



Del fraude digital a la confianza digital:

Fraude, identidad e inteligencia artificial en Colombia

Agosto 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 Colombia: el desafío de la era digital

¿Qué tan presente está el fraude en la vida de los colombianos? La forma en que los colombianos 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 Colombia, 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, DataCrédito 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 Colombia”*, 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

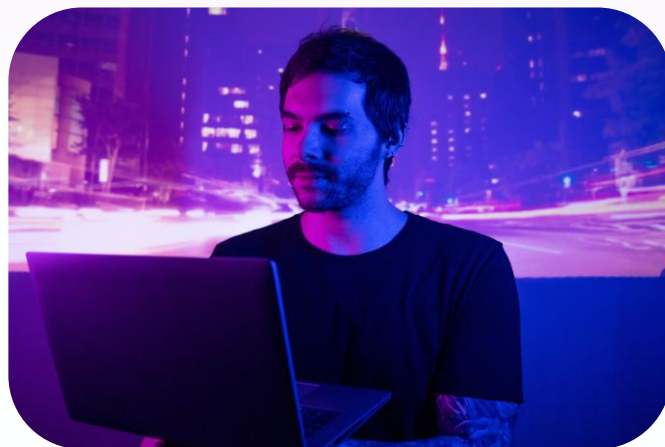
Analizar la percepción, experiencia y nivel de preparación de la población frente al fraude, identificando comportamientos, niveles de confianza y actitudes relacionadas con la prevención, el uso de canales digitales y las nuevas tecnologías.

Metodología

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

Características

- Personas mayores de 18 años.
- Residentes en Colombia.
- Cobertura nacional.
- Muestra: 1.000 personas.





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



El fraude ya forma parte de la realidad cotidiana de los colombianos

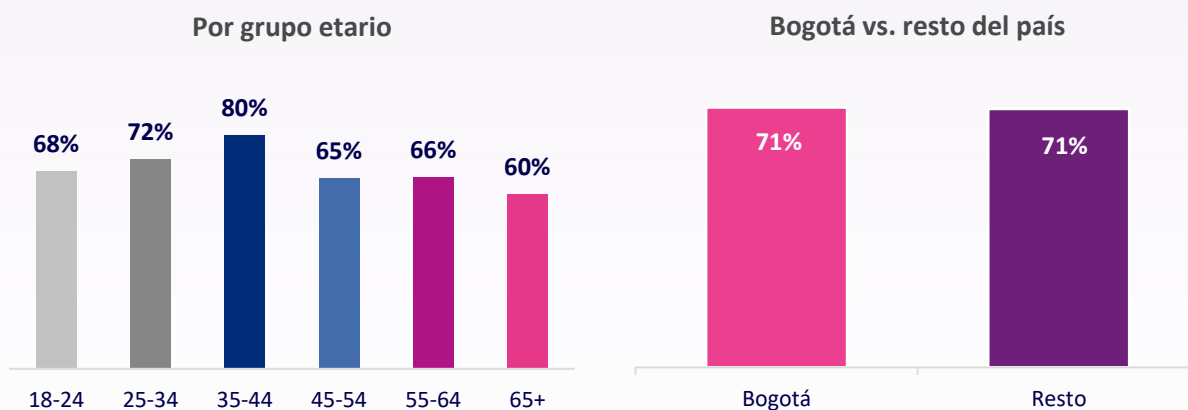
Los intentos de fraude hacen parte de la experiencia cotidiana de los colombianos. Durante los últimos 12 meses, el **71%** de los encuestados **afirma haber recibido al menos un intento de fraude**, y casi cuatro de cada diez (39%) señala que estas situaciones ocurrieron en varias ocasiones. En contraste, solo una cuarta parte (25%) manifiesta no haber recibido ningún intento.



Además, el **70%** de los colombianos afirma conocer a alguien que fue víctima de fraude en los últimos 12 meses, lo que demuestra que este fenómeno **trasciende la experiencia individual** y también **afecta al entorno cercano de la mayoría de la población**.

P1B. ¿Conoce a alguien que efectivamente haya sido víctima de fraude en los últimos 12 meses?

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 al fraude se mantiene alta en todos los grupos de edad. El nivel más alto se registra entre **las personas de 35 a 44 años, donde el 80% afirma haber recibido al menos un intento durante el último año**.

Bogotá y el resto del país registran niveles similares de exposición al fraude (71%). Sin embargo, fuera de la capital son más frecuentes los casos de múltiples intentos (42%), mientras que en Bogotá predominan las situaciones en las que las personas reportan haber recibido un único intento (32%).

Los resultados muestran que el **fraude tiene un alcance transversal**. La alta exposición observada en todos los grupos de edad y territorios evidencia que este riesgo forma parte de la realidad cotidiana de millones de personas, **independientemente de dónde viven o de su etapa de vida**.

Casi la mitad de quienes enfrentaron un intento de fraude terminaron siendo víctimas

El **71% de los colombianos encuestados** afirmó haber recibido al menos un intento de fraude durante el último año. Entre ellos, **cerca de la mitad (46%)** reportó que al menos uno de estos intentos se concretó, convirtiéndose en víctima de fraude. El **54% restante señaló que, aunque fue objeto de un intento, este no llegó a materializarse**.

Mensajes, compras en línea y sitios web lideran los casos de fraude:

CATEGORÍA	MOTIVO	PORCENTAJE
Ingeniería social	Mensajes o chats	27%
	Compra de un producto o servicio no entregado	25%
Comercio electrónico	Páginas web	22%
	Aplicaciones móviles	20%
	Se realizó una transacción que no hizo	18%
Fraude financiero	Usaron mis datos después de una compra o registro	17%
	Se envió una transferencia sin autorización	15%
	Alguien retiró dinero de una cuenta	13%
	Cargos pequeños o recurrentes no reconocidos	10%



¿Cuál es el impacto económico?

El **78%** de las víctimas reportó pérdidas de dinero, mientras que solo el **19%** indicó no haber sufrido una afectación económica (el **2%** prefirió no responder).



Las pérdidas se concentraron principalmente entre **USD 50 y USD 200 (35%)**, seguidas por montos inferiores a **USD 50 (28%)**.

54%

Aunque fue objeto de un intento, este **no** llegó a materializarse.



P2C. Pensando en ese caso de fraude, ¿qué fue lo que ocurrió?

El fraude suele materializarse en actividades cotidianas. Desde conversaciones por mensajes hasta compras, pagos o el uso de servicios financieros, estas modalidades aprovechan los espacios donde las personas interactúan y depositan confianza. Esto refleja cómo el fraude evoluciona al ritmo de los hábitos de los consumidores, integrándose cada vez más a su vida diaria.

Los canales digitales concentran las principales modalidades de fraude reportadas. Los mensajes o chats (**27%**) lideran los casos, seguidos por la compra de productos o servicios no entregados (**25%**), las estafas en páginas web (**22%**) y aplicaciones móviles (**20%**). Esto evidencia que el fraude continúa materializándose principalmente en actividades digitales cotidianas.



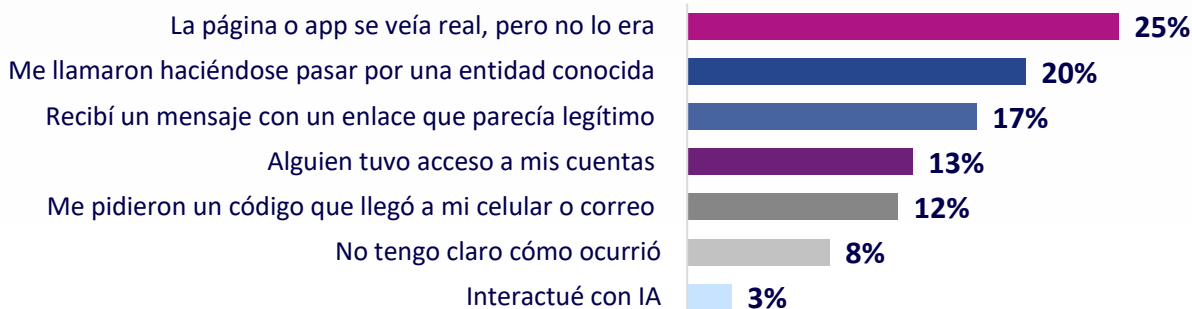
Las transferencias y los enlaces recibidos por mensajería son los principales escenarios donde se materializan los fraudes

Las transferencias de dinero (23%) y el uso de enlaces recibidos por SMS o WhatsApp (23%) son los escenarios más frecuentes en los que se materializa el fraude. Les siguen la navegación en páginas web (21%) y la compra de productos en marketplaces (15%), lo que evidencia que estas situaciones suelen concretarse durante actividades digitales cotidianas. **Estos resultados sugieren que los fraudes tienden concretarse en momentos donde las personas deben tomar decisiones rápidas o actuar con información limitada:** una solicitud de pago, un enlace o una página que aparenta ser real pueden ser suficientes para reducir las señales de alerta y aumentar la probabilidad de que el fraude se materialice.

Categoría	Motivo	Porcentaje
 Transferencias y pagos	• Al hacer una transferencia de dinero	23%
	• Al pagar un producto o servicio en una tienda	13%
	• Al pagar en una tienda usando transferencia o código QR	13%
	• Al recibir una transferencia de dinero	11%
 Navegación e interacción digital	• Al usar un enlace recibido por SMS o WhatsApp	23%
	• Al entrar o navegar en una página web	21%
	• Al registrarme o crear una cuenta	14%
 Compras en línea	• Al comprar un producto en un marketplace	15%
 Sin interacción directa	• No estaba realizando ninguna acción en ese momento	10%

Las modalidades más efectivas para los ciberdelincuentes son aquellas que logran generar confianza o aparentar legitimidad. Las páginas o aplicaciones falsas (25%), las llamadas que simulan provenir de una entidad conocida (20%) y los enlaces que parecen auténticos (17%) fueron las principales estrategias utilizadas para concretar el fraude.

Estrategias utilizadas para concretar el fraude



Los fraudes se materializan en canales cotidianos porque los delincuentes logran aparentar **confianza y legitimidad**.





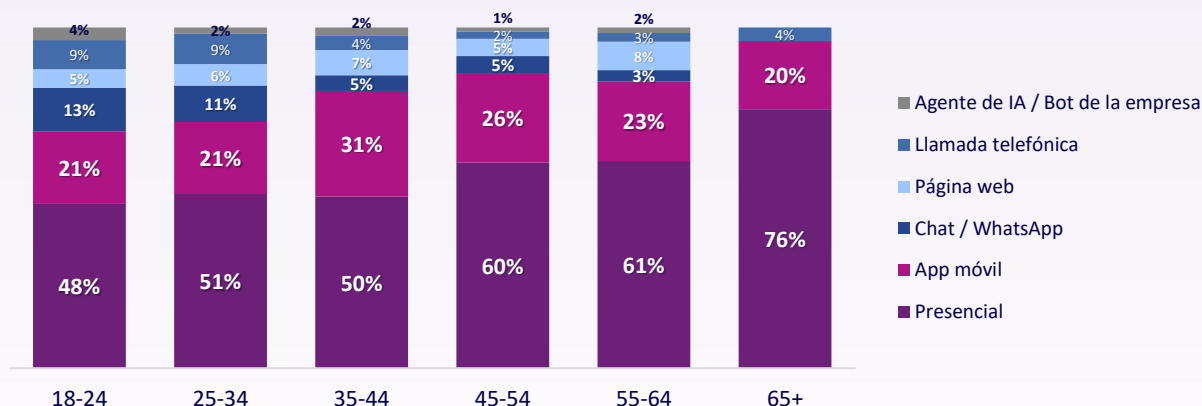
Cómo el fraude moldea la **confianza** digital



La evolución de los canales financieros está marcada por la confianza y la adopción gradual

Aunque la digitalización continúa transformando la forma en que los colombianos realizan sus trámites financieros, los resultados sugieren que la rapidez y conveniencia de los canales digitales conviven con una necesidad igualmente importante: **contar con mecanismos que permitan validar información, resolver dudas y tener mayor certeza al momento de tomar decisiones**. Esto ayuda a explicar por qué el canal presencial (54%) y la app móvil (25%) concentran la mayor parte de las preferencias para realizar trámites financieros, mientras que WhatsApp (7%), las llamadas telefónicas (6%), las páginas web (6%) y los agentes de IA o bots registran un 2%.

Preferencia por canal para realizar trámites financieros, por grupo etario



Esta diversificación es particularmente visible entre los consumidores más jóvenes. Aunque los agentes de IA o bots representan apenas el 2% de las preferencias a nivel general, entre los jóvenes de 18 a 24 años alcanzan el 4%, la participación más alta entre todos los grupos de edad. Si bien todavía se trata de una proporción reducida, este resultado sugiere una **apertura temprana hacia nuevas formas de interacción que podrían ganar relevancia a medida que aumente la familiaridad con estas herramientas**.

Esta evolución ocurre en un contexto donde ciertos canales aún se asocian con experiencias de fraude. Las llamadas telefónicas (57%), los enlaces de pago falsos (54%), los mensajes de texto o SMS (45%), las redes sociales (41%) y WhatsApp (39%) son identificados como algunos de los principales escenarios donde ocurren estas situaciones, lo que demuestra que, a medida que surgen nuevas formas de interacción, **su adopción estará influenciada no solo por las capacidades de la tecnología, sino también por la percepción de riesgo que los usuarios asocian a cada canal**.



La adopción de nuevos canales financieros es un **proceso gradual**. A medida que las personas desarrollan mayor confianza y familiaridad con nuevas tecnologías, comienzan a surgir formas alternativas de interacción, como los **agentes de IA**, especialmente entre las generaciones más jóvenes.



La percepción del fraude sigue siendo alta entre los colombianos

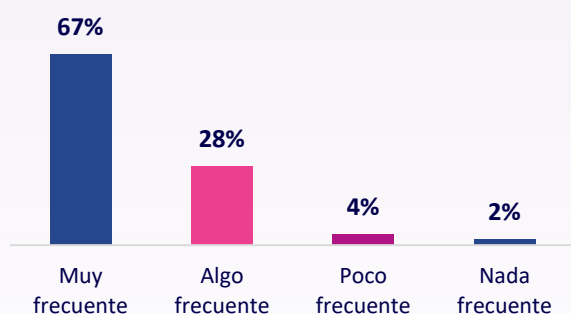


El fraude dejó de percibirse como un hecho aislado:

el 95% de los colombianos cree que ocurre con frecuencia

en el país. De hecho, en comparación con el año anterior, la percepción de riesgo era del 97,7%, es decir que se mantiene en niveles igualmente altos, lo que sugiere que el fraude continúa siendo una preocupación constante para la población.

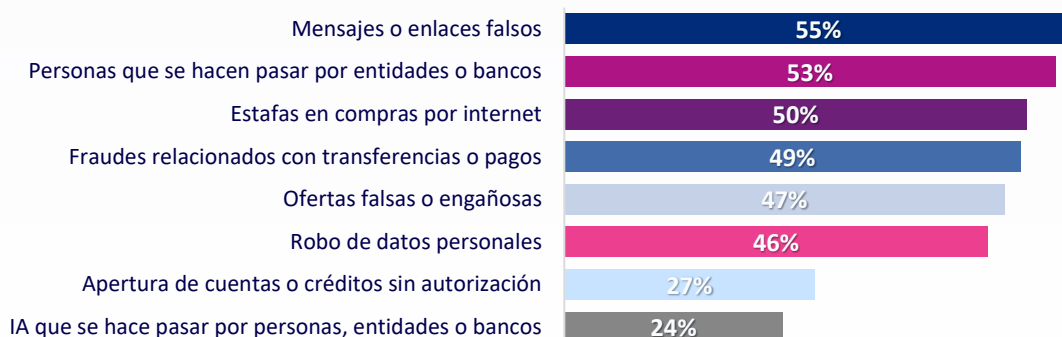
Percepción sobre la frecuencia del fraude en Colombia



Para la gran mayoría de los colombianos, el fraude ocurre con frecuencia.

El 95% considera que los fraudes ocurren con frecuencia y dos de cada tres (67%) creen que suceden **muy frecuentemente**. En contraste, solo el 6% percibe que se trata de un fenómeno poco o nada frecuente.

Percepción de las modalidades de fraude



Los mensajes o enlaces falsos (55%) y la suplantación de entidades o bancos (53%) encabezan las modalidades de fraude percibidas, seguidos por las estafas en compras por internet (50%) y los fraudes relacionados con transferencias o pagos (49%). En contraste, la suplantación mediante IA (24%) y la apertura de cuentas o créditos sin autorización (27%) presentan una menor percepción.



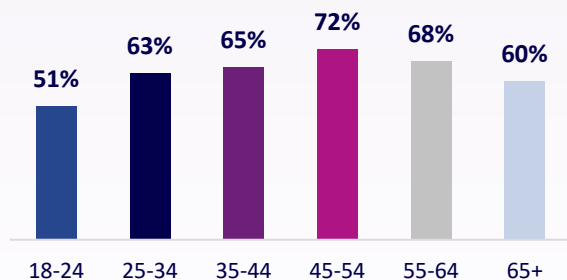
El 81% de los colombianos considera que los intentos de fraude han aumentado frente al año anterior

Además de percibir el fraude como un fenómeno frecuente, los colombianos consideran que estas amenazas siguen en aumento. **El 81% cree que los intentos de fraude han crecido frente al año anterior:** para el 50% el incremento ha sido significativo, mientras que el 31% considera que ha aumentado de manera moderada. Esta percepción refuerza la sensación de una mayor exposición al fraude.

El fraude es percibido principalmente como una amenaza económica, pero también emocional

¿Cuál es el verdadero impacto del fraude? Aunque la pérdida de dinero sigue siendo la principal consecuencia asociada a estas situaciones (86%), sus efectos van mucho más allá del ámbito económico. El 64% de los colombianos considera que las víctimas experimentan estrés o ansiedad, mientras que el 35% menciona afectaciones sociales, como el deterioro de las relaciones personales o la reputación.

Impacto emocional, por grupo etario



El reconocimiento del impacto emocional es más alto entre la población adulta. Mientras el 51% de los jóvenes entre 18 y 24 años considera que el fraude genera estrés o ansiedad, esta percepción alcanza su mayor nivel entre las personas de 45 a 54 años (72%).

La prevención del fraude también depende de qué tan preparados están los consumidores para reconocer los riesgos. Junto con la falta de verificación y el exceso de confianza, los colombianos señalan la falta de educación sobre el uso de plataformas digitales (44%), el desconocimiento de los riesgos (43%) y la presión por responder con rapidez (35%) como algunos de los principales factores que aumentan su exposición al fraude.

Top 5 factores de vulnerabilidad frente al fraude



La confianza digital enfrenta desafíos de conocimiento

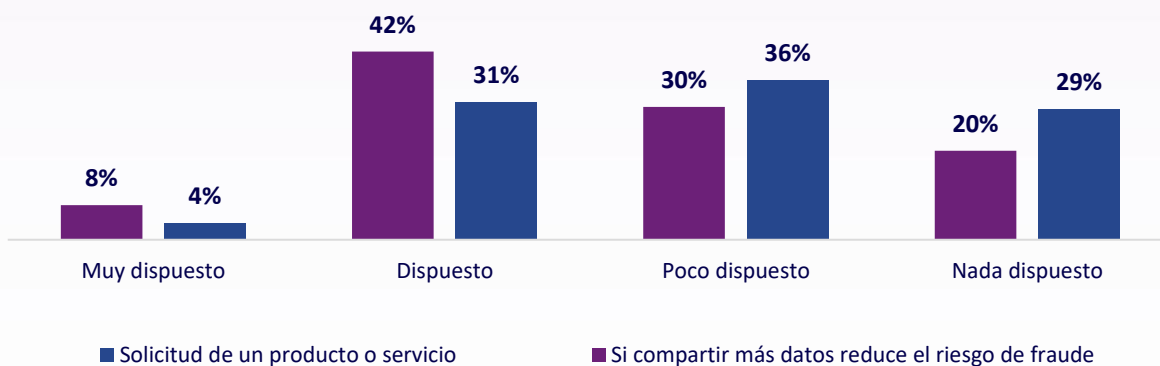


El 60% afirma sentirse **algo o muy seguro** al realizar transacciones digitales.

Sin embargo, esta percepción está impulsada principalmente por quienes se sienten **algo seguros (50%)**, mientras que solo el **10%** declara sentirse **muy seguro**. En contraste, el **40%** aún manifiesta sentirse **poco o nada seguro**, lo que evidencia que persisten reservas frente a estos canales.

La confianza en los entornos digitales no siempre está acompañada de un conocimiento claro sobre el manejo de la información personal. Aunque la mayoría se siente segura al realizar transacciones, persisten dudas sobre qué datos se pueden solicitar y cuáles representan un riesgo para la seguridad de las personas.

Disposición a compartir datos personales y biométricos según el contexto



P10A. ¿Qué tan dispuesto está a compartir sus datos personales y biométricos a la hora de solicitar productos y servicios por primera vez?

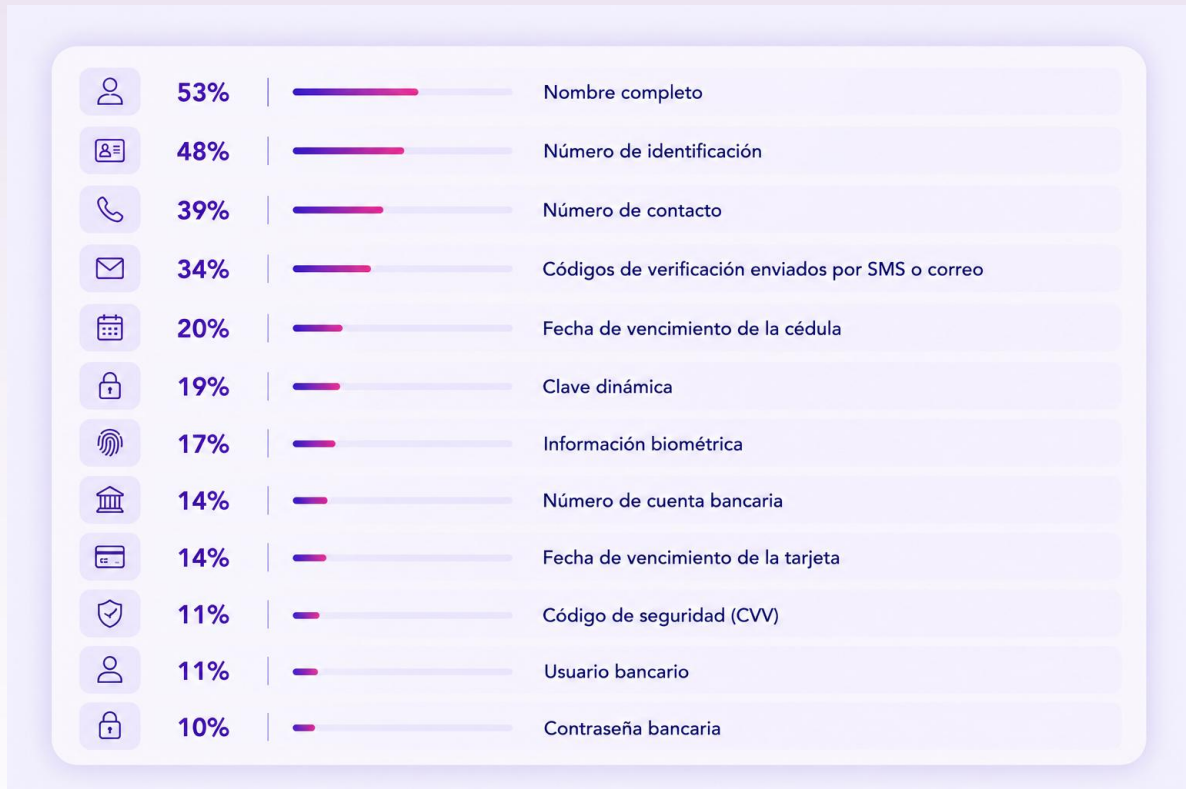
P10B. ¿Qué tan dispuesto estaría a compartir más información personal y biométrica si eso reduce el riesgo de fraude?

En línea con esa desconfianza, el **65%** afirma que **no está dispuesto a entregar sus datos personales o que solo compartiría información básica**.

Sin embargo, cuando compartir más información implica reducir el riesgo de fraude, la disposición aumenta: el **50%** estaría **dispuesto a entregar más datos**, aunque la mayoría lo haría con cautela.



La disposición a compartir información también está relacionada con las dudas sobre qué datos se pueden solicitar



Las respuestas muestran que todavía existe confusión sobre el manejo de información y que datos se pueden solicitar a la hora de hacer un trámite digital.

El **34%** considera válido compartir códigos de verificación, el **19%** una clave dinámica y **1 de cada 10** incluso cree que podría solicitarse una contraseña bancaria.



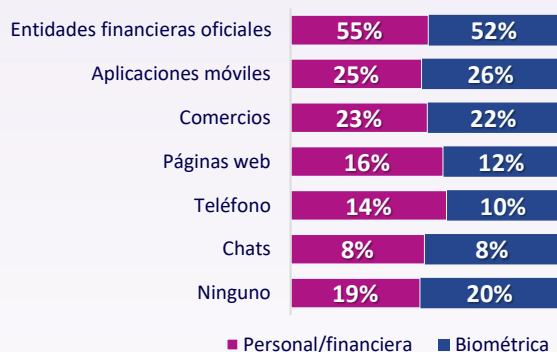
La información como base de la confianza digital



Más de la mitad de los colombianos compartiría información personal, financiera o biométrica con una entidad financiera oficial

Las entidades financieras oficiales presentan los mayores niveles de aceptación para compartir información, tanto **personal o financiera (55%)** como **biométrica (52%)**.

Canales considerados aceptables para compartir información personal y biométrica



En ambos casos, aceptación disminuye considerablemente en **aplicaciones móviles (25%-26%)**, **páginas web (16%-12%)** y **chats (8%)**.

Además, cerca de 1 de cada 5 personas afirma que **no compartiría información personal, financiera o biométrica en ninguno de estos canales (19%-20%)**.

P11B: ¿En cuáles de los siguientes canales consideraría aceptable compartir información personal o financiera?

P11B1: ¿En cuáles de los siguientes canales consideraría aceptable compartir información biométrica como huellas digitales o biometría facial?

Frente a estas reservas para compartir información, las personas adoptan distintas medidas para protegerse del fraude digital, principalmente evitando interacciones que consideran riesgosas:



57%
no contesta llamadas de números desconocidos

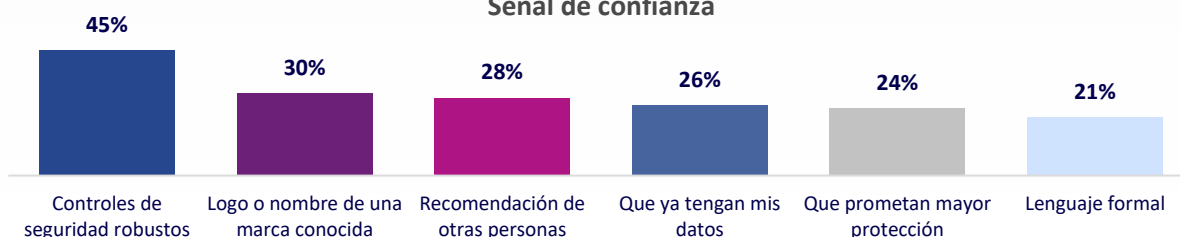


55%
evita hacer clic en enlaces



51%
utiliza únicamente aplicaciones o plataformas conocidas

Señal de confianza



A su vez, la confianza se construye principalmente a partir de señales concretas de seguridad. El 45% afirma que contar con controles de seguridad robustos es el principal elemento que le genera confianza, por encima del reconocimiento de una marca (30%) o la recomendación de otras personas (28%).



Casi 7 de cada 10 personas no han recibido capacitación o información sobre cómo evitar el fraude



P13A: ¿En qué escenarios crees que podrías ser vulnerable al fraude?

Aunque la falta de educación digital es percibida como uno de los factores que aumenta la vulnerabilidad frente al fraude, la mayoría no ha recibido orientación para prevenirlo. El 67% afirma no haber recibido capacitación o información sobre cómo evitar el fraude, frente a solo un 33% que sí ha tenido acceso a este tipo de contenidos.

En un contexto de baja capacitación para prevenir el fraude, la percepción de vulnerabilidad se concentra principalmente en la suplantación de identidad (63%)



P13B: ¿En cuáles de estos casos ha experimentado o conoce fraude?

Las experiencias de fraude reportadas por los consumidores se concentran en actividades y servicios financieros ampliamente utilizados. Las transferencias entre cuentas lideran los casos mencionados (43%), seguidas por las compras en marketplaces (33%) y los pagos con tarjeta (32%). **Esto muestra que las situaciones de fraude suelen estar asociadas a experiencias con las que los usuarios ya están familiarizados y que hacen parte de la gestión habitual de sus recursos.**

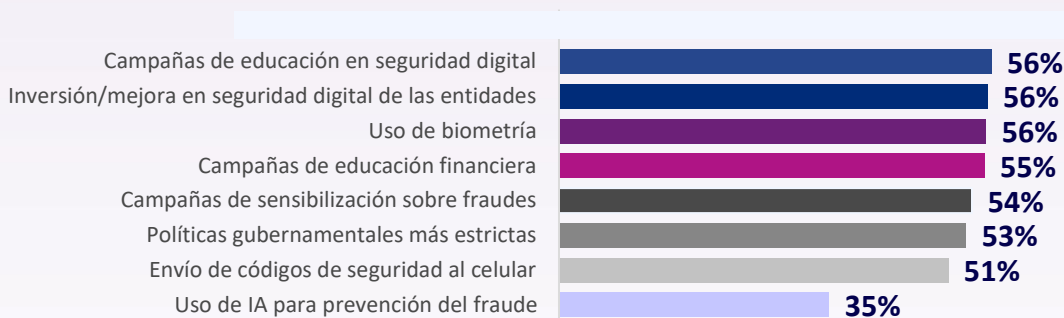
Además, aparecen escenarios vinculados a formas de interacción que **han ganado relevancia en los últimos años, como los pagos a entidades mediante referencias o códigos QR (28%), la interacción con agentes de IA o bots empresariales (22%) y el uso de billeteras digitales (21%).** Estos resultados reflejan cómo las modalidades de fraude evolucionan al mismo ritmo que los servicios y herramientas que las personas incorporan a su vida financiera.



Prevenir el fraude requiere una combinación de educación, tecnología y control

Los colombianos consideran que la prevención del fraude requiere una combinación de educación, herramientas de protección y acciones preventivas. **Las campañas de educación en seguridad digital (56%), la inversión en seguridad digital por parte de las entidades (56%), el uso de biometría (56%) y las campañas de educación financiera (55%) encabezan las medidas consideradas más efectivas para reducir el fraude. En contraste, el uso de inteligencia artificial registra una menor percepción de efectividad como herramienta de prevención, con un 35%.**

Acciones consideradas efectivas para prevenir el fraude

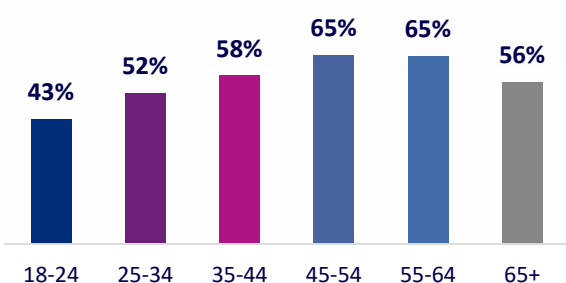


P14. En su opinión, ¿qué tan efectivas son las siguientes acciones para prevenir el fraude?
Top 2 Box: respuestas 4 + 5 en una escala de 1 "Nada efectiva" a 5 "Muy efectiva"

El 56% acudiría a una entidad financiera ante una posible situación de fraude

Al momento de actuar frente a una posible situación de fraude, las entidades financieras se posicionan como el principal punto de apoyo: el 56% acudiría a ellas, muy por encima de amigos o familiares (19%), Google (5%) y redes sociales (3%).

Preferencia por acudir a una entidad financiera, por grupo etario



P15: ¿A quién acude cuándo cree que puede estar en peligro de ser víctima de fraude?

La familiaridad con la tecnología no necesariamente se traduce en una mayor preparación frente al fraude. Aunque los jóvenes de 18 a 24 años han crecido en entornos digitales, son el grupo con menor intención de acudir a una entidad financiera ante una posible situación de fraude (43%). Además, el 22% no tendría un punto de apoyo claro: el 17% no sabría a quién acudir y el 5% no acudiría a nadie, proporciones superiores a las observadas en los demás grupos de edad.



Los colombianos reconocen el fraude, pero no siempre saben cómo reportarlo

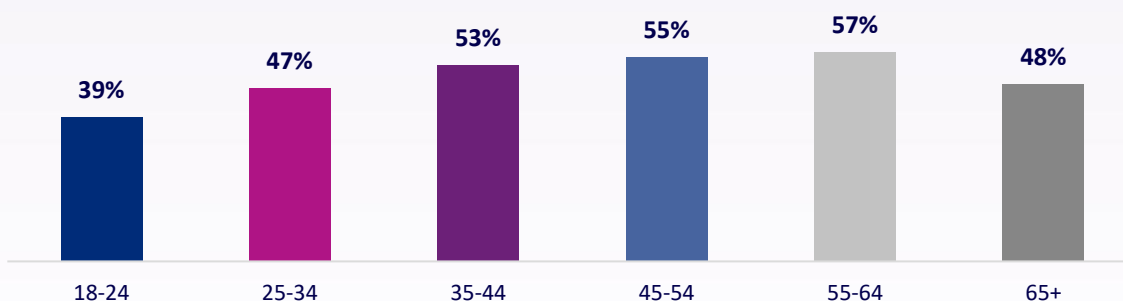


Aunque los colombianos identifican distintas formas de prevenir el fraude, aún persisten dudas sobre cómo actuar cuando este ocurre.

El bajo conocimiento sobre las sanciones también se refleja en la capacidad de actuar frente al fraude: el 50% afirma no saber cómo reportarlo, mientras que el otro 50% sí conoce el proceso.

La capacidad para reportar un fraude aumenta con la edad: mientras solo el 39% de los jóvenes entre 18 y 24 años sabe cómo hacerlo, la proporción aumenta progresivamente hasta alcanzar el **57% entre las personas de 55 a 64 años**. Entre los mayores de 65 años vuelve a ubicarse por debajo de la mitad (48%).

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



P17. ¿Sabe cómo reportar un fraude en su país?

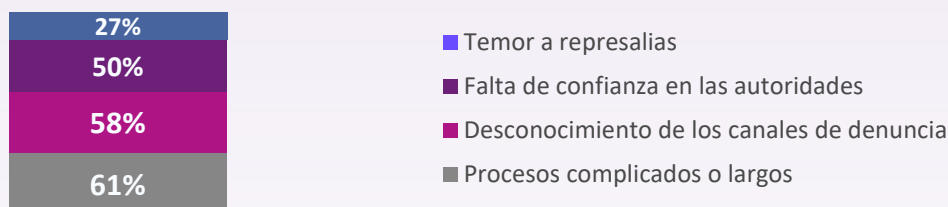
Además, la denuncia sigue siendo limitada: solo el **36%** afirma haber denunciado alguna vez un fraude experimentado o presenciado, mientras que el **64% nunca lo ha hecho**.

Los datos evidencian una oportunidad para fortalecer el conocimiento sobre los canales y mecanismos de respuesta frente al fraude. Reconocer el riesgo es importante, pero también lo es saber qué hacer y a quién acudir cuando ocurre una situación de este tipo.

Los procesos largos son el principal desafío para denunciar un fraude

Los procesos complejos o largos son el aspecto más mencionado por los colombianos al momento de hablar sobre la denuncia de fraudes (61%). A esto se suman el desconocimiento de los canales de denuncia (58%) y la falta de confianza en las autoridades (50%), elementos que pueden influir en la decisión de reportar estos casos.

Principales obstáculos percibidos para denunciar un fraude



P19. ¿Cuáles cree que son los mayores obstáculos para denunciar un fraude?

Denunciar suele ser solo el primer paso. Entre quienes reportaron un fraude, el 86% realizó alguna acción adicional para intentar resolver la situación, mientras que el 14% no llevó a cabo ninguna gestión posterior.

Sin embargo, obtener una solución satisfactoria no siempre es sencillo. El 35% logró resolver el problema y recuperar su dinero, mientras que el 25% no obtuvo una solución, el 15% recibió una devolución parcial y el 13% aún tenía el proceso abierto. Esta percepción también se refleja en la experiencia de resolución: el 61% calificó el proceso como difícil o muy difícil, frente al 39% que lo consideró fácil o muy fácil.

La experiencia posterior a la denuncia podría influir en la disposición de las personas a reportar futuros casos. La dificultad percibida del proceso y los resultados parciales o inconclusos sugieren oportunidades para fortalecer los mecanismos de atención y acompañamiento a las víctimas.



P21. ¿Qué pasó después?



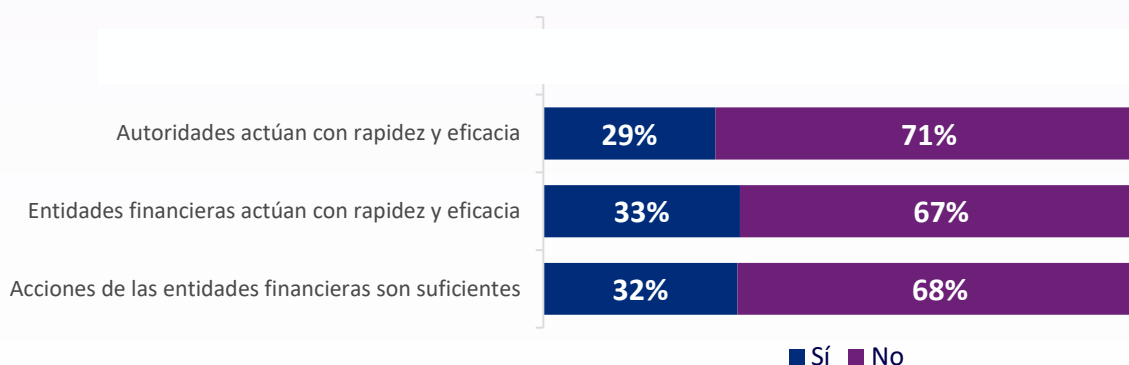
Entre el 67% y el 74% considera que las medidas actuales frente al fraude podrían fortalecerse

La evaluación de las medidas actuales frente al fraude muestra oportunidades de mejora.

Los resultados muestran que una proporción importante de los colombianos considera que todavía existen oportunidades para fortalecer las acciones frente al fraude. El 68% cree que las medidas implementadas por las entidades financieras podrían reforzarse para prevenir estos casos, mientras que el 67% considera que hay espacio para mejorar la rapidez y eficacia de la respuesta de estas organizaciones cuando ocurre un incidente.

La percepción es similar frente a las autoridades. El 71% considera que aún pueden fortalecer su actuación frente al fraude, lo que sugiere que los consumidores no solo esperan mecanismos más efectivos de prevención, sino también respuestas más ágiles y visibles cuando se presentan este tipo de situaciones. **En conjunto, los resultados reflejan una expectativa compartida de continuar fortaleciendo la capacidad de prevención, atención y respuesta frente a un entorno de fraude en constante evolución.**

Percepción sobre la repuesta institucional frente al fraude



P23. ¿Considera que las acciones de las entidades financieras actuales son suficientes para prevenir el fraude?

P24. ¿Cree que las entidades financieras actúan con rapidez y eficacia en casos de fraude?

P25. ¿Cree que las autoridades actúan con rapidez y eficacia en casos de fraude?



La inteligencia artificial redefine la relación entre fraude, prevención y confianza



La IA fortalece la prevención, pero también aumenta la sofisticación del fraude

Después de entender cómo evoluciona el fraude y cómo influye en la confianza que las personas depositan en los entornos digitales, surge una pregunta inevitable: ¿qué papel jugará la inteligencia artificial en esta evolución?

La inteligencia artificial se está consolidando como una herramienta de doble vía frente al fraude. Mientras ofrece nuevas capacidades para detectar riesgos, fortalecer la seguridad y apoyar los mecanismos de prevención, también está contribuyendo a la evolución de modalidades cada vez más sofisticadas y difíciles de identificar.

Esta realidad se refleja en la percepción de las personas. El 88% manifiesta algún nivel de preocupación frente al uso de IA para facilitar fraudes o engaños digitales, mientras que el 55% se siente poco o nada seguro identificando contenidos creados o alterados mediante esta tecnología. A su vez, la confianza en su capacidad para detectar fraudes o suplantaciones aún se encuentra en construcción: solo el 9% manifiesta mucha confianza en este tipo de herramientas.

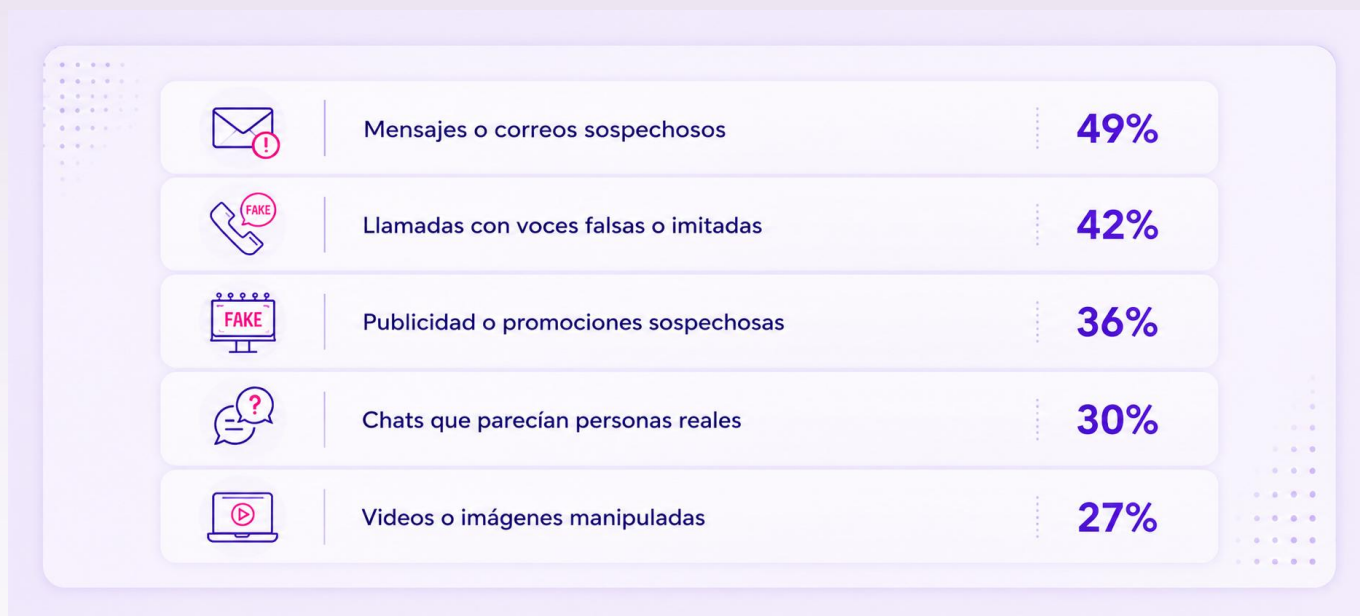
Sin embargo, los resultados muestran que la relación con la inteligencia artificial no está marcada únicamente por la cautela. El 53% estaría dispuesto a permitir el análisis de su información para detectar posibles fraudes y el 86% manifiesta interés en aprender a identificar amenazas creadas con IA.

Más que una percepción de rechazo, los hallazgos reflejan una combinación de cautela, interés y adaptación. Mientras crece la preocupación por su uso para sofisticar el fraude, también aumenta el reconocimiento de su potencial para fortalecer la prevención y la seguridad digital.

Percepciones sobre la IA en la detección de fraude				
	 Nada	 Poco	 Algo	 Mucho
 Preocupación por IA como facilitadora de fraude	4%	8%	30%	58%
 Seguridad percibida para identificar fraude creado/alterado con IA	21%	34%	32%	13%
 Confianza en que la IA detecte fraudes o suplantación	18%	35%	38%	9%
 Disposición a permitir análisis con IA para detectar fraudes	17%	30%	41%	12%
 Interés en aprender a identificar fraudes creados con IA	4%	10%	32%	54%

La IA es percibida simultáneamente como una herramienta de protección y un factor que puede aumentar la sofisticación del fraude. El desafío no parece estar únicamente en el desarrollo de nuevas capacidades tecnológicas, sino en construir la confianza y el conocimiento necesarios para aprovechar sus beneficios sin incrementar la exposición a nuevos riesgos.

La confianza digital depende cada vez más de la capacidad para verificar la autenticidad



A medida que la inteligencia artificial gana presencia en las interacciones digitales, también crece la necesidad de verificar la autenticidad de mensajes, llamadas y contenidos. Los resultados muestran que las principales dudas se concentran en canales de uso cotidiano: el 49% afirma haber recibido mensajes o correos sospechosos durante **los últimos 12 meses, mientras que el 42% reporta llamadas con voces falsas o imitadas. También aparecen la publicidad demasiado personalizada o sospechosa (36%), los chats que parecían personas reales (30%) y los videos o imágenes manipuladas (27%).**

Más allá de la tecnología utilizada, estos resultados reflejan una realidad cada vez más presente en los entornos digitales: distinguir entre una interacción auténtica y una potencialmente fraudulenta se ha convertido en un desafío para muchos consumidores. De hecho, solo el 11% afirma no haber experimentado ninguna de estas situaciones o no estar seguro de haberlo hecho.

Estos hallazgos sugieren que la conversación sobre confianza digital ya no depende únicamente de proteger la información o prevenir el fraude. También implica fortalecer la capacidad de validar la autenticidad de las interacciones que ocurren diariamente en canales digitales, un desafío que cobrará aún más relevancia a medida que la inteligencia artificial asuma un papel más activo en la comunicación, los servicios financieros y la toma de decisiones.

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 colombianos**
El 71% recibió al menos un intento de fraude durante el último año y el 70% conoce a alguien que fue víctima. Además, el 95% considera que los fraudes ocurren con frecuencia y el 81% percibe que los intentos aumentaron frente al año anterior.
- 2 La exposición se traduce con frecuencia en pérdidas económicas**
Entre quienes recibieron intentos de fraude, el 46% terminó siendo víctima de al menos uno. El impacto económico es predominante: el 78% de las víctimas perdió dinero, principalmente por montos entre USD 50 y USD 200 (35%), confirmando que la materialización del fraude tiene consecuencias financieras concretas.
- 3 Los canales digitales cotidianos concentran buena parte del riesgo**
Mensajes o chats (27%), compras de productos o servicios no entregados (25%) y páginas web (22%) lideran las modalidades reportadas. La suplantación juega un papel central: páginas o aplicaciones que parecían legítimas (25%), llamadas que simulaban provenir de entidades conocidas (20%) y enlaces aparentemente auténticos (17%) fueron las principales estrategias utilizadas.
- 4 La prevención convive con brechas importantes de conocimiento**
Aunque el 60% se siente algo o muy seguro realizando transacciones digitales, casi 7 de cada 10 personas (67%) no han recibido capacitación o información para evitar el fraude. Las brechas también alcanzan el manejo de datos: el 34% considera válido compartir códigos de verificación y el 10% cree que una empresa legítima podría solicitar una contraseña bancaria.
- 5 Denunciar y resolver un fraude continúa siendo un proceso complejo**
Solo el 36% ha denunciado alguna vez un fraude experimentado o presenciado y el 50% no sabe cómo reportarlo. Los procesos complicados o largos (61%) y el desconocimiento de los canales (58%) son las principales barreras; además, entre quienes intentaron resolver un fraude, solo el 35% recuperó su dinero.
- 6 La IA genera alta preocupación, pero también interés por aprender a enfrentar sus riesgos**
El 88% está algo o muy preocupado por el uso de IA para facilitar fraudes, mientras que el 55% se siente poco o nada seguro identificando contenidos creados o alterados con esta tecnología. Sin embargo, el 86% muestra interés en aprender a reconocer fraudes creados con IA, señalando una oportunidad clara para fortalecer la educación y prevención digital.

