Brújula 2026: Radiografía del bienestar financiero y digital en México

Entrega de resultados.

Marzo 2026.

TALA

CONDUSEF

De la inclusión financiera a la seguridad patrimonial

Nuestra responsabilidad con la **"Mayoría Global"** en el ecosistema digital

- **Nuestra misión:** Proteger el acceso de los usuarios a la economía digital, garantizando que su información sea su activo más seguro y no su mayor vulnerabilidad.
- **El valor de la confianza:** La protección de datos es el pilar de nuestra relación con el cliente; sin seguridad y confianza, no hay lealtad a largo plazo.
- **Evolución del riesgo:** El foco ya no es solo "dar crédito", sino entender los hábitos de protección del usuario para prevenir la ingeniería social y la suplantación antes de que ocurran.
- **Estándar institucional:** Alinear nuestras prácticas de recolección de datos con la visión educativa de CONDUSEF para crear un entorno financiero libre de miedos.

Confianza, Privacidad y Empoderamiento.

Objetivos estratégicos

Detección:

Identificar la brecha entre la percepción de control del usuario y su comportamiento real.

Medición:

Cuantificar la vulnerabilidad ante técnicas de ingeniería social (Phishing, Vishing, Smishing).

Acción:

Generar insights para el desarrollo de productos financieros más seguros y campañas de educación dirigidas.

Lo que esperábamos encontrar

A pesar de una mayor adopción tecnológica, existe una **falsa sensación de seguridad** que deja al usuario vulnerable ante estafas sofisticadas

- Los usuarios confían más en redes sociales (Facebook) de lo que deberían.
- La falta de denuncia oculta el tamaño real del problema (El silencio del fraude).

Alcance y rigor metodológico

Muestra:

3,028 encuestados (Usuarios de Tala).

Cobertura:

32 entidades federativas (Nacional).

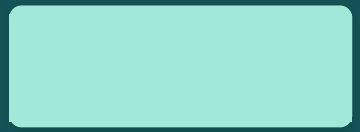
Levantamiento:

29 de diciembre 2025 al 14 de enero 2026.

Rigor:

Datos analizados bajo el marco de protección de datos de Tala y estándares de CONDUSEF.

Hallazgos de alto nivel

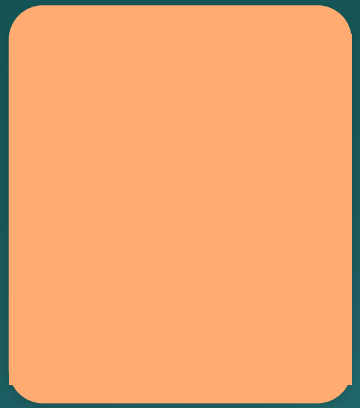


46.8%

Enfrentó emergencias sin preparación en 2025.

63.5%

Identifica los gastos inesperados como el mayor freno al ahorro.



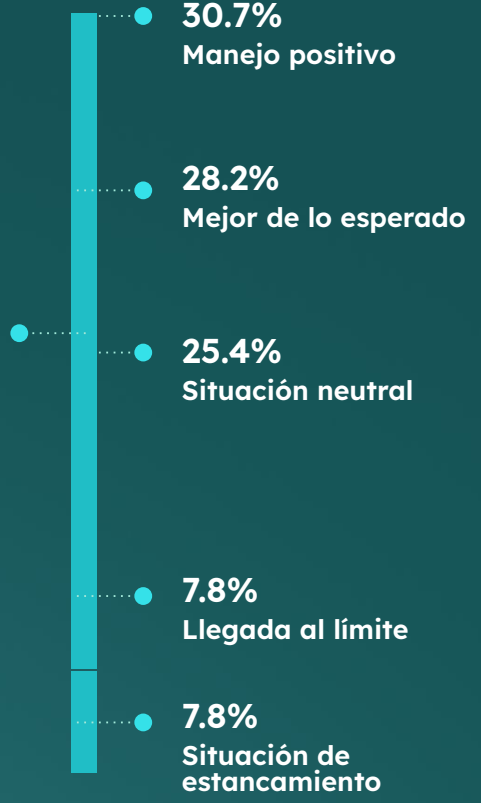
91%

De las víctimas de fraude no denuncian ante autoridades.

Diagnóstico del manejo financiero 2025

Percepción financiera durante 2025 de los usuarios

Brecha crítica entre la percepción de control (58.9%) y la resiliencia real ante contingencias económicas.



Pregunta 1. Si tuvieras que describir tu 2025, financieramente hablando, ¿cómo lo describirías?

Obstáculos para la estabilidad económica

Desafíos financieros por usuario

Pregunta 2. Y ahora, siendo honestos, ¿cuál fue tu principal desafío financiero?

Fugas de capital no planificadas

Gastos hormiga por usuario

- **La digitalización del consumo ha normalizado fugas constantes en categorías de servicios de conveniencia y entretenimiento.**

39.7%
Comida y antojos

23.9%
Intereses y deudas

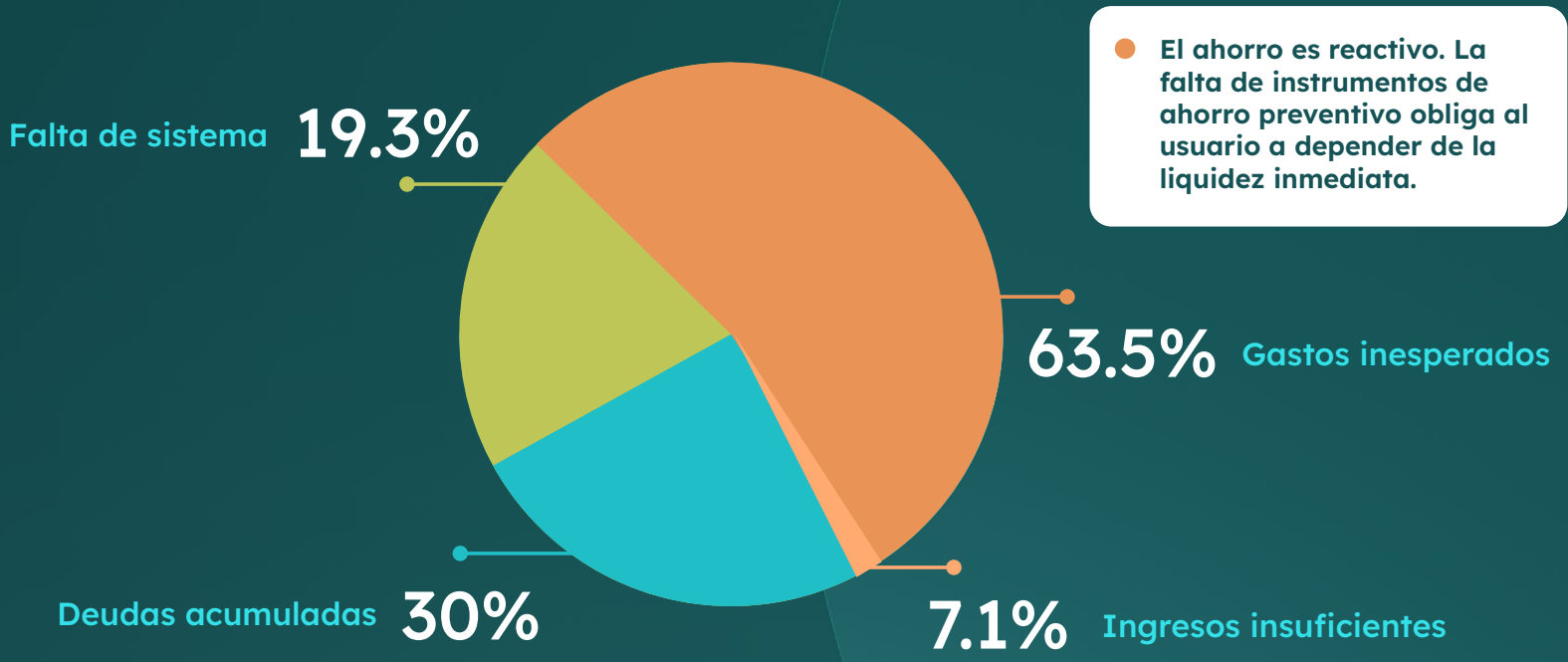
19.7%
Café y refrescos

16.7%
Suscripciones digitales

Pregunta 3. Hablemos de esos pequeños gastos que suman mucho. ¿En qué se te fue el dinero sin que te dieras cuenta?

Causas de la falta de previsión

Limitantes del ahorro

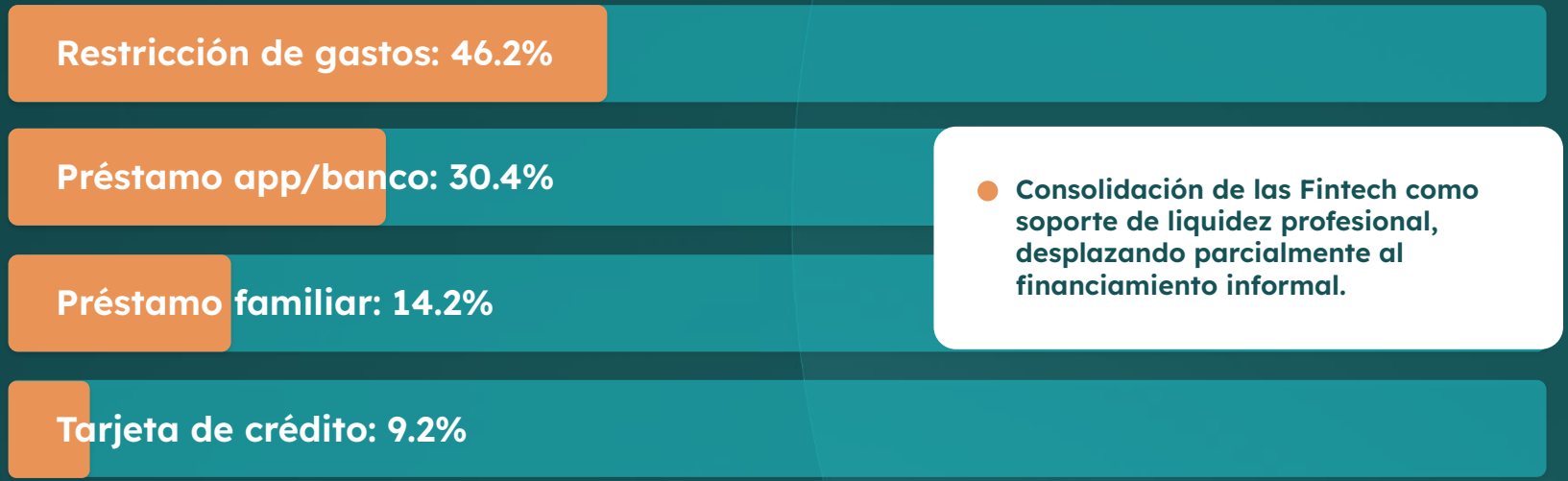


El ahorro es reactivo. La falta de instrumentos de ahorro preventivo obliga al usuario a depender de la liquidez inmediata.

Pregunta: 4. Independientemente de si lo lograste o no, ¿cuál fue tu mayor obstáculo para ahorrar este año?

Métodos para afrontar el fin de mes

Estrategias ante falta de liquidez



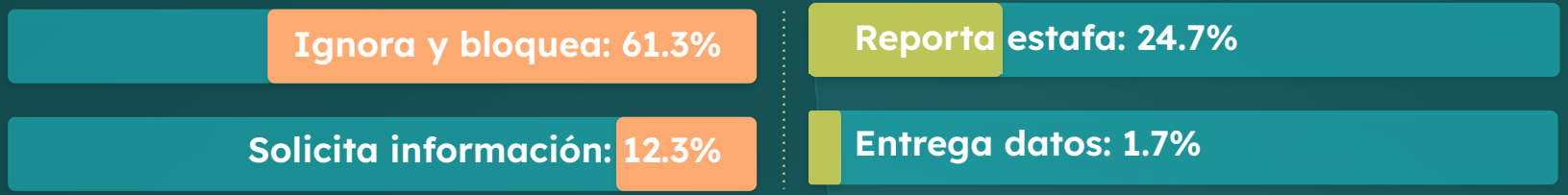
- Consolidación de las Fintech como soporte de liquidez profesional, desplazando parcialmente al financiamiento informal.

Pregunta: 5. Las veces que notaste que no llegabas a fin de mes, ¿qué hacías?

Reacción ante ofertas de crédito en apps de mensajería

Respuesta ante Phishing (WhatsApp)

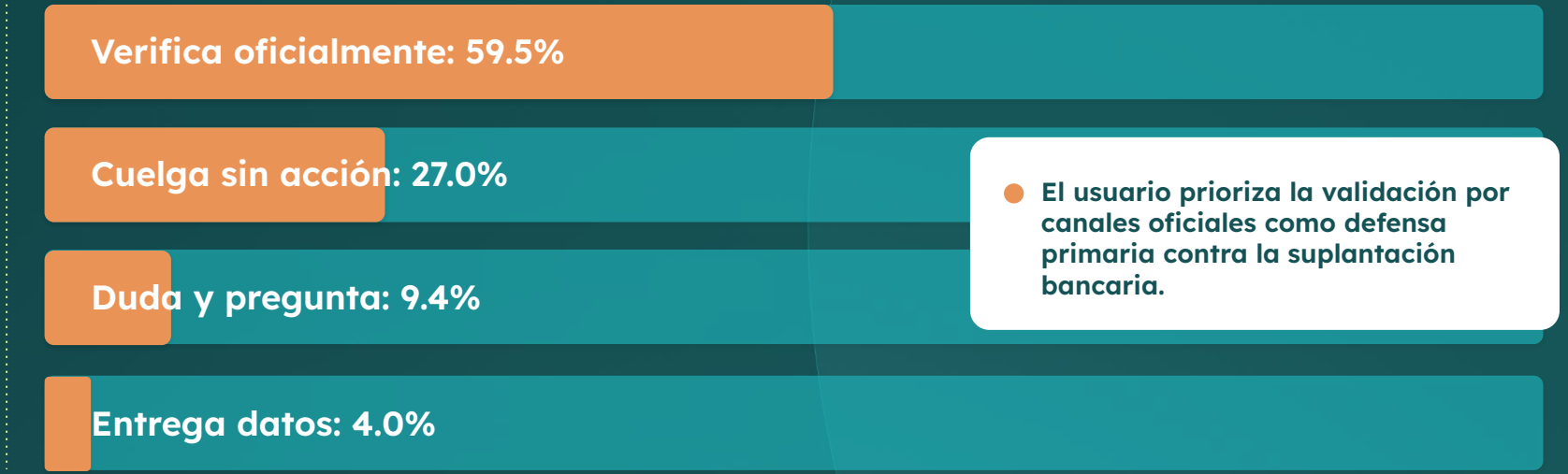
- Alta reactividad defensiva; sin embargo, existe un 14% de exposición crítica ante ingeniería social en canales directos.



Pregunta 6. De la nada, te llega un mensaje a tu WhatsApp de un número que no conoces. Te dicen que tienes un préstamo aprobado y que para que te depositen, solo tienes que mandarles ahí mismo tu nombre y tu cuenta CLABE. ¿Tú qué harías?

Verificación ante alertas bancarias telefónicas

Protocolo ante Vishing (Llamadas)



Pregunta 7: Imagina que te entra una llamada y ves que dice el nombre de tu banco en la pantalla. Contestas, y una persona te dice que hay un "cargo sospechoso" en tu tarjeta y que, para cancelarlo, necesita que le confirmes el código de seguridad de 3 números que viene atrás de tu tarjeta (el CVV). ¿Tú qué harías?

Validación de enlaces de paquetería falsa

Prevención de Smishing (SMS)

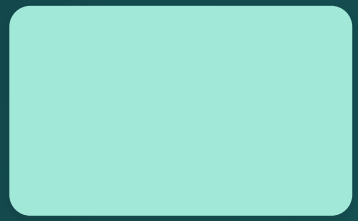
- **Creciente madurez digital en la identificación de enlaces sospechosos y preferencia por la navegación segura.**

Pregunta 8. Estás esperando un paquete. Te llega un mensaje de texto (SMS) que dice: "Tu paquete no se pudo entregar por un error en la dirección. Actualiza tus datos aquí". ¿Tú qué haces?

Manejo de datos en empaques de mensajería

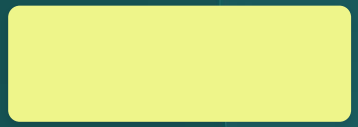
Protección de información física

El rastro físico de datos sigue siendo un vector de vulnerabilidad; el 45% de los usuarios deja expuesta información sensible.



54.9%

Elimina etiquetas



34.7%

Recicla empaque

10.4%

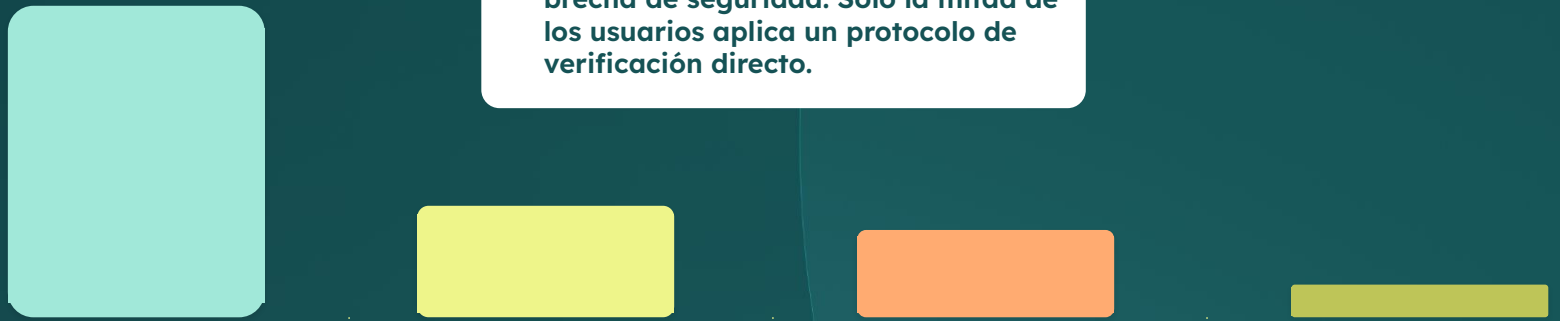
Desecho directo

Pregunta 9. Hablando de paquetería ¿Qué haces con las cajas que recibes de mensajería?

Verificación de identidad entre conocidos.

ingeniería social por suplantación

La confianza interpersonal es la mayor brecha de seguridad. Solo la mitad de los usuarios aplica un protocolo de verificación directo.



50.4%
Verifica por llamada

22.2%
Pregunta motivo

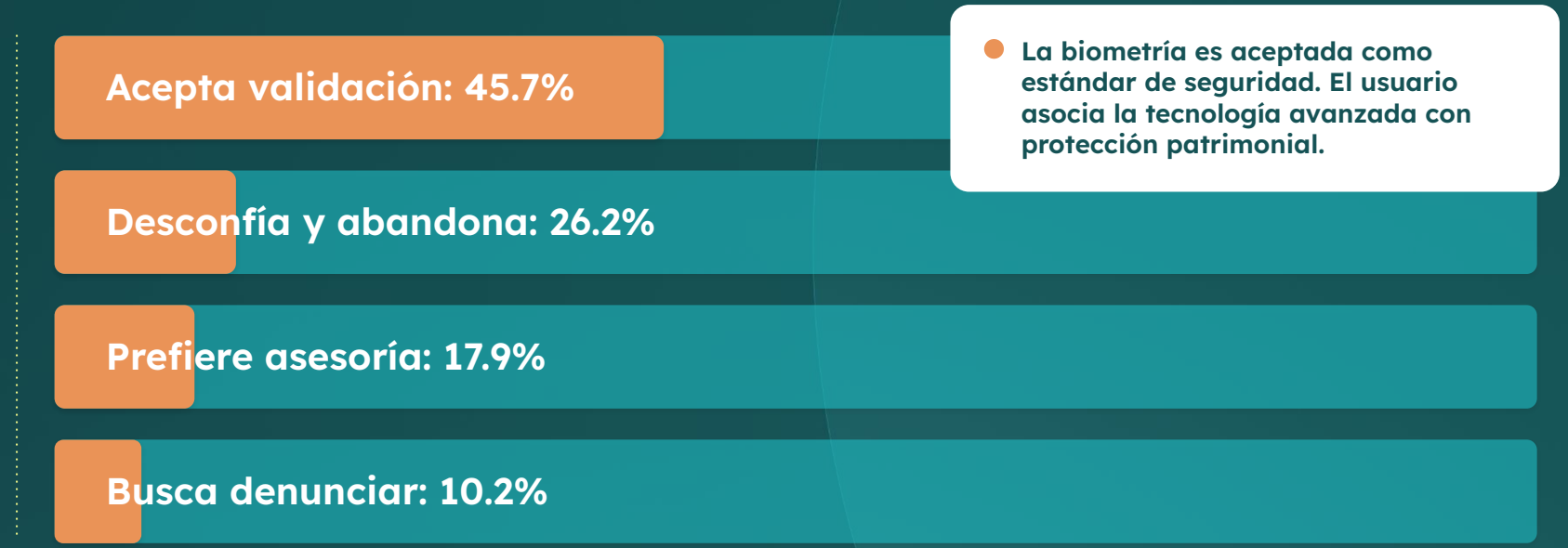
21.9%
No responde

5.6%
Entrega código

Pregunta 10. Un conocido te escribe por WhatsApp: "Oye, ¿me ayudas? Te mandé un código de 6 números a tu celular por error, ¿me lo puedes pasar en cuanto te llegue?". ¿Tú qué haces?

Percepción de los métodos de validación digital

Aceptación de biometría



- **La biometría es aceptada como estándar de seguridad. El usuario asocia la tecnología avanzada con protección patrimonial.**

Pregunta 11. Descargas una app financiera para abrir una cuenta de ahorro. Al crear tu perfil, la app te pide permiso para usar tu cámara, escanear tu INE por ambos lados y que te grabes una "video-selfie" moviendo la cabeza. ¿Tú qué haces?

Interacción con anuncios informales en redes.

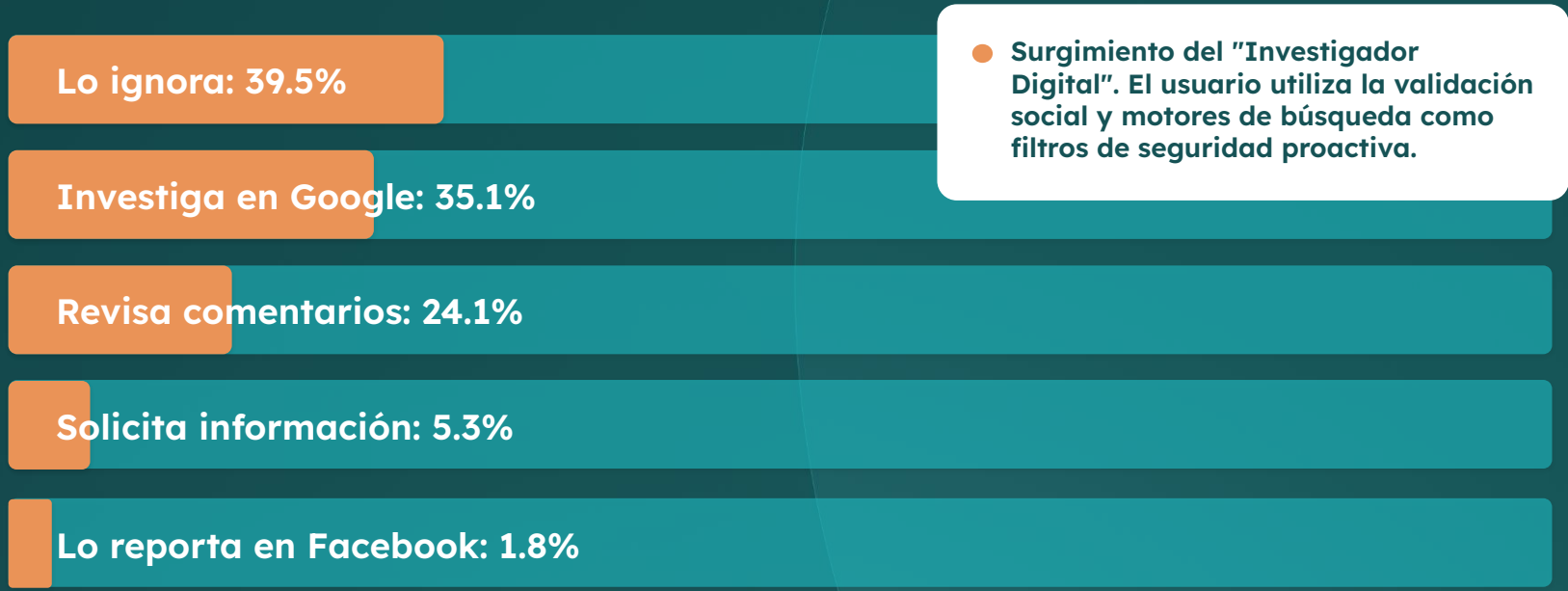
Ofertas de crédito en Facebook

- **Facebook es un ecosistema crítico de fraude. La urgencia económica sigue impulsando a un segmento hacia la informalidad riesgosa.**

Pregunta 12. Ves en un grupo de Facebook que alguien te ofrece tramitarte una tarjeta de crédito o un préstamo rápido y sin revisar Buró. Para iniciar el trámite, te pide que le mandes por WhatsApp foto de tu INE y dos referencias. ¿Tú qué haces?

Filtros de seguridad del usuario en redes sociales.

Comportamiento de usuarios ante anuncios de apps de préstamos en Facebook

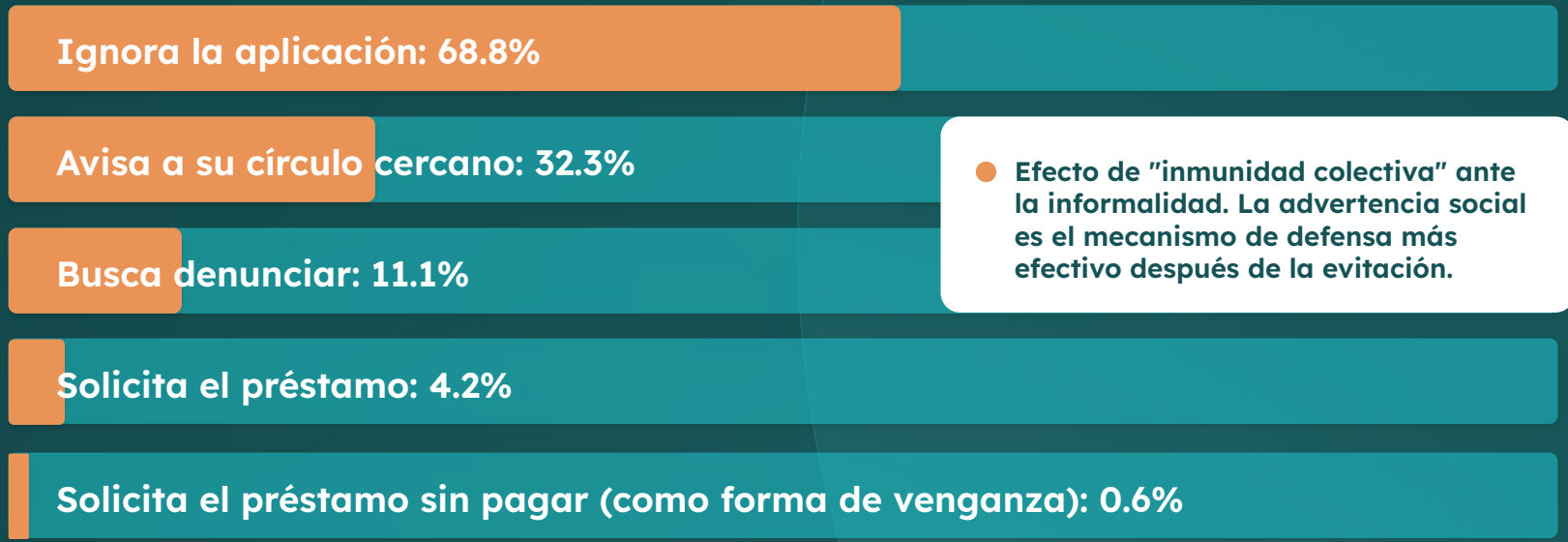


- **Surgimiento del "Investigador Digital". El usuario utiliza la validación social y motores de búsqueda como filtros de seguridad proactiva.**

Pregunta 13. Sobre aplicaciones de préstamos, imagina que en Facebook ves que una persona publica sobre una app que da préstamos rápidos y sin muchos requisitos. ¿Tú qué haces?

Prevención ante esquemas de cobranza agresiva.

Reacción de los usuarios ante la percepción de una aplicación “montadeudas”



Pregunta 14. Te enteras de que una app de préstamos es de las llamadas "montadeudas" (intereses altos, cobranza agresiva, amenazas). Sabiendo esto, ¿tú qué harías o has hecho?

Balance de salud y seguridad financiera 2026

Estabilidad financiera (Diagnóstico)

Persiste una brecha entre la percepción de control y la capacidad real de ahorro preventivo. El ecosistema financiero mexicano sigue siendo reactivo: las emergencias son el principal desestabilizador del patrimonio, consolidando a las Fintech como el soporte de liquidez prioritario frente a los mecanismos de financiamiento tradicionales.

Resiliencia digital (Vulnerabilidad)

El usuario muestra una madurez defensiva creciente contra el fraude directo (Phishing/Vishing). Sin embargo, la ingeniería social basada en la suplantación de identidad y el rastro de datos físicos (logística) permanecen como los vectores de riesgo críticos que requieren intervención educativa inmediata.

Nivel de madurez del usuario (Perfil)

Consolidación del "Investigador Digital". El usuario ha dejado de ser un receptor pasivo para convertirse en un verificador proactivo que utiliza el motor de búsqueda y la validación social como filtros de confianza. La transparencia institucional y la biometría son ahora estándares de seguridad esperados por el mercado.

Fuente: Brújula 2026: Estudio de comportamiento y protección de datos (Alianza Tala-CONDUSEF).

TALA

Tu Aliado en cada paso