Construyendo confianza en un mundo engañoso

Estudio de Experian llevado a cabo por Forrester Consulting

Te damos la bienvenida al informe sobre el fraude 2026 de Experian

En los últimos años, hemos visto una expansión considerable de las amenazas de fraude. El fraude se ha vuelto más organizado y estructurado, con herramientas cada vez más potentes que impulsan un aumento en la escala y la sofisticación de los ataques.

Zonas enteras se han convertido en megafábricas de estafas dedicadas a atacar a personas inocentes de todo el mundo. Y existe una amenaza cada vez mayor de que organizaciones criminales con apoyo o protección estatal participen en estos ataques coordinados, lo que lleva a algunos expertos a sugerir que estamos en medio de la era dorada del fraude.

Para hacer frente a este desafío se requiere de una mayor colaboración, ya que los esfuerzos individuales son mucho más efectivos cuando se combinan. Las organizaciones que forman parte de la red de consorcios contra el fraude de Experian perciben una reducción significativa en las pérdidas por fraude cuando se apoyan en la inteligencia colectiva compartida en el grupo.

También se ha vuelto esencial que las empresas aprovechen las tecnologías más avanzadas de prevención del fraude. La IA se ha convertido en un elemento fundamental para esta defensa, ya que tanto el Machine Learning como la IA generativa permiten identificar mejor a los estafadores, adaptarse rápidamente a los cambios y gestionar de manera más efectiva los sistemas antifraude, lo que ayuda a proteger a las empresas y a sus clientes.

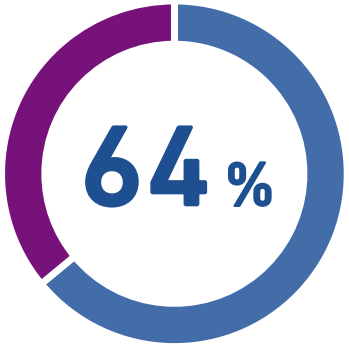
En la investigación de este año, realizada junto con Forrester Consulting, entrevistamos a cerca de mil responsables de toma de decisiones antifraude de nueve países, sobre sus puntos de vista en cuanto a las grandes tendencias que afectan la prevención del fraude. Estoy segura de que sus conocimientos te ayudarán a perfeccionar tu estrategia contra el fraude de cara al próximo año.

Y cuando quieras más información sobre nuestra plataforma integral de prevención del fraude, nuestro equipo de consultores estará encantado de hablar contigo.

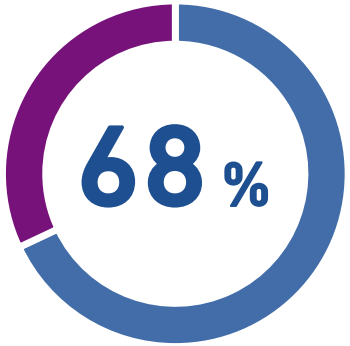
SHAIL DEEP
COO de Experian para EMEA y APAC

Índice de contenidos

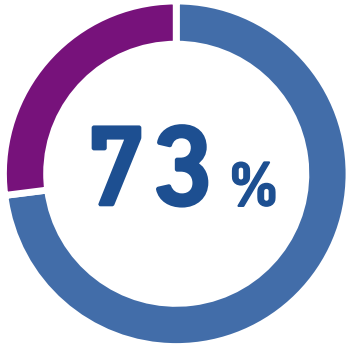
Resumen de los principales hallazgos



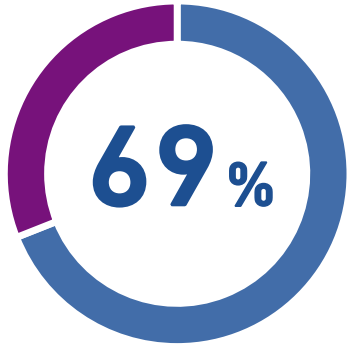
afirma que sus pérdidas por fraude han aumentado año tras año.



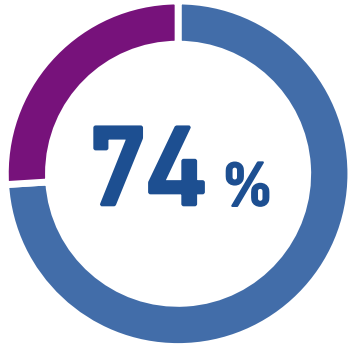
está de acuerdo en que su tecnología actual es inadecuada para contrarrestar una amenaza de fraude en rápida evolución.



tiene interés en invertir en controles pasivos contra el fraude, como análisis del comportamiento o de dispositivos, para minimizar la fricción.



planea integrar la prevención del fraude y la evaluación del riesgo de crédito en una estrategia general de gestión de riesgos.



está de acuerdo en que, en los próximos tres años, la mayoría de las empresas formarán parte de consorcios contra el fraude.

Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

PRIMERA PARTE: Desafíos y prioridades

Informe desde la primera línea

El fraude se ha vuelto más rápido y es más barato de ejecutar que nunca. El doble peligro que representan las ciberamenazas transnacionales cada vez más organizadas y los ataques utilizando GenAI ha aumentado significativamente el volumen y la complejidad de los ataques.

Según un estudio reciente, las bandas de estafadores del sudeste asiático se han convertido en "la red criminal más poderosa de la era moderna", generando entre 50 000 y 70 000 millones de dólares al año con una fuerza laboral de más de 350 000 personas. Además, hay proveedores de "fraude como servicio" en la dark web que ofrecen una gama cada vez mayor de productos que proporcionan a los estafadores las herramientas más avanzadas y capacidades de inteligencia criminal.

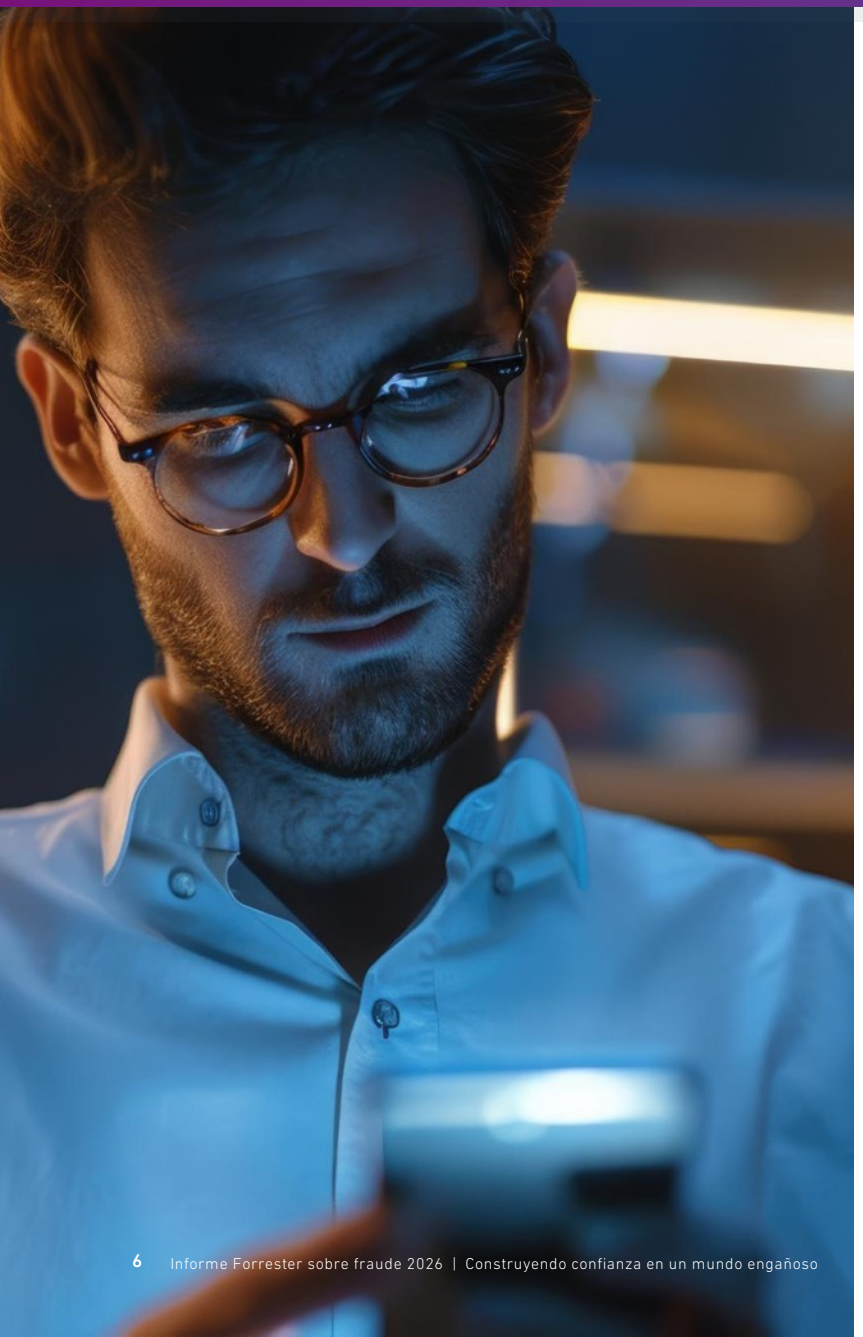
Nuestra investigación muestra que esta amenaza está afectando a empresas de todo el mundo; **más de dos tercios (67 %) de los encuestados esperan más intentos de fraude en 2026 que en el año anterior, un aumento del 10 % interanual.**

Como resultado, el 64 % de las empresas están viendo un aumento en sus pérdidas por fraude con respecto al año anterior. El mismo porcentaje admite que su organización está luchando para mantenerse al día con la rápida evolución de las amenazas de fraude. Y el impacto de este tsunami de fraudes va más allá de las pérdidas, como lo demuestra un 67 % que concuerda en que los casos de fraude están dañando la reputación de su organización.

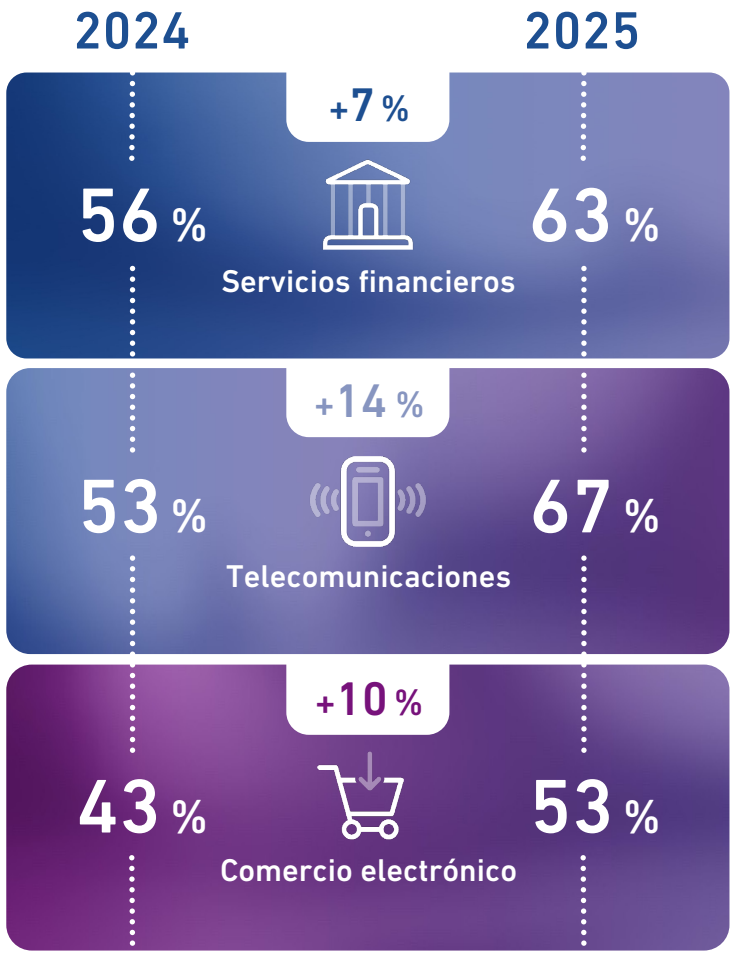
¿Cuáles son los tipos de fraude que han aumentado más?

Al analizar los tres sectores a los que encuestamos, las empresas de telecomunicaciones son las que han visto el mayor aumento en los intentos de fraude en general, con más de dos tercios (67 %) de ellas que han declarado un incremento. Les siguen de cerca los servicios financieros (63 %) y poco más de la mitad (53 %) de los comercios electrónicos.

67 % **espera recibir más ataques de fraude que el año pasado**



Porcentaje de organizaciones que declaran un aumento general en los intentos de fraude en 2024 vs. 2025



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

En comparación con el año anterior, la ingeniería social, el fraude de programas de fidelidad/recompensas y el robo de identidad son las amenazas de más rápido crecimiento para los servicios financieros y las telecomunicaciones. No es de extrañar que la ingeniería social vaya en aumento, dado el potencial que ofrece la GenAI. El estudio también sugiere que los estafadores se centran cada vez más en los programas de fidelidad y recompensas, tal vez debido a la percepción de que los esquemas de incentivos suelen ser menos seguros.

La verificación de identidad se ha convertido en el perímetro de seguridad más importante y en el objetivo principal de los estafadores. A medida que los agentes de IA legítimos interactúan cada vez más con sitios web, junto con la actividad de bots y la presencia de deepfakes, la capacidad de autenticar y verificar con precisión la identidad del cliente resulta vital.

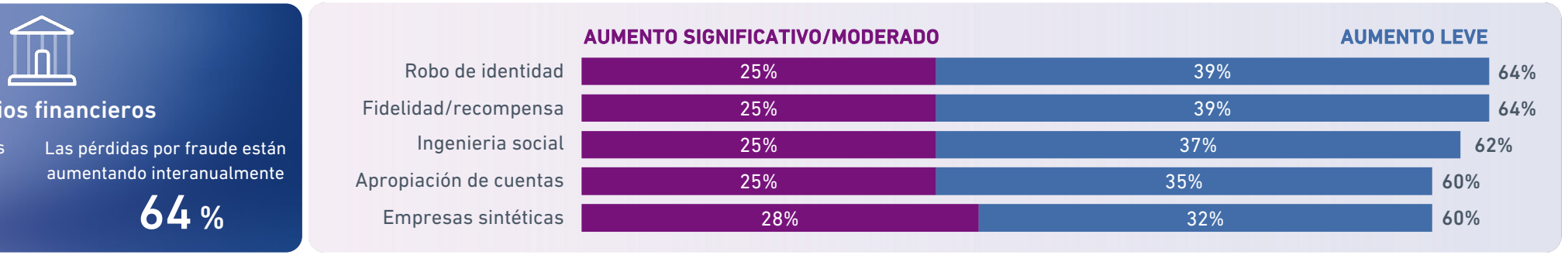
Para el comercio electrónico, el fraude amistoso y el abuso de reembolsos han mostrado el mayor aumento interanual. Los intentos de fraude de identidad sintética también han aumentado, pero no en la misma medida.

Aumento interanual en los tipos de fraudes por sector

Servicios financieros

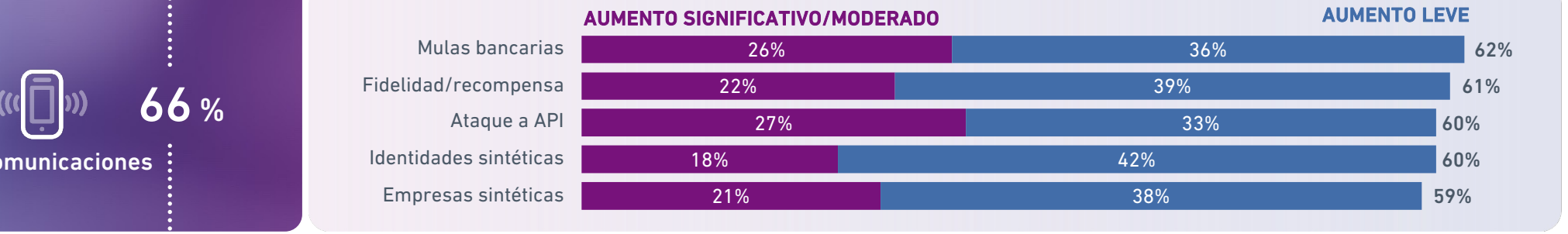
Aumento general de los intentos de fraude: **63 %**

Las pérdidas por fraude están aumentando interanualmente: **64 %**



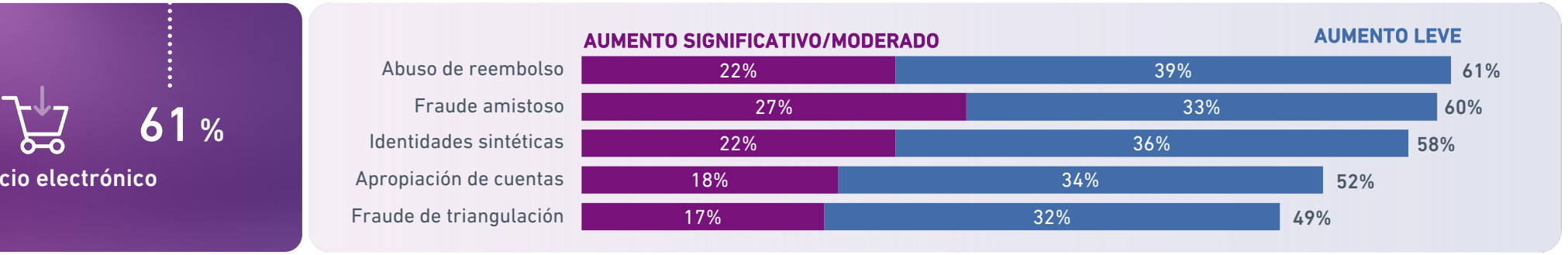
Telecomunicaciones

67 % | 66 %



Comercio electrónico

53 % | 61 %



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

¿Qué tipos de fraude son los más difíciles de detectar y prevenir?

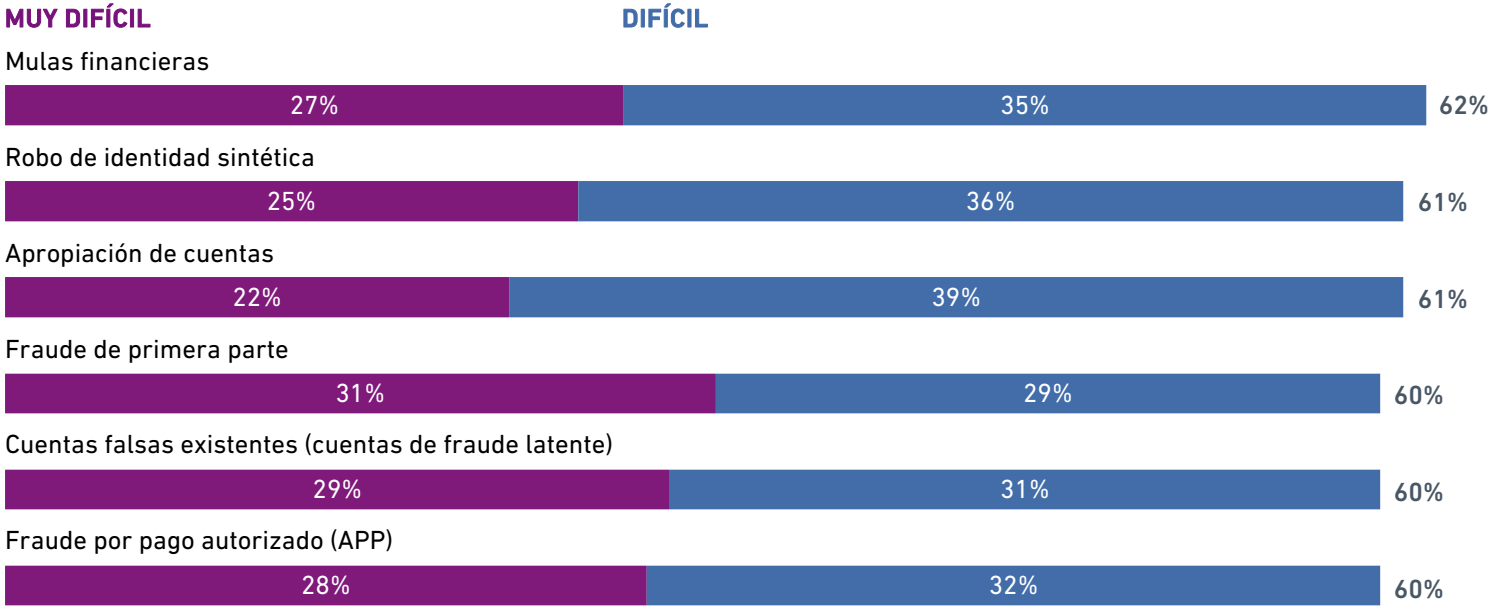
Nuestra investigación muestra que las mulas financieras son el tipo de fraude más difícil de combatir, seguido del robo de identidad sintética y la apropiación de cuentas. Aquí es donde las señales adicionales de fraude desempeñan un papel crucial, ya que permiten un control pasivo continuo de los datos del usuario para identificar patrones que puedan indicar ese tipo de fraude.

Los métodos tradicionales de autenticación ahora pueden sortearse fácilmente mediante ingeniería social impulsada por GenAI y datos de la dark web. Los tipos de fraude que son difíciles de identificar solo se pueden prevenir a través de señales sutiles de dispositivos y comportamientos que alertan cuando el comportamiento del usuario se desvía de lo habitual.

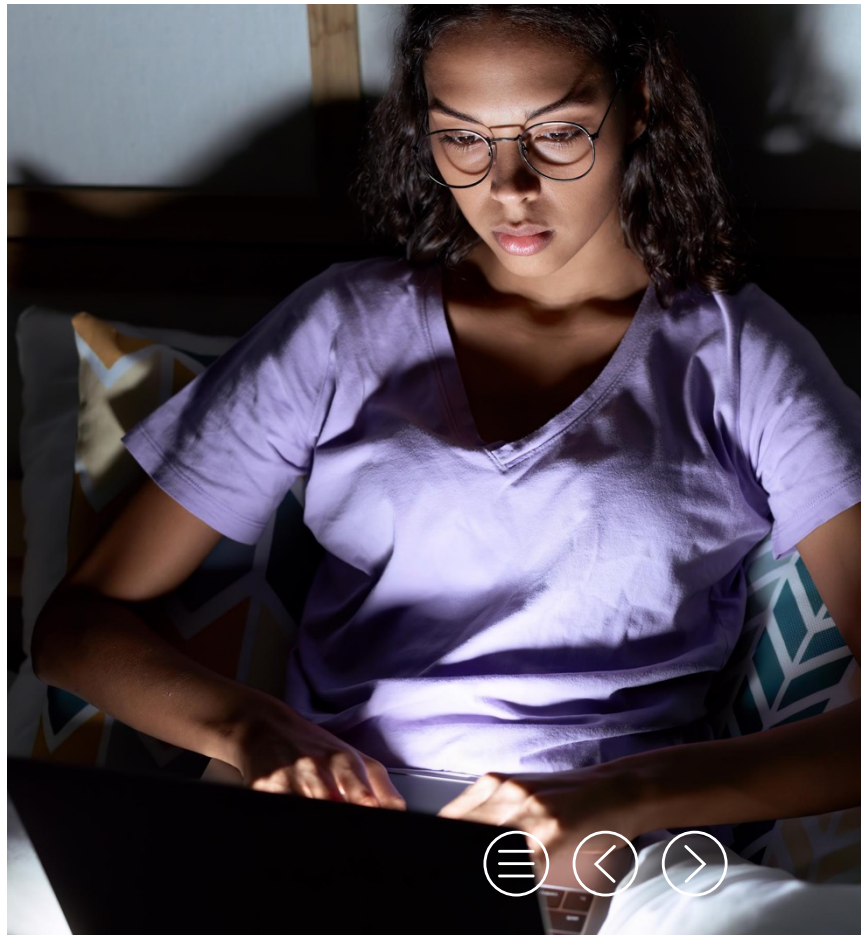
Teniendo en cuenta que pocos encuestados utilizan herramientas de autenticación avanzadas —ya que, en la actualidad, solo el 42 % utiliza datos de los dispositivos y el 39 % utiliza datos biométricos de comportamiento—, tiene sentido que este tipo de fraude siga siendo difícil de prevenir.

Sin estas herramientas, muchas empresas verán aumentar las pérdidas por fraude a medida que los estafadores obtengan acceso a sus sistemas con credenciales comprometidas. El control de la dark web también se ha vuelto esencial para realizar un seguimiento de los datos disponibles y las tácticas de fraude actuales.

¿Cuáles son los tipos de fraude más difíciles de detectar y prevenir?



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025



Principales desafíos en la prevención del fraude

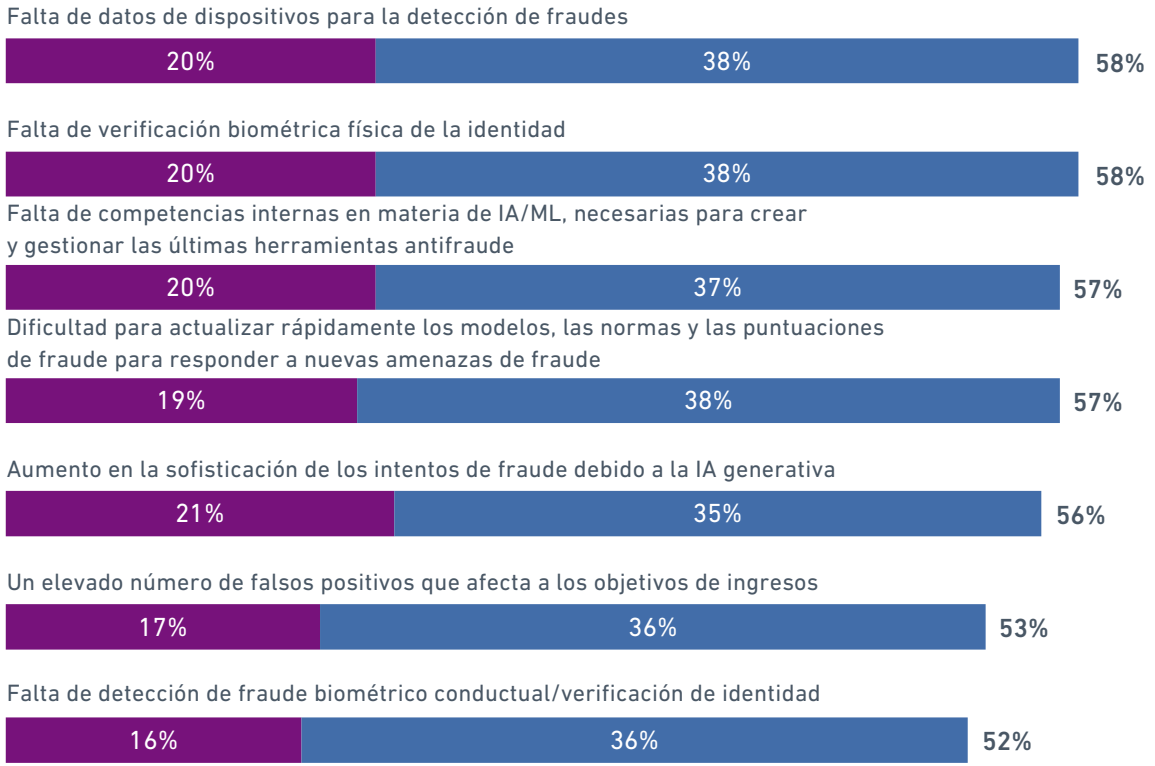
Los tres principales factores que limitan la capacidad de las organizaciones para detectar y prevenir el fraude se basan en la falta de capacidad. Los datos de los dispositivos y la biometría física se identifican como las capacidades clave faltantes y, estrechamente vinculada a esto, está la necesidad de contar con una mayor experiencia en IA/ML para transformar esos datos en decisiones antifraude precisas y seguras.

Nuestra investigación sugiere que muchas empresas se encuentran ante una brecha de capacidades, ya que sus sistemas antifraude actuales se han vuelto insuficientes para controlarlo, pero no tienen la capacidad de introducir las herramientas avanzadas que necesitan. Si bien es cierto que la disyuntiva de "desarrollar vs. comprar" no es nueva, los rápidos avances en la sofisticación de los ataques de fraude han aumentado la presión al respecto.

Las empresas necesitan soluciones ahora, no dentro de un año o más, que es el tiempo que lleva desarrollar una solución interna. Y equilibrar las competencias y capacidades internas con la creciente amenaza de fraude se ha vuelto una cuestión fundamental para el crecimiento futuro. Es interesante observar que cerca de tres cuartas partes (71 %) de los encuestados afirman que están invirtiendo más en tecnología antifraude que en analistas humanos especializados en fraudes.

68 % está de acuerdo en que su conjunto tecnológico actual es inadecuado para contrarrestar una amenaza de fraude en rápida evolución

Principales desafíos que limitan la capacidad de detectar y prevenir el fraude



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

La ola imparable de fraudes generados por GenAI sigue avanzando

Si observamos los factores que aumentan la amenaza de fraude, la GenAI es la fuerza impulsora que conecta las grandes cantidades de datos disponibles en la dark web con cientos de miles de estafadores potenciales. Los "dark LLM" —como WolfGPT y WormGPT— han permitido que cualquier persona con una conexión a Internet adquiera habilidades para realizar diferentes tipos de ataques de fraude.

Como resultado de este rápido cambio en la calidad de los documentos falsos y las imágenes deepfake, el 64 % de los encuestados afirman que sus controles actuales de KYC (Know Your Customer, o conozca a su cliente) y verificación de identidad no están equipados para detectar documentos generados por GenAI.

Cuando los datos reales de los clientes se combinan con documentos e imágenes sintéticas, se vuelven aún más difíciles de identificar. Y a medida que se lanzan al público herramientas cada vez más potentes a costes más bajos, el problema no hace más que empeorar. De hecho, el **60 % está de acuerdo en que solo hemos visto la punta del iceberg en relación con los fraudes impulsados por IA.**

66 % **de los expertos en fraude están de acuerdo en que la GenAI es el mayor desafío que ha existido para la prevención del fraude**

Un ejemplo de este rápido desarrollo es que los deepfakes ahora incluso tienen latidos de corazón. Hasta hace poco, esta señal (la variación del tono de la piel basada en los latidos del corazón) era una forma fiable de detectar un deepfake. Sin embargo, los nuevos deepfakes avanzados pueden replicarla, lo que los hace aún más difíciles de detectar.

No hay duda de que la llegada de la GenAI representa un momento decisivo en la prevención del fraude. La línea divisoria entre lo que es real y lo que es falso se ha difuminado y las consecuencias son inciertas. El 60 % estuvo de acuerdo en que las pérdidas por fraude han aumentado significativamente desde la aparición de la GenAI. Sin embargo, un porcentaje similar (58 %) admite tener dificultades para identificar si la GenAI ha estado involucrada en un ataque, por lo que les resulta difícil medir el impacto.

¿Deberían ser ilegales los deepfakes?

El 61 % de nuestros encuestados están de acuerdo en que cualquier tipo de deepfakes deberían ser ilegales, lo cual beneficiaría a toda la sociedad. Legisladores de todo el mundo están luchando por formular regulaciones sobre los deepfakes, pero el vacío que existe actualmente en la estructura legal indica que la amenaza está casi totalmente fuera de control.

Dinamarca es uno de los pocos países que ha respondido con cierta urgencia a este problema con su reciente propuesta de cambios en la ley de derechos de autor para garantizar que todos tengan derechos sobre su propio cuerpo, rasgos faciales y voz.

Italia también ha tomado medidas decisivas al declarar oficialmente que la creación y distribución de deepfakes dañinos es un delito penal en virtud de su nueva ley nacional de IA. Esta legislación, la primera de este tipo en la UE, introduce penas de cárcel para las personas que producen o comparten ilegalmente contenido generado o manipulado por IA, incluidos los deepfakes. Las sanciones se vuelven aún más severas si la tecnología se utiliza para cometer delitos como fraudes o robos de identidad.

Si bien este es un paso en la dirección correcta, hasta que no se establezcan más precedentes legales, cualquiera puede crear un deepfake en cuestión de segundos, por eso nos preguntamos: ¿deberían ser ilegales los deepfakes de voz y vídeo?

Prioridades para el próximo año

En vista de la creciente sofisticación de las amenazas de fraude, tiene sentido que la principal prioridad para el próximo año sea revisar estratégicamente las soluciones actuales para la detección del fraude (70 %). Los sistemas que han funcionado durante décadas se están volviendo obsoletos y las empresas están tratando de incluir más señales de fraude en sus evaluaciones.

Esta revalorización de las soluciones contra el fraude se vincula estrechamente con la segunda y tercera prioridades: **migrar las soluciones contra el fraude a la nube (68 %) e invertir en nuevas herramientas contra el fraude (68 %).**

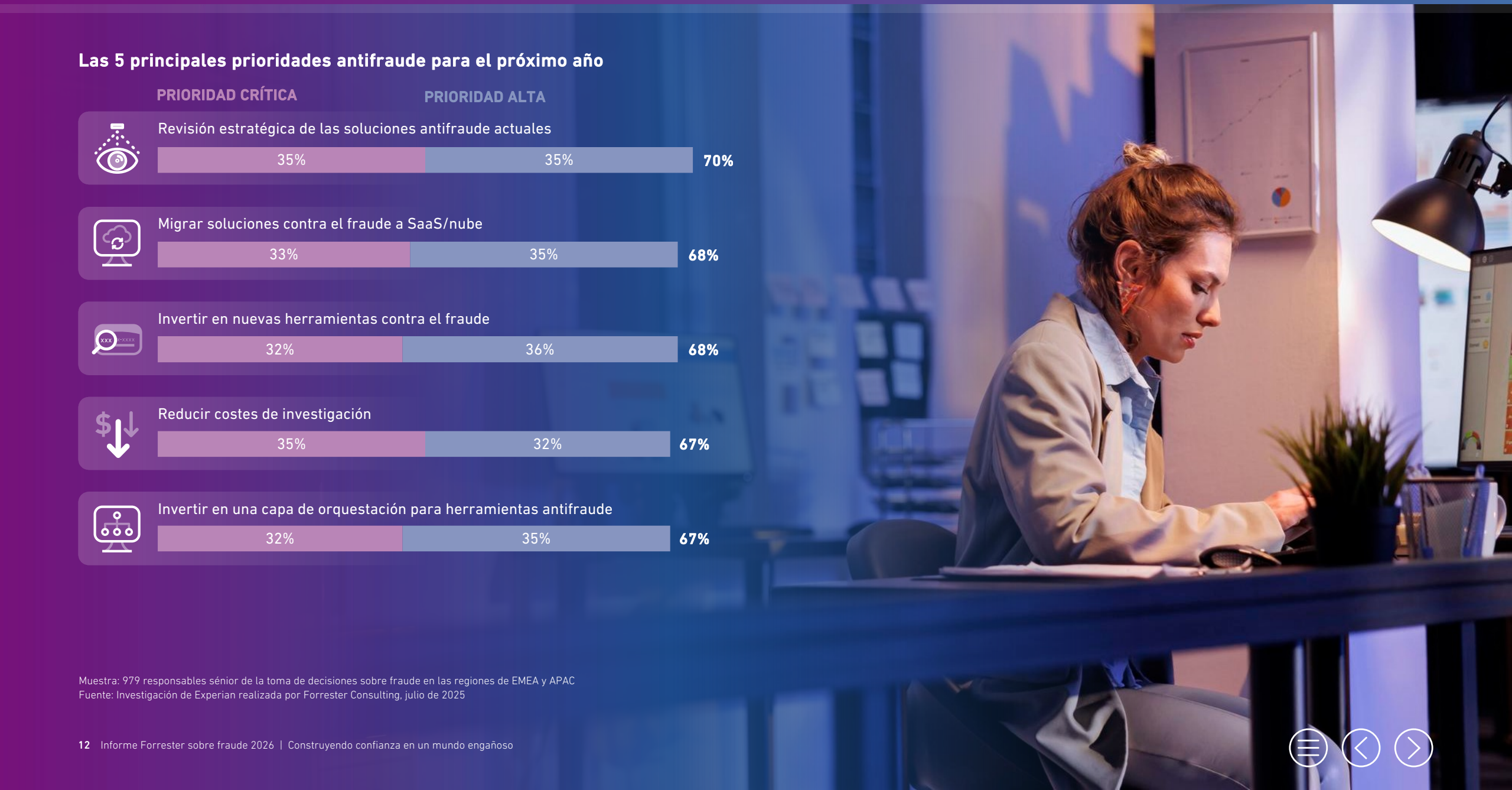
De cara a los próximos 3-5 años, es muy probable que el impacto de la GenAI en el fraude se intensifique. Por consiguiente, seleccionar estratégicamente en qué capacidades de fraude quieres invertir es vital para evitar más pérdidas.

Las empresas con visión de futuro desarrollarán estas capacidades en una plataforma unificada basada en la nube, en lugar de tratar de unir diferentes soluciones locales aisladas. Y, en última instancia, la capacidad de combinar los flujos de trabajo de prevención del fraude y de riesgo de crédito proporcionará los mejores resultados. El 69 % de nuestros encuestados planean integrar la prevención del fraude y la evaluación del riesgo de crédito en una estrategia general de gestión de riesgos en un futuro próximo.

La reducción en costes de revisión manual también es una prioridad. Si bien hay varias formas de lograrlo, una mayor automatización puede desempeñar un papel importante. Actualmente, muchos equipos antifraude recurren a revisiones manuales para afrontar las amenazas, y más de un tercio (35 %) afirma que realizar una revisión manual lleva una semana o más. Con las señales de fraude adecuadas, se pueden automatizar muchas más decisiones, lo que reduce los costes de investigación y permite a los expertos en fraude resolver casos complejos más rápido.

La última prioridad identificada en la investigación **es invertir en una capa de orquestación para las herramientas antifraude (67 %).** El mismo porcentaje de encuestados coincide en que la orquestación de múltiples soluciones contra el fraude en una misma plataforma es el futuro de la prevención del fraude. Las razones son claras: la orquestación mejora la experiencia del cliente y reduce los costes, al requerir solo los controles de fraude necesaria en función de la puntuación de riesgo del cliente.

Las 5 principales prioridades antifraude para el próximo año



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

SEGUNDA PARTE: Soluciones impulsadas por la tecnología

Por qué el Machine Learning es esencial para combatir el fraude

Cuantos más datos se utilicen para realizar una evaluación —como datos de comportamientos y dispositivos—, más precisos serán los resultados.

Sin embargo, para dar sentido a este enorme volumen de datos se necesita el ML. ¿Por qué? Porque solo el ML tiene la capacidad analítica necesaria para extraer información valiosa a partir de conjuntos de datos tan extensos. Nuestra investigación lo deja claro; **el 67 % de los usuarios de ML han visto una mejora tangible en la precisión de la detección de fraudes desde que implementaron el ML.**

El segundo beneficio clave del ML es la capacidad de volver a entrenar modelos de forma periódica con nuevos datos para mantenerse al día de los cambios en las tácticas de fraude. Los sistemas basados únicamente en reglas tienen dificultades para adaptarse a los nuevos tipos de fraude, ya que la incorporación de nuevas reglas añade complejidad y aumenta los falsos positivos y las revisiones manuales. Más de dos tercios (67 %) de los usuarios de ML están de acuerdo en que esta capacidad de volver a entrenar y actualizar continuamente sus modelos de ML les ha ayudado a mantenerse al ritmo de una amenaza de fraude que evoluciona rápidamente. El mismo porcentaje ha visto disminuir su tasa de falsos positivos desde que implementó el ML.

ML

70 %

está de acuerdo en que el ML ha Mejorado su capacidad para detectar el fraude en situaciones que un sistema basado únicamente en reglas habría pasado por alto

¿Cuál es el impacto del ML en las empresas que lo han adoptado?

67 %

Nuestra tasa de falsos positivos ha disminuido desde que implementamos el ML.

68 %

El ML nos ha permitido reducir la fricción relacionada con la seguridad para clientes confiables mediante el uso de verificaciones de fraude pasivas.

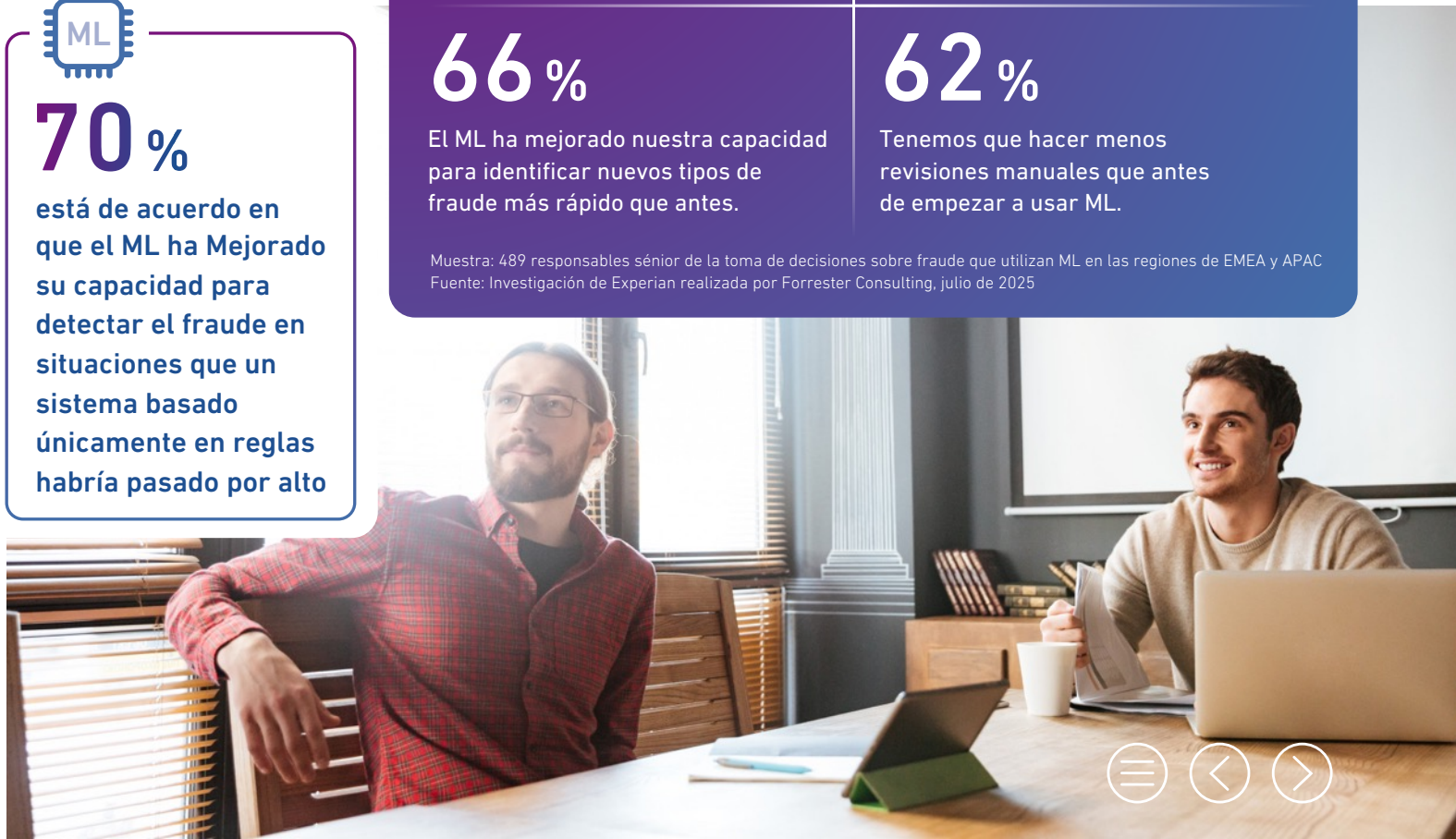
66 %

El ML ha mejorado nuestra capacidad para identificar nuevos tipos de fraude más rápido que antes.

62 %

Tenemos que hacer menos revisiones manuales que antes de empezar a usar ML.

Muestra: 489 responsables sénior de la toma de decisiones sobre fraude que utilizan ML en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

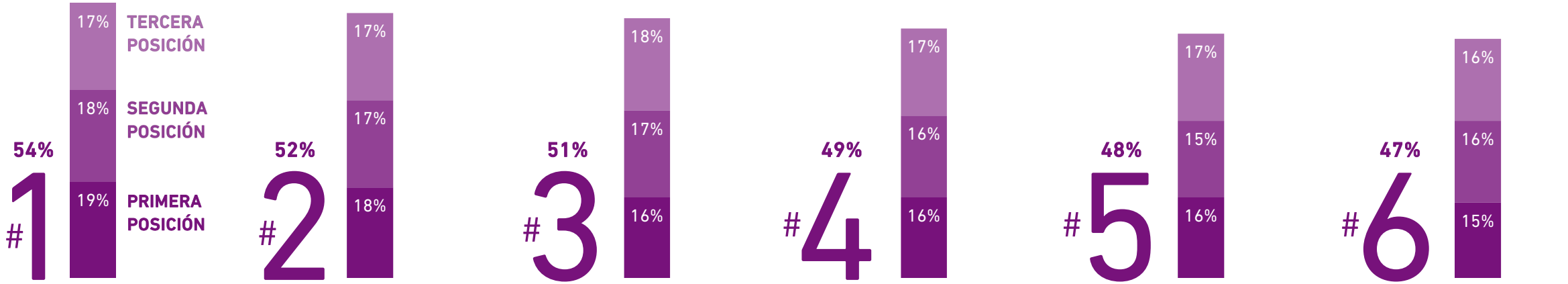


¿Cuáles son los principales beneficios que ofrece el ML?

Nuestra investigación indica que el mayor beneficio de implementar el ML es la capacidad de detectar amenazas de fraude en tiempo real (54 %). Actualmente, solo un tercio (33 %) de las organizaciones puede detectar el fraude en tiempo real; un porcentaje similar (32 %) lo hace en un día o menos, y el 35 % tarda una semana o más.

Estrechamente vinculada a una identificación más rápida está una mejor experiencia del cliente (52 %), que se clasifica como el segundo mayor beneficio. Pero la experiencia del cliente no implica solo decisiones más rápidas; reducir la fricción también es fundamental. Los controles de fraude pasivos que no interrumpen la experiencia del cliente son igual de importantes.

Identificar el fraude en tiempo real es el principal beneficio del ML



Identificación de amenazas de fraude en tiempo real

Mejor experiencia del cliente con menos fricción en materia de seguridad

Mayor precisión en la detección de fraudes en comparación con el uso exclusivo de reglas

Reducción de la cantidad de revisiones manuales

Reducción de falsos positivos

Reentrenamiento continuo para adaptarse a las nuevas tácticas de fraude

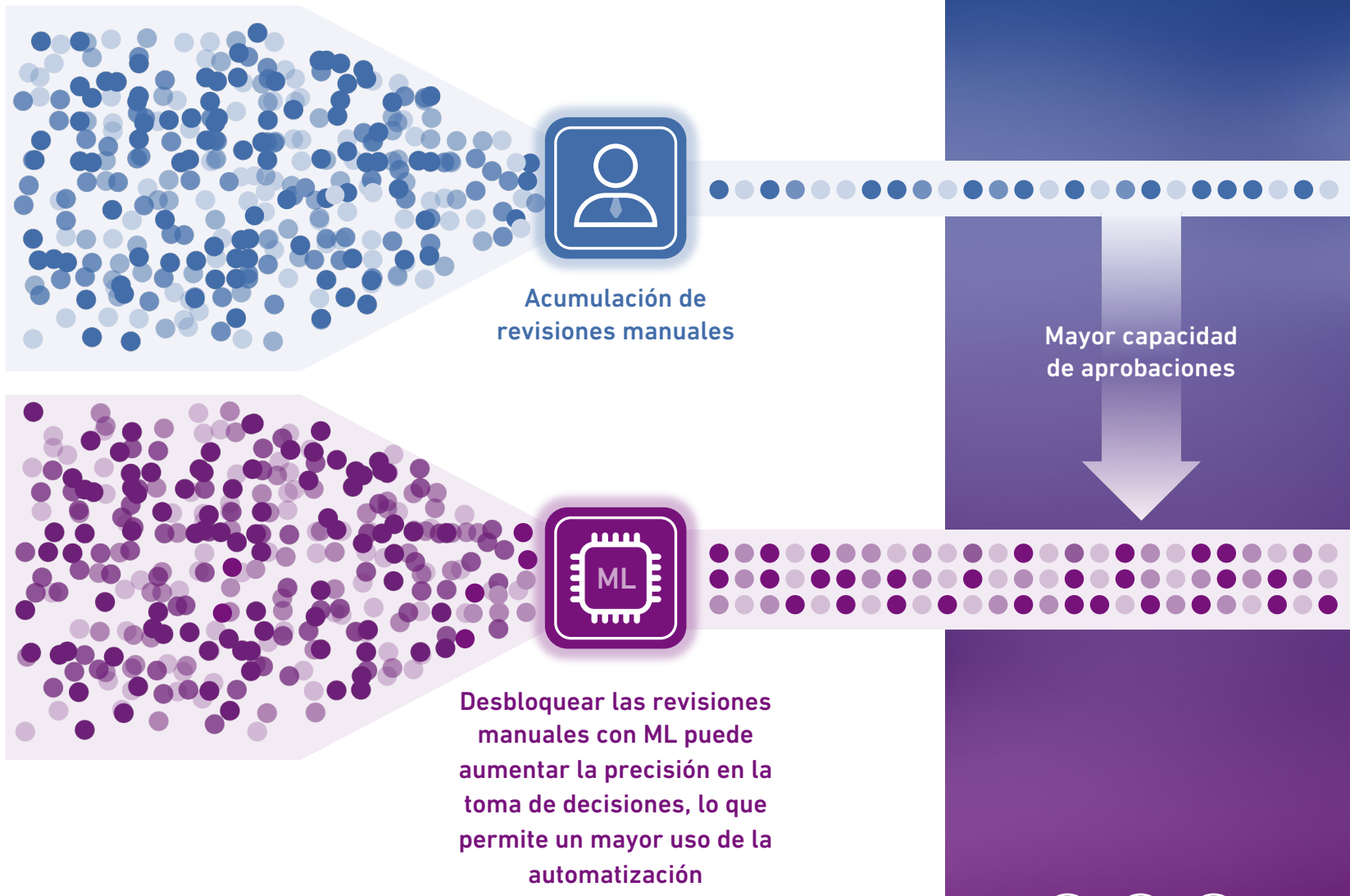
Muestra: 489 responsables sénior de la toma de decisiones sobre fraude que utilizan ML en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

El ML puede reducir significativamente los retrasos causados por la acumulación de revisiones manuales

Casi dos tercios (64 %) de las organizaciones recurren a las revisiones manuales para resolver las alertas de fraude, un porcentaje que aumenta hasta un 70 % en los encuestados del sector del comercio electrónico. Como resultado, los clientes potencialmente confiables experimentan un proceso de solicitud o compra lento y frustrante, con una alta probabilidad de que muchos lo abandonen.

El ML proporciona recomendaciones más precisas, lo que permite una mayor automatización. Casi tres cuartas partes (71 %) de quienes usan ML coinciden en que les permite priorizar mejor los casos de revisión manual, lo que ha mejorado la productividad de sus analistas de fraude.

Solicitudes/compras mensuales con y sin ML



¿Por qué razones no se adopta el ML?

La comparación de nuestra última investigación sobre el uso de ML en el riesgo de crédito con esta investigación sobre fraude es reveladora: algunos responsables de la toma de decisiones sobre riesgo de crédito no entienden la importancia del ML y, por lo tanto, no han invertido en él.

Siguiendo con la comparación, la principal razón que frena a los responsables de la toma de decisiones sobre fraude es la falta de datos de calidad para entrenar a los modelos (73 %), lo que sugiere que muchos ya reconocen el valor que puede aportar.

La importancia de contar con suficientes datos de entrenamiento de alto valor no se puede pasar por alto. La correcta prevención del fraude se basa en disponer de suficientes datos procedentes de diversas fuentes, y con la llegada del ML, el valor de los datos se ha vuelto aún más importante.

Los conjuntos de datos de entrenamiento deben ser grandes y estar etiquetados correctamente para que el ML proporcione predicciones precisas. Los modelos preentrenados listos para usar pueden ayudar a superar este desafío, al igual que el uso de datos sintéticos para ampliar los conjuntos de datos de entrenamiento.

Preocupaciones regulatorias sobre ML

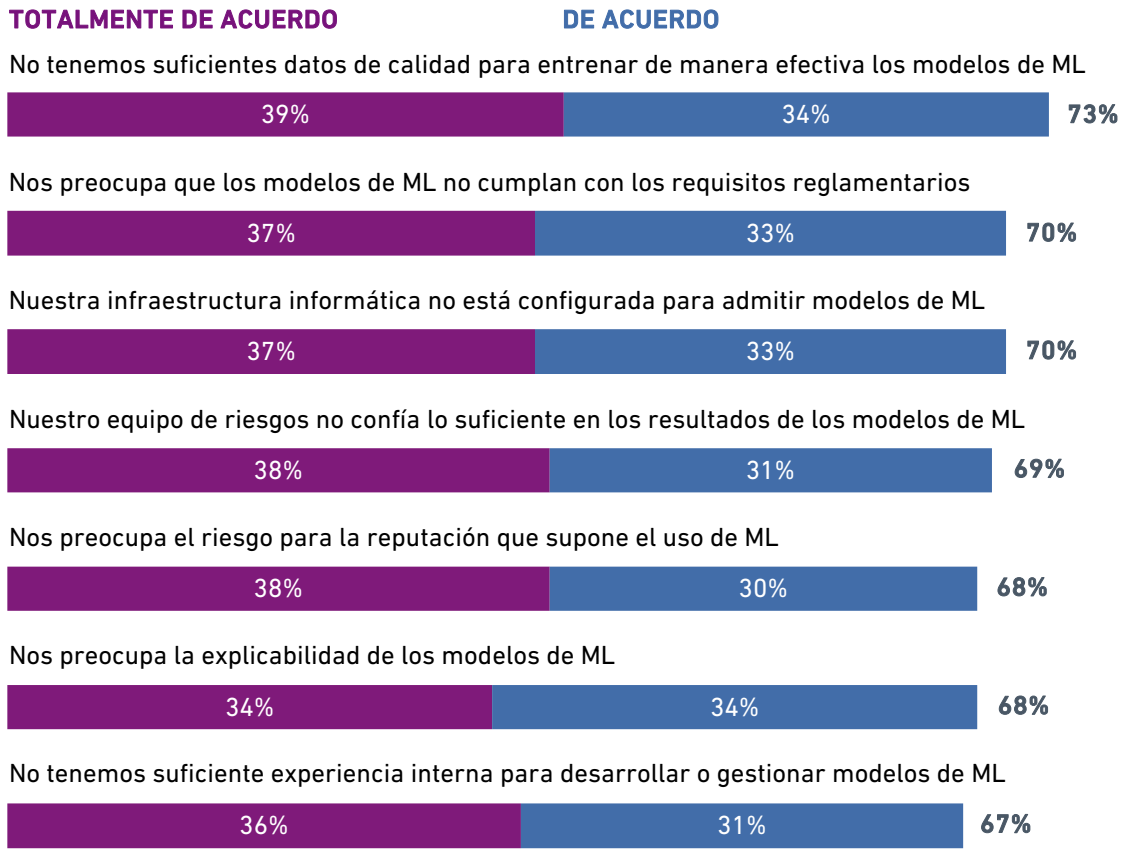
Legisladores de todo el mundo se encuentran en diferentes etapas de la legislación para regular el uso del ML en la detección del fraude con el fin de garantizar la transparencia y la equidad. El ML explicable permite a los clientes rechazados impugnar las decisiones, y la auditabilidad completa ayuda a generar confianza en las decisiones de ML entre los usuarios empresariales.

Los modelos de ML pueden ser completamente explicables y proporcionar razones para cada una de sus decisiones, pero persiste la incertidumbre sobre lo que buscan los reguladores y cómo lograrlo. El 71 % de los encuestados agradecerían una mayor claridad normativa sobre el uso del ML en los sistemas de prevención del fraude.

Más de dos tercios (67 %) coinciden en que la falta de claridad normativa sobre los casos de uso aceptables del ML para combatir el fraude está frenando su adopción de esta tecnología.

- Capacidad interna
- Regulaciones
- Capacidad interna
- Confianza
- Reputación
- Regulaciones
- Capacidad interna

Principales razones por las que no se ha adoptado el ML



Muestra: 490 responsables sénior de la toma de decisiones sobre fraude que no utilizan ML en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

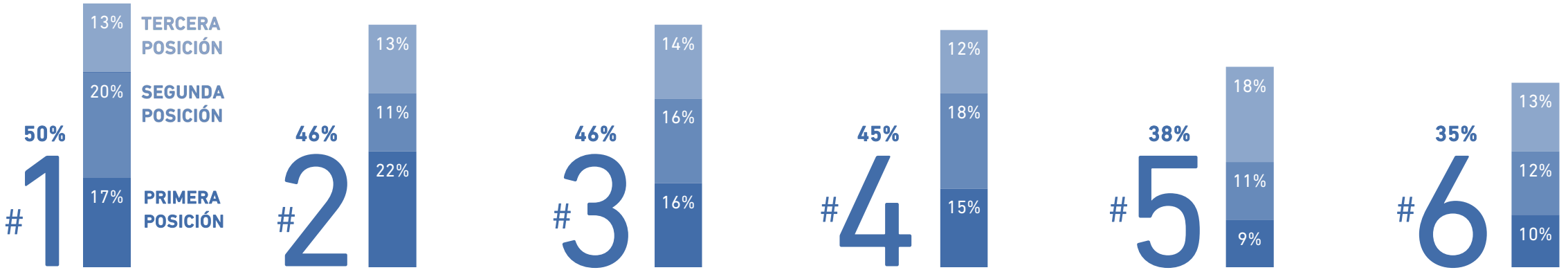
¿Qué factores pueden fomentar la adopción del ML para los no usuarios?

El ROI demostrado de otras empresas es el principal factor que puede fomentar la adopción del ML. Al igual que con cualquier adopción de nuevas tecnologías, la mayoría de las empresas quieren ser las "primeras en ser las segundas", con el fin de aprender de las que las han precedido. Aunque esta es una forma más segura de abordar los cambios de sistema, la grave amenaza actual de fraude exige un enfoque más proactivo a la hora de adoptar las tecnologías más avanzadas para la prevención.

Muchas empresas ya han adoptado el ML con buenos resultados y con un ROI positivo. Para un cliente de Experian que recientemente cambió a un modelo de ML, el plazo para obtener un ROI positivo fue de menos de un mes, ya que fue capaz de identificar un importante ataque organizado poco después de su adopción.

Las empresas interesadas en comprender el valor del ML pueden concertar una evaluación de prueba de valor (POV) offline. Esto les permite ver los beneficios que el ML puede proporcionarles en función de las métricas acordadas, sin necesidad de conectar su sistema al modelo.

ROI demostrables y una orientación regulatoria más clara estimularían la adopción de ML



Muestra: 490 responsables sénior de la toma de decisiones sobre fraude que utilizan ML en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

Asistentes de GenAI y monedero de identidad digital

Un avance destacado en la gestión del fraude son los asistentes de GenAI integrados en las plataformas de prevención de fraude. Estas herramientas pueden consolidar datos importantes —como las reglas y su rendimiento—, las razones del fraude y la duración de las coincidencias (fecha/hora).

También pueden proporcionar los niveles de riesgo del caso, con la justificación adecuada y las instrucciones del "siguiente paso" a seguir para completar una investigación. Además, pueden agilizar los procesos manuales, mejorando así tanto la eficiencia como la precisión en la toma de decisiones.

Nuestra investigación muestra que el 80 % de los encuestados creen que la mayor ventaja de un asistente de GenAI es hacer que sus procesos de prevención del fraude sean más accesibles para los empleados con menos conocimientos técnicos o sin conocimientos de programación.

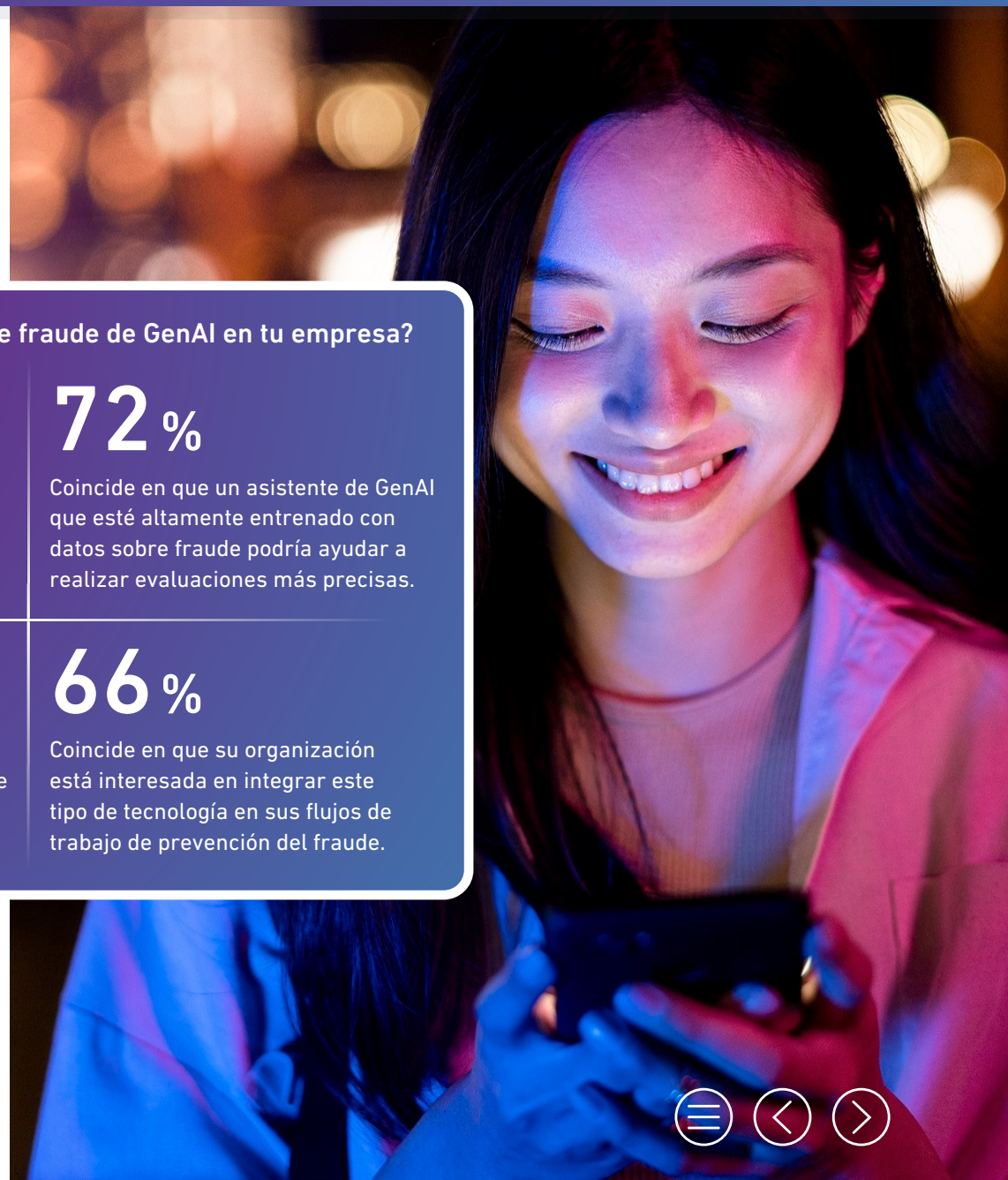
¿Qué podría hacer un asistente de fraude de GenAI en tu empresa?

77 %
Cree que la mayor ventaja de un asistente de GenAI es reducir el tiempo necesario para gestionar los casos de fraude.

72 %
Coincide en que un asistente de GenAI que esté altamente entrenado con datos sobre fraude podría ayudar a realizar evaluaciones más precisas.

71 %
Cree que un asistente impulsado por GenAI podría reducer significativamente el tiempo y el esfuerzo necesarios para gestionar nuevos casos de fraude.

66 %
Coincide en que su organización está interesada en integrar este tipo de tecnología en sus flujos de trabajo de prevención del fraude.



Muestra: 979 responsables sénior de la toma de decisiones sobre fraude en las regiones de EMEA y APAC
Fuente: Investigación de Experian realizada por Forrester Consulting, julio de 2025

El futuro de las identidades digitales

La UE ha esbozado recientemente su plan para que los monederos de identidad digital sean reconocidos tanto dentro como fuera de sus fronteras, según el IDAS 2.0. En los próximos dos años, todos los Estados miembros deberán ofrecer monederos de identidad digital y los proveedores de servicios financieros y de telecomunicaciones deberán aceptarlos.

También se están poniendo en marcha iniciativas de identificación digital en Singapur, Malasia, Australia y muchos otros países. India lidera el grupo con su programa Aadhaar, descrito como uno de los sistemas de identificación digital más sofisticados del mundo y con más de mil millones de usuarios registrados.

Casi tres cuartas partes de nuestros encuestados (74 %) ven los monederos de identidad digital como una oportunidad estratégica para reforzar la prevención del fraude. Una cifra similar (73 %) planea integrar monederos de identidad digital en la experiencia de sus clientes.

Aunque las identificaciones digitales tienen el potencial de reducir de forma significativa los fraudes relacionados con la identidad, los programas educativos de los países y los empresariales son esenciales para generar confianza en ellas y fomentar su adopción. El potencial es significativo, como lo percibe el 70 % de los encuestados que están de acuerdo en que la introducción de monederos de identidad digital cambiará fundamentalmente la forma en la que incorporan y verifican a sus clientes.

74 %

está de acuerdo en que la adopción generalizada de monederos de identidad digital podría reducir la dependencia de métodos tradicionales de KYC y verificación de documentos

El giro cada vez más importante hacia los consorcios contra el fraude

La inteligencia colectiva contra el fraude sin duda tendrá un papel importante que desempeñar en el futuro de la prevención del fraude.

El 73 % de los encuestados están de acuerdo en que la mejor manera de contrarrestar la amenaza del fraude es colaborar y combatirlo juntos.

Sin embargo, este intercambio de información debe ser facilitado por un tercero de confianza: tres cuartas partes (75 %) de los encuestados creen que generar confianza entre los diferentes miembros de un consorcio de fraude es la clave de su éxito.

Para que un consorcio sea efectivo se precisa de un núcleo de gestión central, con conexiones API seguras para cada miembro. Esto permite compartir los datos confidenciales a través de la red, al mismo tiempo que se cumplen las regulaciones de intercambio de datos. El objetivo es que cada aplicación pueda cotejarse con el grupo de inteligencia colectiva sin que los miembros compartan datos directamente entre ellos.

74 %

está de acuerdo en que, en los próximos tres años, la mayoría de las empresas formarán parte de un grupo de datos compartidos sobre fraude.

Para obtener más información sobre cómo funcionan los consorcios y el proceso para unirse a uno, puedes leer la guía para compradores de consorcios de Experian:

EL POTENCIAL DE LA INTELIGENCIA COMPARTIDA

Proceso de transferencia de datos en un consorcio

1

Cada empresa envía datos sobre aplicaciones o compras a la base de datos central por medio de una API segura individual

2

Si los datos de la aplicación activan una alerta dentro del núcleo central, la regla que se ha activado se devuelve a la empresa

3

No se comparten datos directamente entre los miembros de la empresa

Principales conclusiones

La GenAI y los deepfakes han cambiado la amenaza del fraude para siempre. A medida que estas herramientas se vuelven más sofisticadas, las capas adicionales de señales de fraude, como los datos de comportamientos y dispositivos, se han vuelto esenciales para prevenir un rápido aumento de las pérdidas por fraude.

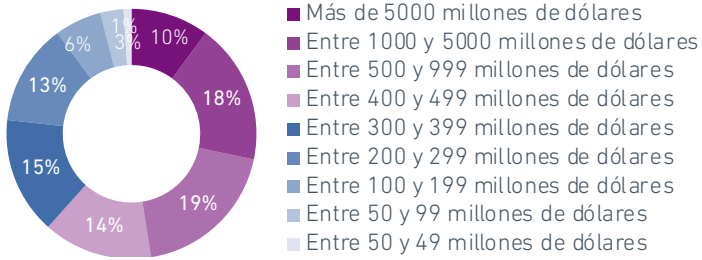
La principal prioridad de cara al próximo año es una revisión estratégica de las herramientas antifraude actuales para identificar las brechas de capacidades, seguida de la migración de las soluciones antifraude a la nube y la inversión en nuevas herramientas antifraude impulsadas por ML.

La mayor ventaja que proporciona el ML es la capacidad de detector el fraude en tiempo real, seguida de la mejora de la experiencia del cliente a través de la reducción de la fricción en los procesos de incorporación o compra, gracias a las señales pasivas de fraude.

El intercambio de inteligencia colectiva contra el fraude a través de consorcios desempeñará un papel fundamental en el future de la prevención del fraude, pero esta colaboración debe ser facilitada por un tercero de confianza para garantizar el cumplimiento normativo y la confianza entre los miembros.

Datos sobre las empresas y la demografía de los encuestados

REVENUE DE LA EMPRESA



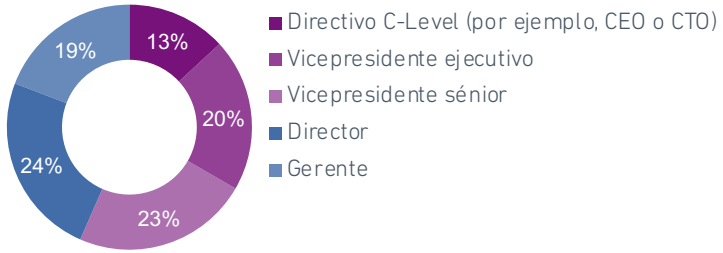
GEOGRAFÍA

N= ~109 por cada país

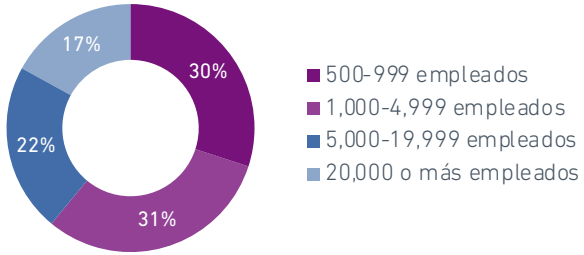
Dinamarca, España, Italia, Alemania, Sudáfrica, Noruega

Nueva Zelanda, Australia, India

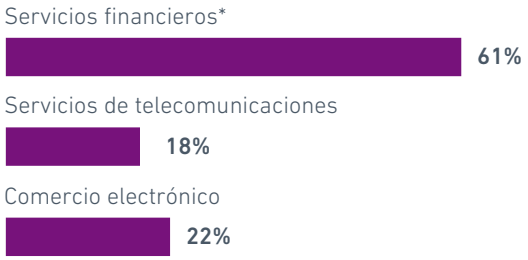
RANGO DE LOS ENCUESTADOS



TAMAÑO DE LA EMPRESA

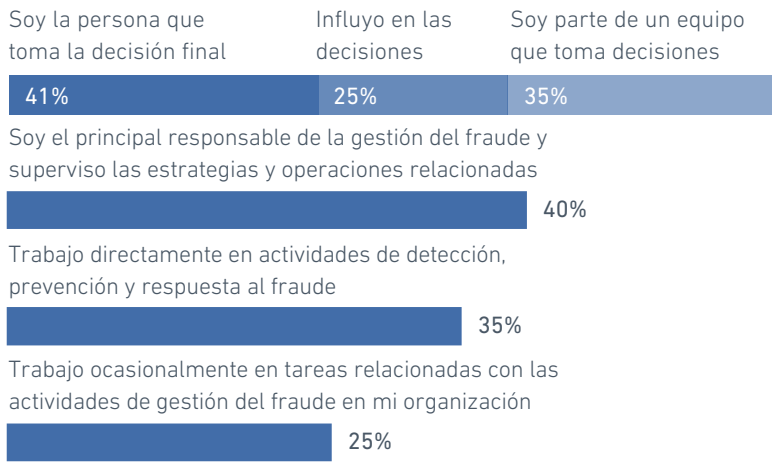


SECTOR



*Banca (38 %), financiación comercial/leasing (21 %), financiación de automóviles (25 %), préstamos al consumo (16 %)

RESPONSABILIDAD DIRECTA EN LA TOMA DE DECISIONES



Glosario

ATAQUES DE FRAUDE A LAS API

Explotar vulnerabilidades en las API para obtener acceso no autorizado a los datos, ataques de denegación de servicios o manipulación de las API de alguna otra forma maliciosa.

FRAUDE DE PAGOS AUTOMÁTICOS AUTORIZADOS (APP)

Los estafadores manipulan a las víctimas para que realicen pagos voluntariamente mediante ingeniería social, como fingir ser parte de una institución financiera de confianza.

BIOMETRÍA CONDUCTUAL

Identificar y analizar los datos asociados con la forma subconsciente en que un usuario concreto interactúa con su dispositivo, sin recopilar datos de información personal identificable (PII). Estos incluyen movimientos del ratón, pulsaciones de las teclas o presión sobre la pantalla táctil, entre muchos otros atributos de comportamiento.

ANÁLISIS CONDUCTUAL

Identificar los ataques de bots comparando la forma en que los humanos interactúan con los dispositivos frente a la forma en que lo hacen los bots.

BOT/RELLENO DE CREDENCIALES

Ataques de fraude automatizados en los que se utilizan listas de credenciales robadas de una organización para intentar obtener acceso no autorizado a una cuenta en otra organización diferente.

PERFILADO O HUELLA DIGITAL DEL DISPOSITIVO

Análisis de un conjunto de parámetros de software y hardware asociados con un dispositivo específico para proporcionar un identificador único y evaluar el riesgo. Estos parámetros incluyen el sistema operativo, la red, el navegador, el idioma, la zona horaria, la relación de pantalla, entro muchos otros.

INFORMACIÓN SOBRE DISPOSITIVOS

Los datos del dispositivo junto con los datos conductuales constituyen la información sobre dispositivos. Esta información ofrece señales de detección de fraude continuas y pasivas.

DEEPFAKES

Vídeo, audio o imágenes que han sido alteradas y manipuladas de manera convincente para representar falsamente a alguien haciendo o diciendo algo que en realidad no hizo ni dijo. En el contexto del fraude, se pueden usar para engañar a los controles de KYC con una identidad falsa.

FRAUDE COMO SERVICIO (FAAS)

Herramientas y servicios de fraude que se venden principalmente en la dark web bajo un modelo de pago por uso.

MULAS FINANCIERAS

Una persona que ayuda a lavar ganancias ilícitas al recibir dinero en su cuenta y luego transferirlo a otra cuenta en nombre de un estafador. Estos intermediarios a menudo son reclutados en las redes sociales y es posible que no sean conscientes de que están cometiendo un delito.

BIOMETRÍA FÍSICA

Características físicas únicas que se pueden utilizar para identificar a los usuarios individuales. Por ejemplo, la detección de vida que realiza el reconocimiento facial.

IDENTIDAD SINTÉTICA

Una combinación de datos PII reales y falsos con los que se crea una identidad ficticia difícil de detectar.

EMPRESA SINTÉTICA

Al igual que una identidad sintética de un consumidor, estas empresas falsas utilizan una combinación de datos reales y falsos para simular una empresa legítima.

FRAUDE DE TRIANGULACIÓN

Una estafa de comercio electrónico en la que un estafador crea una tienda en línea falsa para cobrar pagos de clientes desprevenidos y luego utiliza la información robada de la tarjeta de crédito de un tercero para comprar los productos a un minorista legítimo, que envía los productos al cliente inicial. El cliente recibe su pedido, el estafador se queda con el dinero y el minorista legítimo finalmente recibe una devolución del pago a cargo del propietario de la tarjeta robada, lo que resulta en una pérdida financiera y un daño potencial de su reputación.

Acerca de Experian

Experian es una empresa global de datos y tecnología que impulsa oportunidades para personas y empresas de todo el mundo.

Ayudamos a redefinir las prácticas crediticias, descubrir y prevenir el fraude, simplificar la atención médica, ofrecer soluciones de marketing digital y obtener una mayor perspectiva del mercado de la automoción; todo ello gracias a nuestra combinación única de datos, análisis y software. También ayudamos a millones de personas a alcanzar sus objetivos financieros y a ahorrar tiempo y dinero.

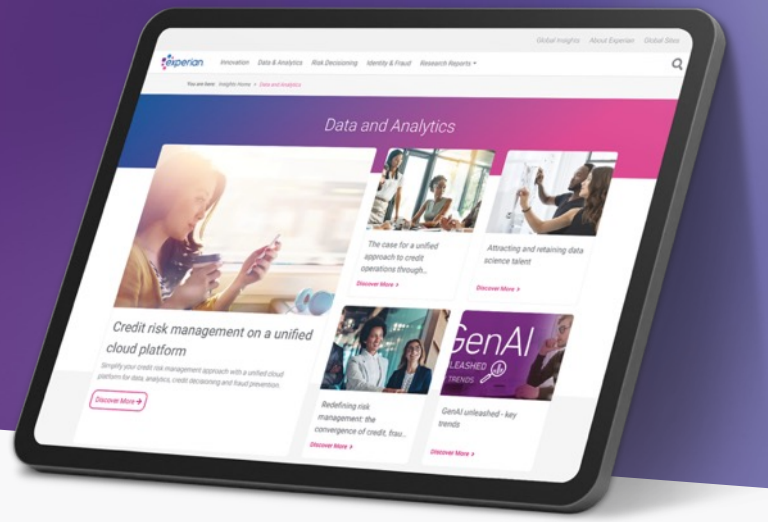
Operamos en una amplia gama de mercados, desde servicios financieros hasta atención médica, automoción, agrofinanzas, seguros y muchos otros sectores industriales.

Invertimos en personas con talento y en nuevas tecnologías avanzadas para desbloquear el potencial de los datos e innovar. Somos una empresa del índice FTSE 100 que cotiza en la Bolsa de Valores de Londres (EXPN) y contamos con un equipo de 25 200 personas en 33 países. Nuestra sede corporativa se encuentra en Dublín, Irlanda.

Más información en **experianplc.com**

Descubre más →

Ponte en contacto con tu comercial local de Experian o visita experianacademy.com



experian

Domicilio social: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ Teléfono: 0844 481 9920 businessuk@experian.com experian.co.uk/business