Estudio impulsado por

MEGA CASINO

JUEGA SOBRE SEGURO

Radiografía del fraude digital entre usuarios de plataformas de juego online en España



Percepción, exposición y capacidad de respuesta ante nuevas formas de fraude digital.

EL **FRAUDE DIGITAL** SE PARECE CADA VEZ MÁS A LO REAL

Webs que imitan plataformas legítimas, mensajes que reproducen el lenguaje de las marcas, falsas promociones, perfiles suplantados o contenidos generados con inteligencia artificial están haciendo que distinguir lo auténtico de lo fraudulento sea cada vez más complejo.

Juega sobre seguro analiza hasta qué punto los usuarios se sienten preparados ante estos riesgos y qué ocurre cuando esa percepción se pone a prueba ante situaciones concretas.

NO SOLO QUÉ **CREEMOS QUE HARÍAMOS**. TAMBIÉN QUÉ **HACEMOS CUANDO TENEMOS QUE DECIDIR.**

El estudio analiza siete dimensiones del fraude digital:

- **Percepción**

¿Creemos que sabemos detectar una estafa?

- **Verificación**

¿Qué comprobamos antes de confiar?

- **Exposición**

¿Con qué frecuencia nos encontramos con contenidos sospechosos?

- **Victimización**

¿Qué ocurre cuando interactuamos con ellos?

- **Detección**

¿Sabemos distinguir una plataforma legal de una imitación?

- **Nuevos riesgos**

¿Qué papel tienen redes sociales, influencers e inteligencia artificial?

- **Reacción**

¿Sabemos qué hacer cuando sospechamos que hemos caído?

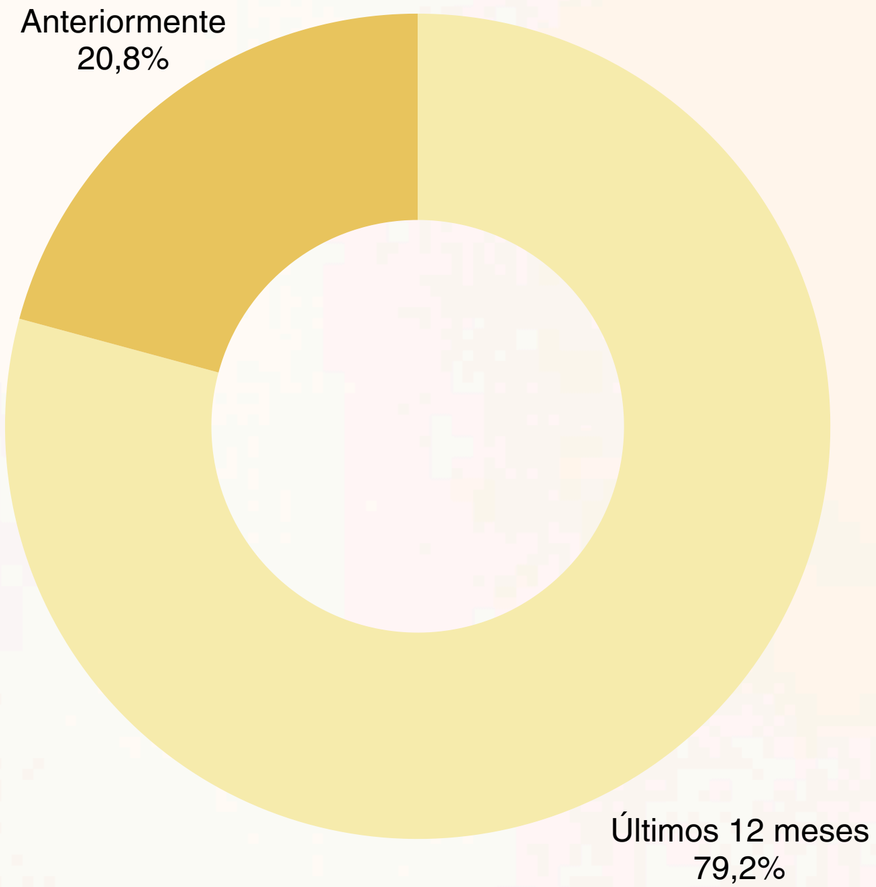
500 USUARIOS DE PLATAFORMAS DE **JUEGO ONLINE**

500 entrevistas online:

Personas **residentes en España de entre 18 y 55 años** que han utilizado alguna vez plataformas de juego o apuestas online.

Participación de **usuarios de las 17 comunidades autónomas**.

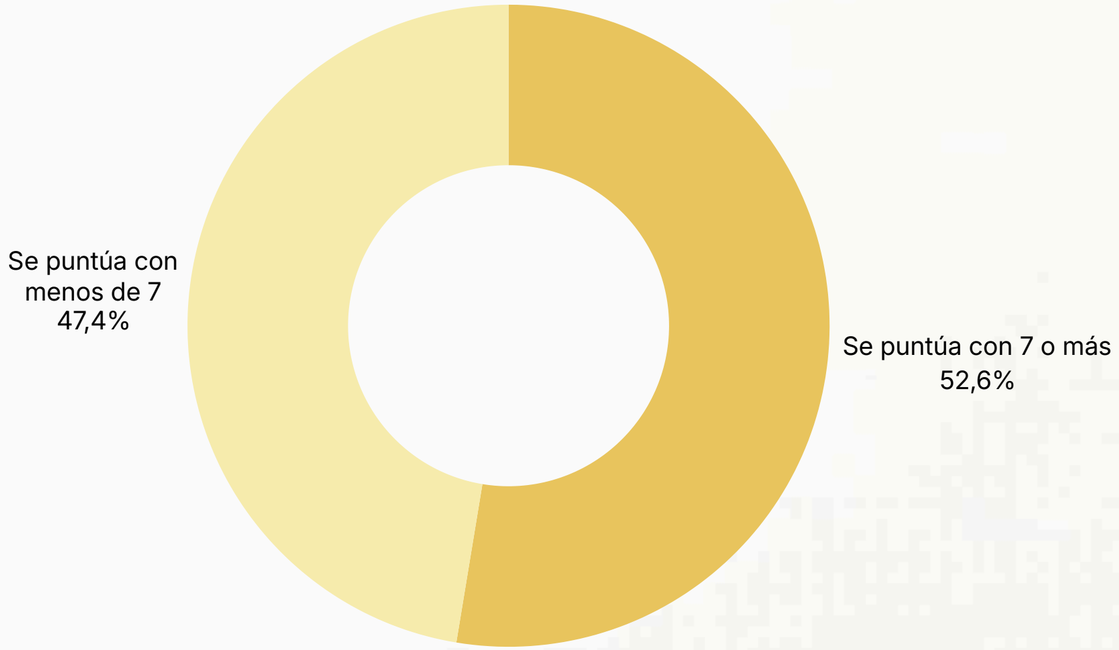
El cuestionario combina preguntas de percepción y comportamiento con pruebas prácticas mediante materiales ficticios.
Nota metodológica: los resultados describen la muestra analizada y no deben extrapolarse al conjunto de la población española como una muestra representativa nacional.



BLOQUE 1

CREEMOS QUE SABEMOS
DETECTAR EL FRAUDE

NOS SENTIMOS RELATIVAMENTE **PREPARADOS FRENTE AL FRAUDE**



6,4/10

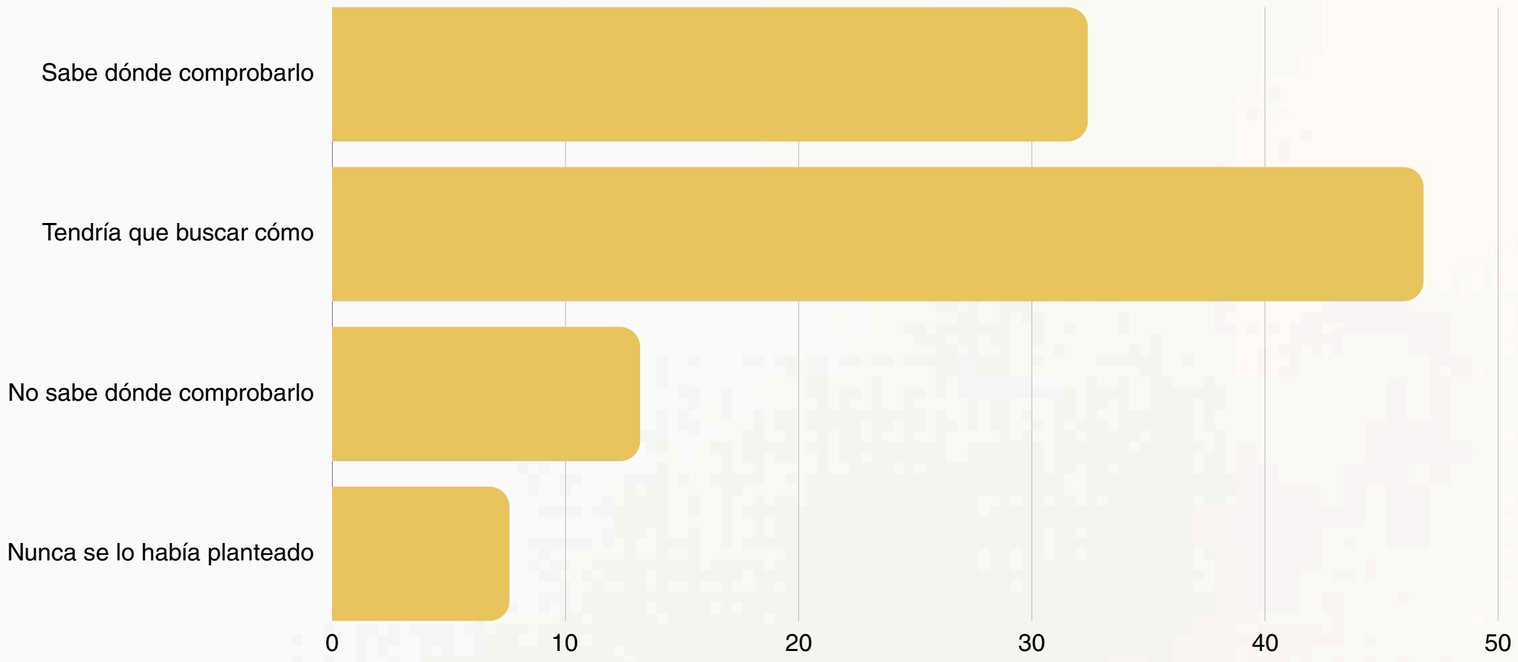
Nota media de capacidad para distinguir una plataforma legal de una ilegal o fraudulenta.

21%

Considera que su capacidad es de 9 o 10 sobre 10

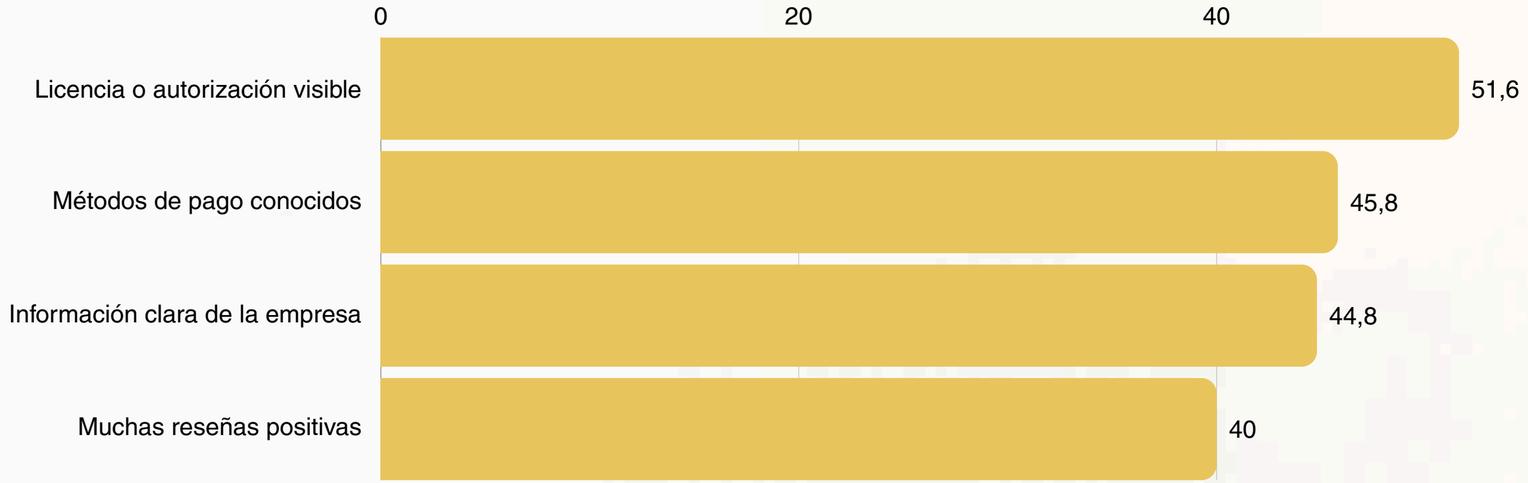
LA PERCEPCIÓN DE SEGURIDAD ES ALTA. LA PRUEBA PRÁCTICA CONTARÁ UNA HISTORIA DIFERENTE.

SOLO 1 DE CADA 3 SABE CÓMO COMPROBAR OFICIALMENTE **SI UNA PLATAFORMA ESTÁ AUTORIZADA**



SABER QUE HAY QUE VERIFICAR NO SIGNIFICA NECESARIAMENTE SABER CÓMO HACERLO.

UNA LICENCIA GENERA CONFIANZA. PERO TAMBIÉN LO HACEN **SEÑALES QUE PUEDEN SER IMITADAS.**



También **influyen** el posicionamiento en **Google, el diseño, los seguidores** o la **recomendación** de una **persona conocida**.

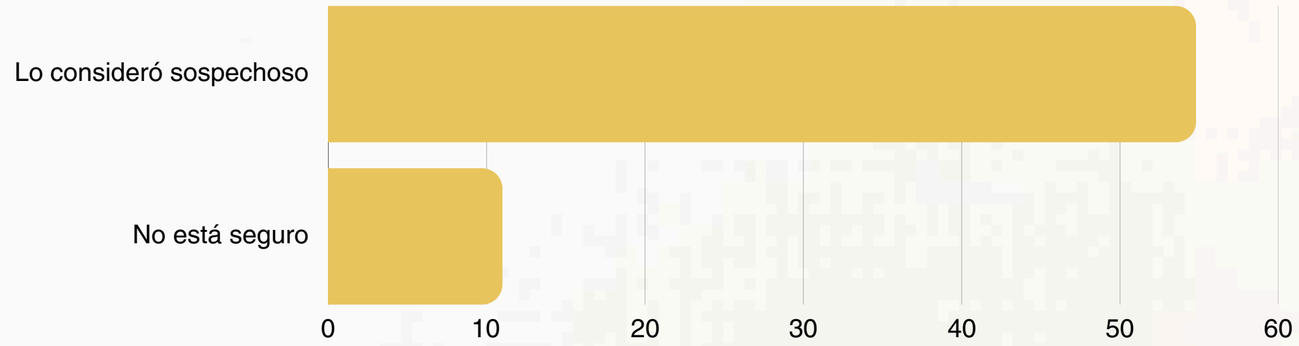
LA APARIENCIA Y LA FAMILIARIDAD CONTINÚAN FUNCIONANDO COMO ATAJOS DE CONFIANZA.

BLOQUE 2

EL FRAUDE YA FORMA
PARTE DE LA EXPERIENCIA
DIGITAL

MÁS DE LA MITAD HA VISTO CONTENIDO DE **JUEGO ONLINE** QUE **LE HA PARECIDO SOSPECHOSO**

Exposición a contenidos sospechosos de juego online
Durante los últimos 12 meses



EXPOSICIÓN POTENCIAL

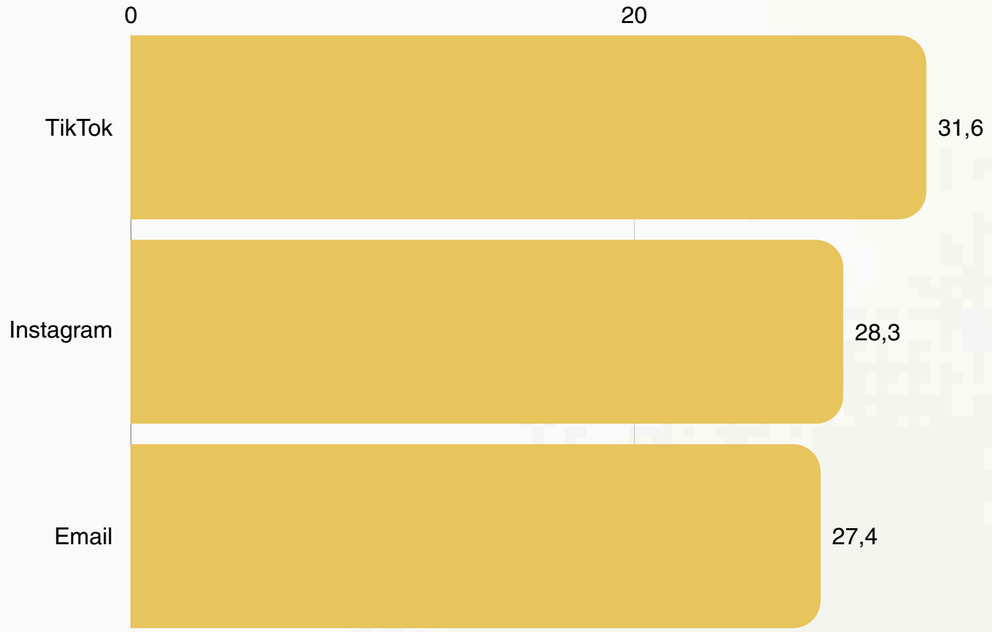
65,8%

Ha visto contenido sospechoso o no está seguro de si lo era.

SE HA ENCONTRADO POTENCIALMENTE ANTE CONTENIDOS SOSPECHOSOS.

TIKTOK E INSTAGRAM: PRINCIPALES CANALES DONDE APARECE EL CONTENIDO SOSPECHOSO

Entre quienes han visto contenido sospechoso o no están seguros.

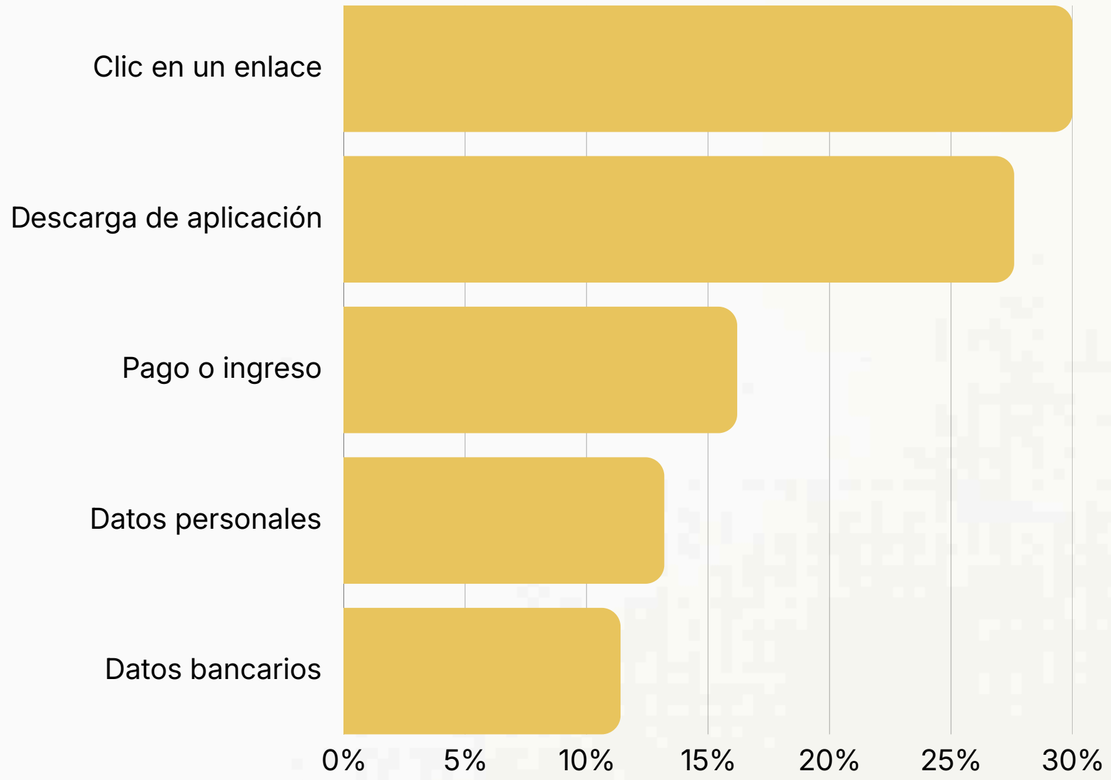


Otros canales:
YouTube, buscadores, páginas web, aplicaciones móviles, SMS, Telegram, Facebook, WhatsApp y X.

Base: 329 participantes. Respuesta múltiple.

EN EL FRAUDE RELACIONADO CON JUEGO ONLINE,
LAS REDES SOCIALES ADQUIEREN UN PESO ESPECIALMENTE RELEVANTE.

LA DUDA MUCHAS VECES APARECE DESPUÉS DEL CLIC



64,2%

Realizó al menos una acción

30,8%

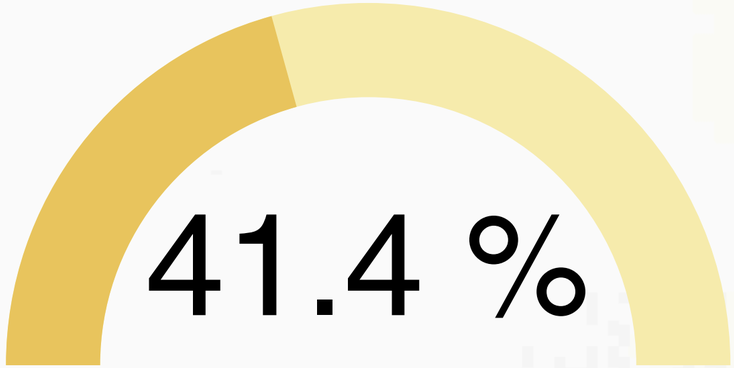
Facilitó datos o realizó un pago

LA PREVENCIÓN DEBE LLEGAR ANTES DE QUE APAREZCAN LAS DUDAS.

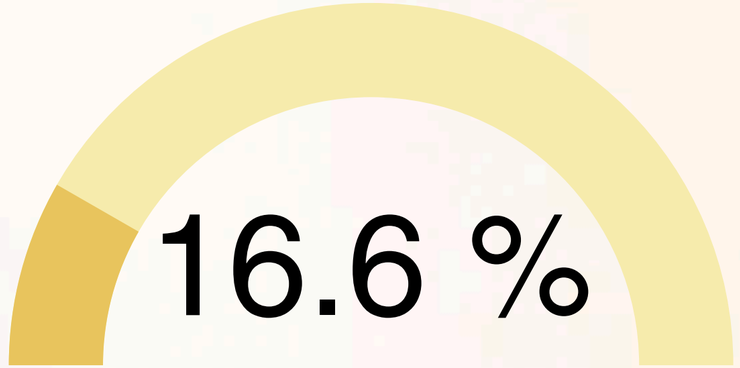
BLOQUE 3

QUANDO ALGO PARECE LEGÍTIMO

4 DE CADA 10 YA SE HAN ENCONTRADO CON ALGO QUE **PARECÍA LEGÍTIMO Y DESPUÉS DEJÓ DE SERLO**



Ha encontrado contenido que parecía legítimo y resultó fraudulento o sospechoso.

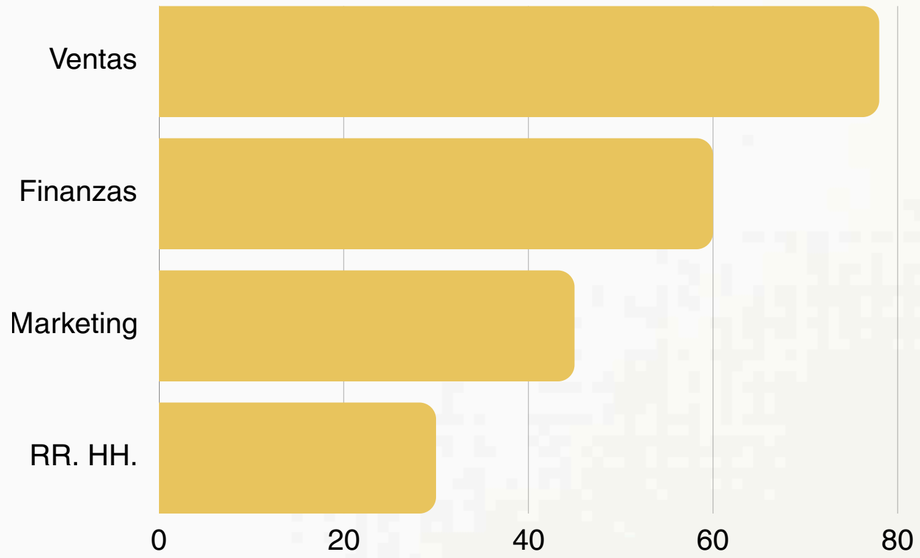


No está seguro de si le ha ocurrido.

EL FRAUDE NO SIEMPRE SE PRESENTA COMO FRAUDE.
SU CAPACIDAD PARA PARECER AUTÉNTICO ES PARTE DEL PROBLEMA.

PARA ALGUNOS USUARIOS, **LAS CONSECUENCIAS FUERON MÁS ALLÁ DEL SUSTO**

Consecuencias sufridas por los afectados
Base: 207 participantes afectados · Respuesta múltiple

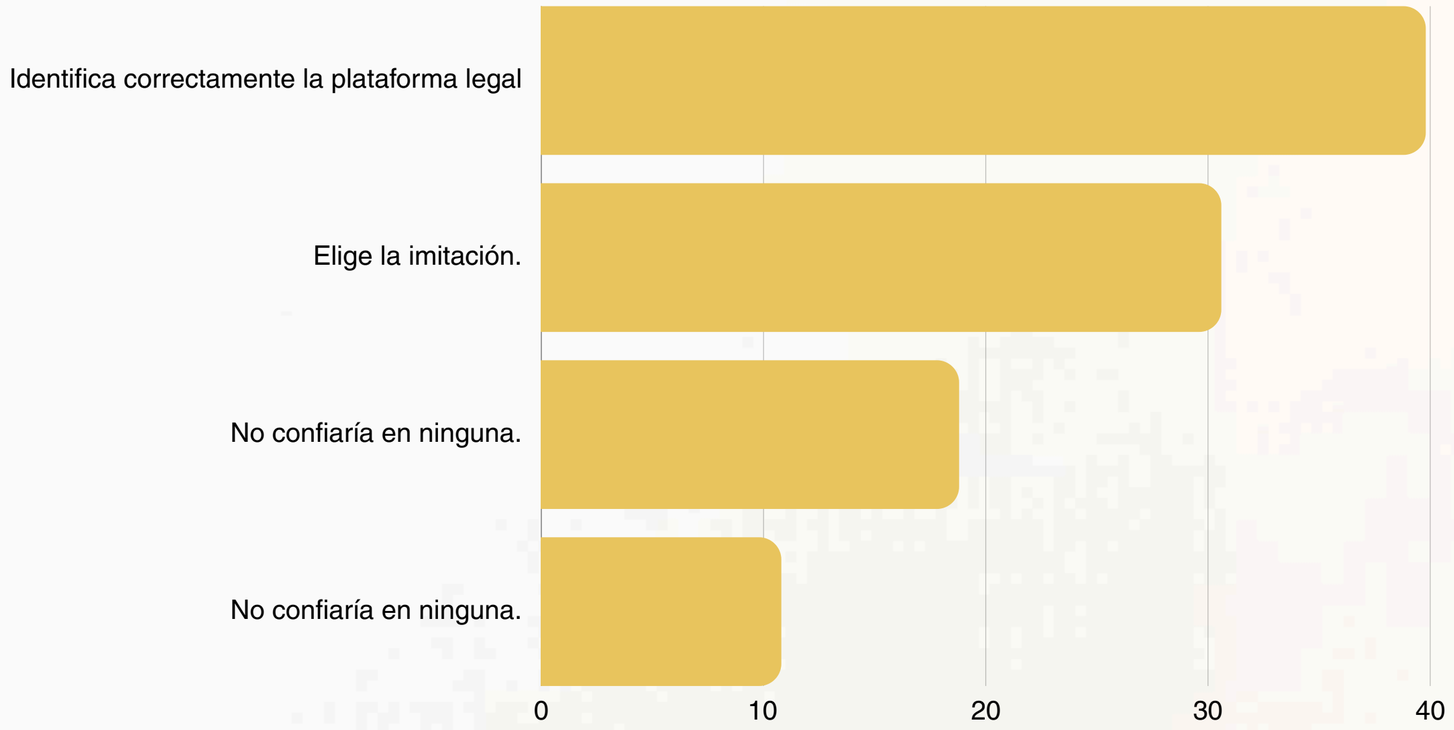


DETECTAR EL PROBLEMA NO SIEMPRE EVITA LAS CONSECUENCIAS.

BLOQUE 4

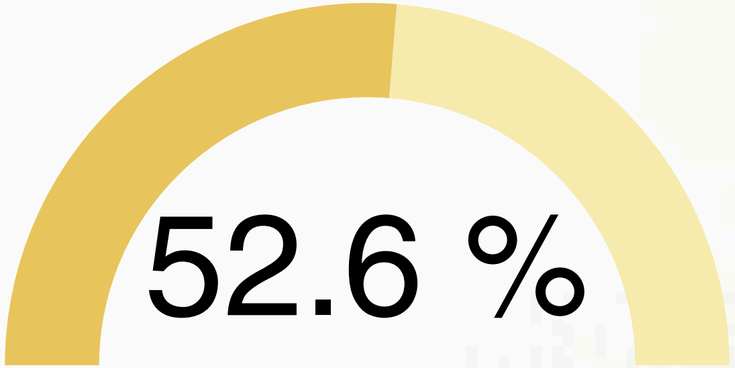
CUANDO PONEMOS A PRUEBA LO QUE CREEMOS SABER

A LA PREGUNTA, ¿CUÁL DE ESTAS DOS PLATAFORMAS **ES LA LEGAL?**

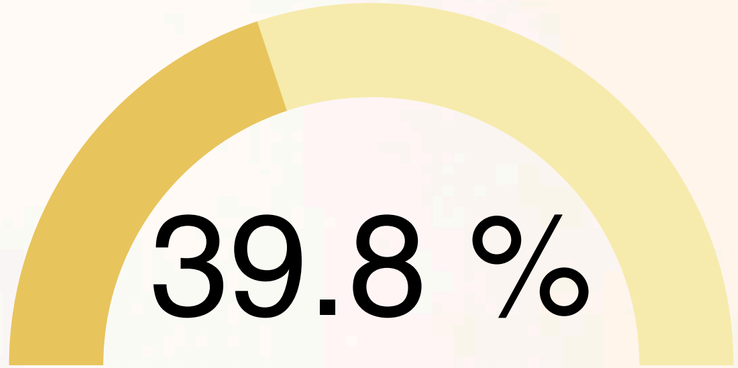


60,2% NO IDENTIFICA INEQUÍVOCAMENTE LA PLATAFORMA LEGAL.

CREEMOS QUE SABEMOS DETECTARLO MEJOR DE LO QUE REALMENTE LO HACEMOS



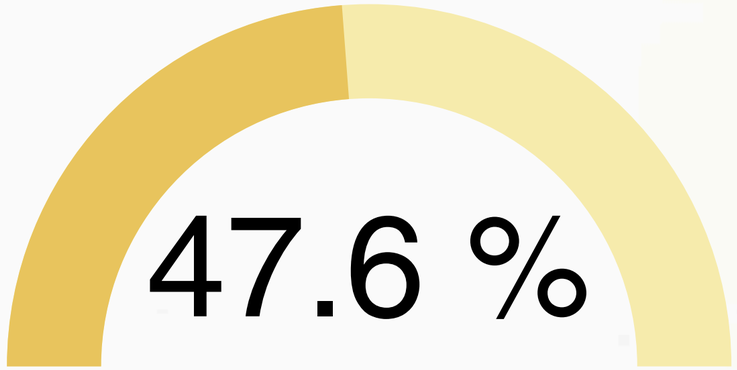
Se considera altamente capaz de distinguir una plataforma legal de una fraudulenta.



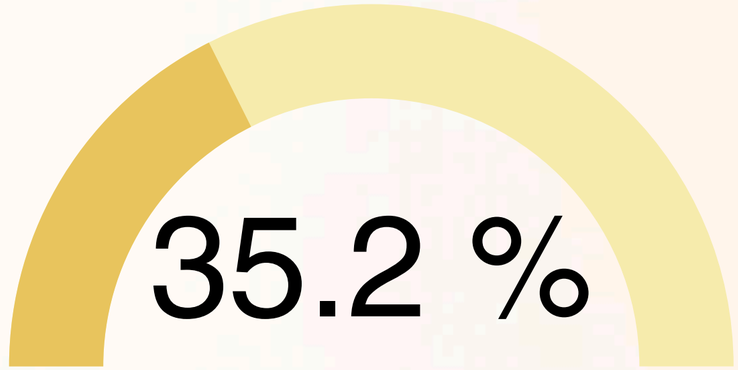
Identifica correctamente la plataforma legal en una prueba práctica.

EXISTE UNA BRECHA CLARA ENTRE PERCEPCIÓN Y CAPACIDAD REAL.
LA AUTOCONFIANZA PUEDE CONVERTIRSE EN UNA FALSA SENSACIÓN DE SEGURIDAD.

INCLUSO QUIENES SE CONSIDERAN **EXPERTOS** PUEDEN EQUIVOCARSE



Identifica la plataforma legal



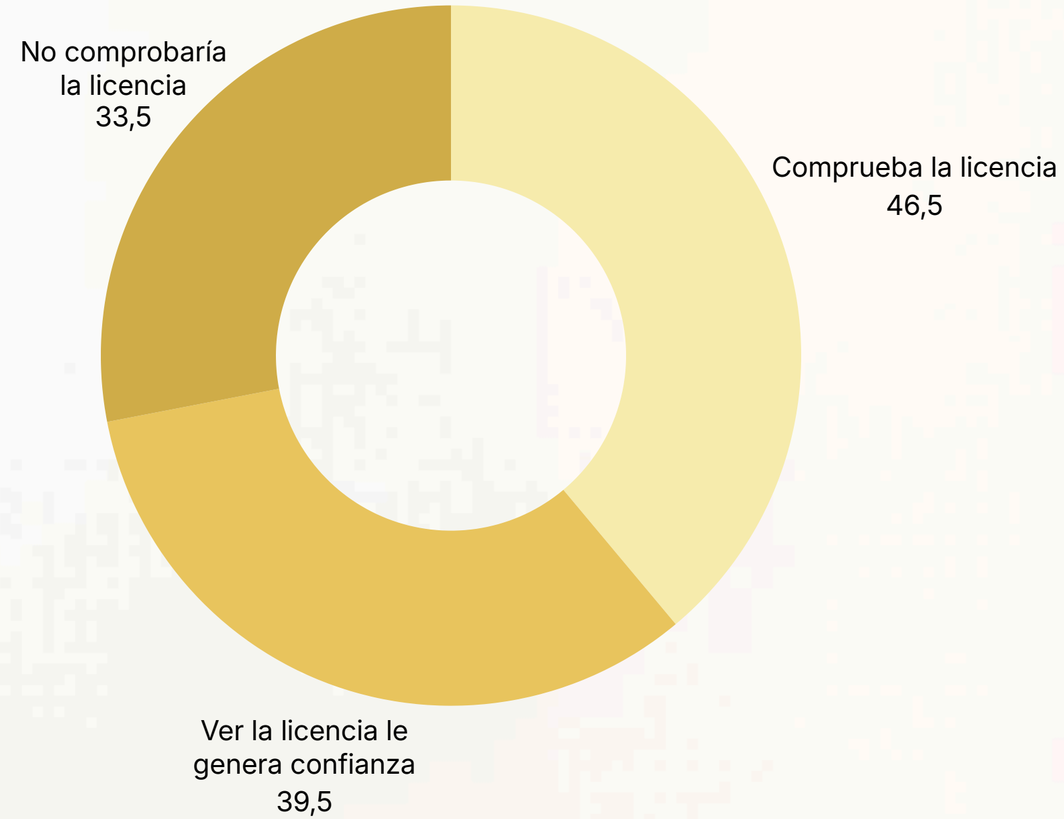
Elige directamente la imitación

17,2%

El resto no confiaría en ninguna o no sabría determinarlo.

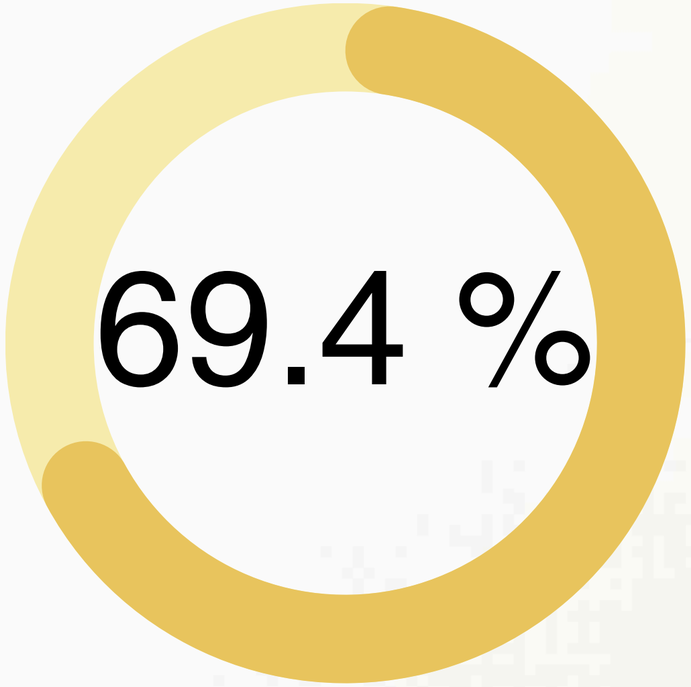
SENTIRSE ESPECIALMENTE PREPARADO
NO GARANTIZA DETECTAR CORRECTAMENTE UNA IMITACIÓN CONVINCENTE.

VER UNA LICENCIA **NO ES LO MISMO QUE COMPROBARLA**



LA PROTECCIÓN ESTÁ EN VERIFICARLA, NO SOLO EN VERLA.

EL **PHISHING** CLÁSICO **SE RECONOCE MEJOR** QUE UNA WEB FALSA



Lo identifica correctamente como fraudulento.

17,2%

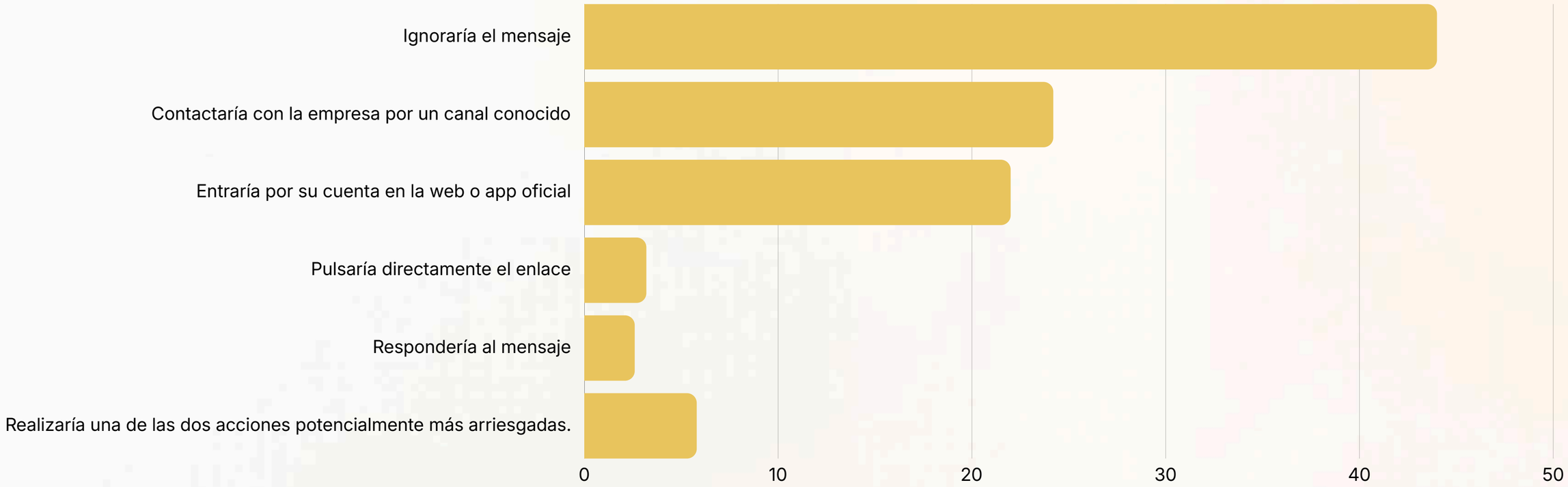
No sabría determinarlo

13,4%

Cree que es auténtico.

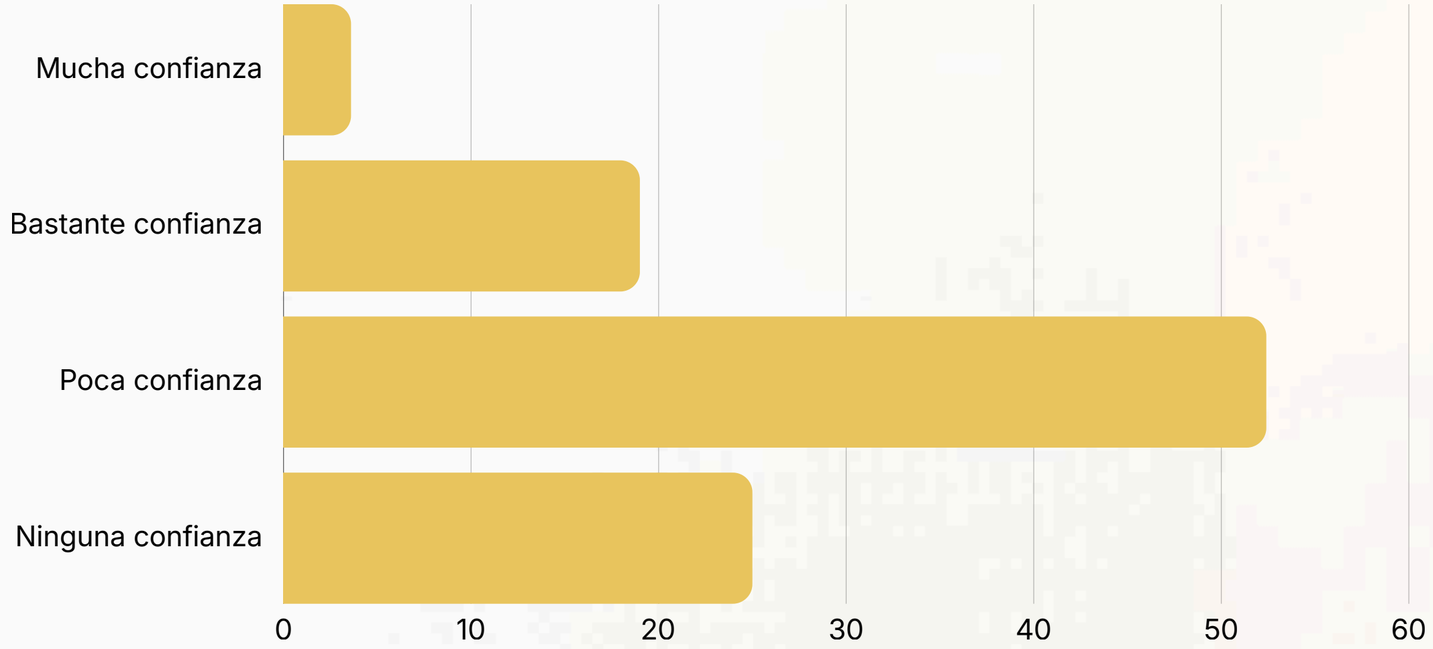
AUN ASÍ, CASI 1 DE CADA 3 NO LO IDENTIFICA INEQUÍVOCAMENTE.

SABER QUE ALGO PARECE EXTRAÑO TAMBIÉN IMPLICA **SABER** CÓMO **REACCIONAR**



EL FRAUDE NO NECESITA CONVENCER A TODO EL MUNDO PARA FUNCIONAR.

ANTE UNA PROMOCIÓN SOSPECHOSA, LA MAYORÍA DUDA. **PERO NO TODOS**.



22,6%

Concedería mucha
o bastante confianza a un anuncio ficticio.

UNA PROMOCIÓN CONVINCENTE
TODAVÍA PUEDE SUPERAR LAS DEFENSAS DE UNA PARTE RELEVANTE DE LOS USUARIOS.

BLOQUE 5

REDES SOCIALES,
PERSONAS CONOCIDAS E IA

UNA CARA CONOCIDA SIGUE FUNCIONANDO COMO **SEÑAL DE CONFIANZA**

38,8%

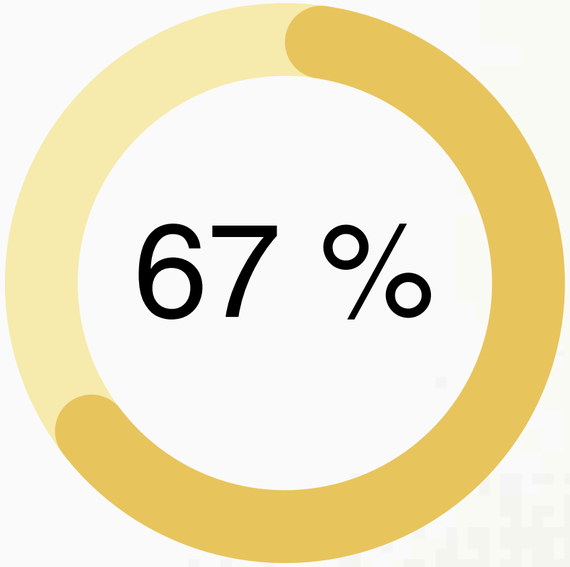
Reconoce que confiaría **mucho o bastante** más en una plataforma desconocida si estuviera recomendada por un influencer, celebrity o persona conocida.



“En un entorno en el que una identidad puede ser suplantada o un vídeo manipulado, reconocer una cara ya no garantiza reconocer la fuente”

LA NOTORIEDAD ACTÚA COMO VALIDACIÓN SOCIAL.

DOS DE CADA TRES CREEN QUE SABRÍAN DETECTAR UN **VÍDEO GENERADO CON IA**



Se considera capaz o probablemente capaz de detectar un vídeo manipulado o generado mediante IA.

33,0%

Considera que probablemente no sería capaz o que no sería capaz.

UNA CONFIANZA ELEVADA
FRENTE A UNA TECNOLOGÍA DISEÑADA PRECISAMENTE PARA PARECER REAL.

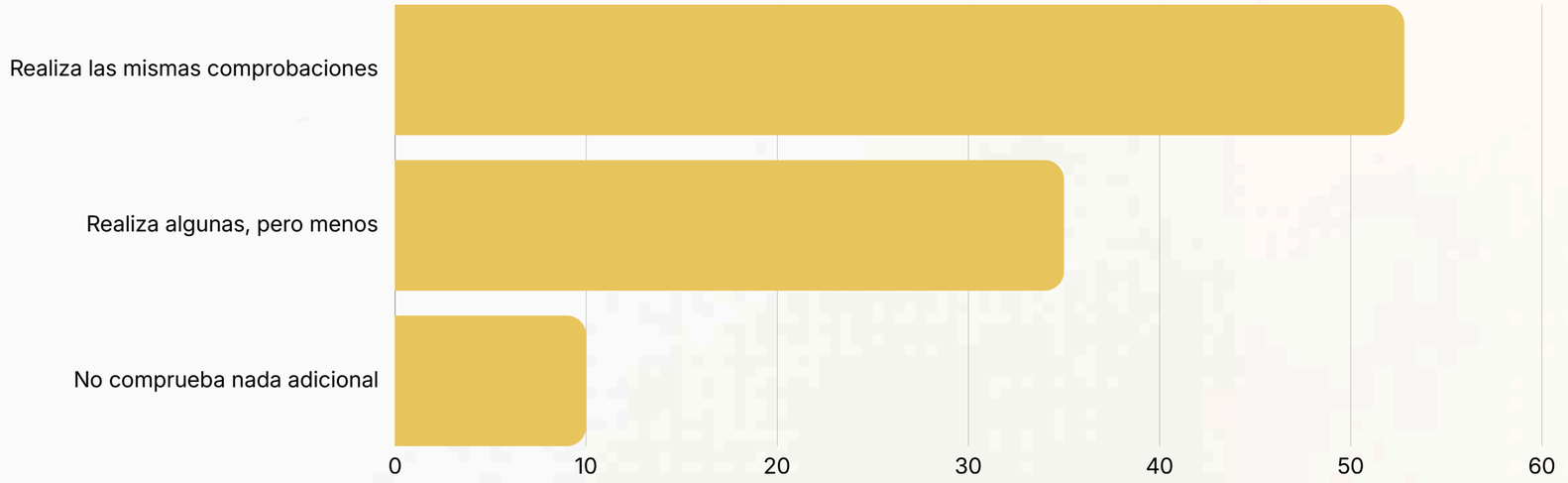
Este dato mide capacidad percibida, no capacidad real de detección.

BLOQUE 6

LOS JÓVENES: MÁS EXPOSICIÓN, NO NECESARIAMENTE MENOS CAPACIDAD

EL **45% DE LOS JÓVENES** REDUCE SUS COMPROBACIONES CUANDO UNA PLATAFORMA LLEGA DESDE **REDES O INFLUENCERS**

USUARIOS DE 18 A 24 AÑOS/Base: 180 jóvenes de 18 a 24 años.



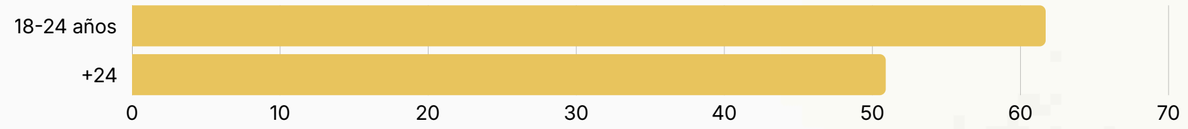
45,0 %

Reduce las comprobaciones o no realiza ninguna adicional.

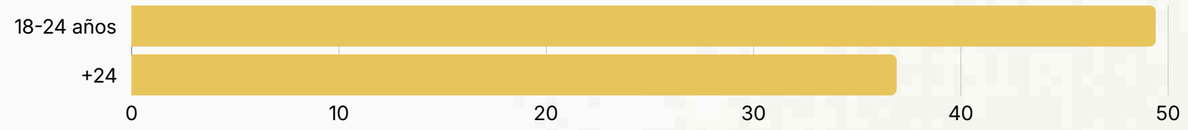
EL CANAL A TRAVÉS DEL QUE DESCUBRIMOS UNA PLATAFORMA PUEDE MODIFICAR NUESTRO NIVEL DE CAUTELA.

LOS JÓVENES ESTÁN **MÁS EXPUESTOS**, PERO TAMBIÉN **DETECTAN MEJOR** ALGUNAS AMENAZAS

HA VISTO CONTENIDO SOSPECHOSO RELACIONADO CON JUEGO ONLINE



PLATAFORMA PARECÍA LEGÍTIMA Y RESULTÓ SOSPECHOSA

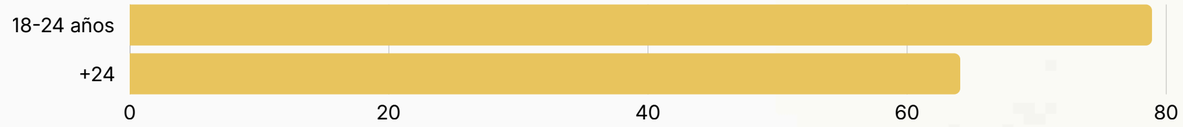


MAYOR EXPOSICIÓN NO EQUIVALE AUTOMÁTICAMENTE A MENOR CAPACIDAD DIGITAL.

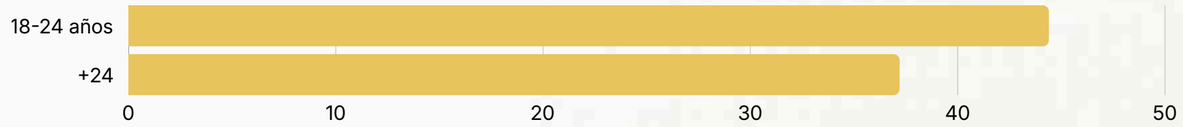
El entorno y la frecuencia de exposición también importan.

LOS JÓVENES ESTÁN **MÁS EXPUESTOS**, PERO TAMBIÉN **DETECTAN MEJOR** ALGUNAS AMENAZAS

DETECTA CORRECTAMENTE EL PHISHING



IDENTIFICA CORRECTAMENTE LA PLATAFORMA LEGAL



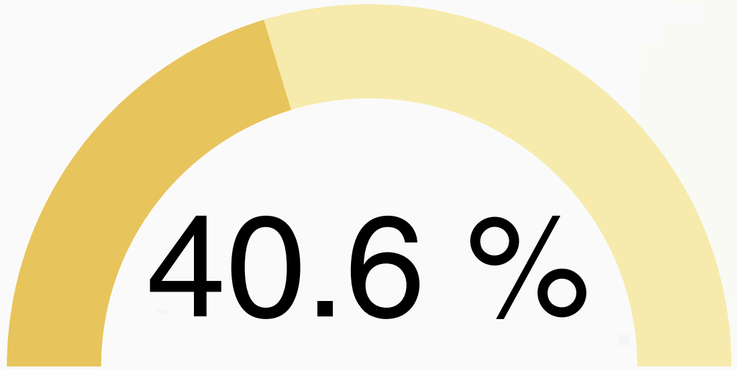
MAYOR EXPOSICIÓN NO EQUIVALE AUTOMÁTICAMENTE A MENOR CAPACIDAD DIGITAL.

El entorno y la frecuencia de exposición también importan.

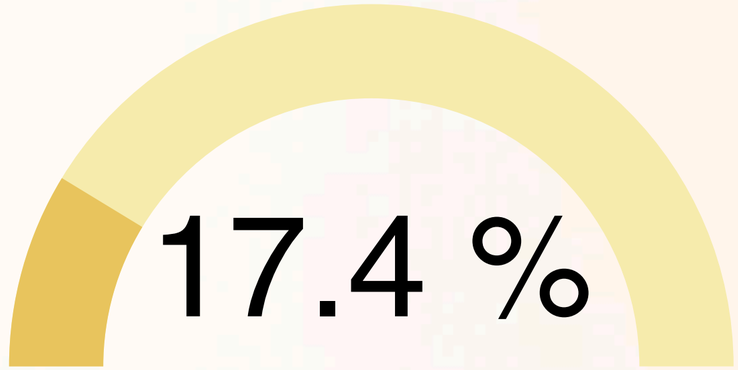
BLOQUE 7

CUANDO YA HEMOS CAÍDO

4 DE CADA 10 NO TIENEN CLARO QUÉ HACER DESPUÉS DE UN POSIBLE FRAUDE



No sabe con seguridad cómo actuar tras introducir datos o realizar un pago en una web sospechosa.

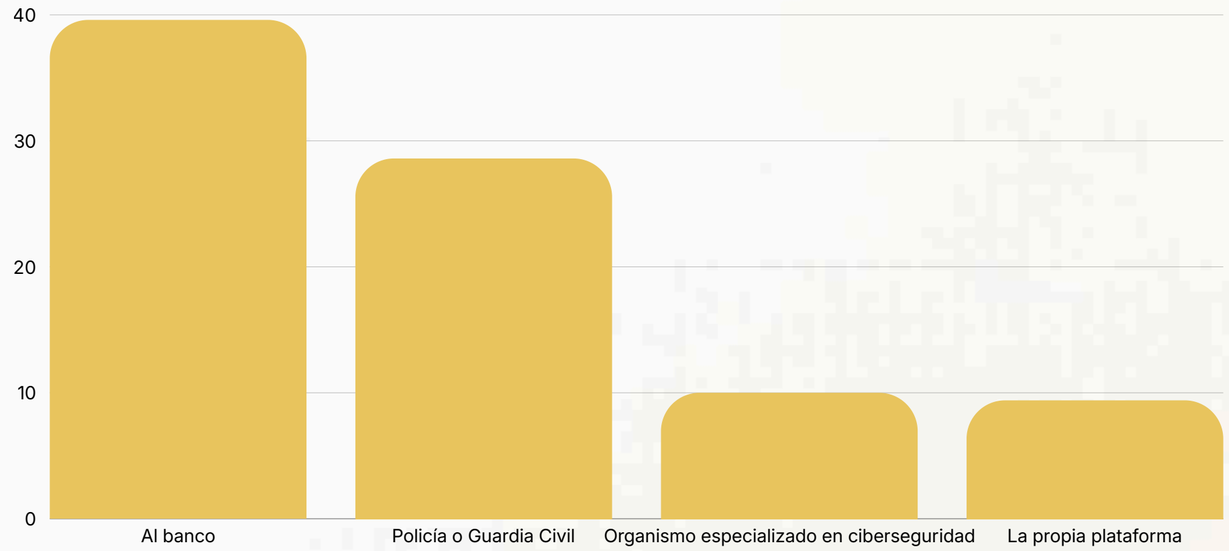


Afirma saber perfectamente qué hacer.

PROTEGER AL USUARIO TAMBIÉN SIGNIFICA EXPLICARLE QUÉ HACER DESPUÉS DE DETECTAR EL PROBLEMA.

QUEREMOS DENUNCIAR. LO QUE FALTA ES TENER CLARO EL CAMINO.

Ante un fraude, ¿a quién acudirían primero?



84,0%

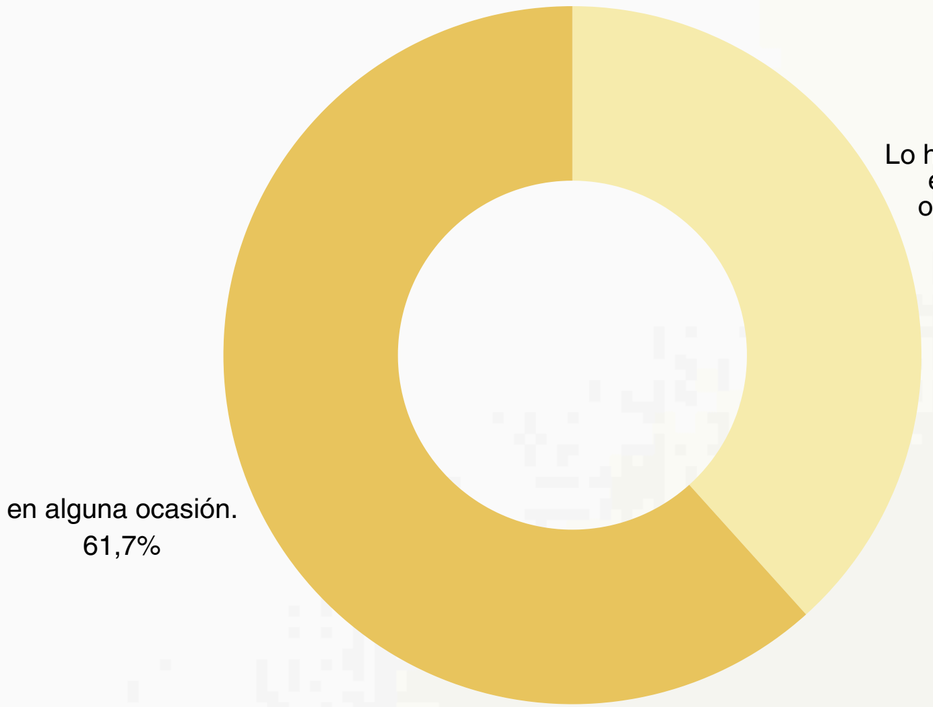
Afirma que denunciaría o probablemente denunciaría un intento de fraude incluso sin haber perdido dinero.

LA PREDISPOSICIÓN EXISTE. EL SIGUIENTE PASO ES SIMPLIFICAR DÓNDE, CÓMO Y A QUIÉN REPORTARLO.

BLOQUE 8

EL FRAUDE DIGITAL MÁS ALLÁ DEL JUEGO ONLINE

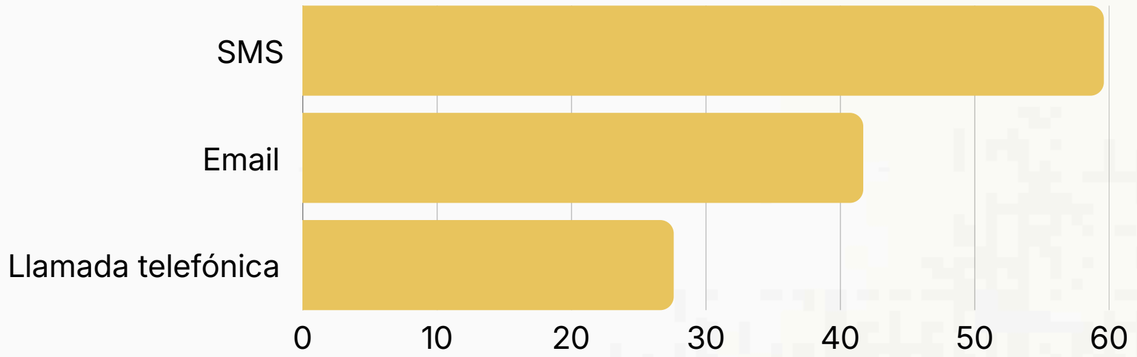
EL **57,4%** ASEGURA HABER **DETECTADO FRAUDE DIGITAL** DURANTE EL ÚLTIMO AÑO



57,4%

Declara haber recibido o detectado algún intento de fraude digital dirigido hacia él o ella..

EN EL FRAUDE GENERAL, EL **SMS** CONTINÚA SIENDO EL **PRINCIPAL CANAL**



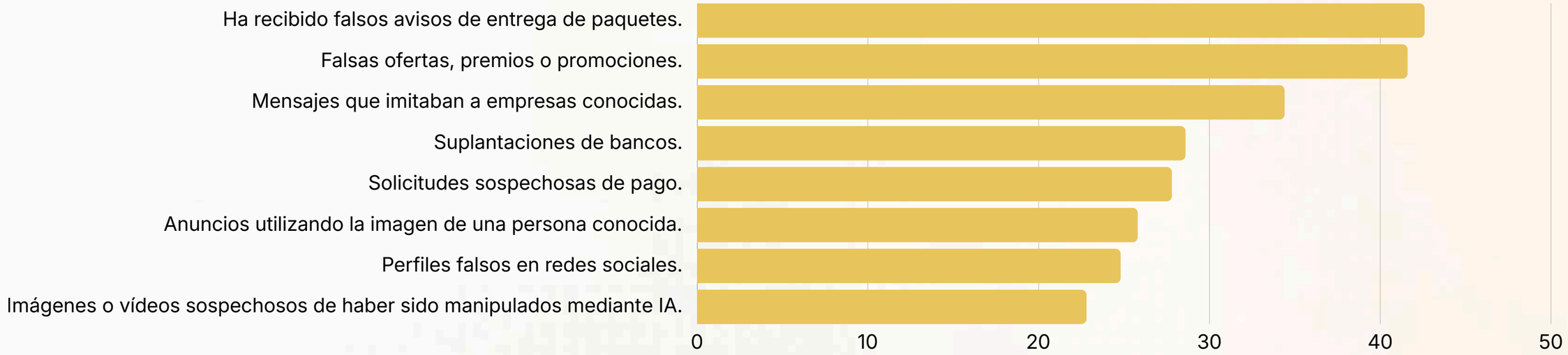
Base: 319 participantes. Respuesta múltiple.

“En el juego online destacan las redes sociales.

En el fraude digital general continúan dominando SMS, email y teléfono.”

EL CANAL DEPENDE DEL TIPO DE FRAUDE.

CUANDO CONCRETAMOS LAS SITUACIONES, **PRÁCTICAMENTE TODOS** RECONOCEN ALGUNA



93,8%

Reconoce haberse encontrado con al menos una de estas situaciones.

PODEMOS ESTAR EXPUESTOS AL FRAUDE **SIN IDENTIFICARLO COMO TAL**



84,5%

Reconoce después haberse encontrado con al menos una de las situaciones concretas planteadas.

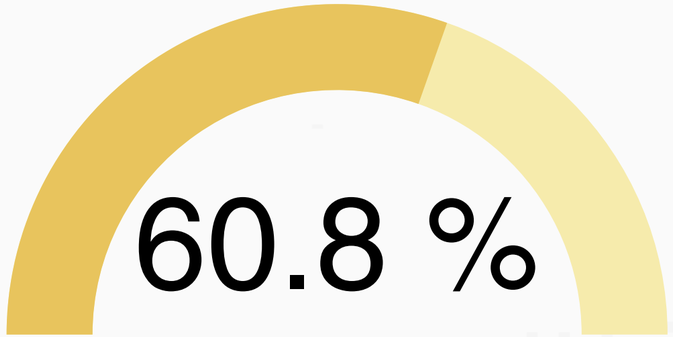
“Este dato no significa que el 84,5% haya sido víctima. Refleja una diferencia entre la percepción general y el reconocimiento de situaciones concretas.”

EXISTE UNA BRECHA ENTRE EXPERIMENTAR UNA SITUACIÓN POTENCIALMENTE FRAUDULENTA E IDENTIFICARLA MENTALMENTE COMO FRAUDE.

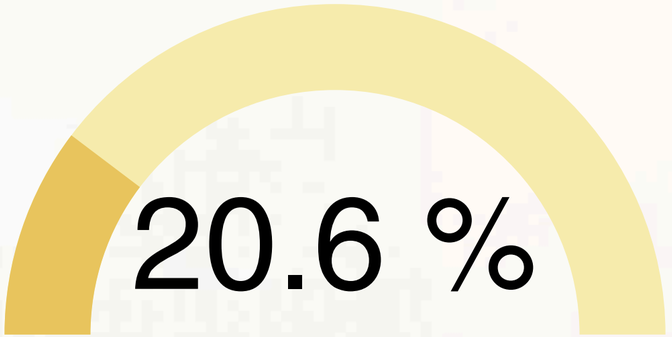
BLOQUE 9

EL FRAUDE DEL FUTURO YA ESTÁ AQUÍ

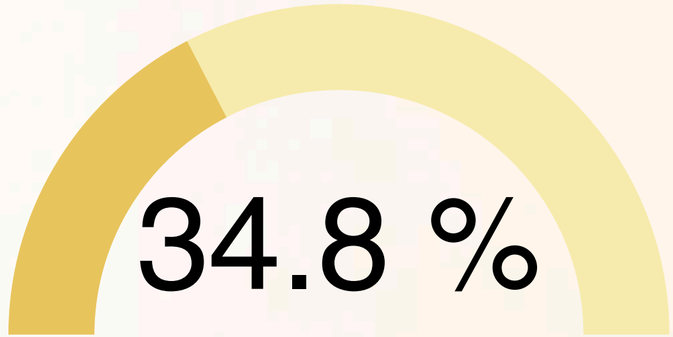
6 DE CADA 10 CREEN QUE HOY ES **MÁS DIFÍCIL DETECTAR UNA ESTAFA** QUE HACE CINCO AÑOS



Considera que detectar una estafa digital es actualmente mucho o algo más difícil.



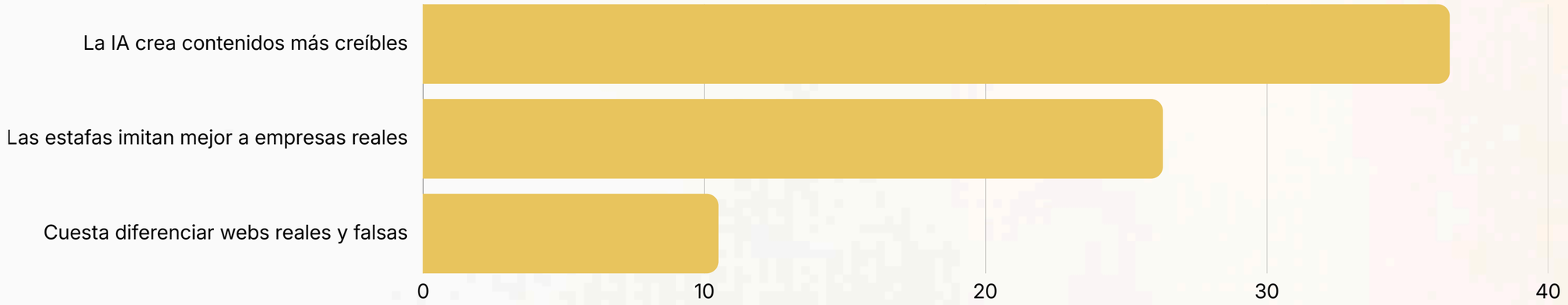
Mucho más difícil



Algo más difícil

LA **INTELIGENCIA ARTIFICIAL** ES EL **PRINCIPAL MOTIVO**

Entre quienes consideran que el fraude se ha vuelto más difícil de detectar:



Base: 304 participantes.

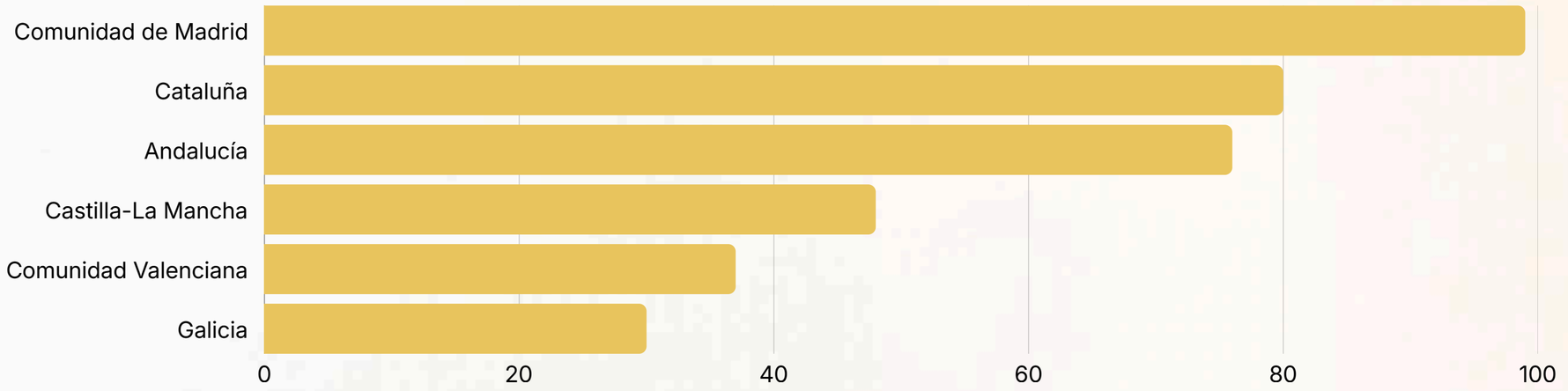
LA SOFISTICACIÓN TECNOLÓGICA ESTÁ CAMBIANDO AQUELLO QUE ENTENDEMOS POR “PARECER REAL”.

BLOQUE 10

RADIOGRAFÍA TERRITORIAL

LA RELACIÓN CON EL FRAUDE **NO ES IGUAL EN TODOS LOS TERRITORIOS**

Para evitar conclusiones basadas en muestras demasiado pequeñas, el análisis principal se concentra en las seis comunidades con al menos 30 participantes:



La muestra permite observar diferencias relevantes entre comunidades en exposición, detección y capacidad de reacción.

LA SOFISTICACIÓN TECNOLÓGICA ESTÁ CAMBIANDO AQUELLO QUE ENTENDEMOS POR “PARECER REAL”.

	Madrid	Cataluña	Andalucía	C.-La Mancha	C. Valenciana	Galicia
Elige la web imitación	35,40%	23,80%	31,60%	**18,80%**	**43,20%**	40,00%
Identifica la web legal	38,40%	**51,20%**	27,60%	47,90%	29,70%	36,70%
Ha vivido una web/app que acabó siendo falsa o sospechosa	**50,50%**	40,00%	30,30%	35,40%	45,90%	40,00%
Detecta correctamente el phishing	71,70%	72,50%	65,80%	**79,20%**	70,30%	**46,70%**
Sabría o cree que sabría reaccionar	59,60%	**75,00%**	57,90%	60,40%	**40,50%**	63,30%

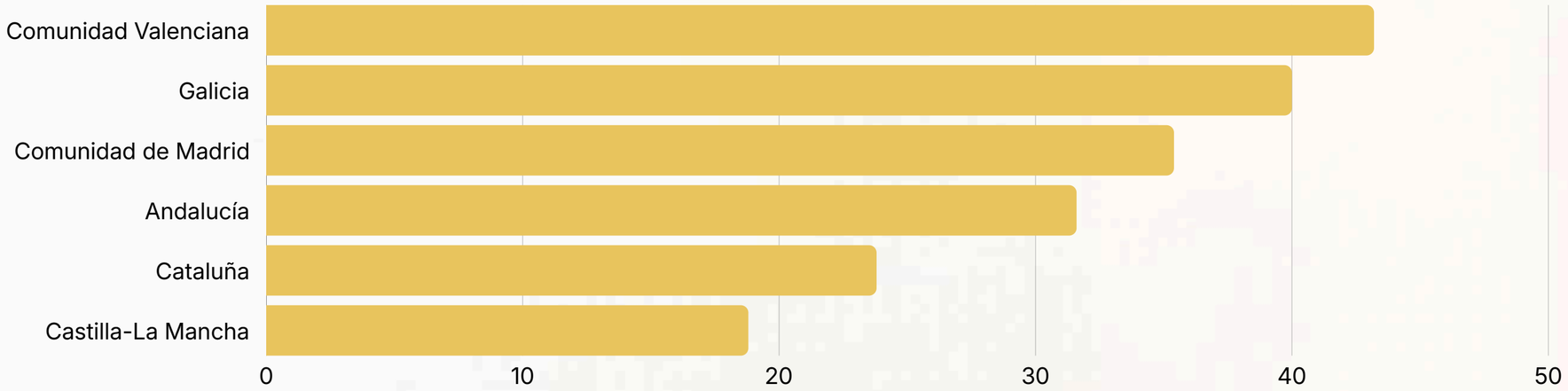
Lectura

Los resultados apuntan a **perfiles diferentes de vulnerabilidad**: algunos territorios destacan por una mayor exposición, otros por una menor capacidad de identificación y otros combinan ambos factores.

Resultados descriptivos de la muestra. Las bases regionales no permiten extrapolar los porcentajes al conjunto de cada comunidad autónoma.

LA COMUNIDAD VALENCIANA PRESENTA EL **MAYOR PORCENTAJE DE ELECCIÓN DE LA WEB FALSA**

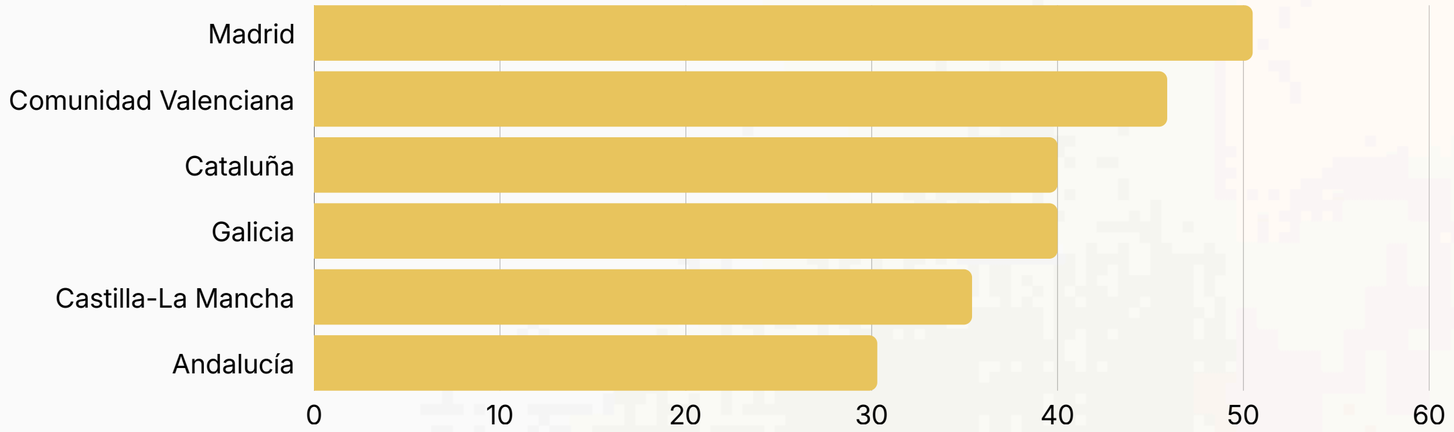
Media del estudio: 30,6%



Lectura
La capacidad para distinguir una plataforma legal de una imitación varía considerablemente entre territorios dentro de la muestra.
La diferencia entre Comunidad Valenciana y Castilla-La Mancha alcanza 24,4 puntos porcentuales en la elección de la web imitación.

MADRID DESTACA POR LA **EXPERIENCIA PREVIA** CON ENTORNOS **QUE INICIALMENTE PARECÍAN LEGÍTIMOS**

Participantes que afirman haberse encontrado con una web, app o promoción que parecía legítima, pero resultó falsa o sospechosa.

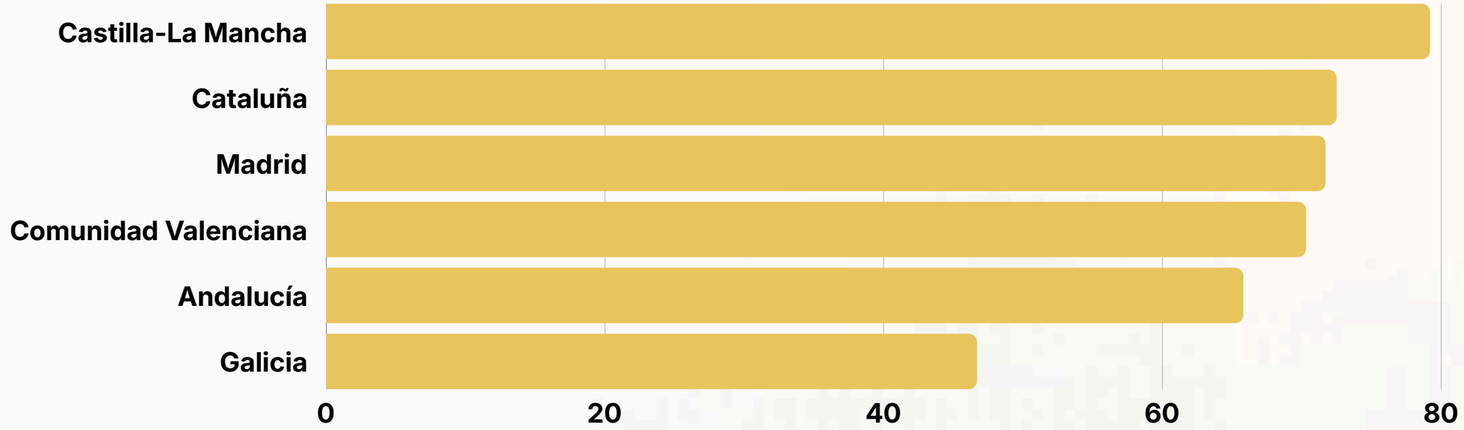


Comunidad Valenciana también se sitúa por encima del conjunto, mientras que Andalucía presenta la menor incidencia declarada entre las seis comunidades analizadas.

UNO DE CADA DOS PARTICIPANTES MADRILEÑOS AFIRMA HABER VIVIDO YA UNA SITUACIÓN DE ESTE TIPO,

CASTILLA-LA MANCHA OBTIENE EL **MEJOR RESULTADO** EN LA **PRUEBA DE PHISHING**

Identifica correctamente el mensaje fraudulento:



La diferencia entre Castilla-La Mancha y Galicia supera los **32 puntos porcentuales**

CATALUÑA PRESENTA LA **MAYOR CAPACIDAD DECLARADA DE REACCIÓN**



42,5%

De los participantes catalanes afirma haber facilitado datos personales o bancarios, o haber realizado un pago, tras interactuar con un contenido que posteriormente le generó dudas.

CONOCIMIENTO, EXPOSICIÓN Y COMPORTAMIENTO NO EVOLUCIONAN NECESARIAMENTE EN PARALELO.

SEIS TERRITORIOS, SEIS LECTURAS

Madrid

Mayor experiencia declarada con plataformas que dejaron de parecer legítimas.
50,5% ha vivido una situación de este tipo.

Cataluña

Mayor identificación de la web legal y mayor capacidad declarada de reacción.
51,2% identifica la plataforma legal y 75,0% cree saber actuar ante un fraude.

Andalucía

Menor experiencia declarada con plataformas falsas o sospechosas.
30,3% afirma haber vivido una situación de este tipo.

Castilla-la Mancha

MMejores resultados ante las pruebas prácticas.
Solo 18,8% elige la imitación y 79,2% identifica correctamente el phishing.

Comunidad Valenciana

Mayor vulnerabilidad ante la imitación y menor claridad sobre cómo reaccionar.
43,2% elige la web falsa y solo 40,5% considera que sabría actuar.

Galicia

Elevada exposición al fraude digital general y mayor dificultad ante el phishing.
76,7% declara haber detectado fraude digital durante el último año, mientras que 46,7% identifica correctamente el mensaje de phishing.

**LOS DATOS NO DIBUJAN UN ÚNICO PERFIL TERRITORIAL DE RIESGO:
EXPOSICIÓN, CAPACIDAD DE DETECCIÓN Y REACCIÓN PRESENTAN COMPORTAMIENTOS DIFERENTES SEGÚN LA COMUNIDAD.**

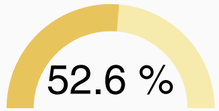
BLOQUE 11

CONCLUSIONES

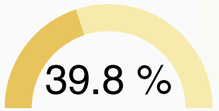
SEIS TERRITORIOS, SEIS LECTURAS

01

NOS SENTIMOS MÁS PREPARADOS DE LO QUE DEMUESTRAN LAS PRUEBAS



Se siente capaz



Acertó en la prueba

La confianza supera la capacidad demostrada.

02

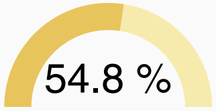
PARECER SEGURO NO SIGNIFICA SER SEGURO

Licencias, reseñas, métodos de pago y caras conocidas pueden generar confianza.

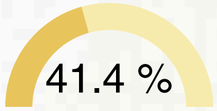
Una señal de seguridad también puede ser imitada.

03

EL FRAUDE YA FORMA PARTE DE LA EXPERIENCIA DIGITAL



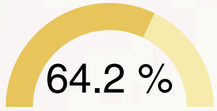
Vio contenido sospechoso



Vivió una situación sospechosa

04

MUCHAS VECES LAS DUDAS LLEGAN DESPUÉS DE INTERACTUAR



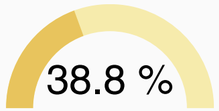
Ha realizado alguna acción con contenidos que después le generaron dudas.

VERIFICAR ANTES DE CONFIAR. PENSAR ANTES DE INTERACTUAR.

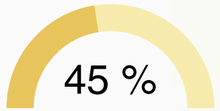
SEIS TERRITORIOS, SEIS LECTURAS

05

REDES SOCIALES, PERSONAS CONOCIDAS E IA CREAN NUEVOS ATAJOS DE CONFIANZA



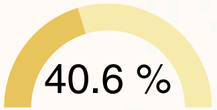
Confiaría más por la recomendación de alguien conocido



De los jóvenes reduce sus comprobaciones al descubrir plataformas por influencers o redes.

06

DETECTAR UN FRAUDE NO BASTA: TAMBIÉN HAY QUE SABER REACCIONAR



No tiene claro qué hacer después de introducir datos o realizar un pago en una web que sospecha fraudulenta.

07

EL RIESGO NO PRESENTA EL MISMO PERFIL EN TODOS LOS TERRITORIOS

Las diferencias regionales muestran que la exposición, la detección y la capacidad de reacción no siguen un patrón único.

La sensibilización debe abordar distintas formas de vulnerabilidad.

LA MAYOR VULNERABILIDAD NO ES NO SABER NADA.

ES CREER QUE YA SABEMOS LO SUFICIENTE.

Los usuarios conocen muchas de las señales.

Saben qué deben comprobar.

Y son cada vez más conscientes del fraude digital.

Pero cuando las imitaciones se vuelven más convincentes, **la intuición deja de ser suficiente.**

Webs, mensajes, promociones, perfiles y vídeos pueden reproducir cada vez mejor las señales que utilizamos para decidir en qué confiar.

Por eso, el reto ya no es únicamente **detectar algo sospechoso.**

Es aprender a:

PARAR. COMPROBAR. DECIDIR.

JUEGA SOBRE SEGURO

Antes de confiar, comprueba.