

Del fraude digital a la confianza digital:

Fraude, identidad e inteligencia artificial en Panamá

Septiembre 2026

La próxima frontera: confianza digital en la era de la inteligencia artificial



La inteligencia artificial está transformando la forma en que las personas acceden a servicios financieros e interactúan con empresas y plataformas digitales. Más que una nueva capacidad, **representa una nueva velocidad**: la posibilidad de analizar información, identificar señales de riesgo y tomar decisiones **en tiempo real**.

Pero esta transformación no ocurre únicamente gracias a los avances tecnológicos. Detrás de ella **están los datos**. La inteligencia artificial aprende, predice y actúa a partir de información, por lo que su capacidad para tomar decisiones precisas depende de la calidad, actualidad y profundidad de los datos disponibles. Cuanto mejor sea la información, mayor será la capacidad de validar identidades, comprender comportamientos, detectar anomalías y diferenciar interacciones legítimas de posibles intentos de fraude.



Esto cobra especial relevancia en los servicios financieros. Ya sea al financiar la compra de un electrodoméstico, solicitar un crédito, abrir una cuenta o realizar un pago, las personas esperan procesos cada vez más rápidos y sencillos, pero también seguros. A medida que las experiencias digitales se vuelven más ágiles e inmediatas, **también aumenta la necesidad de confirmar, en tiempo real**, que una persona es quien dice ser y que una acción puede realizarse con confianza.

Durante años, la conversación estuvo centrada en la prevención: utilizar información para anticipar riesgos antes de que ocurrieran. Este enfoque permitió identificar señales de fraude, detectar comportamientos inusuales y tomar decisiones más seguras. Sin embargo, la llegada de la inteligencia artificial está ampliando ese desafío. A medida que se vuelve más fácil crear contenido sintético, automatizar procesos e incluso suplantar identidades de forma más sofisticada, **ya no basta con identificar posibles riesgos**. También es necesario generar mayor certeza sobre la autenticidad de las personas, las solicitudes y las transacciones.



Es ahí donde surge la **confianza predictiva**. Si la prevención predictiva busca anticipar amenazas, la confianza predictiva busca generar certeza. Se trata de utilizar información, identidad, analítica e inteligencia artificial para validar identidades, verificar autorizaciones y determinar, con un alto grado de certeza y en tiempo real, si una acción puede considerarse confiable. En otras palabras, la capacidad de anticipar riesgos ya no es suficiente por sí sola; ahora también es necesario generar confianza sobre quién está detrás de una acción, si está autorizado para realizarla y si puede considerarse auténtica.



Pero ¿por qué resulta relevante hablar de confianza digital en un estudio sobre fraude?

Precisamente porque la forma en que las personas experimentan el fraude percibe los riesgos y toman decisiones en los entornos digitales influye directamente en la confianza que depositan en ellos. Comprender qué tan expuestos están los consumidores a estas amenazas, cómo las identifican y qué tan preparados se sienten para enfrentarlas resulta fundamental para entender los desafíos que hoy enfrentan los servicios financieros, las interacciones digitales y la construcción de confianza en un entorno cada vez más conectado.



La confianza digital del futuro comenzará a construirse sobre las experiencias del presente.

Analizar cómo evoluciona el fraude, cómo afecta a los consumidores y cómo influye en su percepción de seguridad permite entender los retos que enfrentan hoy los ecosistemas digitales y financieros.



Fraude en Panamá: el desafío de la era digital

¿Qué tan presente está el fraude en la vida de los panameños? La forma en que compran, pagan y gestionan su dinero ha cambiado profundamente en los últimos años. Desde financiar la compra de una nevera, enviar dinero de manera inmediata a un familiar, utilizar una billetera digital o pagar un servicio desde el celular, cada vez más actividades cotidianas ocurren en tiempo real. Sin embargo, esta transformación también ha venido acompañada de nuevos riesgos para los consumidores. A medida que estas experiencias se vuelven más frecuentes e inmediatas, las modalidades de fraude han evolucionado para adaptarse a los nuevos hábitos y canales utilizados por las personas.

En Panamá, estas amenazas pueden llegar a las personas a través de llamadas, mensajes, correos electrónicos, redes sociales y otros canales que forman parte de la vida cotidiana. A este panorama se suma el avance de la inteligencia artificial, una tecnología que está redefiniendo la manera en que se construye la confianza en los entornos digitales. Si bien fortalece las capacidades de detección y prevención del fraude, también puede utilizarse para crear contenidos falsos, suplantar identidades y hacer más difícil distinguir entre lo auténtico y lo fraudulento.

Para entender cómo se manifiesta esta realidad en el país, APC Experian desarrolló el estudio *“Del fraude digital a la confianza digital: cómo la inteligencia artificial está transformando la relación entre identidad, riesgo y confianza en Panamá”*, una investigación que analiza la exposición de los consumidores al fraude, sus experiencias frente a estas amenazas y el papel que tecnologías emergentes como la IA están desempeñando en la evolución de este fenómeno.

Ficha técnica

Objetivo del estudio

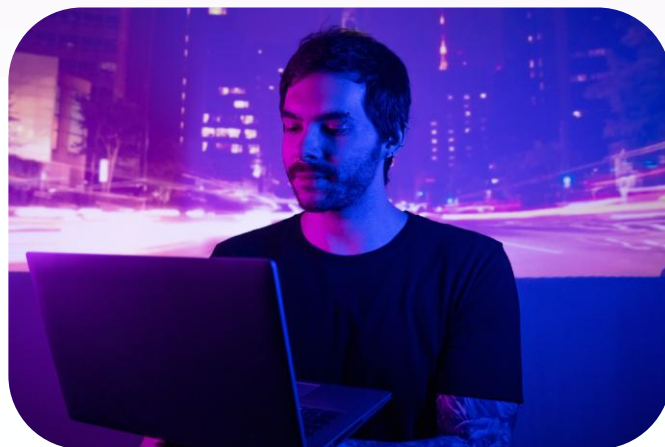
Analizar la percepción, experiencia y nivel de preparación de la población frente al fraude, identificando comportamientos, niveles de confianza y actitudes relacionadas con la prevención, el uso de canales digitales y las nuevas tecnologías.

Metodología

- Tipo de estudio: cuantitativo
- Metodología de recolección: encuesta online
- Instrumento: cuestionario

Características

- Personas mayores de 18 años.
- Residentes en Panamá.
- Cobertura nacional.
- Muestra: 500 personas.





La **confianza** digital frente a la realidad del fraude

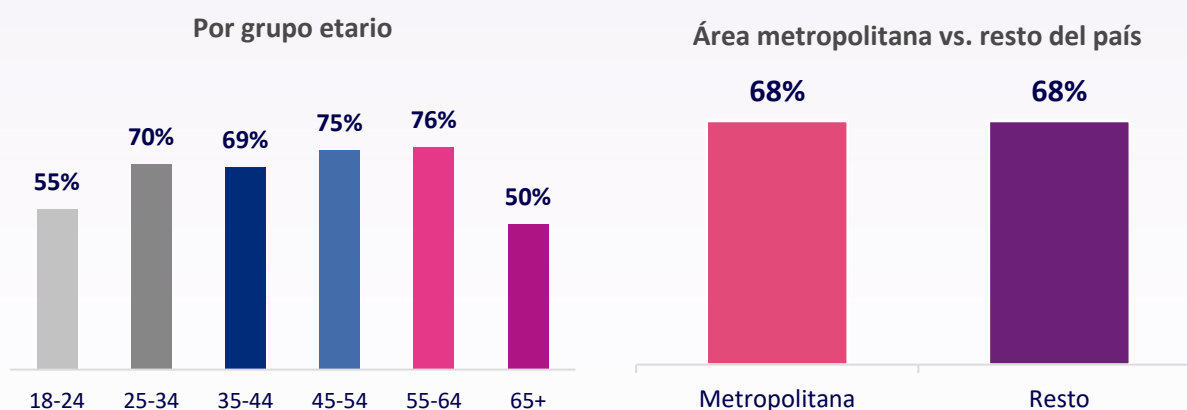


Los intentos de fraude alcanzan al 68% de los panameños, con mayor recurrencia en el área Metropolitana

Los intentos de fraude hacen parte de la experiencia cotidiana de los panameños. Durante los últimos 12 meses, el **68% de los encuestados afirma haber recibido al menos un intento de fraude**, y más de uno de cada tres (35%) señala que estas situaciones ocurrieron en varias ocasiones. En contraste, el **28% manifiesta no haber recibido ningún intento**, mientras que el 4% no lo recuerda.

Además, el **62% de los panameños afirma conocer a alguien que fue víctima de fraude en los últimos 12 meses**, lo que muestra que este fenómeno trasciende la experiencia individual y alcanza también el entorno cercano de la mayoría de la población.

Personas que recibieron intentos de fraude en el último año:



P1A. En los últimos 12 meses, ¿ha recibido algún intento de fraude, aunque no haya caído en él?

La exposición aumenta entre los grupos de edad intermedia y alcanza su mayor nivel entre los 55 y 64 años. En este segmento, el 76% recibió al menos un intento de fraude, seguido por las personas de 45 a 54 años (75%). En los extremos etarios la incidencia es menor: desciende al 55% entre los jóvenes de 18 a 24 años y al 50% entre los mayores de 65.

A nivel geográfico, la ubicación no cambia cuánto se está expuesto al fraude, pero sí su recurrencia. Tanto en el área Metropolitana como en el resto del país, el 68% recibió al menos un intento durante el último año. Sin embargo, los intentos repetidos son más frecuentes en el área Metropolitana: **el 39% afirma haberlos recibido varias veces, frente al 28% en el resto del país.**



Cerca de 4 de cada 10 panameños que enfrentaron un intento de fraude terminaron siendo víctimas

De los 500 encuestados, **340 afirmaron haber recibido al menos un intento de fraude en el último año**. Entre ellos, **cerca de cuatro de cada diez (39%)** reportó que al menos uno de estos intentos se concretó, convirtiéndose en víctima de fraude. El **62% restante** señaló que, aunque fue objetivo de un intento, este no llegó a materializarse.

La materialización del fraude tuvo consecuencias económicas para cerca de dos tercios de las víctimas. El 65% reportó alguna pérdida de dinero, aunque estas se concentraron principalmente en montos inferiores a USD 50 (31%), seguidos por pérdidas entre USD 50 y USD 200 (21%). Por su parte, el 31% señala que el fraude no le generó pérdidas económicas.

En conjunto, los hallazgos evidencian que el fraude sigue teniendo un impacto tangible en las finanzas personales, incluso cuando las pérdidas individuales son relativamente pequeñas.

Mensajes, aplicaciones móviles y compras en línea lideran los casos de fraude

Ingeniería social	
Mensajes o chats	34%
Comercio electrónico	
Aplicaciones móviles	24%
Compra de un producto o servicio no entregado	21%
Páginas web	17%
Fraude financiero	
Se realizó una transacción que no hizo	21%
Cargos pequeños o recurrentes no reconocidos	11%
Usaron mis datos después de una compra o registro	9%
Alguien retiró dinero de una cuenta	8%
Se envió una transferencia sin autorización	7%

Los **mensajes o chats (34%)** constituyen la modalidad de fraude más frecuente entre las víctimas. A estos les siguen las **aplicaciones móviles (24%)**, mientras que la compra de productos o servicios no entregados y las transacciones no realizadas por la víctima alcanzan un **21% cada una**. En conjunto, los resultados muestran que **las interacciones y operaciones digitales concentran los principales escenarios en los que se materializa el fraude**.



Los enlaces recibidos por mensajería y las transferencias son los principales escenarios donde se materializan los fraudes

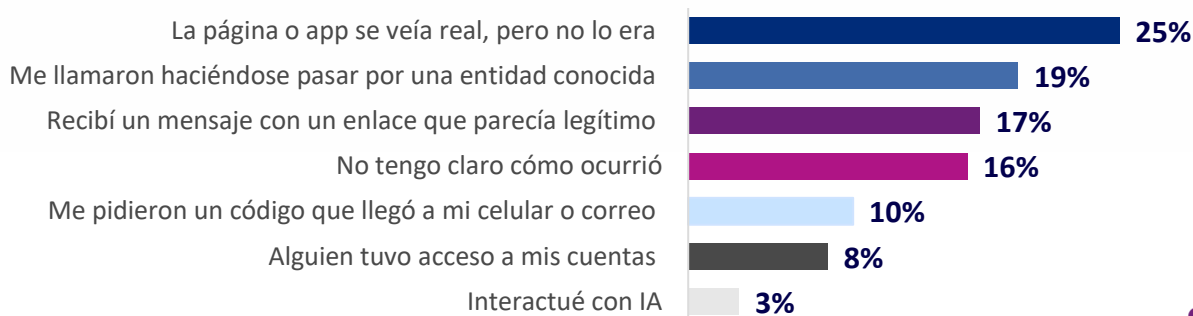
Los resultados muestran que los fraudes se materializan principalmente durante **interacciones digitales y transacciones financieras**. El uso de **enlaces recibidos por SMS o WhatsApp (24%)** y las **transferencias de dinero (22%)** son los escenarios más frecuentes, seguidos por el **registro o creación de cuentas (17%)** y la **navegación en páginas web (16%)**. En conjunto, los hallazgos muestran que el fraude ocurre en distintos momentos de la experiencia digital, desde la interacción con enlaces hasta la realización de operaciones financieras.

Transferencias y pagos	
Al hacer una transferencia de dinero	22%
Al pagar un producto o servicio en una tienda	15%
Al recibir una transferencia de dinero	8%
Al pagar en una tienda usando transferencia o código QR	5%
Navegación e interacción digital	
Al usar un enlace recibido por SMS o WhatsApp	24%
Al registrarme o crear una cuenta	17%
Al entrar o navegar en una página web	16%
Compras en línea	
Al comprar un producto en un Marketplace	15%
Sin interacción directa	
No estaba realizando ninguna acción en ese momento	11%

En estos escenarios, los ciberdelincuentes recurrieron principalmente a **mecanismos de suplantación y engaño para generar confianza**. La situación más frecuente fue el uso de **páginas o aplicaciones que parecían reales (25%)**, seguida por **llamadas de personas que se hicieron pasar por entidades conocidas (19%)** y **mensajes con enlaces aparentemente legítimos (17%)**. Además, el **16% de las víctimas no tiene claro cómo ocurrió el fraude**, lo que evidencia que estos mecanismos no siempre son fácilmente identificables por quienes los experimentan.

Más que un problema de canales específicos, los resultados muestran que el fraude se apoya principalmente en mecanismos de suplantación diseñados para parecer legítimos y generar confianza.

Estrategias utilizadas para concretar el fraude

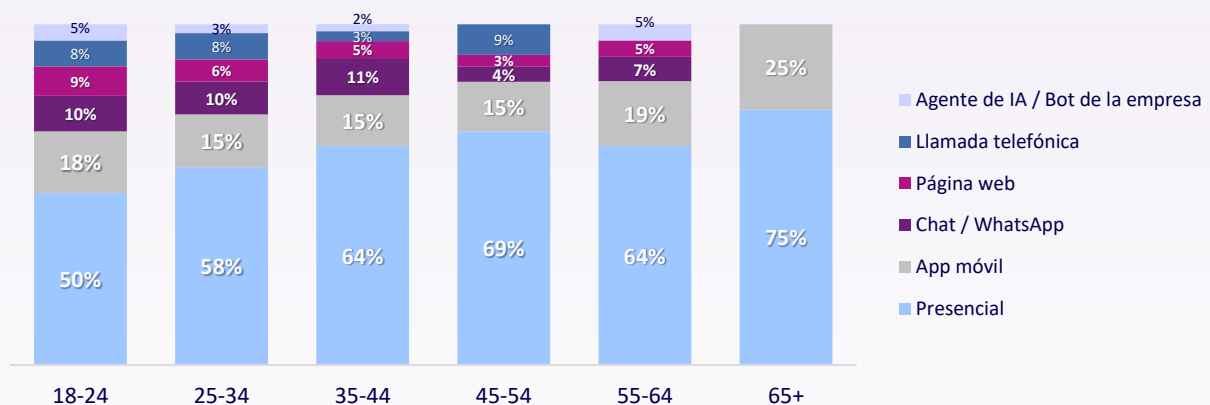


El 60% de los panameños confía más en el canal presencial para realizar trámites financieros

La **app móvil (16%)** ocupa el segundo lugar entre los canales de mayor confianza para realizar trámites financieros, aunque se ubica muy por debajo del canal presencial. Le siguen **Chat o WhatsApp (9%)**, las **llamadas telefónicas (6%)**, la **página web (6%)** y los **agentes de IA o bots de la empresa (3%)**.

La confianza en el canal presencial aumenta con la edad y alcanza su nivel más alto entre los mayores de 65 años.

Confianza en los canales para realizar trámites financieros, por grupo etario



La confianza en el canal presencial se fortalece a medida que aumenta la edad. Mientras **el 50% de las personas entre 18 y 24 años** lo señala como el canal de mayor confianza, la proporción supera el 60% en varios grupos de mayor edad y alcanza **75% entre los mayores de 65 años**. Incluso entre los más jóvenes, ningún canal digital se acerca individualmente al nivel de confianza del canal presencial.

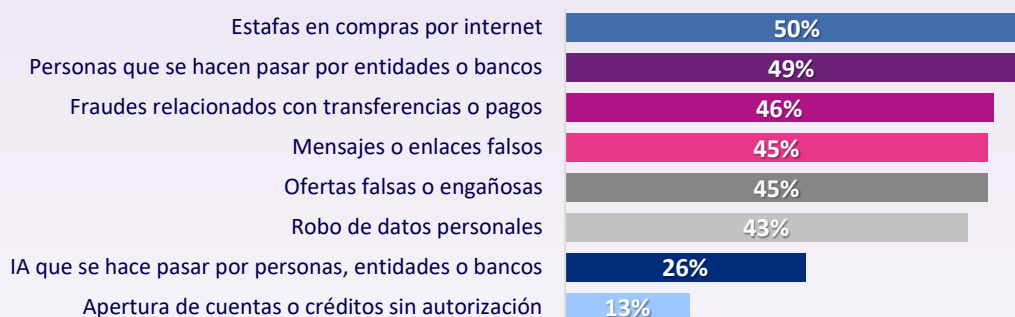
Esta preferencia por el canal presencial también se refleja en la percepción sobre el riesgo de fraude. Las **llamadas telefónicas (53%)** y las **redes sociales (49%)** son consideradas los principales escenarios donde ocurren fraudes, seguidas por los **links de pago falsos (43%)**, **WhatsApp (35%)** y los **marketplaces o plataformas de compraventa (33%)**. En contraste, los **comercios físicos (5%)** presentan una percepción de riesgo considerablemente menor, reforzando la asociación del fraude con los canales e interacciones digitales.

La preferencia por el canal presencial no responde únicamente a hábitos de uso. **También refleja una búsqueda de seguridad y acompañamiento en trámites financieros importantes. A medida que aumenta la edad**, crece la necesidad de validar información directamente con una persona, especialmente en un contexto donde el fraude digital genera mayor preocupación entre los consumidores.



Las estafas en compras por internet lideran la percepción de fraude en Panamá

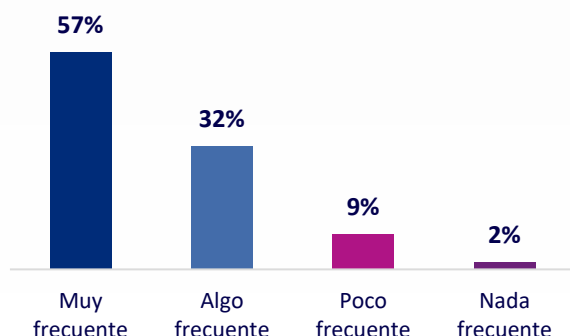
Percepción de las modalidades de fraude más comunes



Las estafas en compras por internet se posicionan como la modalidad de fraude más percibida (50%), seguidas muy de cerca por la suplantación de entidades o bancos (49%) y los fraudes relacionados con transferencias o pagos (46%). Los mensajes o enlaces falsos y las ofertas engañosas alcanzan 45% cada uno. En contraste, la apertura de cuentas o créditos sin autorización registra la menor percepción (13%), seguida por la suplantación mediante IA (26%).

El fraude dejó de percibirse como un hecho aislado: el 89% de los panameños cree que ocurre con frecuencia en el país

Percepción sobre la frecuencia del fraude en Panamá



Para la mayoría de los panameños, el fraude es un fenómeno frecuente en el país. El 89% considera que ocurre con frecuencia y más de la mitad (57%) señala que sucede muy frecuentemente.

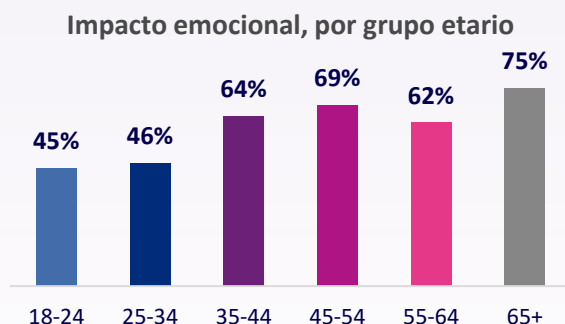
Esta percepción confirma que el fraude dejó de verse como una situación aislada y pasó a formar parte de los riesgos cotidianos asociados a las interacciones y transacciones digitales.

El 79% de los panameños considera que los intentos de fraude han aumentado frente al año anterior

El 46% cree que aumentaron mucho y el 32% que aumentaron algo. En contraste, solo el 3% percibe una disminución, mientras que el 16% considera que se mantienen igual.

Los panameños asocian el fraude principalmente con impactos económicos, seguidos por efectos relacionados con el bienestar emocional

Aunque el principal impacto asociado al fraude sigue siendo la **pérdida de dinero (86%)**, más de la mitad reconoce también consecuencias **emocionales (55%)**, relacionadas con estrés o ansiedad. Por su parte, el **29%** identifica afectaciones sociales, como el deterioro de las relaciones personales o la reputación.



El impacto emocional tiende a aumentar con la edad. Mientras el 45% de las personas entre 18 y 24 años y el 46% de quienes tienen entre 25 y 34 años asocia el fraude con estrés o ansiedad, la proporción sube al 64% entre los 35 y 44 años y al 69% entre los 45 y 54 años. El nivel más alto se registra entre los mayores de 65 años, con 75%.

Asimismo, la vulnerabilidad frente al fraude se asocia principalmente con conductas y conocimientos individuales. El 58% señala no verificar la información antes de actuar y el 49% la falta de educación sobre el uso de plataformas digitales. También destacan el exceso de confianza (43%), el desconocimiento de los riesgos (42%) y la falta de educación financiera (31%).

Top 5 factores de vulnerabilidad frente al fraude



La confianza en las transacciones digitales sigue siendo moderada entre los panameños

Aunque las transacciones digitales forman parte de la vida cotidiana, los niveles de confianza aún son moderados. **El 53% afirma sentirse poco o nada seguro al realizarlas, mientras que el 47% manifiesta algún nivel de seguridad.** Al mismo tiempo, la mayoría mantiene una actitud cautelosa frente al intercambio de información personal y biométrica.

Disposición a compartir datos personales y biométricos según el contexto



En línea con esta percepción de inseguridad, **el 77% se muestra poco o nada dispuesto** a compartir sus datos personales y biométricos al solicitar un producto o servicio por primera vez.

Sin embargo, **cuando compartir más información implica reducir el riesgo de fraude, la disposición aumenta: el 34% estaría dispuesto a entregar más datos**, aunque la mayoría (66%) aún mantiene algún grado de resistencia.

La disposición a compartir información también está relacionada con el conocimiento sobre qué datos puede solicitar una empresa legítima.

48%	Nombre completo
40%	Número de identificación
30%	Códigos de verificación enviados por SMS o correo
29%	Número de contacto
25%	Dirección de residencia
20%	Fecha de vencimiento de la cédula
19%	Fecha de vencimiento de la tarjeta
16%	Número de cuenta bancaria
15%	Código de seguridad (CVV)
13%	Número de sus tarjetas
13%	Información biométrica
11%	Contraseña bancaria
9%	Usuario de su banco
5%	Clave dinámica

Estas respuestas evidencian brechas de conocimiento sobre la información que una empresa legítima puede solicitar.

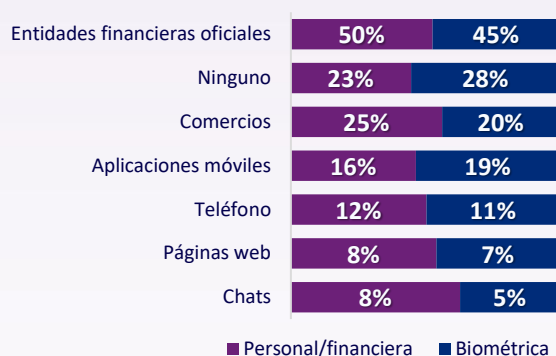
El **30%** considera válido compartir **códigos de verificación**, mientras que el **15%** cree que podría solicitarse el **código de seguridad (CVV)**, el **13%** el número de la tarjeta y el **11%** una contraseña bancaria.



La confianza sigue siendo un factor clave al compartir información personal y biométrica

La disposición a compartir información personal, financiera y biométrica varía significativamente según el nivel de confianza que generan los distintos canales. Los niveles de aceptación son más altos en entornos percibidos como confiables, como las entidades financieras, donde el 50% compartiría información personal o financiera y el 45% información biométrica. En contraste, la disposición disminuye de forma importante en otros espacios digitales y comerciales.

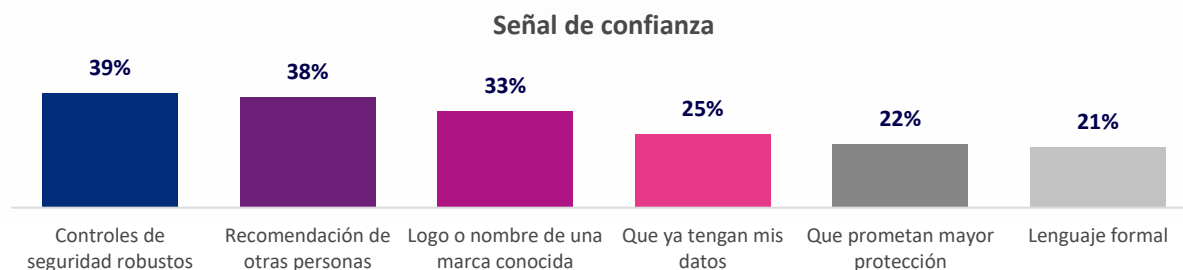
Canales considerados aceptables para compartir información personal y biométrica



La aceptación disminuye considerablemente fuera de las entidades financieras oficiales: solo entre el 6% y el 25% compartiría información en aplicaciones móviles o comercios. Además, el 28% no compartiría información biométrica en ningún canal, frente al 23% para información personal o financiera.

La cautela al compartir información también se refleja en las prácticas cotidianas de protección, principalmente al evitar hacer clic en enlaces (47%), usar únicamente plataformas conocidas (44%) y no contestar llamadas de números desconocidos (44%). Solo 6% no realiza ninguna acción específica.

La confianza se construye principalmente a partir de señales de seguridad y respaldo, especialmente los controles de seguridad robustos (39%), las recomendaciones de otras personas (38%) y el reconocimiento del logo o nombre de una marca conocida (33%).



El fraude digital se diversifica y alcanza nuevos escenarios en Panamá

Las compras con tarjeta de crédito (53%) y la suplantación de identidad (52%) son los escenarios donde los panameños perciben una mayor vulnerabilidad frente al fraude. También destacan el comercio electrónico (38%), la apertura de billeteras digitales (33%) y la solicitud de créditos (28%), reflejando que los riesgos se extienden a distintos momentos de la experiencia financiera digital.

Además de los escenarios tradicionales, comienzan a aparecer nuevas formas de interacción digital asociadas al fraude. El 14% afirma haber experimentado o conocido casos relacionados con la interacción con agentes de IA o bots empresariales, lo que evidencia cómo estas tecnologías empiezan a incorporarse en las percepciones de riesgo de los consumidores.

	Compras con tarjeta de crédito	53%		Apertura billeteras digitales	33%
	Suplantación de identidad	52%		Solicitud de créditos	28%
	Comercio electrónico	38%			

	Transferencias de dinero entre cuentas	34%		Compras en marketplaces	33%		Pagos con tarjeta	30%
	Nunca he tenido esa experiencia	24%		Pagos en tiendas usando transferencias o QR	18%		Billeteras digitales	15%

Esta percepción de vulnerabilidad se refleja en las experiencias de fraude conocidas. **Las transferencias entre cuentas lideran con un 34%**, seguidas por las compras en marketplaces con 33% y los pagos con tarjeta con 30%. **El 24% nunca ha tenido o conocido una experiencia de fraude**, mientras que **el 14% identifica casos al interactuar con agentes de IA o bots empresariales**.

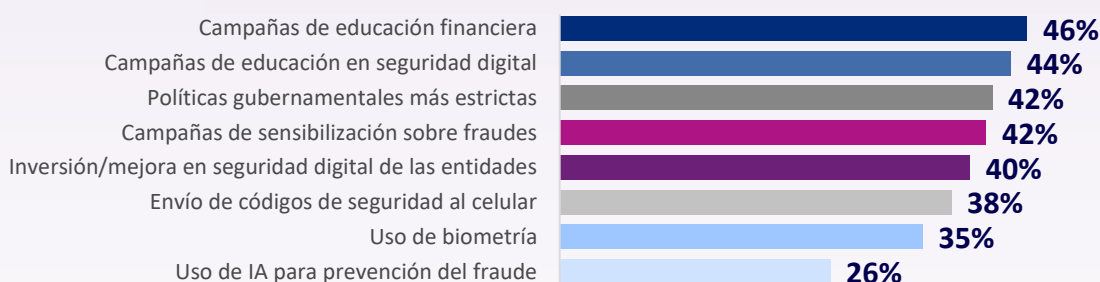
La tienda física concentra la mayor percepción de seguridad con 65%, seguida por el pago con tarjeta (14%) y las transferencias o billeteras digitales (10%). Si bien los procesos asistidos por inteligencia artificial representan hoy una proporción reducida (1%), **su presencia refleja cómo estas nuevas formas de interacción ya comienzan a formar parte de la experiencia financiera de algunos usuarios**.



La educación y la prevención son las acciones consideradas más efectivas para reducir el fraude

Los panameños atribuyen un papel central a la educación y la prevención en la reducción del fraude. Las campañas de educación financiera (46%) y las campañas de educación en seguridad digital (44%) son las acciones consideradas más efectivas. En contraste, el uso de inteligencia artificial para la prevención del fraude registra la menor efectividad percibida, con 26%.

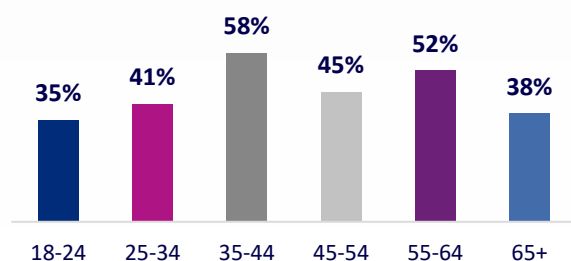
Acciones consideradas efectivas para prevenir el fraude



El 45% acudiría a una entidad financiera ante una posible situación de fraude

Ante una posible situación de fraude, las entidades financieras son el principal punto de apoyo para el 45% de los panameños, seguidas por amigos y familiares con 26%. En contraste, el 9% no sabría a quién acudir y el 7% no recurriría a nadie.

Preferencia por acudir a una entidad financiera, por grupo etario



La preferencia por acudir a una entidad financiera varía según la edad y alcanza su mayor nivel entre las personas de 35 a 44 años, con 58%. Esta proporción también supera el 50% entre quienes tienen de 55 a 64 años, mientras que los jóvenes de 18 a 24 años registran el nivel más bajo, con 35%; además, un 11% de estos jóvenes no sabría a quién acudir ante un posible fraude.



El conocimiento sobre cómo reportar un fraude aún muestra oportunidades de mejora

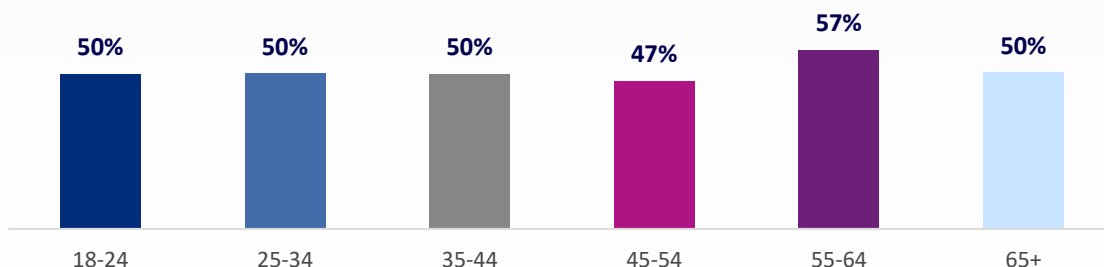
El conocimiento sobre cómo reportar un fraude está dividido entre los panameños. **El 50% afirma saber cómo hacerlo, mientras que el otro 50% desconoce el procedimiento.** Esto muestra que el acceso a información sobre los mecanismos de denuncia aún no es homogéneo entre la población.

Los resultados sugieren que existe una oportunidad para fortalecer la divulgación y orientación sobre los canales disponibles para reportar fraudes. A medida que las interacciones digitales ganan relevancia en la vida cotidiana, conocer cómo actuar ante un incidente se convierte en un elemento importante para la protección de los consumidores.

El conocimiento sobre cómo reportar un fraude está dividido: el 50% de los panameños afirma saber cómo hacerlo, mientras que el otro 50% desconoce el procedimiento.

A diferencia de otros indicadores, el conocimiento sobre cómo reportar un fraude se mantiene relativamente estable entre los grupos etarios. **Las personas de 55 a 64 años registran la mayor proporción, con 57%,** mientras que entre los demás grupos el resultado oscila entre 47% y 50%.

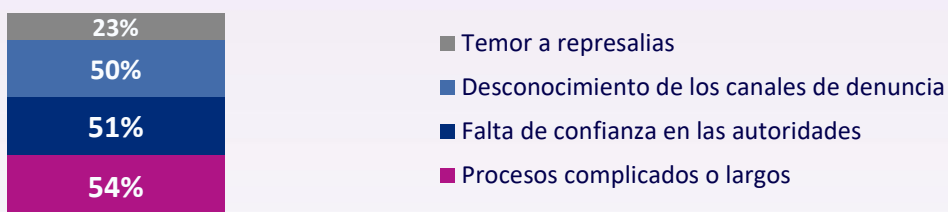
Personas que sí saben cómo reportar un fraude, por grupo etario



La respuesta ante un fraude aún enfrenta desafíos para los consumidores

Los panameños señalan distintos factores que pueden dificultar la respuesta ante una situación de fraude. **Los procesos complicados o largos (54%), la falta de confianza en las autoridades (51%) y el desconocimiento de los canales de reporte (50%) encabezan las respuestas, mientras que el temor a represalias (23%) presenta una incidencia menor.**

Principales obstáculos percibidos para denunciar un fraude



Entre quienes buscaron resolver una situación de fraude, los resultados muestran experiencias mixtas. **El 39% logró recuperar completamente su dinero, mientras que el 10% recuperó solo una parte y el 11% aún mantenía el proceso abierto al momento de la encuesta.**

Sin embargo, no todos obtuvieron una respuesta favorable. El 26% señala que no logró resolver el problema y el 75% califica el proceso como difícil o muy difícil, lo que sugiere oportunidades para fortalecer la experiencia de atención y acompañamiento a las víctimas de fraude.



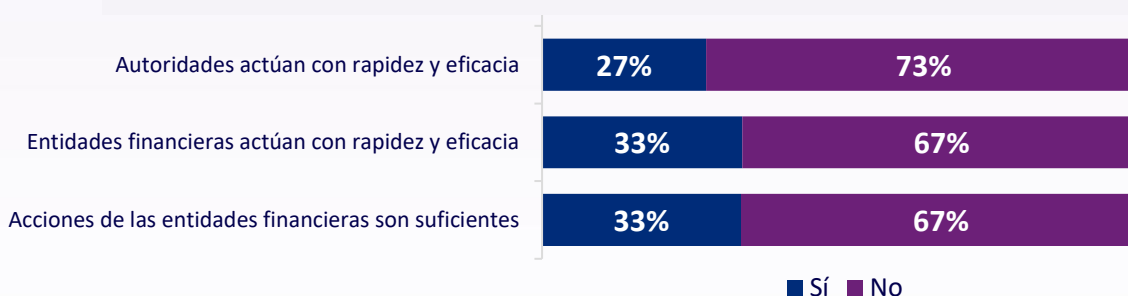
Entre el 67% y el 73% considera que las medidas actuales frente al fraude podrían fortalecerse

La mayoría de los panameños identifica oportunidades para fortalecer la prevención y respuesta frente al fraude

Los resultados muestran que una proporción importante de los panameños considera que las medidas actuales frente al fraude podrían fortalecerse.

El 67% considera que las acciones de las entidades financieras para prevenir el fraude pueden mejorar, mientras que una proporción similar (67%) opina lo mismo sobre su capacidad de respuesta ante estos casos. Asimismo, el 73% considera que existe espacio para fortalecer la actuación de las autoridades frente al fraude.

Percepción sobre la respuesta institucional frente al fraude



Los resultados reflejan que los consumidores esperan un fortalecimiento continuo de las acciones orientadas a prevenir, detectar y responder al fraude. **La confianza en los entornos digitales no depende de una sola institución, sino de la articulación de esfuerzos que permitan ofrecer experiencias más seguras a lo largo de todo el proceso.**



Los panameños muestran interés en aprender y adaptarse a una nueva realidad impulsada por la IA

La inteligencia artificial está transformando la forma en que los consumidores interactúan con los entornos digitales. En este contexto, **el 79% de los panameños manifiesta estar algo o muy preocupado por la posibilidad de que estas herramientas faciliten fraudes o engaños, mientras que el 46% se declara muy interesado en aprender a identificar fraudes creados con IA**, reflejando una creciente disposición a adaptarse a esta nueva realidad digital.

	Nada	Poco	Algo	Mucho
Preocupación por IA como facilitadora de fraude	7%	14%	33%	46%
Seguridad percibida para identificar fraude creado/alterado con IA	23%	37%	28%	12%
Confianza en que la IA detecte fraudes o suplantación	22%	40%	30%	8%
Disposición a permitir análisis con IA para detectar fraudes	22%	32%	37%	8%
Interés en aprender a identificar fraudes creados con IA	6%	14%	35%	46%

Identificar contenidos creados con IA sigue siendo un desafío

El 60% se siente poco o nada seguro de reconocer si una llamada, mensaje, imagen o video fue generado o alterado con IA, lo que muestra que distinguir entre contenidos auténticos y sintéticos sigue siendo una tarea compleja para muchos consumidores.

La IA gana espacio en la prevención, pero aún construye confianza

El 62% expresa poca o ninguna confianza en que la IA pueda detectar fraudes o suplantaciones de identidad. Esto sugiere que aún existe una oportunidad para fortalecer el conocimiento sobre el uso de estas herramientas en la prevención del fraude.

La confianza será clave para impulsar la adopción de soluciones basadas en IA

El 55% se muestra poco o nada dispuesto a permitir que herramientas de IA analicen su información para detectar posibles fraudes, reflejando la importancia de la transparencia y la confianza en el uso de los datos.

Existe una alta disposición para aprender sobre fraude e IA

El 46% afirma estar muy interesado en aprender a identificar fraudes creados con inteligencia artificial, reflejando la voluntad de los consumidores de adquirir nuevas herramientas para desenvolverse con mayor confianza en entornos digitales.



La autenticidad de los contenidos digitales se convierte en un nuevo desafío de confianza



Publicidad o promociones sospechosas

39%



Mensajes o correos sospechosos

36%



Llamadas con voces falsas o imitadas

28%



Chats que parecían personas reales

27%



Videos o imágenes manipuladas

24%

Las dudas sobre la autenticidad de los contenidos aparecen en distintos puntos de contacto digital. La publicidad o promociones sospechosas (39%) y los mensajes o correos sospechosos (36%) encabezan las situaciones que más generan incertidumbre, seguidas por llamadas con voces falsas o imitadas (28%), chats que parecían personas reales (27%) y videos o imágenes manipuladas (24%).

Estos resultados evidencian cómo el avance de la inteligencia artificial está transformando la manera en que las personas evalúan la autenticidad de las interacciones digitales. La capacidad de generar mensajes, imágenes, videos o voces cada vez más convincentes plantea nuevos desafíos para distinguir entre contenidos legítimos y potenciales intentos de engaño.

En este contexto, la confianza digital depende cada vez más de la capacidad de los consumidores para verificar la información que reciben. **A medida que las herramientas basadas en IA ganan presencia en la vida cotidiana, fortalecer el conocimiento y las habilidades para identificar posibles señales de fraude se convierte en un elemento clave para navegar con mayor confianza en los entornos digitales.**



La siguiente evolución: los agentes de IA

La inteligencia artificial está entrando en una nueva etapa. Más allá de responder preguntas o generar contenido, los agentes de IA comenzarán a desempeñar un papel cada vez más activo en las interacciones digitales y financieras. **Estos sistemas podrán buscar información, comparar alternativas, interactuar con organizaciones e incluso ejecutar acciones en representación de las personas.**

Este cambio tiene implicaciones profundas para la forma en que se construye confianza. Si hoy gran parte de los esfuerzos de prevención y seguridad se concentran en validar la identidad de las personas y detectar riesgos, el siguiente desafío será verificar quién o qué está actuando en su nombre.

De verificar personas a verificar agentes

Durante años, la pregunta fundamental de la confianza digital ha sido relativamente simple: *¿la persona es quien dice ser?*

En los próximos años surgirá una nueva pregunta: *¿el agente que está actuando representa realmente a esa persona y tiene autorización para hacerlo?*

A medida que los agentes de IA participen en procesos relacionados con crédito, pagos, compras, administración financiera u otras interacciones digitales, será necesario generar mecanismos capaces de validar identidades, autorizaciones, contexto e intención de forma continua.

La capacidad de estos agentes para operar de manera segura dependerá de la información que los respalda. La inteligencia artificial aprende, interpreta y toma decisiones a partir de datos, por lo que la calidad, actualidad y profundidad de la **información serán fundamentales para validar interacciones, verificar permisos, detectar comportamientos inusuales y generar confianza en tiempo real.**

Para compañías como Experian, **esta evolución representa una extensión natural de capacidades que durante años han contribuido a fortalecer la toma de decisiones, la prevención del fraude y la construcción de confianza.** La combinación de datos, identidad, analítica avanzada e inteligencia artificial que hoy permite evaluar riesgos y validar interacciones será cada vez más relevante en un entorno donde personas y agentes inteligentes interactuarán de manera frecuente



La siguiente etapa no estará marcada únicamente por **experiencias más rápidas o personalizadas**. El verdadero desafío será construir mecanismos que permitan a personas, organizaciones y agentes inteligentes interactuar de manera **segura y confiable**.



La próxima frontera de la confianza digital no será únicamente **verificar identidades humanas**. Será la capacidad de combinar datos, identidad e inteligencia artificial para validar agentes, autorizaciones e interacciones **en tiempo real**.



Conclusiones

- 1 El fraude ya forma parte de la experiencia cotidiana de los panameños**
El 68% recibió al menos un intento de fraude durante el último año y el 35% señala haberlos recibido varias veces. Además, el 62% conoce a alguien que fue víctima, mientras que el 79% percibe que los intentos han aumentado frente al año anterior.
- 2 La exposición al fraude se materializa con frecuencia en pérdidas económicas**
Entre quienes recibieron intentos de fraude, cerca de 4 de cada 10 (39%) terminaron siendo víctimas. El 65% de estas reportó alguna pérdida de dinero, principalmente por montos inferiores a USD 50 (31%) o entre USD 50 y USD 200 (21%).
- 3 Las interacciones digitales concentran los principales escenarios de fraude**
Los mensajes o chats (34%) y las aplicaciones móviles (24%) lideran las modalidades entre las víctimas. El fraude se materializa especialmente al usar enlaces recibidos por SMS o WhatsApp (24%) y realizar transferencias (22%), mientras que la suplantación mediante páginas o aplicaciones aparentemente reales (25%) es la principal estrategia utilizada.
- 4 La prevención convive con brechas de conocimiento y una fuerte cautela digital**
El 64% no ha recibido capacitación o información para prevenir el fraude y el 53% se siente poco o nada seguro realizando transacciones digitales. A esto se suman brechas sobre la información que puede solicitar una empresa legítima, mientras el canal presencial concentra ampliamente la mayor confianza para realizar trámites financieros (60%).
- 5 Denunciar y resolver un fraude continúa siendo un proceso complejo**
Solo el 26% ha denunciado alguna vez un fraude y la mitad no sabe cómo reportarlo. Los procesos complicados o largos (54%), la falta de confianza en las autoridades (51%) y el desconocimiento de los canales (50%) son las principales barreras; entre quienes buscaron una solución, solo el 39% recuperó completamente su dinero.
- 6 La IA genera preocupación, pero también abre una oportunidad para fortalecer la prevención**
El 79% está algo o muy preocupado por el uso de IA para facilitar fraudes, mientras que el 60% se siente poco o nada seguro identificando contenidos creados o alterados con esta tecnología. En contraste, el 80% muestra interés en aprender a reconocer fraudes creados con IA, evidenciando una oportunidad para fortalecer la educación y prevención digital.

