iupana™

Blindaje digital:

guía para la protección de la identidad y prevención del fraude en finanzas de LatAm

En colaboración con:

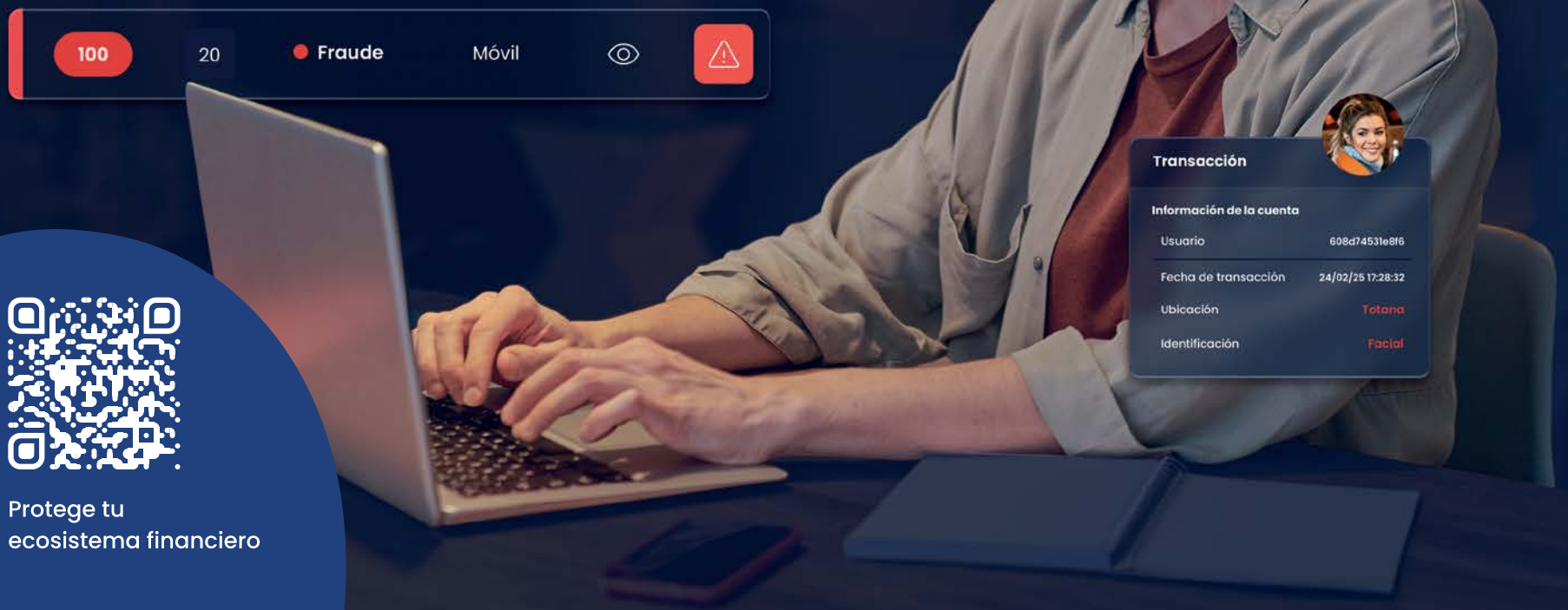
facephi | GOLD SPONSOR

jumio | SILVER SPONSOR

UNICO | BRONZE SPONSOR

facephi

Detección avanzada de cuentas mula



Protege tu
ecosistema financiero

Tabla de contenidos

La nueva era de inteligencia para proteger la información

Durante la Guerra Fría (1945-1991), las labores de inteligencia y contrainteligencia se enfocaban en el espionaje y la protección de información estratégica entre EE. UU. y la URSS para asegurar su poder global. Décadas después, y en la era digital, los ciberataques impulsados por inteligencia artificial (IA) buscan sustraer fondos, datos de bancos y fintechs, mientras la ciberseguridad y la protección contra fraude, también con IA, trabajan para detenerlos.

Este enfrentamiento moderno de inteligencia versus contrainteligencia –ahora artificial, pero capitaneada por estafadores reales–, pone en riesgo la confianza de los clientes y la reputación de las instituciones financieras.

El fraude con tecnología de punta busca superar controles o encontrar fisuras en la estructura de seguridad de un banco o fintech, poniendo en aprietos el valor de blindaje que estas instituciones deben transmitir.

En un mundo de banca digital, donde el onboarding remoto es clave, detectar deepfakes, clonaciones o documentos falsos se ha vuelto una batalla diaria. Los bancos deben innovar constantemente para mantener la identidad de sus clientes protegidas y, con ello, la confianza.

Este white paper tiene como objetivo advertir, explicar y señalar los aspectos clave que bancos y fintechs deben seguir de cerca para reducir los riesgos de fraude, sobre todo en una era de IA que está llevando las técnicas a un nivel más profesional.

Señalamos cómo prevenir las nuevas tecnologías utilizadas para superar pasos de identificación digital, explicamos cómo grupos financieros, como Banorte de México, invierten en su seguridad y enlistamos tendencias y tecnologías clave, sostenidas en IA, para prevenir ciberataques cada vez mejor orquestados.

Porque, coincidiendo con un entrevistado: solo la inteligencia puede combatir la inteligencia.

Queremos que este white paper ayude a las áreas de tecnología de bancos y fintechs, que impulse el desarrollo profesional de las personas involucradas y así evitar daños de reputación.

Antony Pinedo
Periodista ***iupana***

facephi

Identidad digital segura para frenar el fraude

Para más información,
visita **www.facephi.com**

Columna de expertos

Anticiparse al fraude: el nuevo imperativo en la era de la banca digital

Mauricio Arias
Director General para LATAM de Facephi

Cada día enfrentamos amenazas más audaces, dinámicas y sofisticadas. La suplantación de identidad, por ejemplo, se ha convertido en una de las formas más comunes y perjudiciales de fraude digital. El costo global de las ciberestafas alcanzó los 1.026 trillones de dólares en 2024, según la Global Anti-Scam Alliance (GASA). En este contexto, proteger la identidad digital y los activos financieros no puede limitarse a una respuesta reactiva: hoy, la clave está en anticiparse.

Uno de los desafíos más relevantes en el sector financiero es la proliferación de cuentas mula, utilizadas por redes criminales para el blanqueo de capitales y fraudes transaccionales. En 2023, solo en Estados Unidos, estas cuentas movieron más de 3,1 billones de dólares, de acuerdo con Nasdaq Verafin. Este fenómeno no solo compromete la integridad de las instituciones bancarias, sino que también involucra a usuarios que, muchas veces sin saberlo, se convierten en facilitadores de delitos financieros.

En Facephi creemos que ya no basta con verificar si alguien es quien dice ser, el verdadero salto cualitativo reside en la prevención proactiva. Por eso apostamos por un enfoque tecnológico avanzado que no solo autentica al usuario, sino que también interpreta señales contextuales, analiza el comportamiento digital y detecta patrones anómalos que permiten anticipar posibles fraudes antes de que ocurran.

No se trata únicamente de identificar a la persona detrás de la operación, sino de comprender su intención.

Tecnologías como inteligencia artificial, la multibiometría o sistemas de credenciales verificables deben actuar como un engranaje, no como herramientas aisladas. Esto no solo refuerza la detección, sino que aporta una comprensión más profunda del contexto y de la intencionalidad detrás de cada transacción.

Los ciudadanos debemos estar protegidos sin que nuestra experiencia de usuario se vea afectada, por eso es relevante a su vez en el desarrollo de tecnología implementar soluciones invisibles, sin fricciones y adaptadas al perfil de riesgo de cada usuario, protegemos su seguridad sin entorpecer su operativa diaria.

Sin embargo, la lucha contra el fraude no se gana solo con tecnología, sino también con colaboración. Las alianzas estratégicas entre bancos, fintechs y proveedores especializados están marcando la diferencia. Creando ecosistemas en los que compartir conocimiento, creando estándares comunes y adelantarse juntos al siguiente movimiento del fraude.

El futuro de la ciberseguridad financiera no pasa únicamente por innovar, sino por coordinar. Y en ese futuro, la capacidad de anticiparse será lo que realmente marque la diferencia entre estar protegido o ser vulnerable.

facephi

Facephi es una compañía tecnológica española que opera a nivel internacional y está especializada en la protección y verificación de la identidad digital que cotiza en el BME Growth. Sus soluciones se diseñan para crear procesos más seguros, accesibles y libres de fraude, prevenir la suplantación de identidad y garantizar un tratamiento ético de los datos personales.

facephi.com

Estrategias tecnológicas para reforzar la identificación y prevenir el lavado de dinero: el caso de los cárteles mexicanos

El aumento de presión desde Estados Unidos exige que las entidades financieras adopten nuevas estrategias transversales y herramientas tecnológicas que refuercen sus procesos de conocimiento del cliente.

Las instituciones financieras que empleen un mayor nivel de herramientas tecnológicas para crear procesos continuos de monitoreo estarán mejor posicionas para enfrentarse a los nuevos retos en el frente de la prevención de lavado de activos y el resguardo de la seguridad, como la designación de algunos cárteles mexicanos como organizaciones terroristas internacionales.

Este año, Estados Unidos elevó sus estándares de supervisión al clasificar a varios grupos no solo como bandas criminales, sino como organizaciones con fines terroristas, incrementando las labores de cumplimiento y reporte para las empresas que mueven remesas entre uno de los corredores de dinero más activos del mundo.
Para el sector financiero, la clave estará en balancear el peso de las nuevas exigencias, de la mano de la tecnología de punta, que afine los filtros de identidad del usuario, para incluso ofrecer una capa extra de protección a lo que exige la regulación.

> Invertimos muchísimo dinero en estructuras de gobernanza, recursos humanos, tecnológicas, operativas que nos permiten no solo cumplir con la regulación local, sino inclusive ir más allá en la vigilancia y supervisión de las operaciones de nuestros clientes".

Marcos Ramírez
CEO del Grupo Financiero Banorte

"Estamos dos o tres escalones arriba de los que nos piden", agregó durante la presentación de los resultados del primer trimestre de 2025 del principal conglomerado financiero mexicano.

El no cumplir con estas exigencias puede exponer a los negocios financieros, como remesadoras, bancos o fintechs a severas sanciones —incluyendo multas, restricciones, aislamiento del sistema global y la suspensión de operaciones —, además de la vulneración de la reputación y la relación de confianza con los clientes.

Por ende, las entidades requieren robustecer sus estrategias de prevención, e incluso apoyarse en empresas tecnológicas especializadas en detectar documentos o identidades falsas o patrones de comportamiento sospechosos de blanqueo de capitales.

Banorte reconoce que estar completamente exentos de riesgos es imposible, pero asegura que esa es la aspiración.

“No estoy minimizándolo y vamos a seguir muy atentos, vigilando todo y apretando todos nuestros modelos y todos nuestros canales de supervisión para impedir que por aquí entren los malos”, sentenció Ramírez.

Conoce a tu cliente, de punta a punta

Todo esto implica transformar el Know Your Customer (KYC) en un proceso continuo, no limitado al onboarding de los nuevos clientes, sino extendido a lo largo de toda la relación comercial. Las entidades deben monitorear activamente el destino de los recursos y detectar desviaciones del comportamiento esperado de los consumidores.

La respuesta ante este entorno no puede limitarse a controles tradicionales: las entidades deben adoptar un enfoque integral que combine herramientas de inteligencia artificial (IA), analítica de datos y biometría, entre otros, con un cumplimiento riguroso de estándares internacionales y locales.

> “No basta, simplemente, con conocer con quién estás tratando. Ahora el nivel de conocimiento tiene que ser mayor desde el inicio de la contratación”.

Rafael Fuentes
Consejero del estudio de abogados Pérez-Llorca en el área de Antilavado de Dinero, Anticorrupción y Cumplimiento.

En este sentido, las entidades deben tener en cuenta que, por ejemplo, mientras que según las disposiciones de Estados Unidos basta con establecer una relación indirecta para aplicar sanciones, en México se requieren pruebas más estrictas y categorizaciones distintas, lo que genera un desfase normativo.

También que, como explica el abogado “los estándares que aplican para lavado de dinero no son los mismos que los del financiamiento al terrorismo”.

Este desajuste se convierte en un punto crítico cuando se trata de operaciones transfronterizas; en

particular las remesas, que son una fuente legítima de ingresos para millones de mexicanos, pero que pueden ser un canal utilizado por el crimen organizado.

“Al ser una actividad naturalmente vinculada al efectivo y al cruce de fronteras, las remesas requieren un conocimiento estricto del cliente, pero también un entendimiento de su perfil operativo”, explica Fuentes.

La incorporación de tecnologías de IA está tomando un rol central para detectar documentos falsificados, identificar patrones anómalos en tiempo real y reducir falsos positivos en los sistemas de monitoreo. “No es solo firmar un contrato, es entender al cliente durante toda la vida del producto y adecuar el control al nivel de riesgo”, añade.

Javier Barrachina, director de R&D de Facephi, una plataforma para la protección de la identidad digital, coincide en que la IA está reduciendo la exposición, también en momentos cruciales de la contratación de productos y servicios que, aunque debe ser ágil y rápida, también blindada.

> “En procesos como el onboarding digital, la IA valida identidades de forma automatizada y segura, cruzando datos de documentos, biometría facial y señales contextuales. Esto reduce el fraude de identidad y mejora la experiencia del usuario, eliminando fricciones innecesarias”.
>
> **Javier Barrachina**
> Director de R&D de Facephi

Tecnologías biométricas para reforzar el KYC

Las zonas geográficas de alto riesgo, donde operan organizaciones criminales, representan un desafío particular para los procesos de verificación de identidad. Según investigaciones, los cárteles suplantan o coaccionan a individuos para abrir cuentas bancarias, enviar remesas o acceder a productos financieros.

La documentación tradicional –como credenciales de identidad nacional o comprobantes de domicilio– puede ser manipulada o falsificada con

facilidad. Ante ello, tecnologías como la verificación biométrica, la validación cruzada con bases de datos oficiales y el uso de IA para detectar documentos falsos se vuelven esenciales.

Las entidades deben monitorear activamente el destino de los recursos y detectar patrones de comportamiento rotos para elevar las banderas rojas.

> Todas las instituciones financieras del país tienen que estar volviendo a revisar todos sus procesos de cumplimiento, porque sí es algo serio y hay que tomárselo así".

Felipe Vallejos
Presidente de la Asociación Fintech México

"La tecnología no es solo para el servicio al usuario, también se utiliza en las áreas de cumplimiento de las fintechs, que es un sector listo para poder hacer una detección y monitoreo efectivo de este tipo de organizaciones y poder cumplir con estas reglas de manera rápida. Creo que estamos bastante bien posicionadas", dijo el también gerente general de la plataforma de criptomonedas Bitso, que utiliza monedas estables para brindar servicio de remesas, en un encuentro con periodistas a inicios de mayo.

Fabiola Seminario
Periodista ***iupana***

Antony Pinedo
Periodista ***iupana***

Columna de expertos

¿Le otorgarías un crédito a alguien con historial de fraude?

Conoce el primer Buró de Fraude Digital, capaz de reconocer al 70% de los defraudadores del mercado mexicano.

Con más de una década de experiencia en inteligencia artificial aplicada a los sectores bancario y fintech, he aprendido que la tecnología debe desarrollarse con un enfoque centrado en el usuario, especialmente para enfrentar uno de los desafíos más crónicos del entorno digital: el fraude.

La identidad digital es cada vez más frágil. Y al tiempo que la verificación biométrica impulsa la inclusión financiera y la eficiencia, también se ha abierto un frente al fraude digital, cada vez más sofisticado.

Paradójicamente, la misma tecnología que puede vulnerar, también es clave para proteger. La IA, aplicada correctamente, se convierte en una extensión poderosa de las soluciones antifraude, capaz de reconocer patrones y anticipar amenazas.

En América Latina, el 51 % de las pérdidas por fraude provienen de canales digitales.

El crecimiento de los servicios digitales sin mecanismos claros de verificación, sumado a la falta de coordinación entre actores clave, han posicionado a México como líder en fraude digital.

Nuestro informe A Year in Fraud 2024 reveló un incremento del 84% en fraudes por suplantación digital en tan solo un año en México. Más que generar alarma, esto debe encender una señal para colaborar.

Hoy, el reto no es implementar más tecnología, sino articular redes de colaboración y reconocer la identidad como lo que es, algo vivo y profundamente humano.

Fernando Paulín
CEO - México
UNICO

4 tendencias de riesgos digitales: deepfakes, datos robados, suplantación y bots

La inteligencia artificial y el mercado negro de datos personales están escalando los riesgos digitales, obligando a los negocios financieros a reforzar sus defensas.

Los ciberdelincuentes están intensificando sus intentos de fraude y cibertaques hacia fintechs y bancos en América Latina, explotando deepfakes y datos personales robados para suplantar identidades, afectando a empresas y usuarios en procesos de onboarding digital para ahorro o crédito.

En la región, donde propuestas fintechs como Nu o Mercado Pago lideran la digitalización financiera, los videos o fotografías manipuladas, y otros esquemas impulsados por inteligencia artificial generativa, podrían generar pérdidas de hasta $ 40.000 millones en el sector financiero global para 2027, según Deloitte.

> Los ciberdelincuentes cada día tienen técnicas más sofisticadas; el tema de fraude se va a poner más complejo con avances como los deepfakes".
>
> **Daniel Rodríguez**
> Director de Tecnología de la fintech de crédito Juancho Te Presta

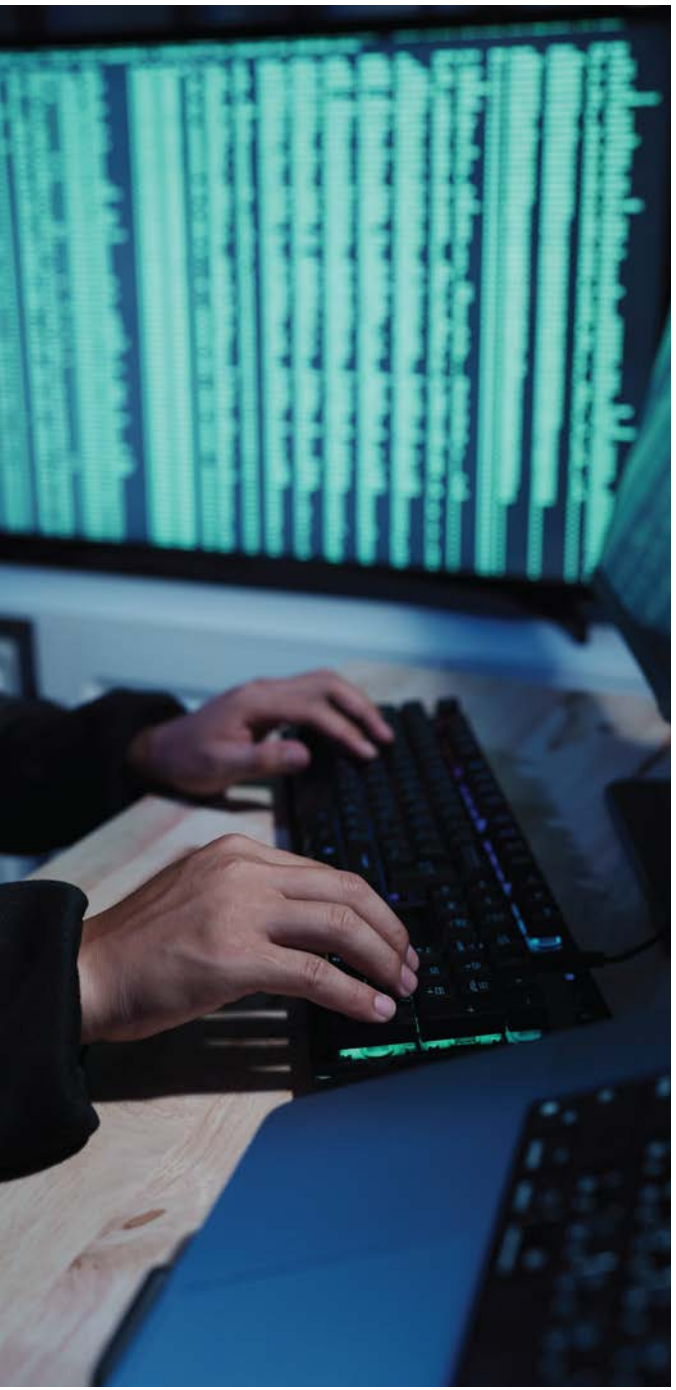
Ante este panorama, hemos enlistado las 4 tendencias de fraude de identidad que debes tener en cuenta en tu estrategia de mitigación de riesgos:

1. Deepfakes: rostros falsos, riesgos reales

Los deepfakes, impulsados por inteligencia artificial generativa (GenAI por sus siglas en inglés), representan una amenaza creciente, capaz de retar validaciones biométricas al imitar rostros y voces con precisión.

Starling Bank, una entidad financiera del Reino Unido, alertó en septiembre de 2024 sobre un aumento significativo en estafas que emplean la clonación de voz con IA. Los delincuentes replican la voz de una persona con tan solo tres segundos de audio y utilizan voces clonadas para solicitar transferencias de dinero bajo pretextos urgentes.

> **El deepfake probablemente evolucione hasta que te veas idéntico. Te pueden alterar o suplantar la voz, casi toda la biometría. Entonces, se va a poner más complicado con este tipo de avances y definitivamente lo que hay que hacer es combatir inteligencia artificial con inteligencia artificial", anota Rodríguez desde Colombia.**



En 2024, la oficina en Hong Kong de una empresa multinacional perdió HK$ 200 millones (unos US$ 25 millones) tras una estafa con deepfakes de video, donde estafadores imitaron al director financiero y otros colegas en una videollamada, engañando a un empleado para que realizara transferencias fraudulentas; este es un caso que grafica los riesgos crecientes de la inteligencia artificial en fraudes financieros.

2. Contrabando de datos: el mercado negro digital

El contrabando de datos, que circulan en mercados negros de Europa del Este, permite a ciberdelincuentes adquirir números telefónicos y documentos de identidad válidos, alimentando fraudes en fintechs de crédito.

> “El que está metido años en este tema ya sabe que existen estos famosos proveedores de información”.
>
> **Mario Cruz**
> Fundador de la fintech peruana de préstamos Wolet

Según Cruz, las mafias compran las bases de datos de números telefónicos y los vinculan a un documento de identidad.

“Si no tienes una buena validación de identidad y no sabes si eso lo está haciendo un bot, tienes un vacío. Vas a aceptar a estas supuestas personas como válidas, cuando esta persona, el dueño del documento de identidad, no te está pidiendo un crédito”, complementó.

En Perú, en 2024, el Registro Nacional (Reniec) fue víctima de la filtración de datos y se expusieron números de cédulas y datos personales de millones de ciudadanos, vendidos en mercados negros, habilitando fraudes en plataformas digitales, según El Comercio. Aunque luego la entidad pública dijo que la base de datos filtrada estaba desactualizada.

3. Suplantación de identidad: el engaño personalizado

La suplantación de identidad sigue siendo uno de los fraudes más frecuentes en plataformas digitales. Las fintechs y bancos son especialmente vulnerables por la creciente oferta de onboarding digital.

En febrero de 2025, autoridades mexicanas desmantelaron un

laboratorio clandestino en Ciudad de México, disfrazado como peluquería, donde se elaboraban documentos oficiales falsos; se hallaron equipos de cómputo con bases de datos reales y actualizadas de ciudadanos, así como herramientas para la creación de credenciales apócrifas, lo que sugiere la posibilidad de manipulación de datos biométricos como huellas dactilares.

En este contexto, la captación de los documentos con cámara, los procesos de verificación de biometría —facial, del iris o de voz, o incluso de comportamiento— como manipulación de los dispositivos, son puntos críticos del onboarding y exigen contar con tecnología que identifique elementos que a vista humana son imperceptibles.

Banca Mifel, en México, ofrece cuentas de ahorro con rendimientos de manera remota, el proceso lo realiza con múltiples factores de autenticación para prevenir quedar expuestos a esquemas de robo de identidad o fraudes.

> Llega un código al celular del cliente, quien tiene que garantizar ese código. Además, después hacemos llamadas de confirmación, y eso lo hacemos de forma aleatoria. No significa que en el camino no podamos tener de repente un usurpador, pero sería muy difícil: se tendría que haber robado tu INE (identificación mexicana), tener tu celular, haber contestado el código de confirmación y si aleatoriamente le tocó la llamada".

Daniel Becker
CEO, Banca Mifel

También, los montos de saldos mensuales que pueden resguardar las cuentas, incluso las de alto valor, están limitados para prevenir movimientos excesivos de fondos.

"Lo acotamos por diferentes maneras. Yo diría que nuestros procesos de seguridad están bastante sólidos".

4. Bots automatizados: ataques silenciosos

Los bots están sofisticándose y ejecutan ataques automatizados que emulan el comportamiento humano, burlando sistemas de validación con rapidez y precisión. Son una de las herramientas preferidas de los ciberdelincuentes para escalar el fraude digital.

Entre marzo y mayo de 2024, Kaspersky detectó más de 4.700 páginas de phishing respaldadas por bots en América Latina, diseñadas para interceptar códigos de autenticación de doble factor.

> **Cada día es una lucha... tienes que estar aprendiendo, innovando y trabajando con aliados", explicó Rodríguez, de Juancho Te Presta.**

Antony Pinedo
Periodista ***iupana***

Mitzy González
Periodista ***iupana***

Columna de expertos

Investigación de Jumio revela que la confianza en la vida digital desmejora ante el auge del fraude y los deepfakes impulsados por IA

La cuarta edición del Estudio 2025 de Jumio revela una caída en la confianza digital, impulsada por deepfakes, desinformación y ciberdelincuencia. De más de 8,000 encuestados entre México, Estados Unidos, Reino Unido y Singapur, el 79% de los mexicanos percibe el fraude con IA como una amenaza mayor que el robo de identidad.

La confianza digital se ve impactada por el crecimiento de la preocupación por la IA.

El 76% de los mexicanos son más escépticos sobre el contenido online por el fraude con IA, frente al 69% global. Solo el 37% confía más en la autenticidad de cuentas en redes sociales, mientras que el 36% afirmó confiar más en las noticias online, a pesar de la posibilidad de encontrarse con deepfakes o contenido manipulado.

La mayoría de los consumidores mexicanos expresan preocupación por fraudes impulsados por IA

- Documentos de identidad falsos (86%)
- Emails fraudulentos para engañar a la gente para entregar contraseñas o dinero (84%)
- Falsificaciones de vídeo y voz (83%)
- Contenidos manipulados en las redes sociales (83%)

Aunque reconocen los riesgos del entorno digital, muchos carecen de herramientas para detectar contenido auténtico.

Ante el avance del fraude con IA, los consumidores esperan que las empresas tecnológicas asuman el liderazgo

Aunque el 93% de los consumidores confía más en sí mismos para proteger sus datos ante la falta de regulación, el 43% cree que las Big Tech deberían ser responsables de frenar el fraude con IA, frente al 18% que se atribuye esa responsabilidad.

El Estudio 2025 de Jumio destaca una creciente brecha de confianza online, impulsada por amenazas en evolución como el fraude como servicio (FaaS) con kits de herramientas que facilitan ataques sofisticados incluso a estafadores sin experiencia mediante identidades sintéticas, deepfakes y bots.

Estos cambios, obligan a las empresas a reforzar sus defensas contra el fraude con IA. Paralelamente, el estudio revela que los consumidores están dispuestos a asumir verificaciones más rigurosas, especialmente en banca, donde el 80% lo acepta.

Los consumidores merecen seguridad avanzada y mayor transparencia de las empresas.

A medida que crece la vida digital, las empresas deben ofrecer seguridad avanzada para combatir el fraude de IA, ofreciendo verificación de vanguardia, monitoreo en tiempo real y un enfoque de "confianza cero", además ganarse la confianza del consumidor.

Conoce más de los resultados clave del Estudio Sobre Identidad Online

Aquí

Samer Atassi

VP para América Latina

jumio

Gestión proactiva de los riesgos digitales aterrizada a una región con deudas de inclusión financiera

Las entidades financieras de LatAm ya no pueden limitarse a reaccionar ante las amenazas digitales: deben anticiparlas. Con inteligencia artificial, biometría avanzada y otras tecnologías, la banca tiene el reto de seguir cerrando su brecha de atención.

El phishing, la suplantación de identidad y el uso indebido de los datos personales son amenazas digitales que se han sofisticado a tal punto que obligan a las entidades bancarias a abandonar sus modelos de defensa reactiva para adoptar estrategias de gestión proactiva del riesgo.

Para Javier Barrachina, R&D director de Facephi —dedicada a validación de la identidad digital—, en esta nueva era de fraude tecnológico proteger los activos de los usuarios y las instituciones empieza por salvaguardar su información.

> “Uno de los principales desafíos actuales es el fraude de identidad, impulsado por la proliferación de herramientas, como los deepfakes y las identidades sintéticas. Estas tecnologías permiten a los atacantes crear perfiles falsos altamente convincentes, comprometiendo los sistemas tradicionales de verificación”.

Javier Barrachina
R&D director de Facephi

Pero ¿qué significa proteger la identidad digital de un cliente financiero en una región como Latinoamérica, donde persisten las brechas de digitalización, educación e inclusión?

Ante este panorama, la agilidad de la infraestructura tecnológica se vuelve una herramienta tan importante como la actualización constante de la misma.

Julio González, gerente de Tecnología y Data de la entidad de microfinanzas Fondo Esperanza de Chile, explicó que la organización ha experimentado un proceso de modernización digital, donde se han priorizado la protección de la infraestructura. No obstante, la organización también reconoce que la seguridad efectiva debe ser inclusiva: los mecanismos de autenticación y control no pueden convertirse en barreras adicionales para los usuarios.

Detecta el fraude de manera proactiva con inteligencia conectada

La función de Cross-Transaction Risk conecta elementos de identidad en toda la red de Jumio para revelar patrones de comportamiento tanto confiables como fraudulentos.

- Tomar decisiones más rápidas y fundamentadas
- Detectar y detener el fraude de forma proactiva
- Reducir los costos operativos
- Aumentar la confianza de los usuarios

jumio®

Obtén más información en
jumio.com/es

> Si la seguridad excluye entonces no sirve y no cumple su propósito en nuestra misión".

Julio González
Gerente de Tecnología y Data del Fondo Esperanza

Así, tecnologías como la biometría adaptada a móviles de diferentes gamas y las soluciones de identidad digital interoperables (como la Clave Única de Chile, una contraseña para autenticar digitalmente la identidad de una persona) se presentan como herramientas clave para lograr un balance entre seguridad y usabilidad.

Para el sector financiero la prioridad no es solo endurecer los sistemas frente a ataques, sino también garantizar que todos los segmentos de la población –especialmente los más vulnerables– puedan acceder de manera segura y sin fricciones a los servicios digitales.

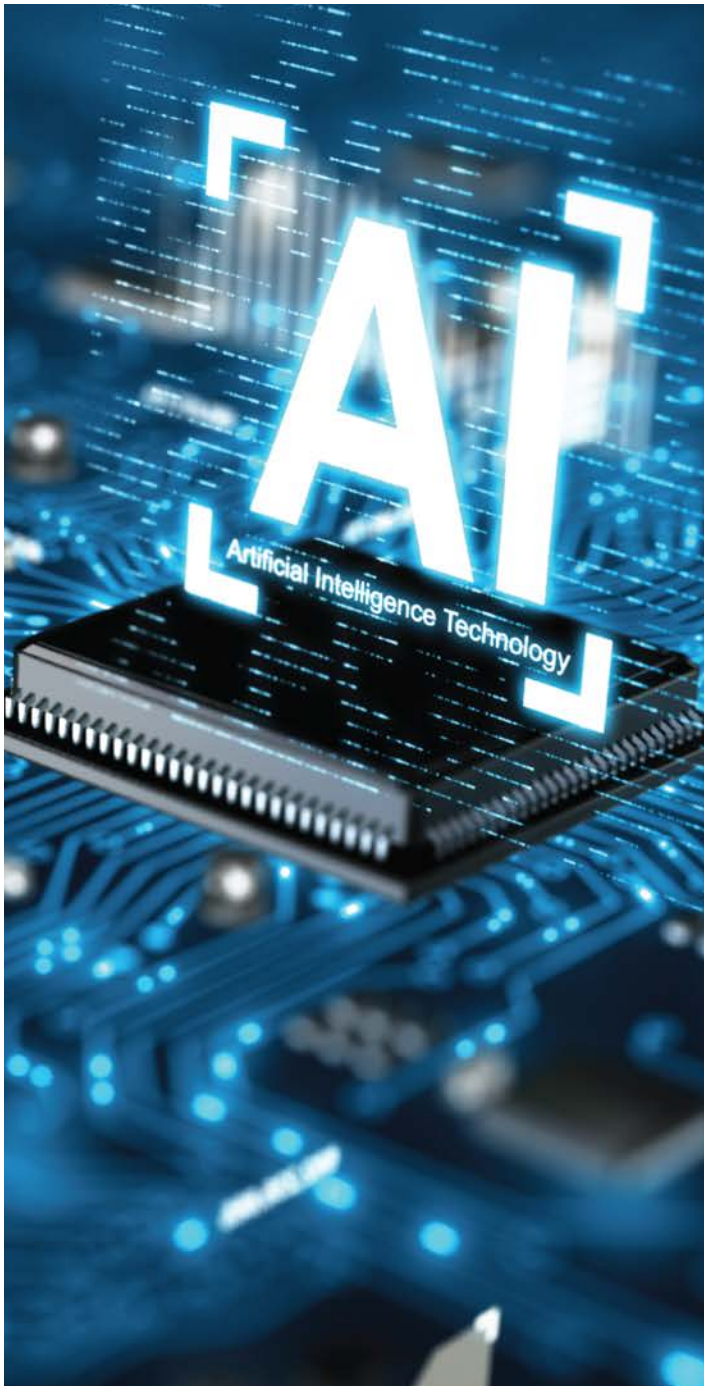
"La continuidad operativa y la capacidad de responder rápido ante incidentes son fundamentales. Esto será clave para anticiparnos y reaccionar cuanto antes ante cualquier comportamiento anómalo o interrupción en nuestros servicios digitales", agrega González.

Uso de IA: nuevas fronteras para la protección digital

En ese contexto, la inteligencia artificial (IA) está revolucionando la forma en que las instituciones financieras enfrentan el riesgo digital. Su capacidad para analizar grandes volúmenes de datos en tiempo real permite detectar patrones anómalos y prever ataques antes de que ocurran.

En Fondo Esperanza, la IA ya forma parte de la operación diaria en áreas generales de análisis de datos. También, exploran cómo utilizar la herramienta en procesos críticos como el onboarding digital, enfocándose en la verificación de identidad. Gracias a su colaboración con la Fundación Microfinanzas BBVA, accionista del fondo, han podido aprender de experiencias en la protección de datos biométricos y en la adopción de tecnologías de identificación seguras que cumplen con normativas de protección de datos.

Estas capacidades prometen transformar la gestión de riesgos, llevando a las entidades a un modelo



más preventivo que reactivo, que evoluciona con cada interacción y ajusta sus predicciones a nuevas amenazas.

Barrachina, de Facephi, coincide en la necesidad de enfoques holísticos que integren múltiples capas de tecnología, protección y anticipación. Incluso, el blockchain aporta valor al permitir procesos auditables, con integridad garantizada en cada transacción.

> **La combinación de biometría avanzada, IA y análisis de contexto está revolucionando la forma en que las instituciones financieras enfrentan los riesgos digitales", enumera Barrachina.**

El must tecnológico de seguridad en la banca

De esta manera vemos cómo la tecnología de seguridad ya no opcional, sino una obligación estratégica, que lleva a los bancos, de cualquier tamaño y segmento, a priorizar una infraestructura de seguridad robusta, capaz de ofrecer protección avanzada sin sacrificar el acceso a los servicios. Hoy, las mejores prácticas apuntan a arquitecturas en la nube con segmentación de tráfico, controles de acceso granulares y herramientas de monitoreo, que permitan detectar y mitigar incidentes en tiempo real.

El futuro de la seguridad digital no solo será más tecnológico, sino también más personalizado y predictivo. Para el gerente de Fondo Esperanza, los próximos grandes avances vendrán de la mano de:

- **Análisis predictivo:** que permita correlacionar señales débiles y prevenir amenazas.

- **Soluciones modulares y adaptables:** ideales para organizaciones sociales y financieras que necesitan eficiencia en el gasto tecnológico.

- **Identidad digital soberana:** con portabilidad y control ciudadano sobre los datos personales (derechos ARCO: acceso, rectificación, cancelación y oposición).

> **Los avances en identidad digital, como la portabilidad y el control ciudadano de los datos, serán fundamentales para proporcionar una autenticación segura sin crear nuevas barreras de acceso", destaca el ejecutivo.**

Desde Facephi se refuerza esta visión con una proyección clara: "el futuro de la autenticación se orienta hacia soluciones más inteligentes, invisibles y personalizadas".

Tecnologías como el reconocimiento de voz con análisis emocional, la biometría del iris y la autenticación continua marcarán el nuevo estándar en el que cada interacción del usuario se convierta en una oportunidad para verificar su identidad sin interrumpir su experiencia.

Fabiola Seminario
Periodista ***iupana***

iupana™

Blindaje digital: guía para la protección de la identidad y prevención del fraude en finanzas de LatAm

Junio 2025

iupana.com