevención de lavado de activos
- Cambios regulatorios relacionados con la responsabilidad
- Experiencia de cliente mejorada

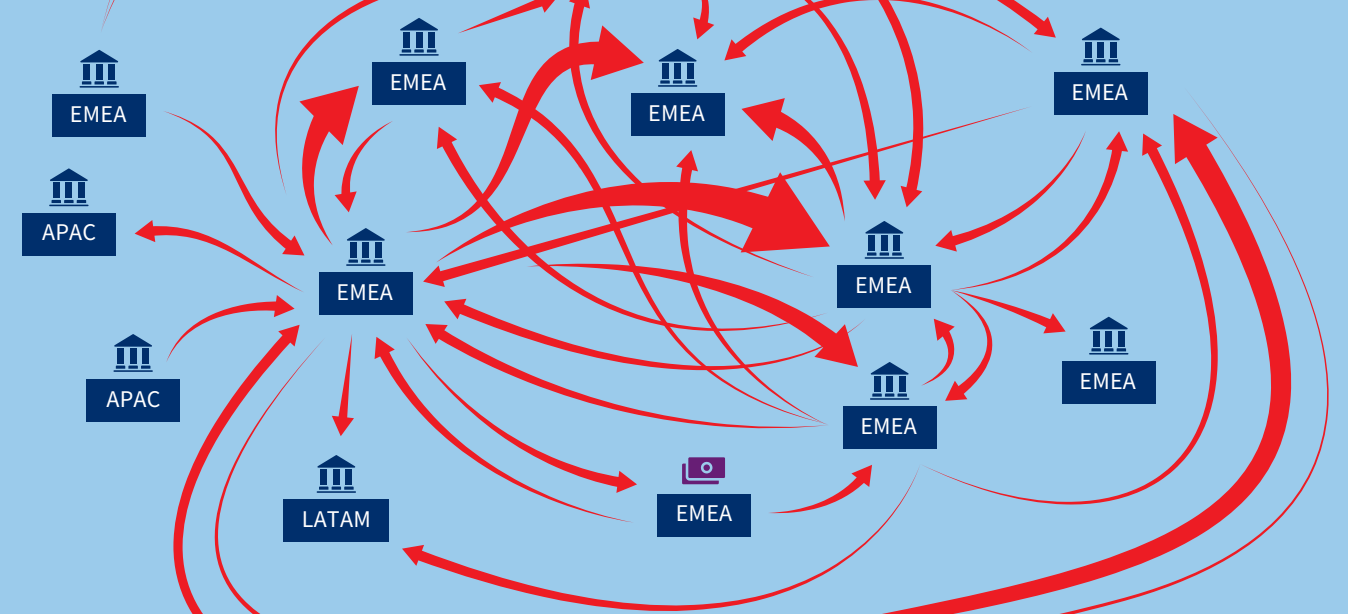
5 El fraude está cada vez más coordinado a través de las fronteras internacionales

Informes de inteligencia de amenazas sugieren aumentos significativos en coordinación y conexiones transfronterizas por parte de los ciberdelincuentes. Es de esperar que grupos de fraude organizados lancen más ataques coordinados en 2024.

Los ingresos internacionales representan el 39 % de los ingresos totales, pero comprenden el 57 % de todo el fraude para organizaciones de servicios financieros y comercio electrónico a nivel mundial[26].

Redes de mulas enlazadas por identidades digitales operan en regiones y dentro de entidades financieras, haciendo intentos de pago en una organización y después moviéndose a otras[27].

Una línea más gruesa indica un mayor volumen de identidades digitales e intentos de pago asociados.



Porcentaje de denuncias de fraude que fueron transfronterizas ante la Comisión Federal de Comercio[28]

1 % 1992 → **11 %** 2022

6 Adoptar una vista de 360 grados del cliente se está volviendo un imperativo para mejorar la evaluación de riesgo

Un enfoque más integrado y eficaz de la gestión de fraude comienza por comprender la multitud de canales e interacciones que utilizan los clientes para interactuar con las empresas.

82 % de los consumidores que compran en línea con su tarjeta de crédito también son usuarios activos de banca digital del mismo banco que expidió la tarjeta de crédito, lo cual significa que la inteligencia de identidad digital se puede compartir en canales para impulsar la confianza y prevenir el fraude más complejo[29].

3/4 de quienes respondieron reportan que el fraude ha afectado negativamente su marca y la experiencia de sus clientes[30].

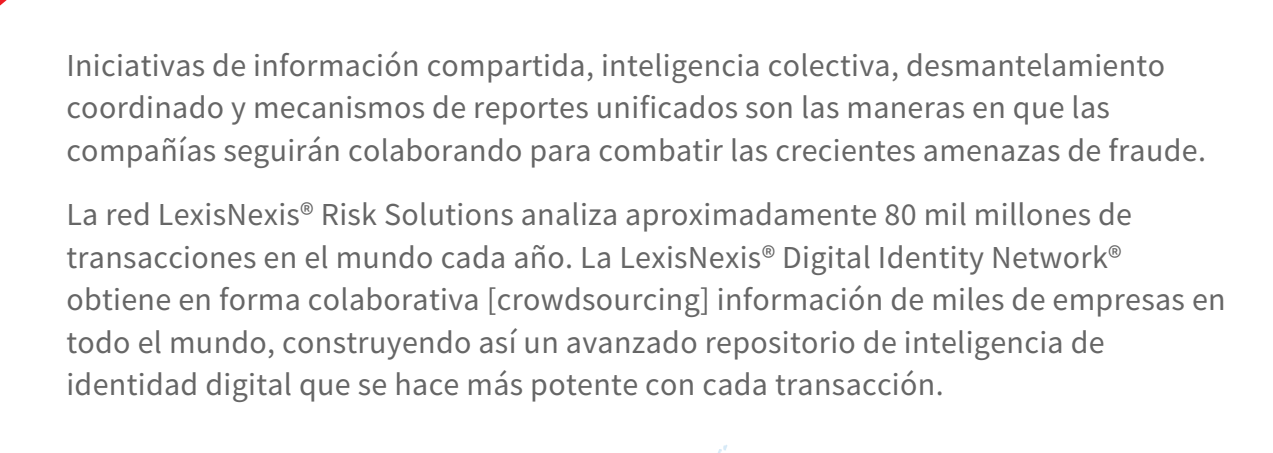
133% Aumento de 2021 a 2022 en el número de bancos que utilizan la red LexisNexis® Digital Identity Network® en canales tanto de banca digital como del protocolo 3D Secure CNP[31].

60%+ Mejora en la evaluación de riesgo durante eventos de pago posteriores por haber recolectado inteligencia digital contextual al momento de iniciar sesión[32].

7 Lucha colaborativa contra el fraude

Iniciativas de información compartida, inteligencia colectiva, desmantelamiento coordinado y mecanismos de reportes unificados son las maneras en que las compañías seguirán colaborando para combatir las crecientes amenazas de fraude.

La red LexisNexis® Risk Solutions analiza aproximadamente 80 mil millones de transacciones en el mundo cada año. La LexisNexis® Digital Identity Network® obtiene en forma colaborativa [crowdsourcing] información de miles de empresas en todo el mundo, construyendo así un avanzado repositorio de inteligencia de identidad digital que se hace más potente con cada transacción.



Esta visualización muestra ejemplos de redes regionales de fraude detectadas en la Red Digital Identity Network® durante un periodo de tres meses y dirigidas a bancos y operadores de redes móviles.

Esta red de fraude solo muestra conexiones de más de 10 identidades digitales. Una línea más gruesa indica un volumen más alto de ataques.

A medida que los ataques contra el sector financiero se vuelven más complejos, los defraudadores a menudo inician sus ataques obteniendo nuevos contratos de telefonía móvil o apropiándose de cuentas de clientes de servicios inalámbricos para su utilización posterior en intentos de apropiación de cuentas o nuevos fraudes con cuentas.

Al menos **USD 2,4 millones** valor del fraude bloqueado

Al menos **USD 10,3 millones** expuestos al fraude en toda la red[33]

Tipo de datos clave de la red LexisNexis® Digital Identity Network® crecen rápidamente

Tasa de crecimiento de año contra año por tipo de datos[34]

Números telefónicos	28 %
Identificadores de dispositivos activos	10 %
Dirección IP	20 %
Dirección de correo electrónico	19 %
Transacciones calificadas	14 %

LexisNexis® Digital Identity Network®

Países y territorios visibles en la Digital Identity Network®[35]

Cada segundo	90
Cada minuto	193
Cada hora	230
Cada día	238
Cada mes	245
Todas	249

Manténgase un paso al frente del fraude.

LexisNexis® RISK SOLUTIONS

1 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
2 LexisNexis Risk Solutions y Forrester, Estafas de transferencias autorizadas: Cómo las entidades financieras pueden transformar una epidemia en una oportunidad, 2023
3 Informe anual sobre el fraude en las finanzas del Reino Unido, 2022
4 Payment Systems Regulator, Informe sobre las estafas de APP, 2023
5 Payment Systems Regulator, Informe sobre las estafas de APP, 2023
6 Comisión Europea, Estudio sobre la aplicación y el impacto de la Directiva (UE) 2015/2366 sobre servicios de pago. (PSD2)
Autoridad Bancaria Europea, Directrices sobre la exclusión de red limitada en virtud de la DSP2
The Fintech Times, Los bancos " disruptores" son los que más fraudes cometen contra la APP, según un informe de PSR, 2023
7 Comisión Europea, Estudio sobre la aplicación y el impacto de la Directiva (UE) 2015/2366 sobre servicios de pago. (PSD2)
8 Vixio, Perspectivas en línea para América Latina, 2023
9 Games Magazine Brazil, 2023
10 SBC News, 2023
11 Financial Times, La India lucha contra el aumento del fraude digital, 2023
12 Reuters, Australia presenta un proyecto de ley para regular los proveedores de pagos digitales, 2023
13 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
14 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
15 Deloitte Center for Financial Services, Utilizar la biometría para luchar contra el creciente fraude de identidad sintética, 2023
16 Deloitte Center for Financial Services, Utilizar la biometría para luchar contra el creciente fraude de identidad sintética, 2023
17 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
18 World Economic Forum, ¿Cómo combatir el preocupante aumento del uso de deepfakes en la ciberdelincuencia?, 2023
19 World Economic Forum, ¿Cómo combatir el preocupante aumento del uso de deepfakes en la ciberdelincuencia?, 2023
20 World Economic Forum, ¿Cómo combatir el preocupante aumento del uso de deepfakes en la ciberdelincuencia?, 2023
21 Aite Novarica y LexisNexis Risk Solutions, Ataques de fraude multifacéticos, biometría del comportamiento como herramienta defensiva, 2022
22 Aite Novarica and LexisNexis Risk Solutions, Ataques de fraude multifacéticos, biometría del comportamiento como herramienta defensiva, 2022
23 Informe anual sobre el fraude en las finanzas del Reino Unido,, 2022
24 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
25 Aite Novarica and LexisNexis Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
26 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
27 LexisNexis® Risk Solutions Informe sobre los delitos cibernéticos, 2022
28 Comunicado de prensa de la Federal Trade Commission, Los informes de la FTC resumen los esfuerzos para combatir el fraude transfronterizo y el ataque de ransomware, 2023
29 LexisNexis® Risk Solutions Informe sobre los delitos cibernéticos, 2022
30 LexisNexis Risk Solutions El verdadero costo del fraude, 2023
31 LexisNexis® Risk Solutions Informe sobre los delitos cibernéticos, 2022
32 LexisNexis® Risk Solutions Informe sobre los delitos cibernéticos, 2022
33 LexisNexis® Risk Solutions Informe sobre los delitos cibernéticos, 2022
34 Análisis de datos del LexisNexis® Digital Identity Network®
35 Análisis de datos del LexisNexis® Digital Identity Network®