AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

INFORME ANUAL

TENDENCIAS DE FRAUDE EN EMPRESAS 2025-2026

www.asociacioncontraelfraude.com

Bienvenida

INFORME DE **TENDENCIAS DE FRAUDE** EN EMPRESAS 2025

Jorge Hernández

Presidente de la AEECF

Un año más, desde la Asociación de Empresas Españolas contra el Fraude (AEECF), no solo renovamos nuestro compromiso: lo reforzamos, lo actualizamos y lo ponemos al servicio de todo el ecosistema empresarial.

Lanzamos con orgullo la 9ª edición del Informe de Tendencias de Fraude en Empresas, un estudio que ya se ha consolidado como referente nacional en prevención de fraude corporativo y ciberseguridad aplicada. Una herramienta estratégica para quienes lideran, protegen y transforman sus organizaciones en tiempos de incertidumbre digital.

El fraude ya no es una amenaza futura: es una realidad diaria que evoluciona más rápido que muchas respuestas empresariales. Su impacto va mucho más allá de lo económico; compromete la reputación, la confianza del cliente y la continuidad del negocio.

Este informe no se limita a ofrecer cifras. Es un termómetro del nivel de madurez en la defensa antifraude. Un radar que detecta qué herramientas funcionan, qué tecnologías están infrautilizadas y dónde están las brechas que aún nos hacen vulnerables.

Entre sus hallazgos: el auge del fraude por ingeniería social y el repunte de ataques sobre clientes reales, la infrautilización del machine learning pese a su eficacia comprobada, una atención post-fraude que aún no está a la altura de las expectativas del cliente, el uso de IA para llevar a cabo engaños y estafas, phishing, vishing o smishing. .

Y una clara conclusión: solo la anticipación, la colaboración y la inteligencia compartida pueden marcar la diferencia.

Por eso, desde la AEECF queremos agradecer profundamente a todas las empresas participantes su transparencia y compromiso. Su colaboración no solo genera valor para sus organizaciones, sino para todo el ecosistema.

Y si tu empresa aún no forma parte de esta red, hoy es el momento perfecto para sumarse. Porque en un escenario donde el fraude se reinventa cada día, pertenecer a una comunidad que comparte datos, estrategias y conocimiento es más que una ventaja competitiva: es una necesidad estratégica.

La lucha contra el fraude no es individual. Es una causa común. Y desde la AEECF, te invitamos a liderarla con nosotros.

Gracias por formar parte de esta misión compartida. O por decidir hacerlo a partir de hoy.

Índice

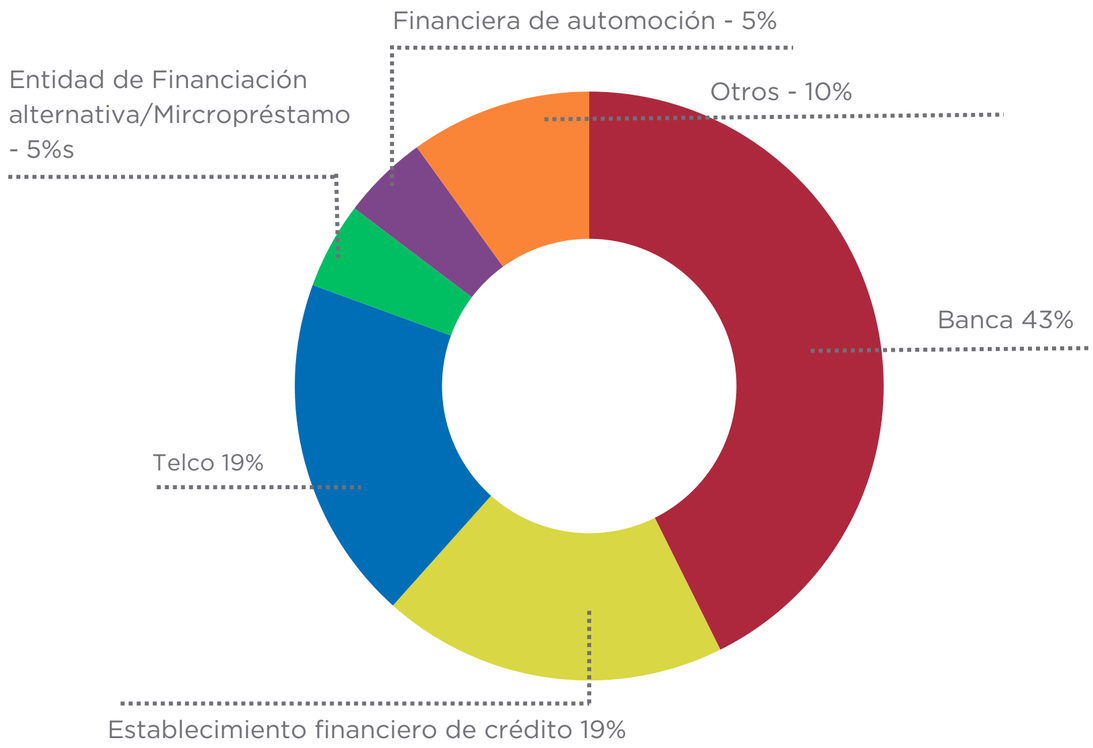
BLOQUE I

Análisis Demográfico

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

1.1 Sectores y departamentos



GRAF. 1.1: ANÁLISIS SECTORIAL DE LA MUESTRA

La **banca** representa un **43%**, Se trata de un sector que tradicionalmente es el principal objetivo de los ataques de los defraudadores dada la naturaleza de sus operaciones y transacciones con un impacto financiero directo a los consumidores.

A continuación están representados los **establecimientos financieros de crédito (19%) y el sector Telco (19%)**. Se trata de sectores que encaran fraudes similares como identificación online de clientes y suplantaciones de identidad. Ambos sectores han ido convergiendo en tipos de fraude a medida que el sector Telco ha ido financiando diferentes productos.

DEPARTAMENTOS

El **71% de las respuestas proviene directamente de departamentos de fraude**, lo que garantiza una visión especializada, operativa y muy cercana a la gestión real del riesgo. La baja presencia de áreas como operaciones **(10%) o seguridad corporativa (5%)** deja entrever que aún hay margen para mejorar la coordinación interdepartamental en la lucha contra el fraude. Así como la ausencia de áreas clave como ciberseguridad, riesgos o compliance, que en otros entornos están cada vez más involucradas en la defensa antifraude.

Este sesgo funcional refuerza la visión táctica del problema, pero limita el enfoque estratégico y transversal que requiere el fraude moderno, especialmente ante amenazas híbridas que combinan ingeniería social, brechas técnicas y fallos de gobernanza.

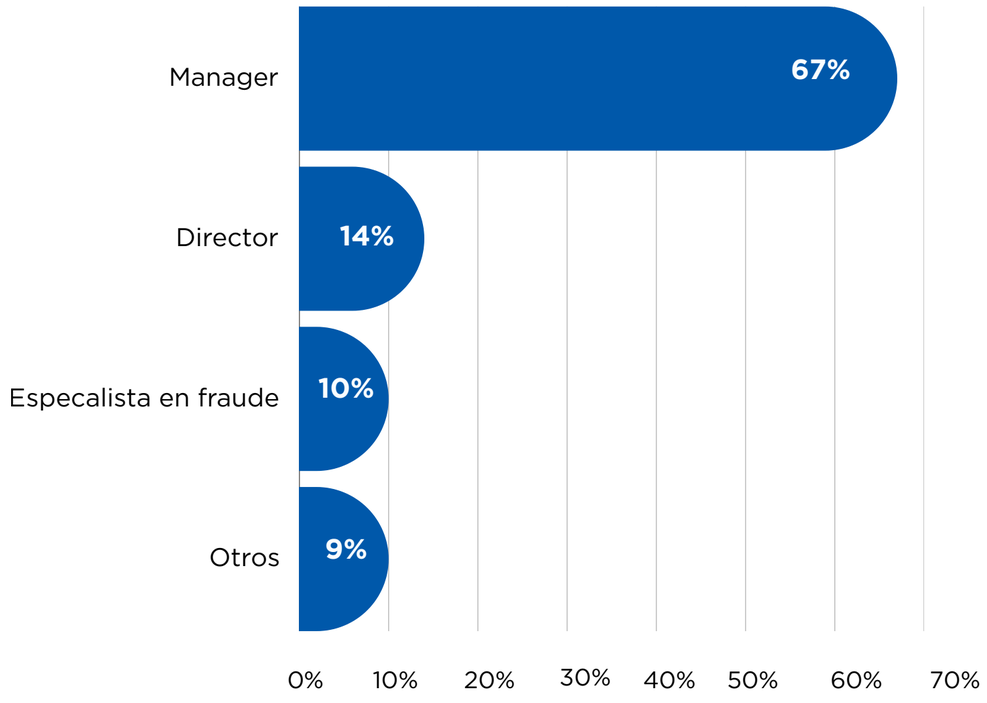
«El 71% de las respuestas proviene directamente de departamentos de fraude, se ha consolidado como área independiente de la gestión del fraude.»

1.2 Roles

La **mayoría de los participantes (67%)** ocupa cargos de manager, lo que garantiza una **visión operativa con capacidad de ejecución**, pero también con conocimiento táctico del día a día del fraude. Solo un 14% ocupa puestos directivos, lo que sugiere que la alta dirección aún participa de forma limitada en este tipo de diagnósticos, a pesar de su relevancia estratégica.

Por otro lado, el **10%** de **especialistas en fraude** refuerza el valor técnico de las respuestas, sumado a la opinión de **otros cargos (9%)** que asumen la detección del fraude.

«El 71% de los participantes trabaja directamente en áreas antifraude: una visión experta y de primera línea.»



GRAF. 1.2: Roles

«2 de cada 3 respuestas provienen de managers: visión de campo y control táctico del fraude.»

BLOQUE II

Recusos dedicados al fraude

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

BLOQUE II: RECUSOS DEDICADOS AL FRAUDE

2.1 Tamaño del equipo de fraude

El 58% de las empresas encuestadas dispone de **equipos de fraude compuestos por más de 20 personas**, lo que refleja una **estructura robusta y especializada**, especialmente en sectores como banca y telcos. Esto sugiere una clara **priorización del riesgo de fraude** y una madurez avanzada en su gestión.

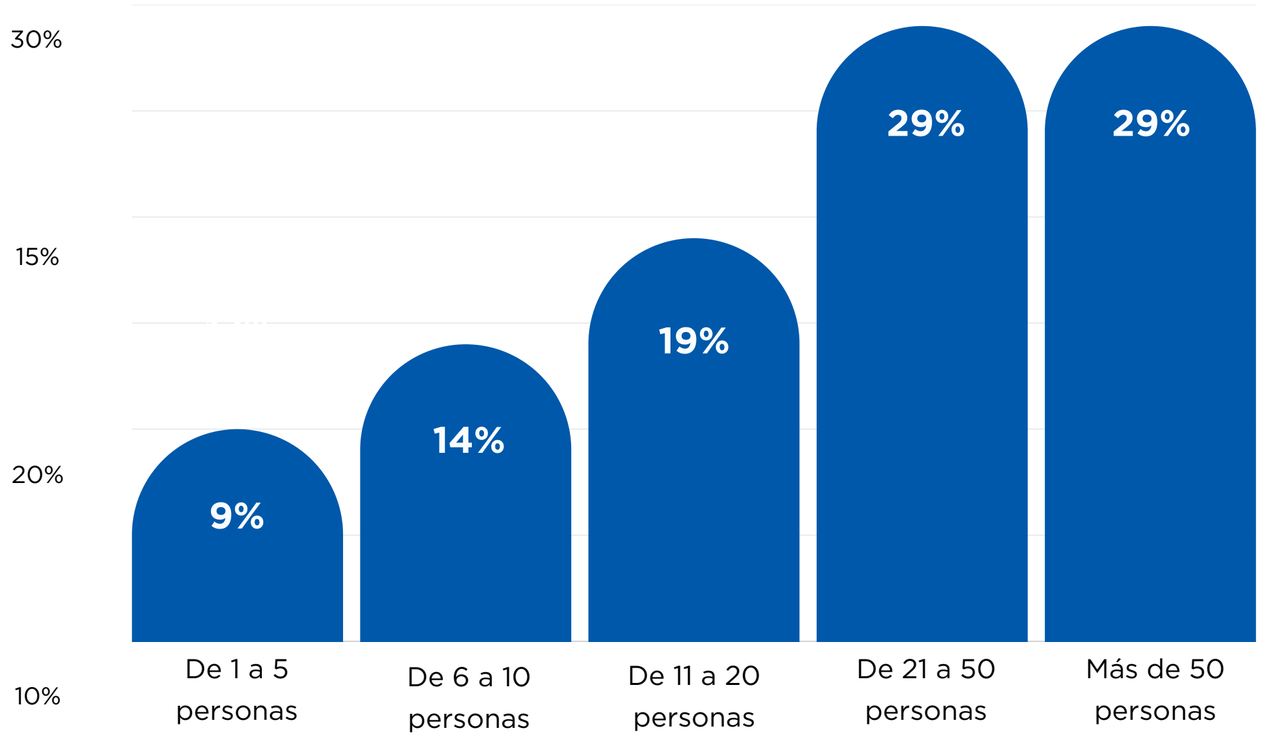
Por otro lado, un 24% de las entidades tiene **equipos de menos de 10 personas**, lo que puede indicar una estructura aún en crecimiento o o con menor exposición digital.

Este abanico de tamaños confirma que el fraude se está gestionando ya como **una función crítica con equipos dedicados, multidisciplinares y escalables,** acorde al crecimiento del riesgo y la sofisticación de los ataques.

«Los equipos medianos pierden peso en 2025: las empresas apuestan por escalar o externalizar.»

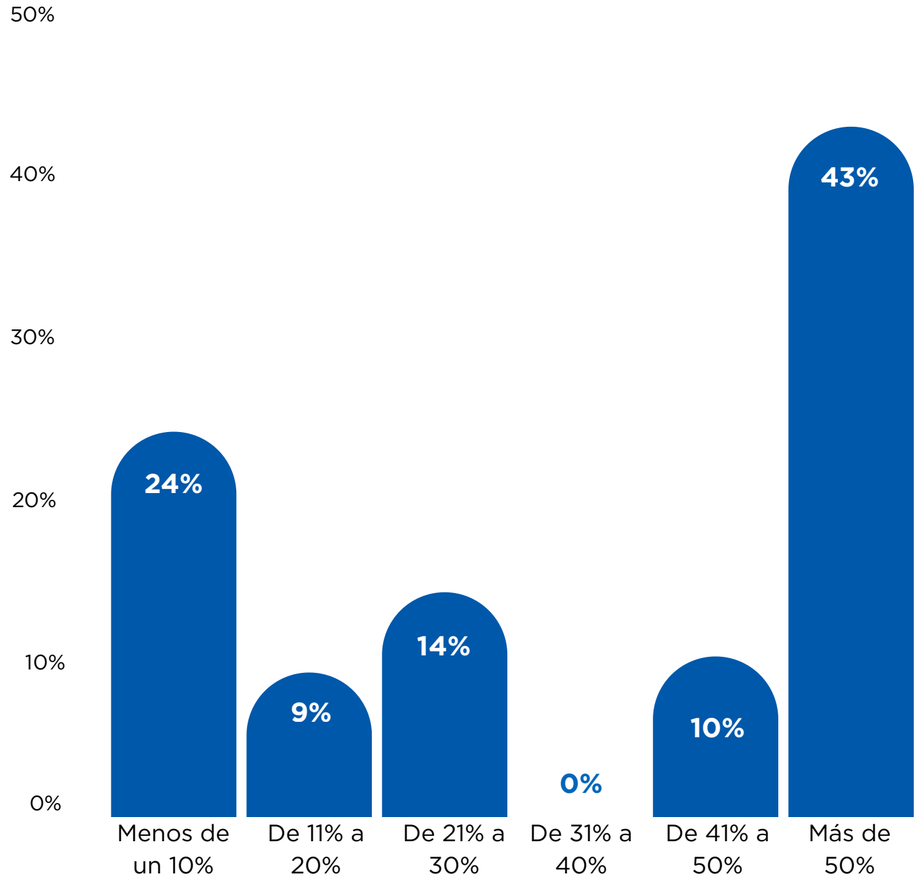
Solo el 9% de las compañías gestiona el fraude con equipos de menos de 5 personas

Respecto al estudio 2024, los equipos más grandes experimentan un ascenso de 7 puntos, mientras los medianos (11 a 50 personas) bajan en conjunto, posiblemente reflejando una bifurcación en el modelo: o bien se escalan hacia unidades más potentes, o bien se reducen y delegan parte del control en proveedores externos o soluciones automatizadas.



GRAF. 2.1: Tamaño del equipo de fraude

2.2 Externalizacion de las funciones de fraude



GRAF. 2.2: Miembros externos del equipo de Fraude

Casi la mitad de las organizaciones **(43%) tiene más del 50% de su equipo antifraude conformado por personal externo**. Esto se corresponde a entidades de tamaño grande así como a necesidades de flexibilidad operativa, especialización técnica o contención de costes fijos.

«Los equipos medianos pierden peso en 2025: las empresas apuestan por escalar o externalizar.»

Un 24% de las entidades tienen menos del 10% de personal externo, lo que suele corresponder a entidades de menor tamaño e indica una **estructura interna más alineada con los valores corporativos de control directo**.

Este escenario híbrido refleja un mercado donde la **lucha contra el fraude se profesionaliza, pero también se fragmenta,** dependiendo del tamaño, recursos y modelo operativo de cada entidad.

«El 43% de las empresas ya externaliza más de la mitad de su equipo antifraude.»

BLOQUE III

Percepción del fraude

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

3.1 Percepción del fraude

Los datos evidencian un cambio significativo en la forma en que las organizaciones enfrentan el fraude: ya no se trata únicamente de pérdidas económicas, sino de su impacto sistémico y estratégico.

La **dimensión reputacional** emerge como la principal preocupación para el **32%** de las empresas. Esto confirma una tendencia ya observada en informes internacionales como el "*Global Economic Crime and Fraud Survey 2024*" de PwC, que destaca que el 56% de los fraudes tienen consecuencias reputacionales que afectan directamente al negocio y a la relación con el cliente.

En cambio, un **28%** de las organizaciones aún lo consideran como una **pérdida contable**. Y aunque esta perspectiva sigue siendo relevante para la gestión financiera, puede reflejar una menor madurez en la incorporación del fraude como riesgo estratégico o para su uso en el análisis preventivo.

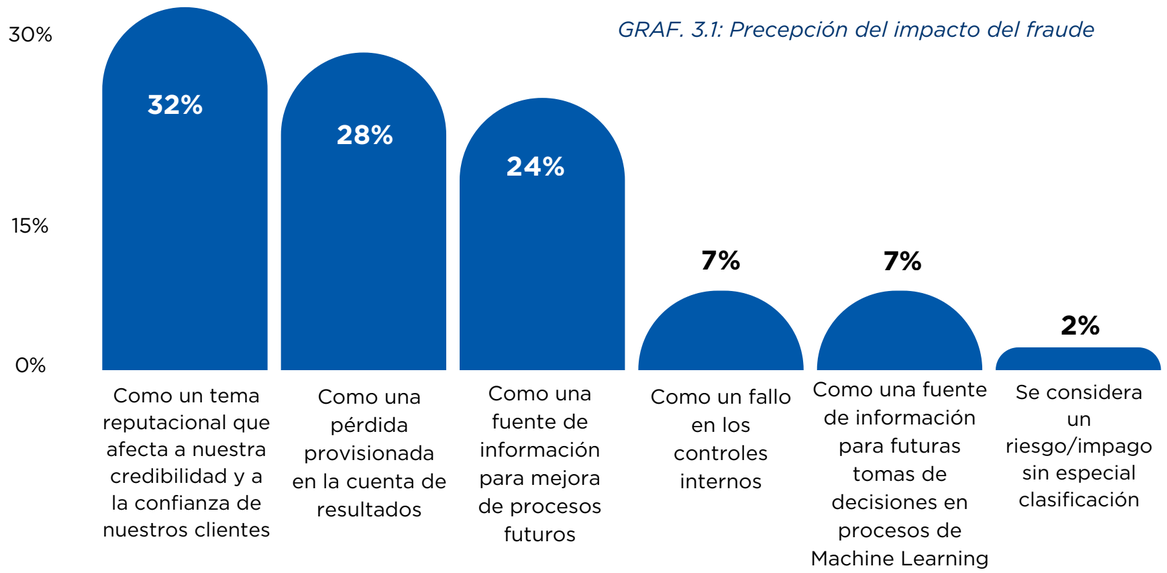
Un **24%** de las empresas ven el fraude como una **fuente de información** para ajustar los procesos y un **7%** como un valioso input para decisiones en procesos de **machine learning**, lo que refleja una visión avanzada en términos de ciberinteligencia. Ambos enfoques son fundamentales en un contexto donde la automatización y la detección temprana basada en patrones comportamentales son claves para prevenir fraudes complejos.

«El 31% de las organizaciones identifica el fraude como una amenaza directa a su reputación.»

Solo **un 7 %** vincula el fraude con fallos en los controles internos, lo cual sugiere una mayor sensación de madurez en los sistemas de control o una transición hacia una visión más holística del riesgo, aunque, según el informe Occupational Fraud 2024 de la ACFE, más del 50 % de los fraudes ocurren debido a la ausencia de controles efectivos o a que el perpetrador logra anularlos.

Por su parte, el hecho de que ninguna empresa limite la clasificación de fraude a dictámenes legales o judiciales indica una evolución importante en la gestión interna del riesgo, evitando la dilación de respuestas por burocracia legal.

GRAF. 3.1: Precepción del impacto del fraude



3.2 Distribución geográfica

Cuando se consulta a las empresas sobre la distribución territorial del fraude, **el 67% de las entidades considera que el fraude afecta a todas las comunidades autónomas según el volumen de solicitudes** o actividad económica que registran. El **33% restante opina sin embargo que algunas comunidades presentan siempre una mayor incidencia de fraude**.

El análisis de la distribución geográfica entre comunidades autónomas arroja los siguiente resultados:

- **Cataluña** lidera el ranking con el 37% de los casos reportados, manteniendo su posición respecto al Informe de Fraude de 2024.
- Le sigue la **Comunidad de Madrid** con un 26%.
- La **Comunidad Valenciana** registra un 16%.
- **Andalucía** concentra un 11% de los casos.
- **Castilla-La Mancha y Galicia** representan un 5% cada una.
- El resto de comunidades (11 en total) no registran casos de fraude en este estudio.

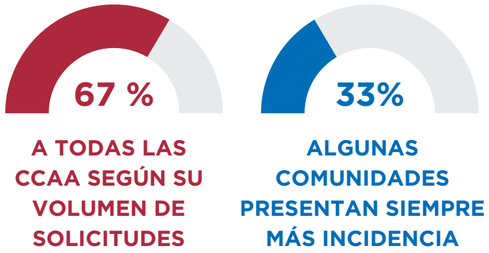
Este reparto territorial indica que más del 90% de los fraudes se concentran en cuatro comunidades autónomas: Cataluña, Madrid, Comunidad Valenciana y Andalucía.

«Cataluña y Madrid acaparan el 63% de los fraudes detectados en las empresas españolas.»

En la edición anterior del informe, Cataluña registraba un 33% de los casos, mientras que la Comunidad Valenciana se situaba en segundo lugar con un 17%, seguida por Madrid y Andalucía (ambas con un 13%). En el presente ejercicio, Cataluña y Madrid amplían su peso relativo (37% y 26%, respectivamente), lo que confirma un empeoramiento de la concentración territorial del fraude, especialmente en Madrid, que incrementa su incidencia en 13 puntos porcentuales.

De nuevo esta concentración refleja una clara correlación entre volumen de actividad económica, digitalización y concentración poblacional con la incidencia de fraude. Cataluña y Madrid, principales motores económicos del país, también albergan los ecosistemas digitales más amplios y complejos, lo que los convierte en objetivos prioritarios para actores fraudulentos.

Asimismo, el hecho de que el resto de comunidades no hayan registrado casos no implica ausencia de fraude, sino posibles limitaciones en la capacidad de detección, menor actividad digital o una baja participación en la muestra.



GRAF. 3.2: Distribución geográfica del Fraude


Cataluña 37%

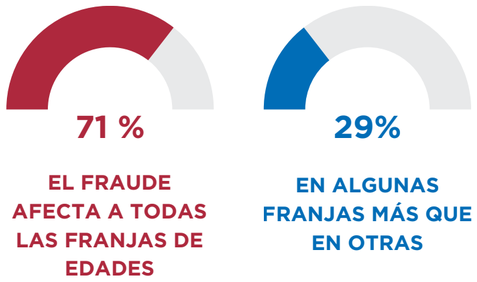

Comunidad de Madrid 26%


Comunidad Valenciana 16%


Adalucia 11%


Castilla La-Mancha y Galicia -5%

3.3 Distribución por edad



GRAF. 3.3: Franjas de edad afectadas

El **71%** de las empresas encuestadas considera que el fraude afecta **a todas las franjas de edad**, mientras que un **29%** detecta mayor incidencia en **algunos grupos concretos**.

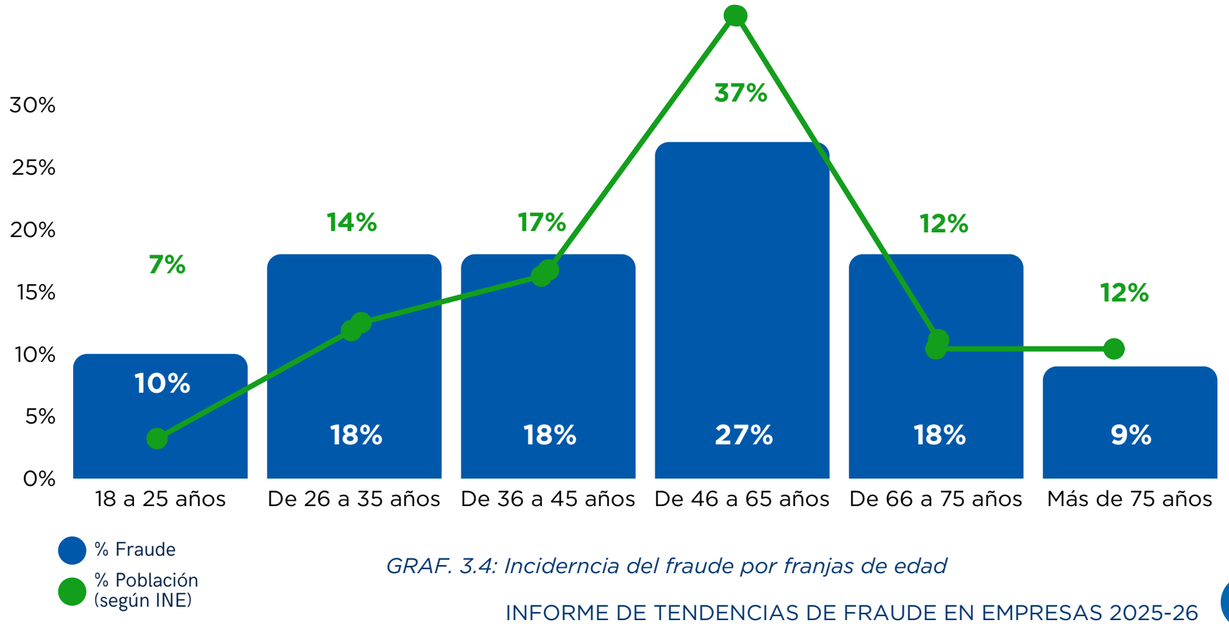
Analizando los datos obtenidos en cuanto a franjas de edad más afectadas por el fraude, el grupo de edad (46-65 años) es el más vulnerable según las empresas, seguido de cerca por personas de 26 a 45 años (36%). Llama la atención que los jóvenes (18 a 25 años) solo aparecen con un nivel de afectación percibida del 10%, mientras que las edades más maduras (de 66 años en adelante), suponen un 27% de los afectados.

La concentración del 63% en el tramo de 26 a 65 años suele explicarse por su alto grado de exposición operativa y digital tanto en su faceta vital como profesional. Esto les convierte en objetivos habituales de técnicas como phishing corporativo, fraude del CEO o ingeniería social avanzada.

«Cae la incidencia del fraude en menores de 35 años respecto al Informe 2024. Se observa una alineación entre % de edades y % de fraude de edades lo que puede significar una mejora en las estadísticas y una mayor educación digital.»

La baja incidencia declarada entre menores de 25 años y mayores de 75 no debe llevar a una conclusión errónea: puede deberse a menor presencia en operaciones económicas digitales, no a una menor vulnerabilidad real. De hecho, así lo confirman estudios como el "*Cybersecurity Report 2024*" de Kaspersky , que apunta que los jóvenes entre 18 y 30 años están más expuestos al fraude digital por confianza excesiva y falta de protocolos.

Respecto al informe del año anterior, los menores de 35 años representaban el 42% de la incidencia. La disminución al 27% en el actual informe refleja una mejora en prevención sobre los perfiles más jóvenes, quizás gracias a una mayor educación digital o a cambios en los vectores de ataque.

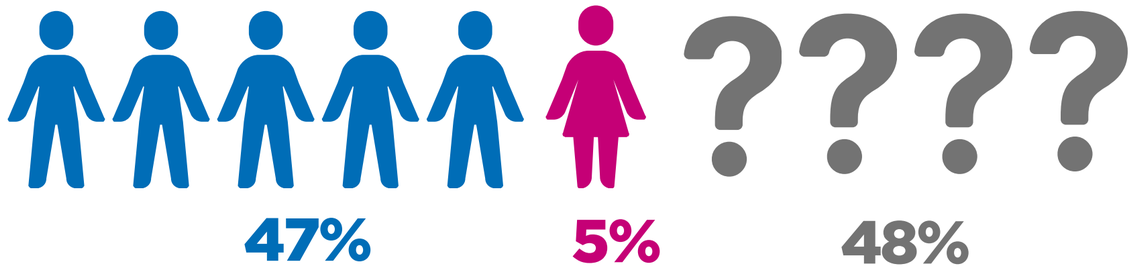


GRAF. 3.4: Incidernia del fraude por franjas de edad

3.4 Clasificación por Sexo

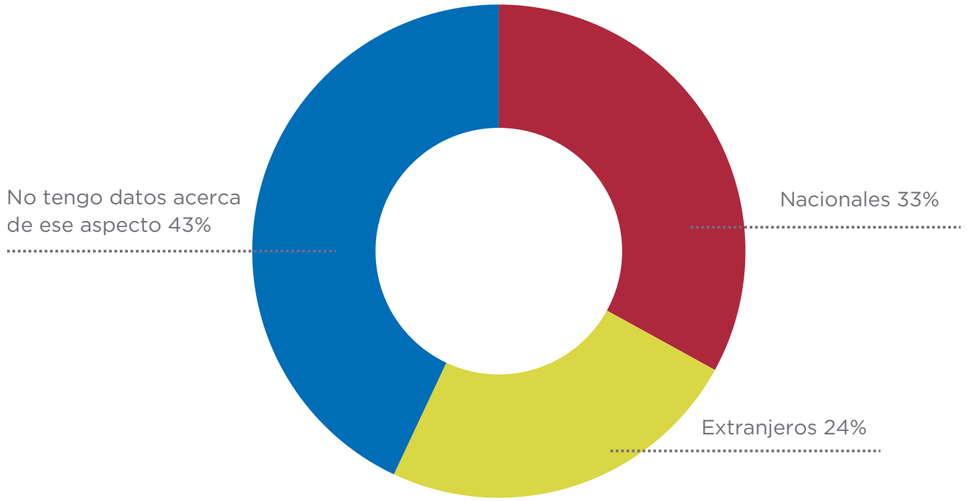
Los datos nos indican que casi la mitad de las empresas (48%) no dispone de información al respecto de esta cuestión. Las que si recogen esta información, opinan que el **47% de los fraudes afecta a hombres, y apenas un 5% a mujeres**.

La falta de datos limita una lectura concluyente, pero apunta a una posible mayor exposición de los hombres al fraude.



GRAF. 3.5: Clasificación por sexo

3.5 Nacionalidad del defraudador



GRAF. 3.6: Nacionalidad de defraudador

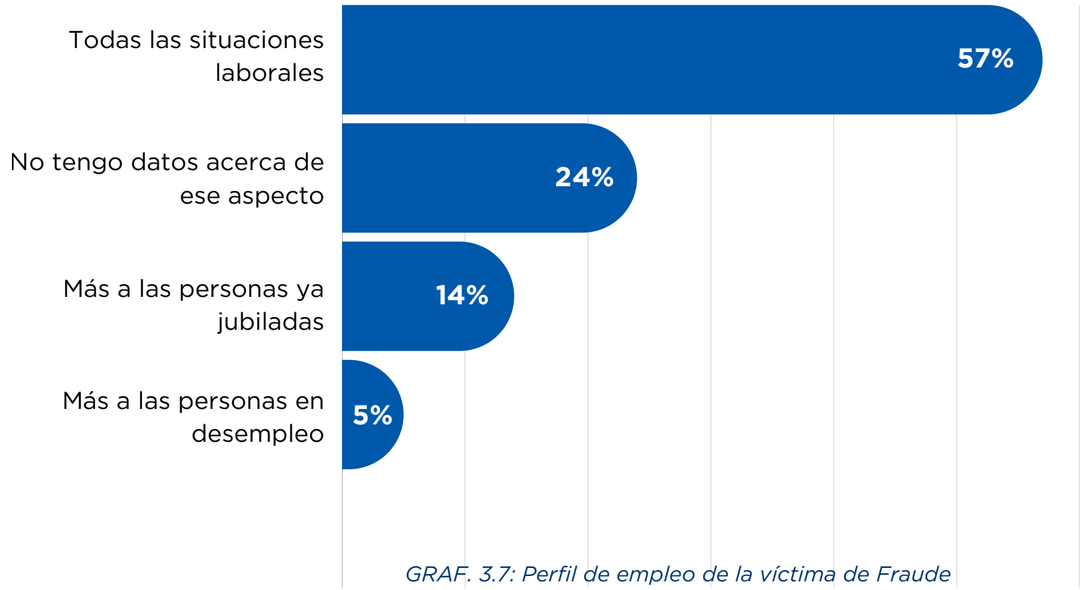
Un preocupante **43%** de los casos las empresas **no disponen de información** sobre la nacionalidad. Esto refleja una importante **brecha en la trazabilidad de los ataques**.

Las empresas que si disponen de información relativa a nacionalidad, afirman que el **33% de los defraudadores identificados son nacionales, mientras que el 24% son extranjeros**.

La falta de información sobre sexo, edad, nacionalidad y perfil en general del defraudador limita la capacidad de las empresas para reforzar sus estrategias antifraude, reduce la precisión de los sistemas de inteligencia artificial y dificulta la detección preventiva. Además, en un entorno donde el fraude internacional crece, no saber el origen del ataque y la ausencia de trazabilidad deja a las empresas más expuestas.

«Los datos del informe revelan que un porcentaje muy elevado de empresas desconoce información clave sobre el perfil del defraudador, como sexo (48%) o nacionalidad (43%).»

3.6 Perfil de empleo de la víctima de Fraude



GRAF. 3.7: Perfil de empleo de la víctima de Fraude

«El 57% de las empresas afirma que el fraude digital impacta en todas las situaciones laborales sin distinción.»

Un **57% de las empresas encuestadas afirma que cualquier perfil laboral puede ser víctima de fraude,** lo que refleja la transversalidad de este fenómeno. Este dato está **alineado con la evidencia internacional,** donde el fraude financiero y digital ha evolucionado para adaptarse a cualquier canal, perfil o situación.

Respecto al informe 2024, s**e observa una ligera caída del 61% al 57% en la percepción de que el fraude afecta por igual a todas las situaciones laborales**. Esto puede interpretarse como un avance hacia una segmentación más detallada del perfil de víctimas, pero también confirma que sigue sin haber un sistema maduro de análisis del perfil socio-laboral de los afectados.

El hecho de que un **14% destaque a las personas jubiladas como un grupo especialmente vulnerable** es coherente con los informes del Centro Europeo de Cibercrimen de Europol, que señalan un repunte del fraude digital dirigido a mayores, especialmente mediante técnicas de phishing emocional o fraudes de soporte técnico. Esta población tiende a tener menor alfabetización digital y, en muchos casos, gestiona sus finanzas de forma más conservadora, lo que la convierte en blanco de los defraudadores.

La mención a **autónomos y empleados de pymes (5%) también merece atención**: son colectivos menos protegidos, muchas veces sin departamentos de ciberseguridad o protocolos robustos, lo que los convierte en objetivo prioritario de fraudes como el BEC (Business Email Compromise) o fraudes de facturación.

Resulta llamativo que **ninguna empresa considere que las personas desempleadas sean más vulnerables**. Podría interpretarse como una falta de visibilidad sobre esta población, aunque desde el punto de vista operativo también puede deberse a que estas personas no interactúan tanto con canales de riesgo como lo haría un trabajador activo o jubilado.

Finalmente, **un 24% de las entidades reconoce no disponer de información sobre esta variable**. Este vacío informativo limita una vez más la capacidad de diseñar estrategias segmentadas y pone de relieve la necesidad de mejorar los mecanismos de análisis de perfiles de víctimas en las organizaciones.

BLOQUE III: PERCEPCIÓN DEL FRAUDE

3.7 Nivel de ingresos de las víctimas de Fraude

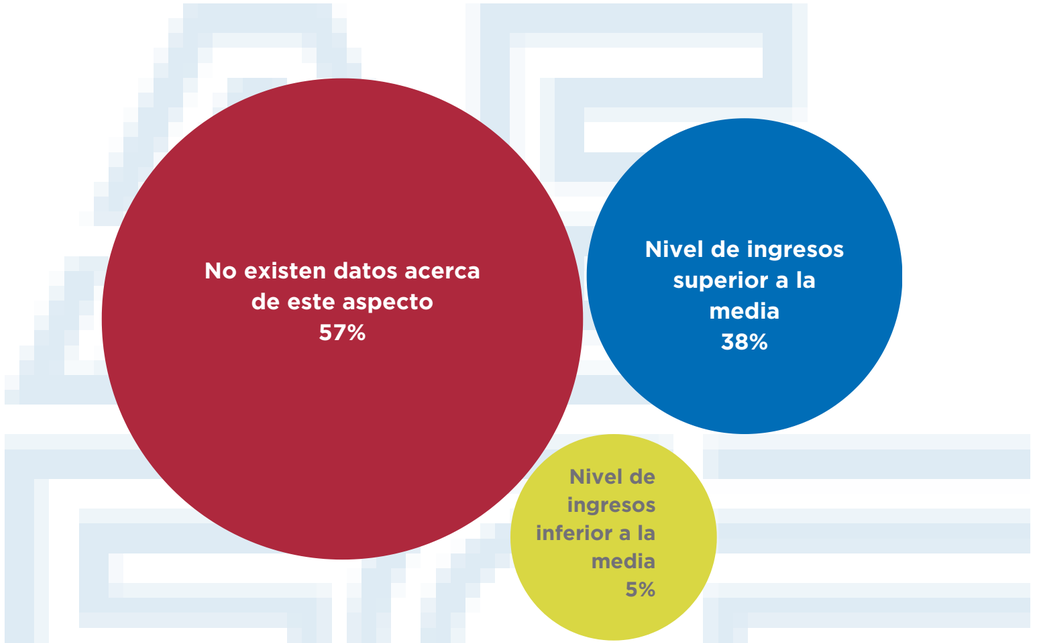
El dato más revelador es que el **57% de las empresas carece de información sobre el nivel de ingresos de las víctimas de fraude**, lo que representa una debilidad notable en el análisis del perfil de riesgo. En un entorno donde la hiperpersonalización y el análisis de datos son clave para la prevención, esta carencia limita el desarrollo de modelos predictivos efectivos y estrategias antifraude diferenciadas por perfil socioeconómico.

El segundo dato llamativo es que el **38% identifica como víctimas más frecuentes a personas con ingresos superiores a la media**, lo que contradice el estereotipo de que el fraude se concentra en los colectivos más vulnerables. Este resultado puede explicarse por mayor volumen de operaciones económicas y exposición en canales digitales o simplemente un perfil mas atractivo para fraudes dirigidos como phishing financiero, fraude de inversión o estafas de alto retorno.

Tan solo un 5% asocia el fraude con personas de bajos ingresos, lo que podría reflejar tanto un sesgo en la percepción como una menor trazabilidad de los casos entre estos colectivos. En el ámbito europeo, por ejemplo, la European Anti-Fraud Office (OLAF) ha destacado que las víctimas con ingresos más bajos pueden ser más propensas a fraudes como préstamos rápidos o suplantación en ayudas, aunque menos detectables por los sistemas financieros tradicionales.

«El 38% de las víctimas de fraude son personas con ingresos superiores a la media, según las empresas.»

Comparando con el informe 2024, donde un 69,57% de las entidades no disponía de información sobre los ingresos de las víctimas, se observa una mejora de más de 12 puntos porcentuales en el conocimiento sobre esta variable (ahora el 57%). Aunque el avance es positivo, sigue siendo mayoritario el desconocimiento, por lo que urge seguir impulsando una gestión más rica en datos sobre el perfil económico de los afectados.



GRAF. 3.8: Nivel de Ingresos de la víctima

3.8 Niveles formativos de las víctimas de Fraude

El **67%** de las empresas encuestadas coincide en que **el fraude no discrimina por nivel de formación**. Este dato pone de relieve una realidad cada vez más reconocida: la sofisticación de los ataques y las vulnerabilidades humanas, más allá del conocimiento académico. La ingeniería social, el phishing emocional o los fraudes tipo "CEO" se apoyan más en la confianza y en el engaño que en la ignorancia técnica.

No obstante, el **14%** señala que las personas con **menor nivel educativo son más vulnerables**. Este dato es consistente con investigaciones del **Instituto Nacional de Ciberseguridad (INCIBE)** y de organismos como la **ENISA**, que destacan una mayor incidencia de fraudes en colectivos con baja alfabetización digital, especialmente en estafas como falsas ofertas de empleo, fraudes en compraventa online o suplantaciones de identidad.

Por otro lado, ningún encuestado considera que las personas con formación superior estén más expuestas. Esto podría sugerir una percepción errónea o sesgo, ya que los profesionales con alta cualificación y acceso a sistemas críticos son objetivos prioritarios en fraudes como BEC (Business Email Compromise) o ataques dirigidos (spear phishing).

La **carencia de información** (**19%**) sigue siendo preocupante, aunque menor que en otras categorías analizadas. Aún así, **casi 1 de cada 5 organizaciones no monitoriza el nivel educativo de los afectados**, lo que impide diseñar campañas formativas o de concienciación realmente eficaces.

Comparado con el año anterior (2024), se mantiene estable la percepción de que el fraude afecta a todos los niveles educativos (65% vs. 67% actual). Lo que sí mejora ligeramente es el nivel de conocimiento, con una **reducción de 7 puntos porcentuales en el porcentaje de entidades** que no disponen de datos (de 26% a 19%), lo que apunta a un avance en esta caracterización concreta del perfil de las víctimas.

GRAF. 3.9: Niveles formativos de las víctimas de Fraude

BLOQUE IV

Evolución del Fraude

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

4.1 Intentos de fraude respecto a solicitudes

La mitad de las empresas encuestadas (**52%**) **reporta un aumento en los intentos de fraude**, lo que confirma la **tendencia creciente de presión delictiva en los entornos digitales corporativos**. Este dato está alineado con las cifras de organismos como INTERPOL y Europol, que alertan de un incremento constante en ciberestafas orientadas a empresas, especialmente mediante técnicas como el fraude de CEO, la suplantación de identidad o la manipulación de sistemas de pago.

El **43%** que no observa cambios aparentes no implica necesariamente una mejora. Que no se detecten más fraudes no significa que no existan más intentos, sino que podrían estar pasando desapercibidos ante herramientas obsoletas o mal calibradas.

Tan solo un **5%** indica haber **reducido los intentos**, una cifra anecdótica que probablemente se corresponda con sectores que han implementado recientemente **tecnologías avanzadas de verificación**, segmentación de clientes o inteligencia artificial aplicada a la prevención.

Los resultados refuerzan la necesidad urgente de mantener inversiones constantes en **herramientas de detección temprana**, formación del personal y estrategias de respuesta ante incidentes.

En comparación con el informe 2024, se aprecia una ligera mejora. El año pasado, **un 78% de las empresas afirmaba haber sufrido un incremento en los intentos de fraude**, mientras que este año **esa cifra desciende al 52%**, aumentando en paralelo el grupo que no detecta cambios (43% frente al 22% anterior). Esto podría indicar una cierta estabilización en algunos sectores o un efecto positivo de medidas antifraude implantadas recientemente.

«Cae 26 puntos el porcentaje de empresas que reporta un aumento de intentos de fraude en el último año.»

GRAF. 4.1: Intentos de fraude

4.2 Intentos de fraude bloquedos

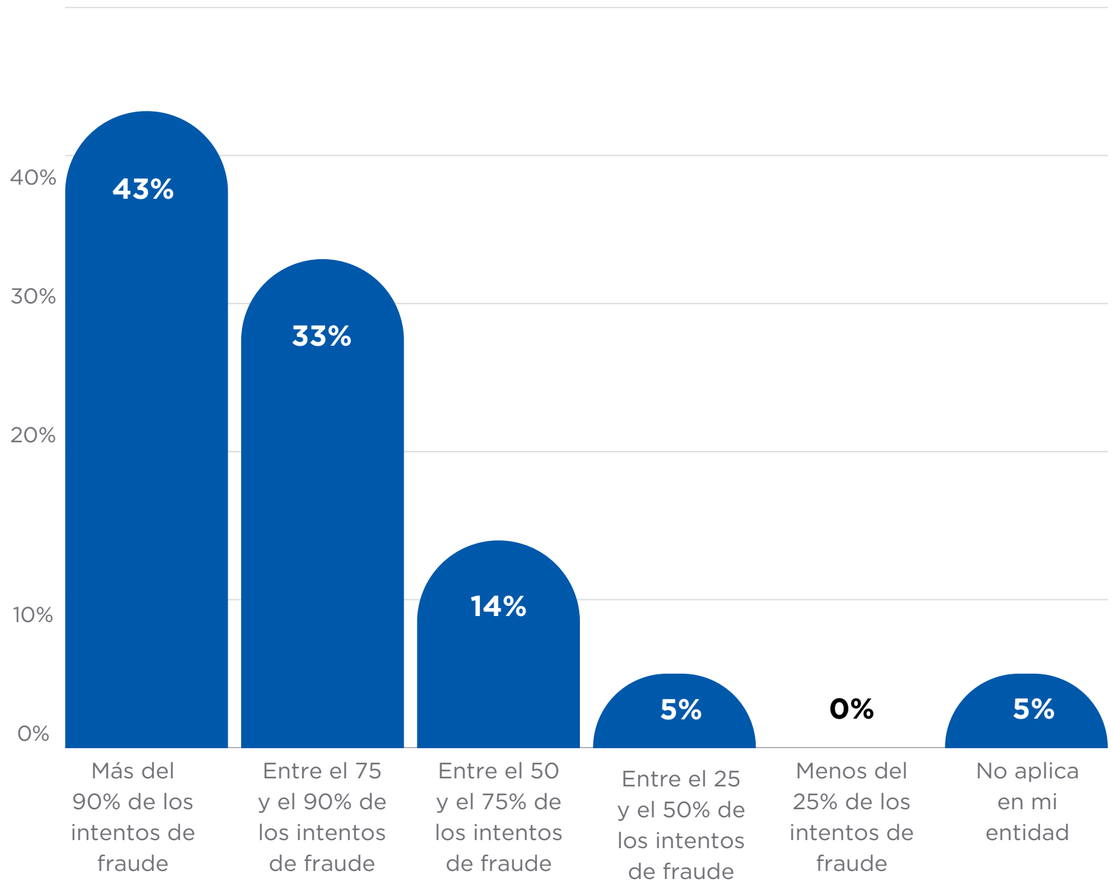
Los resultados muestran una percepción mayoritaria de alta eficacia en la contención del fraude. De hecho, el **76%** de las empresas c**ree estar bloqueando al menos el 75% de los intentos de fraude,** lo que sugiere la existencia de **s**istemas de defensa bien implantados, como herramientas de scoring, validación documental automatizada o machine learning aplicado a la prevención.

Sin embargo, este alto grado de confianza debe leerse con cautela. Estudios recientes de entidades como *Forrester Research* o el *Informe de Fraud Management* de Experian 2024 alertan sobre una falsa sensación de control cuando no se actualizan los indicadores clave de rendimiento (KPIs) ni se revisan los patrones de fraude emergente. Es decir, las cifras de efectividad pueden estar infladas por la detección de fraudes ya conocidos, sin considerar la sofisticación creciente de nuevas modalidades.

El **14%** que sitúa su **ratio de éxito entre el 50%-75%** aún se encuentra en un rango aceptable, pero señala áreas de mejora, posiblemente ligadas a procesos menos automatizados o falta de interoperabilidad entre herramientas antifraude.

Tan solo un **5%** indica bloquear entre el **25% y el 50%** de los intentos, lo cual representa una situación crítica que podría poner en riesgo tanto los activos económicos como la reputación de la empresa, especialmente si se trata de sectores con alto volumen de operaciones digitales.

«El 76% de las empresas asegura bloquear más del 75% de los intentos de fraude.»



GRAF. 4.2: Porcentaje de intentos de fraude bloqueados

4.3 Incrementos de casos de fraude

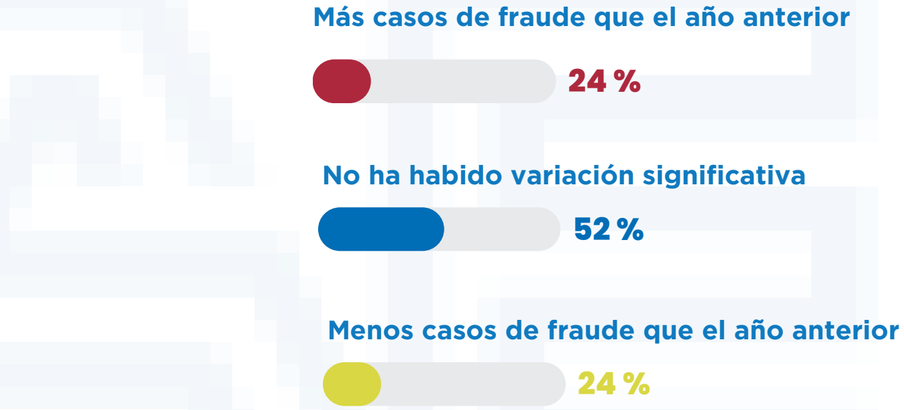
A diferencia de la percepción sobre los intentos de fraude, en este caso los datos apuntan a una cierta **estabilidad**: **más de la mitad de las empresas (52%) no perciben un cambio relevante en el volumen de fraudes consumados**. El resto de respuestas está dividido de forma equitativa entre quienes han visto aumentar los casos y quienes reportan una mejora.

Esta lectura es ambivalente. Por un lado, puede interpretarse como una **señal positiva**: el fraude detectado no está creciendo en la mayoría de las organizaciones, lo que podría indicar una mayor capacidad de disuasión y control. Por otro lado, también puede reflejar una **meseta peligrosa**, donde las empresas se están adaptando al nivel actual de fraude sin lograr reducirlo estructuralmente.

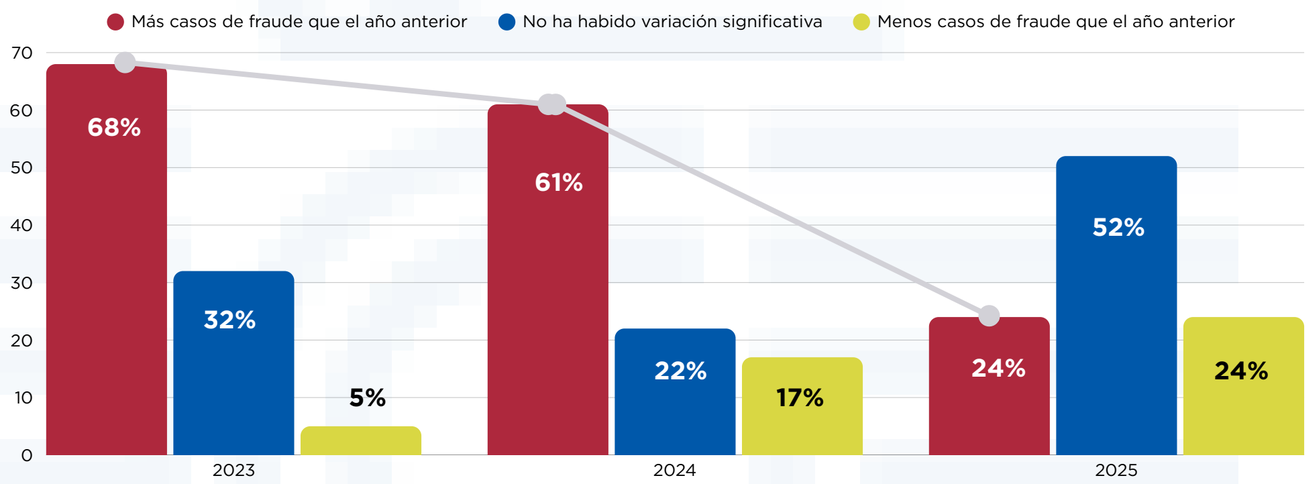
El **24%** que declara haber registrado más casos evidencia que el **riesgo sigue presente y activo**. Es probable que en estas organizaciones los defraudadores hayan encontrado nuevos vectores de ataque o que las medidas de control no hayan evolucionado con la misma rapidez que las amenazas.

Otro **24%** reporta una disminución, lo que muestra que algunas compañías sí han conseguido resultados tangibles, posiblemente mediante la **automatización del fraude scoring, implementación de herramientas basadas en IA o capacitación continua al personal.**

En el informe 2024, un **61% de las empresas afirmaba haber sufrido un aumento de casos consumados**, mientras que ahora solo el 24% mantiene esa percepción. Es decir, hay una caída de 37 puntos porcentuales, lo que indica una **mejora clara en la contención del fraude efectivo respecto al ejercicio anterior.**



GRAF. 4.3: Incrementos de casos de fraude 2025



GRAF. 4.4: Incrementos de casos de fraude - Evolución anual

«El fraude consumado se contiene: solo el 24% de las empresas percibe un aumento, frente al 61% del año anterior.»

4.4 Casos de Fraude Consumados

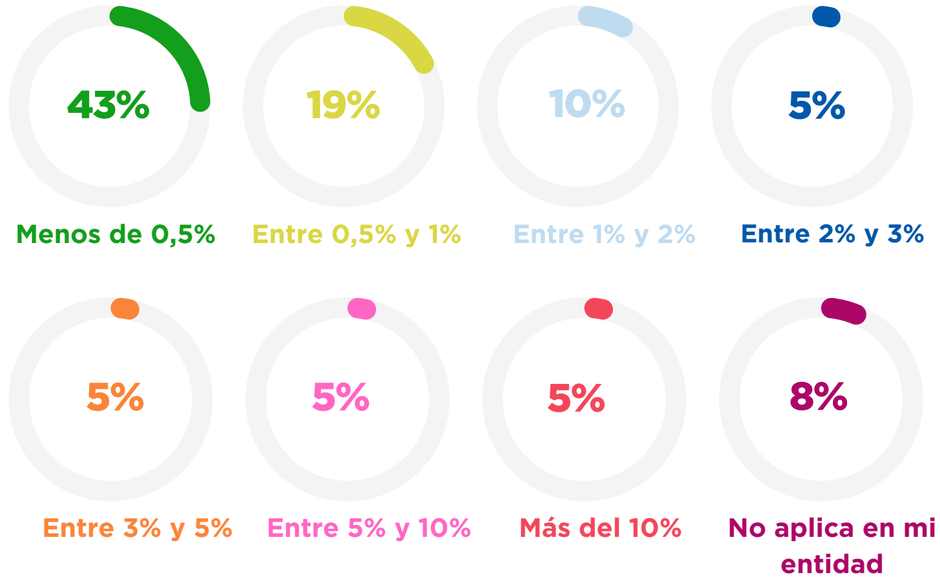
Los datos muestran que **una amplia mayoría (62%) de las empresas logra contener el fraude consumado por debajo del 1%** de los intentos, lo que refleja un elevado nivel de madurez en los controles antifraude en un número significativo de organizaciones. Especialmente relevante es el hecho de que el **43%** logra mantener esta tasa por debajo incluso del 0,5%.

Este resultado es coherente con el auge de soluciones de verificación de identidad reforzada, inteligencia artificial aplicada a la detección de anomalías y herramientas de prevención basadas en comportamiento.

No obstante, un **20%** de las empresas se encuentra en **niveles de fraude consumado superiores al 2%,** y un **5%** reconoce **superar el 10%**, lo que **pone de relieve vulnerabilidades críticas** en sus modelos de defensa. Estas cifras no solo representan un riesgo económico, sino que también pueden tener un impacto reputacional severo, especialmente en sectores regulados como banca, seguros o telecomunicaciones.

El **10%** que declara que esta métrica "no aplica" puede incluir entidades que no cuentan con la capacidad de medir esta ratio, lo cual plantea también una alerta sobre **madurez analítica e implementación de KPIs clave.**

En el estudio de 2024, el **52,17%** de las empresas situaba su nivel de fraude consumado por debajo del 1%. En la edición actual, la suma de los tramos "menos del 0,5%" (43%) y "entre 0,5% y 1%" (19%) es de un total del **62%**, lo que representa una **mejora de 10 puntos porcentuales**. Esto confirma una evolución positiva en la capacidad de contención del fraude, posiblemente impulsada por una mayor inversión en tecnologías antifraude y formación interna.



GRAF. 4.5: Casos de Fraude Consumados

«El 62% de las empresas logra contener el fraude por debajo del 1% de los intentos.»

4.5 Pérdidas económicas a causa del Fraude

GRAF. 4.6: Pérdidas económicas a causa del Fraude vs Año anterior

«Solo el 28% de las empresas reporta más pérdidas por fraude que el año pasado, frente al 52% del año anterior.»

Los resultados revelan un escenario equilibrado: mientras una parte de las empresas (29%) ha logrado reducir sus pérdidas económicas derivadas del fraude, otra proporción idéntica ha sufrido un aumento. La mayoría (43%) no ha experimentado cambios relevantes.

Este escenario sigue reflejando el enfrentamiento entre **la mejora en la prevención tecnológica** y los controles de admisión, con la **persistencia de ataques más sofisticados y dirigidos** que logran esquivar barreras en empresas con menor resiliencia o capacidad de respuesta.

En el informe de 2024, **el 52,17% de las empresas reportó más pérdidas económicas que el año anterior**. Este año, esa cifra se ha reducido significativamente a **28%**, lo que representa una **mejora de 22 puntos porcentuales**. Al mismo tiempo, las entidades que han logrado reducir sus pérdidas han aumentado del 17,39% al 29%, lo que indica una tendencia positiva hacia una mayor contención del impacto económico del fraude.

La reducción de pérdidas en casi un tercio de las empresas, puede estar relacionado con **la integración de soluciones de machine learning, autenticación reforzada y segmentación de clientes por riesgo**. También podrían influir campañas de concienciación interna o una mayor inversión en vigilancia transaccional.

Por el contrario, el **28%** que informa de **más pérdidas** evidencia claramente la necesidad de reforzar su postura antifraude.

BLOQUE V

Canales del Fraude

AEECF
ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

5.1 Canales de fraude

El canal **digital directo** sigue siendo, con diferencia, el entorno más explotado por los defraudadores (**44%**). Este dato confirma una tendencia ya consolidada en el ecosistema del fraude: los canales online, especialmente los accesos no mediados por terceros, son el terreno ideal para ejecutar ataques como suplantaciones de identidad, fraudes de suscripción, robo de credenciales y simulaciones de usuarios legítimos (identity takeover). Este dato permanece en la misma línea que el informe 2024, donde el **canal online** (**43,59%**) también encabezaba el ranking.

El **25%** correspondiente al **prescriptor online** indica que los fraudes también se originan a través de intermediarios digitales, como agregadores de productos financieros, comparadores o afiliados. Aquí se pueden dar manipulaciones en los procesos de alta, suplantaciones o uso de datos falsificados para generar leads fraudulentos. La trazabilidad y autenticación en este entorno suelen ser más limitadas, lo que aumenta el riesgo.

El hecho de que el **canal telefónico siga representando el 16%** de los casos muestra que el fraude no es exclusivamente digital. El uso de técnicas como el **vishing** o las llamadas falsas de soporte técnico siguen siendo eficaces, especialmente en colectivos menos digitalizados o ante personal con poca formación en verificación segura. Finalmente, el **15%** asociado a **prescriptores presenciales** o **sucursales** revela que, aunque menos frecuente, el fraude también tiene lugar en entornos físicos o híbridos, particularmente donde existen procesos de verificación manual que pueden ser manipulables o carecer de controles de autenticación robusta.

GRAF. 5.1: Canales de fraude

«El 44% de los fraudes se produce por el canal directo online, consolidando de nuevo su liderazgo como vía de ataque.»

5.2 Distribución entre tipologías de clientes

Los dos fraudes mas comunes detectados son Cliente nuevo- persona física y por primera vez aparece el de suplantación de identidad sobre cliente conocido. Se observa un **mayor impacto respecto a nuevo cliente persona jurídica** o **suplantación de identidad** sobre cliente conocido respecto a años anteriores, lo que sugiere una **mejora en las políticas antifraude** en este tipo de clientes.

Con un **47%** de menciones como **frecuente o muy frecuente**, el fraude en **cliente nuevo-persona física** mantiene su posición como **la más vulnerable al fraude**, repitiendo el patrón observado en ediciones anteriores. El onboarding sigue siendo el "talón de Aquiles" en la estrategia antifraude, especialmente cuando no se aplica una verificación de identidad robusta y automatizada.

Un preocupante **38%** de las organizaciones declaran sufrir **suplantación de identidad sobre cliente conocido** con alta frecuencia. Esto refuerza la tendencia detectada en 2024, pero con un ligero incremento, lo que evidencia que los ataques sobre clientes reales (mediante phishing o filtraciones de datos) están creciendo.

Los datos refuerzan una tendencia ya apuntada por informes como el de TransUnion ("*Global Digital Fraud Trends 2024*"), que alerta del creciente protagonismo de los fraudes sobre cuentas legítimas como el principal vector de ataque, especialmente en sectores como telecomunicaciones y servicios financieros. Este informe indica que el **52%** del fraude se produce ya con **identidades reales**, especialmente cuando estas han sido previamente verificadas, lo que se alinea con el riesgo creciente en los casos de suplantación y fraude sobre clientes ya existentes.

Los intentos de fraude dirigidos a clientes persona jurídica, tanto nuevos como conocidos, se perciben como significativamente menos frecuentes en comparación con los perfiles de persona física. En concreto, solo el **10% de los fraudes en nuevos clientes jurídicos son considerados frecuentes, y apenas un 5% en clientes jurídicos ya conocidos.**

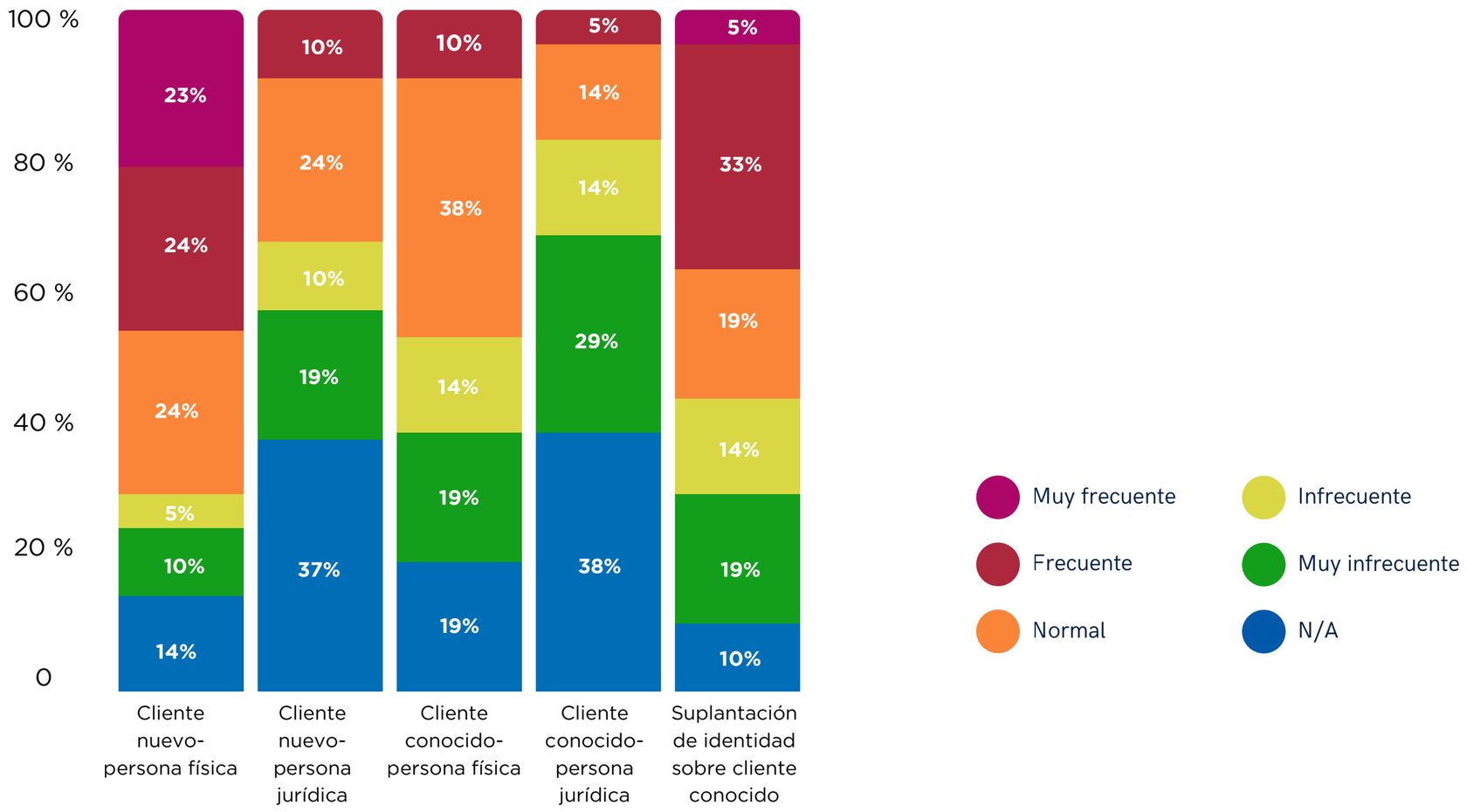
Comparando con la edición anterior del Informe de Fraude en empresas de la AEECF, se observa poca variación en los perfiles más vulnerables:

- El **fraude al cliente nuevo (persona física)** sigue siendo el más repetido, aunque baja del 83% (en 2024) a un 72% en 2025 (de "normal" a "muy frecuente"). Es una caída notable que podría explicarse por una mayor diversificación de vectores o bien una mejora en prevención.
- La **suplantación de clientes conocidos** se incrementa ligeramente respecto al informe anterior, reforzando la urgencia de adoptar herramientas de detección de anomalías post-onboarding.

El fraude sigue entrando principalmente por la puerta del onboarding, especialmente cuando se trata de clientes nuevos y sin historial previo. Pero el incremento de la suplantación de clientes legítimos alerta de un fenómeno en alza: la explotación de la confianza y de brechas de seguridad externas como vía para el fraude interno.

«El 72% del fraude se sigue concentrando en nuevos clientes-persona física: el onboarding digital, principal vector de ataque.»

5.2 Distribución entre tipologías de clientes



GRAF. 5.2: Distribución entre tipologías de clientes

5.3 Denuncias casos fraude

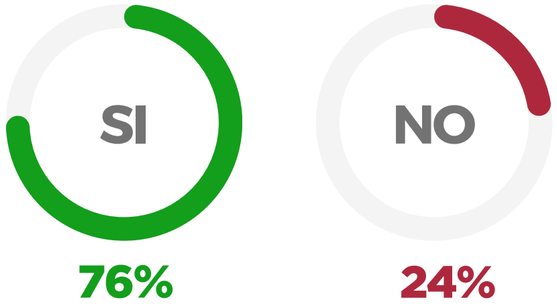
El dato de que **tres de cada cuatro empresas afirmen denunciar los intentos de fraude** refleja una evolución positiva en la concienciación y en la asunción de un rol activo frente al delito digital. No obstante, que el **24% no denuncie**, sigue siendo una cifra preocupante.

Pero aunque un **76%** de las empresas declara que **sí denuncia**, este dato se matiza considerablemente cuando observamos que el **69%** de las organizaciones denuncia menos de una cuarta parte de los fraudes que detecta.

Este resultado deja entrever un fenómeno conocido como **"subdenuncia estructural"**. Es decir, aunque las empresas tienen políticas de denuncia, en la práctica solo se activan para fraudes más graves, complejos o económicamente relevantes. Se prioriza el coste/beneficio de la denuncia, dejando fuera intentos frustrados o de escasa cuantía.

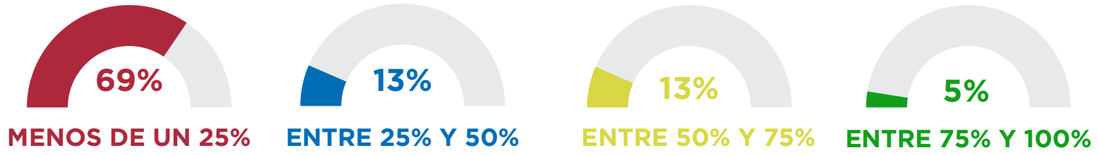
Que solo un **5%** de las empresas llegue a denunciar **más del 75% de los casos** demuestra lo lejos que estamos de una cultura de tolerancia cero frente al fraude. Esto debería impulsarse desde la regulación sectorial, la incentivación fiscal, o incluso la reputación positiva para las empresas colaboradoras.

Mientras no sea una práctica extendida, seguiremos incurriendo en **infrarepresentación del fenómeno del fraude** en los datos oficiales, pérdida de inteligencia compartida y habrá una mayor sensación de impunidad para los defraudadores.



GRAF. 5.3: ¿Se denunciam los intentos de fraude?

«Solo el 6% de las compañías denuncia de forma sistemática más del 75% de los casos de fraude.»



GRAF. 5.4: Porcentaje de casos que se denuncian

BLOQUE V: CANALES DEL FRAUDE

5.4 Donde se denuncia el fraude

En el presente estudio, el **100%** de las empresas declaran que **sus denuncias son canalizadas exclusivamente a través de las Fuerzas de Seguridad del Estado**, reflejando una fuerte **dependencia del canal policial tradicional** para formalizar las incidencias de fraude. El uso del I**NCIBE baja del 4% a 0% respecto al año anterior**, lo cual indica una regresión en su presencia como canal empresarial.

Este comportamiento tiene dos lecturas principales:

1. **Confianza institucional y operativa en cuerpos especializados** como la Unidad Central de Ciberdelincuencia de la Policía Nacional o el Grupo de Delitos Telemáticos de la Guardia Civil.
2. **Desconocimiento o infrautilización de canales alternativos**, como el servicio de asesoramiento y derivación del INCIBE a través del número 017, que sigue sin penetrar en el entorno empresarial a pesar de sus esfuerzos de visibilidad.

Este sesgo en los canales también puede indicar una **visión reactiva del fraude,** donde solo se actúa cuando ya hay un delito consumado o una pérdida evidente, y no en etapas tempranas o preventivas.

El INCIBE, por su parte, estaría desaprovechado como **herramienta de apoyo técnico, prevención y asesoramiento legal,** sobre todo en casos donde las empresas dudan si formalizar la denuncia o cómo proceder ante un ataque no consumado.

En conclusión, aunque el aumento de denuncias policiales es positivo, **la falta de diversificación de canales debilita la estrategia global de respuesta al fraude**. La empresa necesita combinar denuncia formal, soporte técnico preventivo (como ofrece INCIBE), y circuitos internos de respuesta rápida. Pero el escenario español aún está lejos de ese modelo híbrido y coordinado.

Denunciar no solo es un deber legal y ético, sino una acción estratégica que **fortalece el ecosistema de inteligencia colectiva**, permite alertar a otras organizaciones y facilita la actuación de cuerpos policiales y entidades públicas. Las denuncias también son fundamentales para alimentar bases de datos compartidas y sistemas de scoring antifraude basados en machine learning.

Las razones más frecuentes suelen estar relacionadas con dificultad o burocracia del proceso de denuncia, falta de certeza jurídica sobre la viabilidad de perseguir el intento, subestimación del impacto potencial del fraude o temor reputacional.

Esta actitud puede tener un efecto contraproducente: normalizar el fraude como un “coste asumido del negocio”, lo que daría margen a los defraudadores para actuar con mayor flexibilidad.

5.5 Tipos de fraude

Los fraudes más prevalentes en 2025 siguen claramente ligados al entorno digital. El **fraude de suscripción online** lidera el ranking (**20%**), lo cual se asocia a un crecimiento en la contratación digital de productos y servicios sin verificación presencial robusta.

Esto favorece el uso de identidades robadas o manipuladas, especialmente en sectores como telecomunicaciones, seguros o banca minorista. Respecto al estudio del 2024, se registra una subida de 3 puntos en 2025 (del 17% al 20%).

Le siguen muy de cerca dos grandes amenazas estructurales:

- **El robo de datos mediante malware o ingeniería social** (**18%**), fenómeno que sigue escalando con la expansión del ransomware, keyloggers o las campañas de phishing.
- **El uso fraudulento de tarjetas** (**17%**), que refleja una combinación de carding, clonaciones y compras no autorizadas en e-commerce.

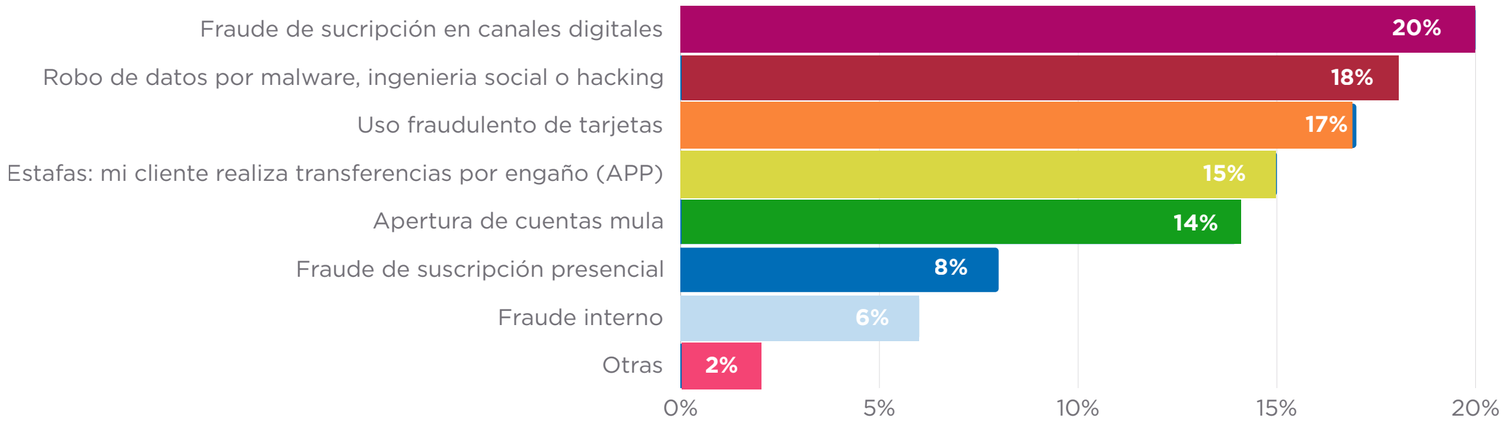
Un **15%** de los fraudes son del tipo **APP** (Authorized Push Payment), donde el propio cliente realiza la transferencia por engaño, lo que muestra que el eslabón humano sigue siendo el más débil del sistema.

La **apertura de cuentas mula** (**14%**) también se mantiene como un riesgo relevante, clave en esquemas de blanqueo de capitales y fraudes interbancarios. Este tipo de fraude afecta especialmente a entidades financieras y plataformas de pago que aún no han robustecido sus procesos de onboarding.

Los fraudes de **suscripción presencial** (**8%**) han perdido peso relativo, desplazados por los canales digitales, mientras que el fraude interno desciende respecto al año anterior 7 puntos (del 13% al 6%) pero continúa siendo una amenaza latente.

«1 de cada 5 empresas sufre suscripciones falsas en canales online.»

«Las Estafas (App) aparecen este año como de los fraudes mas destacados.»



GRAF. 5.5: Tipos de fraude

5.6 Frecuencia de los tipos de fraude

Los datos recabados este año confirman que las organizaciones no se enfrentan a un único tipo de fraude dominante, sino a un ecosistema híbrido de amenazas donde confluyen tanto técnicas tradicionales (como la manipulación documental) como ataques más avanzados basados en ingeniería social o robo de credenciales digitales.

El ranking de 2025 considerando las tipologías más frecuentes (frecuente+muy frecuente) confirma una continuidad respecto al informe de 2024, aunque con algunos matices importantes en la evolución:

- **Manipulación de documentos de identidad: 57%**
- **Suplantación de identidad: 48%**
- **Identidad inventada en fraude online (fraude sintético): 48%**
- **Cuentas manipuladas o simuladas: 43%**
- **Manipulación de documentos de ingresos (nómina, IRPF, etc.): 43%**
- **Robo de datos por malware o phishing: 38%**

En 2024, la **suplantación de identidad y la manipulación de documentos** ya lideraban el listado de fraudes frecuentes, pero en 2025 este último se consolida ya como el más extendido (24% muy frecuente y 33% frecuente). Esto sugiere que, pese al avance en herramientas antifraude documentales, los atacantes siguen encontrando fisuras, especialmente en procesos no automatizados o con revisión manual.

El **fraude sintético** (identidad inventada) registra un ligero repunte respecto a 2024, y ya un **29%** lo califica como muy frecuente. Esta técnica es especialmente peligrosa por su capacidad de pasar desapercibida en validaciones tradicionales, al no corresponder a una identidad previamente registrada como fraudulenta.

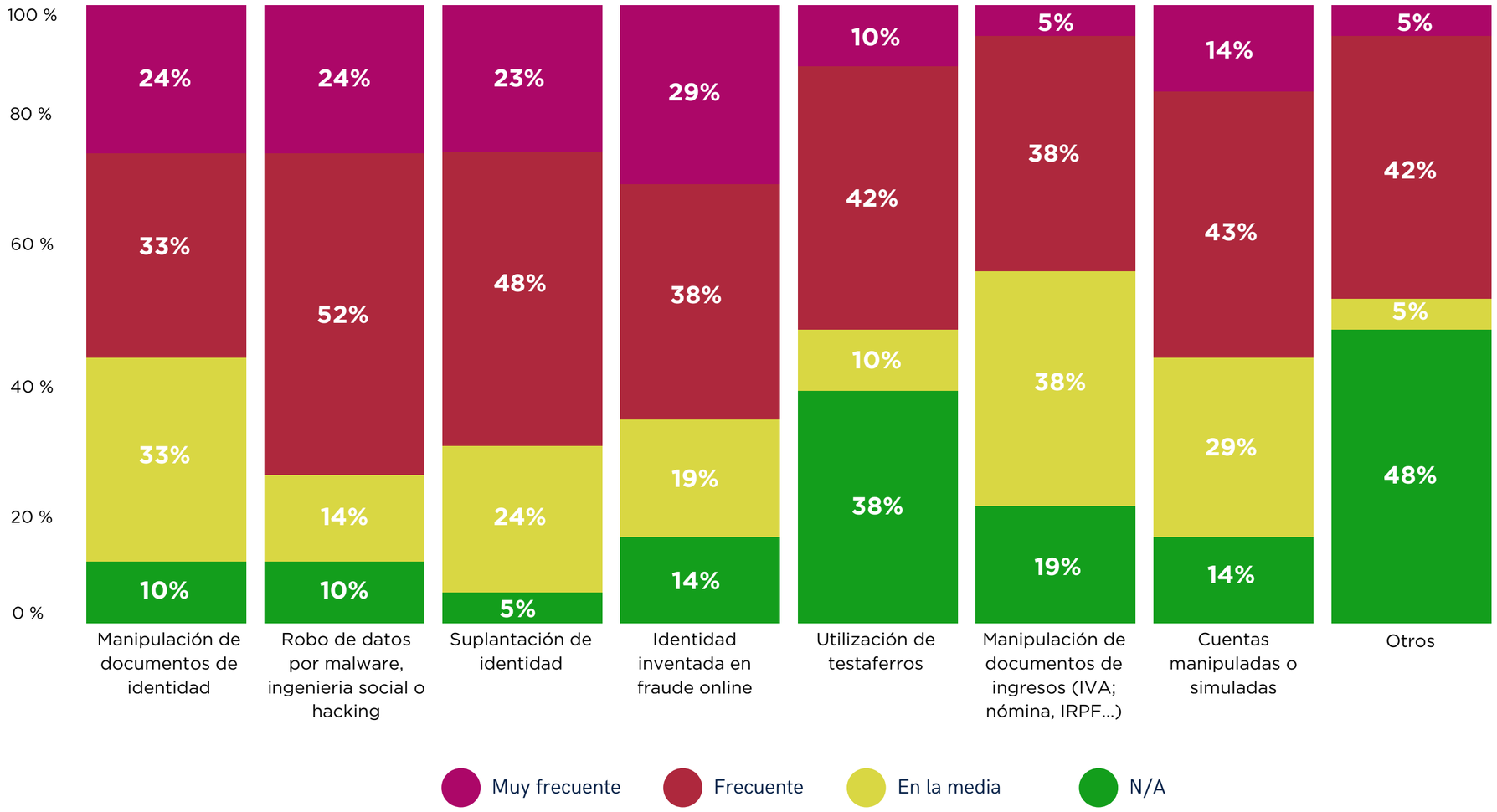
En cuanto al **robo de datos por malware o ingeniería social**, aunque la cifra de “muy frecuente” se mantiene en un **24%**, un significativo **52%** lo sitúa en un nivel medio. Esto sugiere que las entidades son conscientes del riesgo constante de estas intrusiones, pero en muchos casos no detectan su impacto hasta que se produce un fraude derivado (suplantación, acceso indebido, manipulación).

La utilización de **testaferros** baja significativamente en menciones. Un **38%** afirma no haber sufrido este tipo de fraude, y apenas un **10%** lo considera frecuente. Esta caída, ya iniciada en 2024, refleja un cambio en las tácticas de los defraudadores, que prefieren técnicas más difíciles de rastrear o más digitalizadas.

Los fraudes internos o de alta sofisticación (como suplantación de proveedores, desvío de pagos o fraude BEC) pueden quedar diluidos en esta categorización. Como ya advertimos en el informe 2024, su baja mención no implica menor riesgo, sino una mayor dificultad para ser correctamente identificados o atribuidos como fraude externo.

«La suplantación de identidad es una tendencia en auge que se ha intensificado en los últimos años..»

5.6 Frecuencia de los tipos de fraude



GRAF. 5.6: Frecuencia de los tipos de fraude

5.7 Importe medio fraudes

Acceso a cuentas de cliente existente por robo de datos, ingeniería social o hacking

El **importe medio se sitúa de 2.000 a 3.000 euros**, lo que sugiere casos de menor cuantía, pero con alta incidencia y frecuencia.

Destacar que algunas **entidades afirman desconocer el importe o no aportan datos**, lo que pone de manifiesto una **falta de trazabilidad o control centralizado del impacto económico del fraude.**

El hecho de que **no todas las organizaciones disponen de métricas consolidadas ni de cuadros de mando específicos para monitorizar el fraude digital, es una constante que observamos en otras categorías o productos de este informe.**

Fraudes por cuentas mula

Las respuestas obtenidas para este tipo de fraude oscilan entre los **1.750 y los 9.000 euros**, lo que sugiere que **aunque el impacto por incidente no es elevado**, se trata de un fraude **altamente distribuido y utilizado como infraestructura para fraudes mayores** (recepción de fondos ilícitos, blanqueo, etc.).

Los **importes medios son muy dispares**, lo que señala una falta. de homogeneidad a la hora de valorar este fraude entre las entidades financieras.

Algunas entidades afirman no conocer el dato o no disponer de él, una señal que refuerza la **necesidad de mejorar la trazabilidad y seguimiento de fraudes facilitadores o intermedios.**

Este tipo de fraude, por su bajo umbral económico pero alto volumen potencial, **requiere medidas preventivas automatizadas y una vigilancia basada en patrones transaccionales.**

Solicitud financiación de terminales

El **importe medio declarado oscila entre 500 euros y 1000 euros**. Hay que señalar que afecta a entidades con grandes volúmenes de financiación por lo que los importes agregados suponen varios millones de euros al año.

Algunas entidades **no aportan datos o desconocen. el importe medio**, reflejando una falta de trazabilidad o control centralizado del impacto económico. de este fraude:

Este tipo de financiación (móvil, tabletas, dispositivos electrónicos) ha sido uno de los canales más utilizados por los defraudadores en Europa, especialmente en esquemas de suplantación masiva, según reportes recientes de la European Payments.

Adquisición de vehículos

La mayoría de respuestas sitúan el impacto económico medio entre los **16.700 y 30.000 euros**, siendo los **20.000 euros** el valor más repetido. Este patrón sugiere que se trata de fraudes de ticket alto y generalmente únicos o puntuales, vinculados a operaciones de financiación o leasing.

Sin embargo, algunas **entidades indican no dispone del dato o no realiza seguimiento específico**, lo que vuelve a señalar **carencias en la medición granular del fraude por canal o producto.**

Financiación al consumo

Los importes declarados muestran **una notable homogeneidad**, con valores que se sitúan entre los **1.300 y los 2.000 euros** por incidente. Este rango es coherente con el perfil típico del fraude en financiación al consumo, que suele centrarse en importes bajos para evitar alertas y facilitar la repetición del delito.

Algunas entidades no realizan un seguimiento específico del importe medio del fraude de Financiación al consumo, lo que indica la necesidad **la necesidad de mejorar la visibilidad y el seguimiento del fraude por producto.**

El patrón detectado sugiere que este tipo de fraude **se apoya en volumen, no en importes individuales elevados**, lo que exige **mecanismos automatizados de detección temprana** y validación reforzada en la fase de onboarding y scoring crediticio.

Solicitud de prestamos personales

El rango de respuestas cuantificadas se sitúa entre **5.000 y 30.000 euros**. La media estimada a partir de los datos proporcionados es de **17.700 euros por incidente**.

Comparado con el informe de 2024, donde los importes medios se situaban por debajo de los 12.000€, se observa un **aumento sustancial**, lo que refuerza la necesidad de endurecer controles previos y análisis antifraude en la concesión de préstamos.

5.7 Importe medio fraudes

Solicitud de tarjeta de credito

Las respuestas recibidas reflejan importes homogéneos, con valores entre los **1.000 y 1.500 euros**, lo que arroja una media estimada de **1.250 euros por caso de fraude.**

Este dato está en línea con lo observado en el informe anterior (2024), lo que sugiere una estabilidad en el nivel económico de este tipo de fraude. Sin embargo, su baja cuantía individual no debe restar importancia, ya que su recurrencia y facilidad de ejecución pueden convertirlo en una vía recurrente para defraudadores.

Estos ataques suelen ir acompañados de **suplantación de identidad y uso de documentación falsa o robada**, por lo que el refuerzo en los procesos de onboarding y scoring es clave.

Transferencias autorizadas por engaño (App)

En el caso del fraude por **transferencias autorizadas por engaño (APP)**, los importes reportados oscilan entre **2.250 y 15.000 euros**, con una media aproximada situada en torno a los **6.800 euros por incidente**.

Respecto al informe 2024, se **observa un ligero incremento en el importe medio reportado**, lo que puede asociarse al creciente perfeccionamiento de los engaños y a una mayor confianza del defraudador en que la operación no será revertida.

Hay que señalar que **esta tipología de fraude es la que mas ha subido en 2025**, según los señalado en el apartado 5.5 tipos de fraude de este informe.

Uso fraudulento de tarjetas

En este tipo de fraude, el importe medio reportado es de **570 euros por caso**, si bien en algunas entidades se reportan importes medios de hasta 2.000. euros..

Este patrón es coherente con la **naturaleza frecuente pero de bajo impacto económico** del fraude con tarjetas, donde el daño suele estar acotado a operaciones limitadas por importes medios o pequeños antes de que el cliente o la entidad bloquee la tarjeta.

Comparado con el informe 2024, la media se mantiene estable, lo que sugiere una cierta contención de este tipo de fraude, probablemente favorecida por la implantación generalizada de **tecnologías como la tokenización, 3D Secure y autenticación reforzada .**

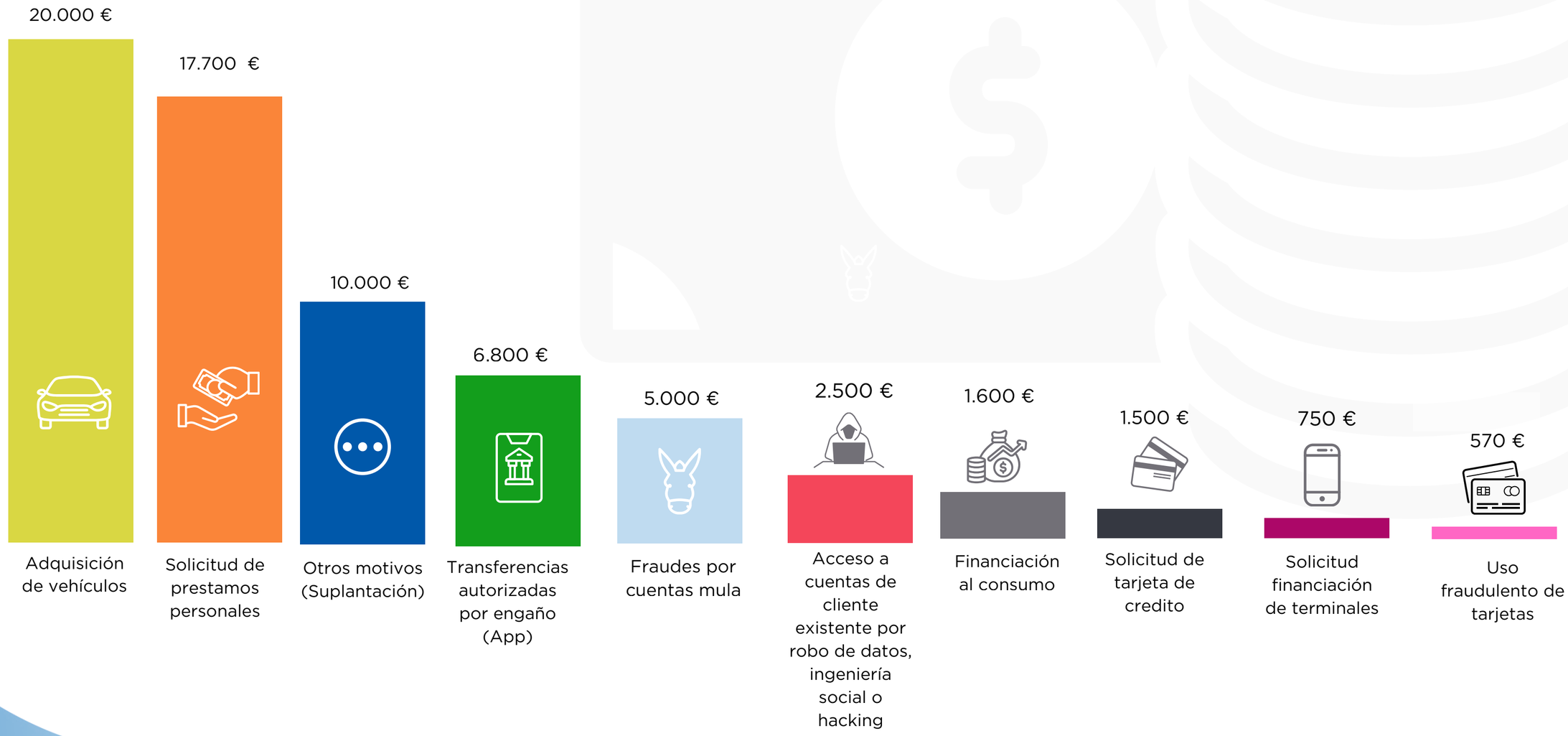
Otros motivos

Se han indicado. las **suplantaciones de identidad** con un importe medio de **10.000 €**.

Este apartado, aunque poco representativo estadísticamente, pone de relieve que **algunos fraudes no encajan en las tipologías más habituales,** y que pueden implicar montos significativos cuando se producen, como en los casos de f**raudes personalizados o sofisticados** (por ejemplo, fraude interno, fraude documental avanzado, fraudes sobre canales no digitales, etc.).

5.7 Importe medio fraudes

GRAF. 5.7: Importe medio fraudes



BLOQUE VI

Herramientas de lucha contra el fraude

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

6.1 Herramientas contra el fraude

Los datos muestran preferencia por tecnologías enfocadas a la **verificación documental y de identidad,** que en conjunto superan el **62% del total**, evidenciando que las empresas priorizan la verificación inicial del usuario como primera barrera frente al fraude. Así lo corrobora el informe "*2024 Global Identity and Fraud Report*" de Experian, que afirma que el 73% de las empresas a nivel mundial ya considera el control de identidad digital como su principal prioridad de inversión para los próximos dos años.

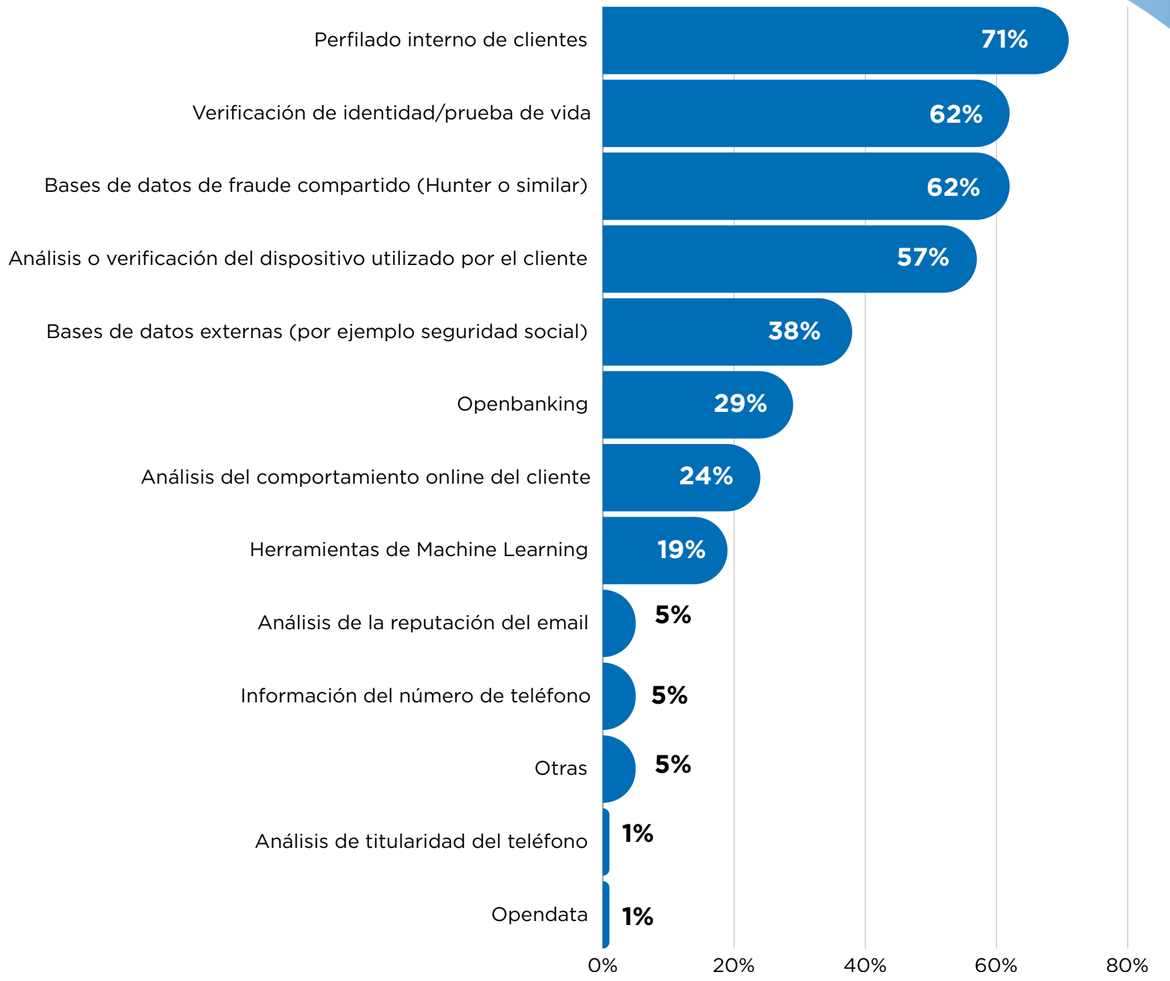
Sigue resultando lo más significativo el peso del **perfilado interno de clientes** (**71%**) y muy representativas las de **fraude compartido (62%)**, que demuestran la importancia de la inteligencia histórica y colaborativa como mecanismos fundamentales para anticipar riesgos. Este enfoque se alinea con el modelo propuesto por la European Forum for Information Sharing (EFIS), que destaca que el intercambio sectorial de datos de fraude reduce en hasta un 45% los intentos exitosos en entidades financieras.

Por otro lado, herramientas más sofisticadas como el **análisis del comportamiento online o el uso de Machine Learning** aún están infrautilizadas (**24% y 19% respectivamente**), a pesar de su alto valor en la detección de fraude dinámico y adaptativo. Según el último Global Economic Crime and Fraud Survey 2024 de PwC, el uso de inteligencia artificial para análisis de patrones permitió a las organizaciones reducir en un 36% el tiempo de detección de fraude.

El **nulo uso de opendata o análisis de titularidad del teléfono**, y el bajo uso de fuentes de validación adicionales como la reputación del email, ponen de relieve que aún hay mucho margen de mejora en la integración de señales externas y datos contextuales.

Frente al informe 2024, observamos **una ligera caída en el uso de herramientas avanzadas** como el Machine Learning y el comportamiento online, que en el informe anterior tenían mayor protagonismo. Esta contracción podría deberse a barreras como el coste de implementación o la falta de perfiles técnicos para su adopción. En contraste, aumentan herramientas más tradicionales y accesibles, como la validación documental y las bases de datos internas, mostrando una tendencia a **reforzar las capas básicas de control.**

«El perfilado de interno de clientes y la verificación de identidad siguen siendo protagonistas en la lucha contra el fraude.»



GRAF. 6.1: Herramientas contra el fraude

6.2 Satisfacción de las herramientas

Las herramientas que mayor satisfacción generan son las **basadas en datos colaborativos** e históricos:

- **76% están satisfechos con bases de fraude compartido** (*Hunter o similar*)**.**
- Le siguen las **bases de datos internas (67%) y externas (57%).**

Este patrón muestra que **las empresas valoran muy positivamente los sistemas que permiten nutrirse de información colectiva o propia, especialmente si es útil para validar perfiles o detectar patrones de fraude repetido.**

Las soluciones de **validación de documentos e identidad** también tienen buena valoración general, pero presentan una mayor dispersión:

- Aunque un 43% está satisfecho con la validación de documentos, un 19% no la usa aún.
- En verificación biométrica (prueba de vida), el 33% no la utiliza todavía.

Estos datos revelan que, si bien son herramientas aceptadas, aún existe un grado considerable de implementación parcial, lo que podría deberse a obstáculos como coste, integración o madurez de la tecnología.

«El 76% de las empresas confía en los datos compartidos para frenar el fraude: la colaboración gana peso.»

«Machine Learning y Openbanking siguen sin despegar: más del 40% de las empresas no los usa aún en su estrategia antifraude.»

Las tecnologías con niveles bajos de satisfacción o directamente con poco uso:

- El **análisis del email** y la **información del teléfono** tienen más de un 50% de "no aplica" (NA) y **solo entre 10%-19% de satisfacción**.

- **Openbanking, Opendata** y **Machine Learning** siguen sin despegar: entre el 38% y 71% no las utiliza, y la **satisfacción no supera el 29%**.

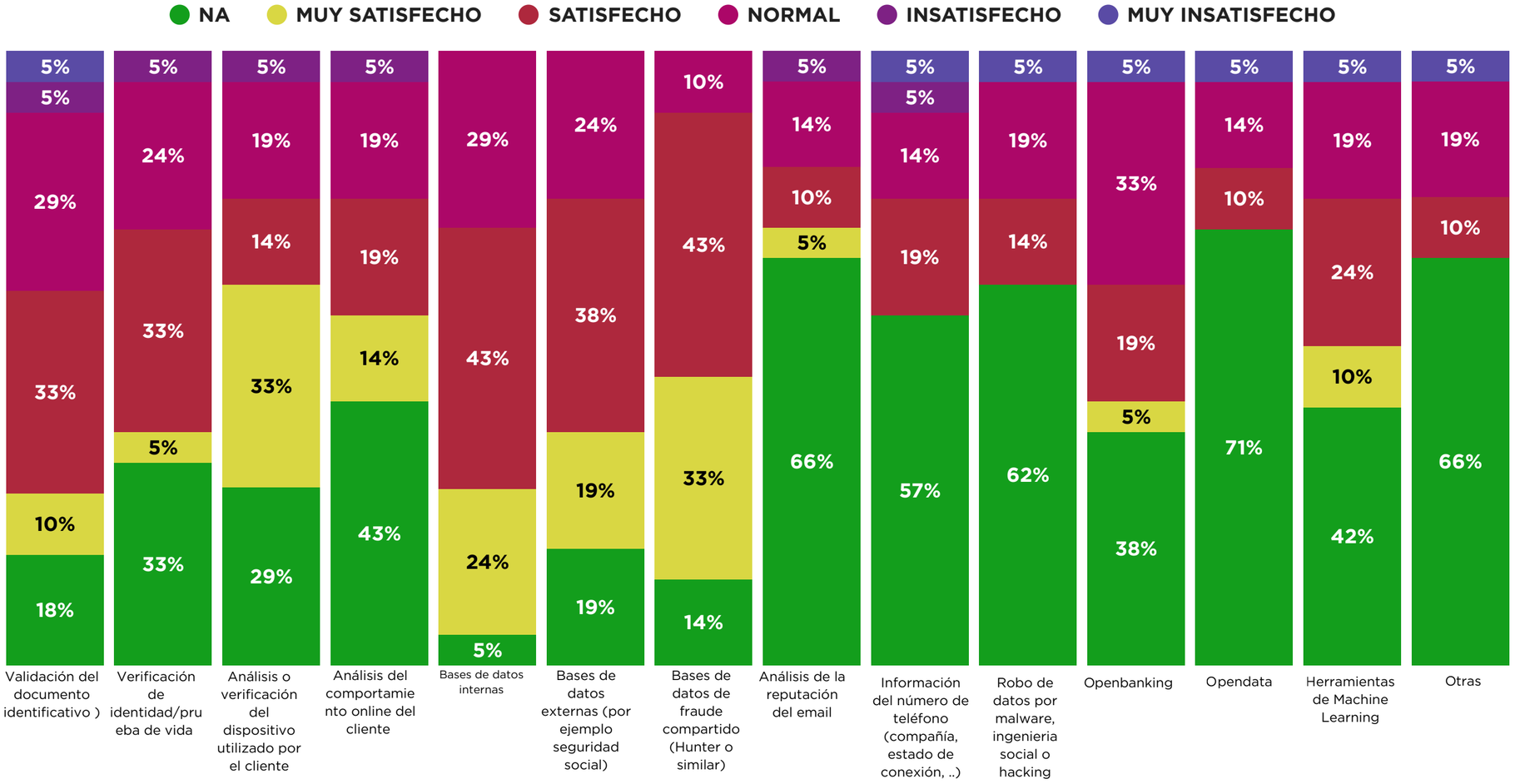
Esto indica que, pese a su potencial, siguen siendo tecnologías poco exploradas o mal implementadas, quizá por falta de interoperabilidad, recursos o resultados poco tangibles.

Respecto al año anterior, se observan algunas mejoras claras en la percepción de las bases de fraude compartido, que han pasado de 34% satisfechos en 2024 a un 76% en 2025, reflejando un creciente valor de la colaboración interempresarial en lucha contra el fraude.

Por el contrario, tecnologías avanzadas como el Machine Learning, Openbanking u Opendata siguen mostrando altas tasas de no adopción, lo que sugiere que la transformación digital de las herramientas antifraude aún no ha madurado al ritmo que exige el entorno actual.

El ecosistema antifraude empresarial en España se apoya mayoritariamente en el poder del dato compartido e histórico, mientras que la innovación tecnológica aún no ha logrado despegar en términos de adopción o satisfacción.

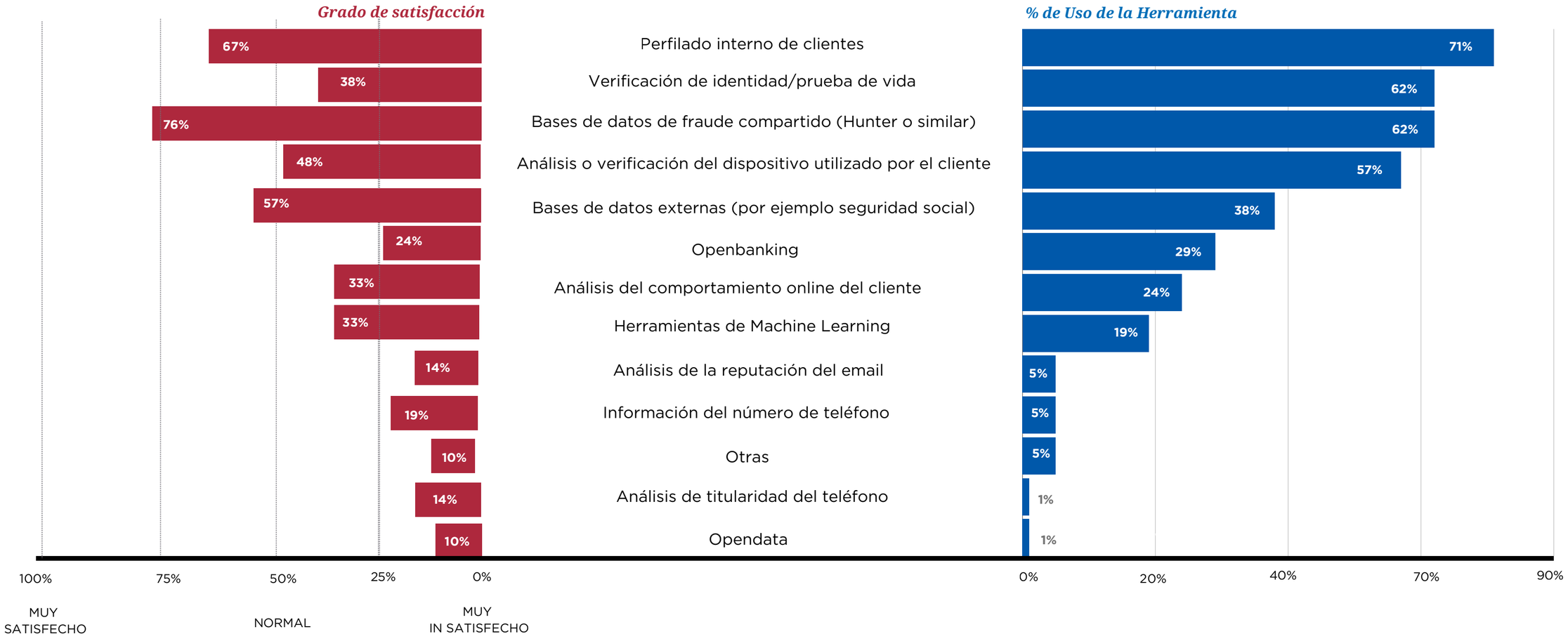
6.2 Satisfacción de las herramientas



GRAF. 6.2: Satisfacción de las herramientas

6.3 Satisfacción y % de utilización de las herramientas antifraude

7.2. Satisfacción y % de utilización de las herramientas antifraude



GRAF. 6.3: Porcentaje de Uso de la Herramienta vs Grado de Satisfacción

6.4 Problemas con las herramientas

GRAF. 6.4: Problemas con las herramientas

El análisis revela que los principales obstáculos que las empresas encuentran en sus herramientas de detección y prevención de fraude están encabezados por dos grandes frentes: **el impacto negativo en la experiencia de cliente y la consiguiente pérdida de clientes (67%)** y la **elevada tasa de falsos positivos (53%)**. Ambos problemas no solo afectan a la eficacia operativa, sino también a la reputación y la rentabilidad de las organizaciones.

En un segundo nivel de incidencia aparecen **la falta de automatización**, que obliga a una supervisión manual por parte de un gestor **(43%)**, y la **falta de compartición de datos (19%),** lo que dificulta la detección de patrones intersectoriales o la anticipación a amenazas emergentes. También destaca la percepción de que la **implantación o evolución** de estas soluciones es **compleja (19%)**, así como que **no cubren todas las fuentes de información necesarias (24%).**

Problemas de menor frecuencia, aunque igualmente relevantes, incluyen que sean **herramientas difíciles de utilizar (5%)**.

Por último llama la atención que ninguna empresa haya reportado que las soluciones no estén frenando gran parte del fraude actual, ni que estén obsoletas frente a nuevas tipologías, lo que podría indicar un nivel de efectividad aceptable en cuanto a adaptación técnica, aunque no exento de fricciones e incidencias operativas.

«El 67% de las empresas señala a la experiencia de cliente como la gran “víctima” de las herramientas antifraude.»

6.5 Herramientas a futuro

Las prioridades de inversión y desarrollo tecnológico de las empresas en materia antifraude apuntan hacia soluciones que refuercen la verificación de identidad y la autenticación avanzada, con un claro enfoque en evitar suplantaciones y fraudes de apertura de cuentas.

Destaca que el **análisis de titularidad del teléfono** sea la herramienta más citada como futura incorporación **(43%)**, por delante de las clásicas bases de datos internas o externas, lo que refleja la creciente relevancia del teléfono móvil como vector de verificación y, a la vez, como posible puerta de entrada para defraudadores.

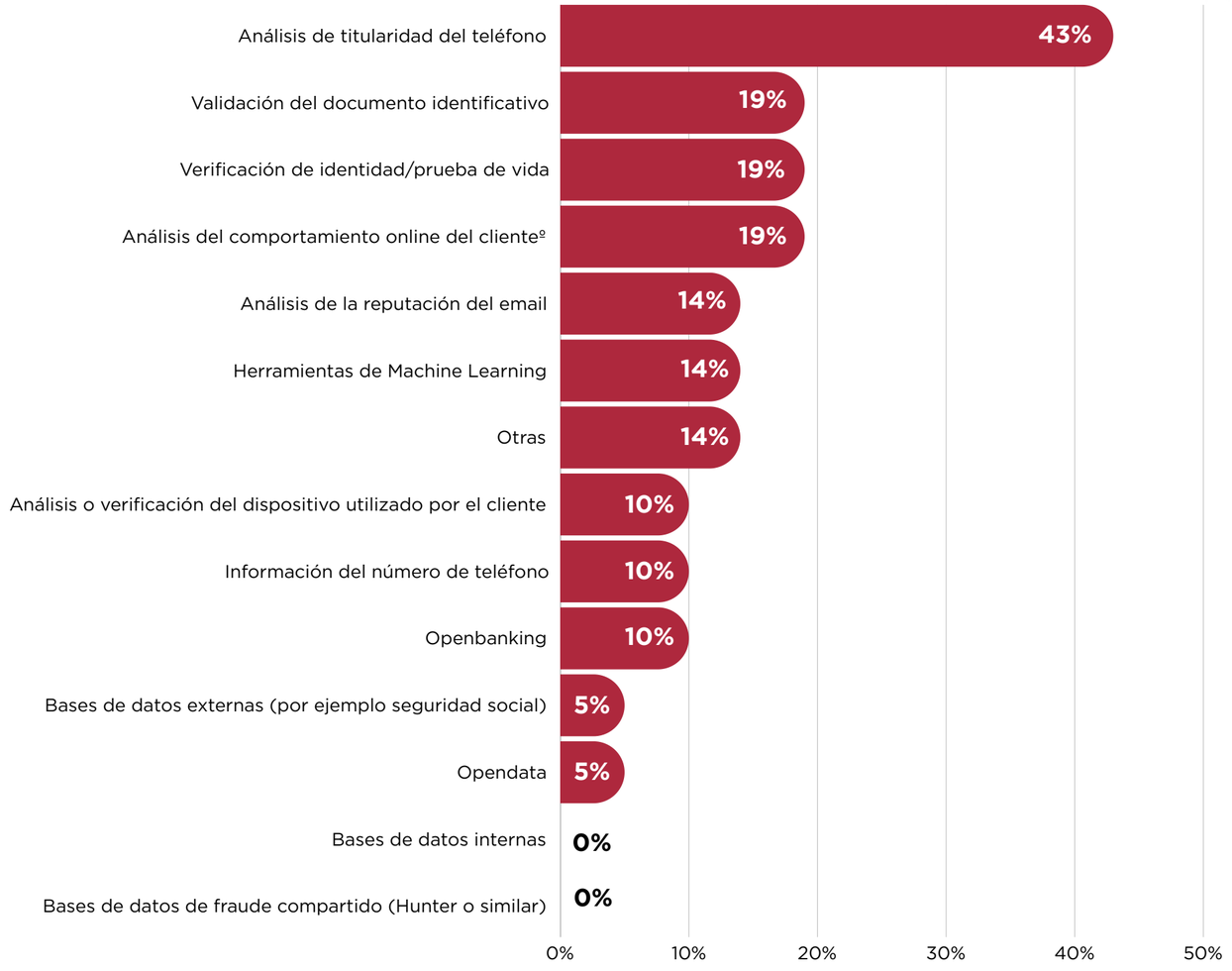
En **segundo nivel de prioridad**, con un **19%** de menciones, se sitúan varias tecnologías:

- **Validación avanzada de documento identificativo**, para detectar manipulación en la imagen.
- **Verificación biométrica/prueba de vida**, que confirma que el documento pertenece al portador real.
- **Análisis del comportamiento online del cliente**, que aplica biometría del comportamiento para detectar anomalías en la interacción.

Otras herramientas emergentes con **entre un 10% y un 14%** de interés incluyen **machine learning, opendata, bases de datos de fraude compartido y análisis de la reputación del email**. Este conjunto apunta hacia un futuro con más inteligencia predictiva y análisis cruzado de datos para anticipar el fraude antes de que se materialice.

Sorprende que elementos tradicionalmente clave, como **bases de datos internas y externas o el openbanking, apenas reciban menciones (0%-5%)**. Esto podría indicar que, o bien ya están integrados en la operativa habitual, o que se perciben como menos diferenciales frente a nuevas técnicas de análisis.

«El 43% de las empresas apuesta por el análisis de titularidad del teléfono como nueva arma antifraude.»



GRAF. 6.5: Herramientas a futuro

BLOQUE VII

Inversión en prevención del fraude

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

7.1 Inversiones en prevención y concienciación

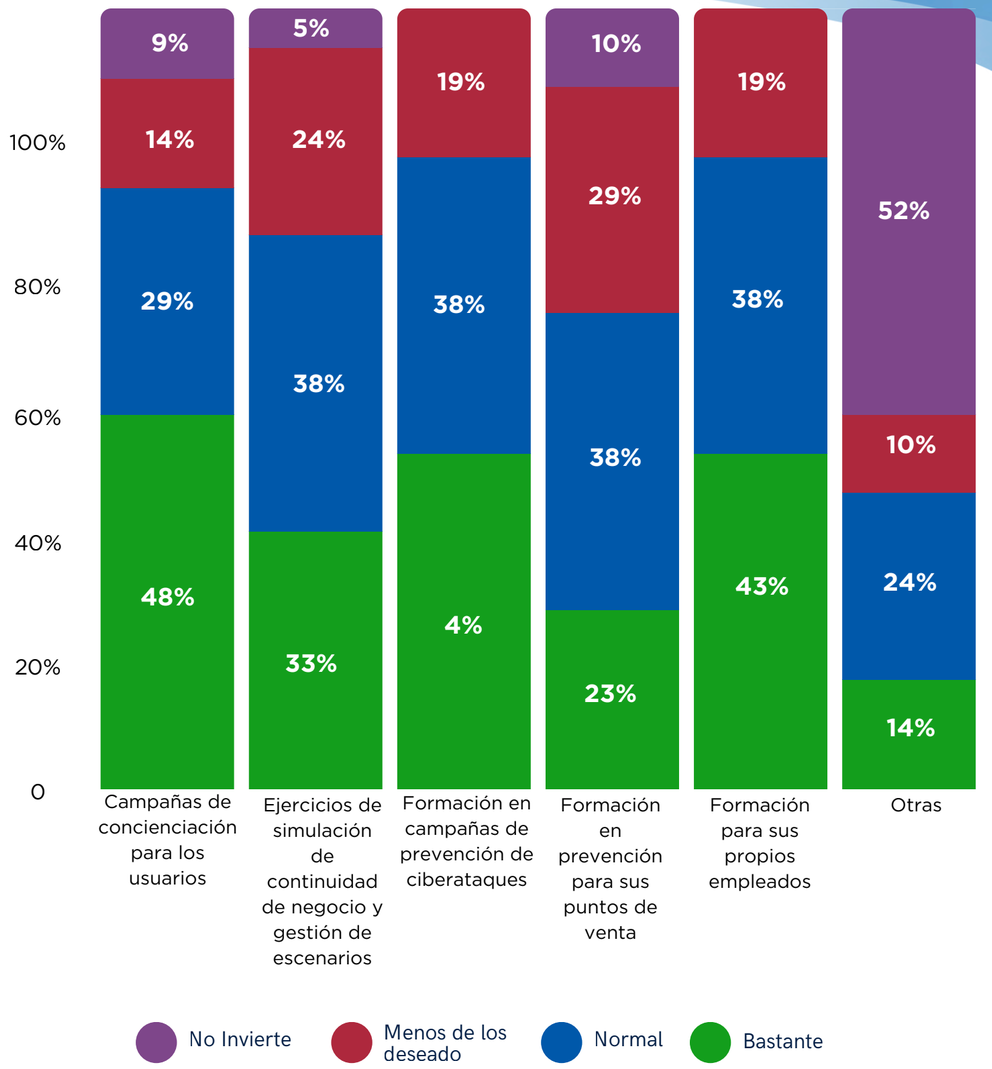
Los datos reflejan que una mayoría relevante de empresas está **apostando activamente por la formación y concienciación como herramienta preventiva contra el fraude**. Las acciones con mayor grado de inversión sostenida ("bastante") son las **campañas hacia usuarios (48%**) y la **formación interna en ciberseguridad (43%)**, lo que evidencia una clara **estrategia dual centrada tanto en la sensibilización del cliente como en la preparación de los equipos internos**.

En el caso de los **ejercicios de simulación ante ciberataques**, el **71%** de las empresas afirma realizar esta actividad con **frecuencia normal o alta**, lo que indica una creciente madurez operacional en escenarios de contingencia, alineándose con las mejores prácticas marcadas por el European Union Agency for Cybersecurity (ENISA), que recomienda ejercicios regulares como herramienta clave para anticipar y contener incidentes.

Por otro lado, hay dos áreas con margen de mejora: solo el **24%** declara invertir "bastante" en **formación a puntos de venta**, y hasta un 29% lo hace por debajo del nivel deseado. Esta brecha es crítica considerando que los puntos físicos son a menudo **objetivo de fraudes documentales o de suplantación**, especialmente en sectores como telcos o retail financiero.

Finalmente, cabe destacar que más de la mitad de las empresas (**52%**) no invierte en otras iniciativas distintas a las recogidas en esta tabla, lo cual **refleja una estructura formativa aún muy dependiente de esquemas tradicionales**, y con escasa exploración de formatos alternativos como gamificación, microlearning o experiencias inmersivas, que podrían aumentar la efectividad de la concienciación.

En comparación con 2024, se observa una consolidación de la formación en ciberataques y simulacros, pero una estabilidad preocupante en los niveles bajos de inversión en puntos de venta y en innovación formativa. Esto puede comprometer el alcance integral de las políticas antifraude, especialmente en canales híbridos donde conviven lo digital y lo presencial.



GRAF. 7.1: Inversiones en prevención y concienciación

7.2 Importe aproximado de inversión en concienciación/prevención/formación

El análisis de los presupuestos dedicados a formación y concienciación antifraude revela una realidad polarizada: mientras algunas organizaciones hacen esfuerzos significativos en ámbitos concretos, una parte considerable de las empresas aún no realiza inversiones relevantes en esta materia.

El área de **mayor compromiso presupuestario** es la formación **en campañas de prevención de ciberataques**, donde un 33% de las empresas invierte entre **10.000 y 25.000 €**, y un 10% adicional lo hace entre **5.000 y 10.000 €**. Esta cifra, junto al hecho de que un 29% de las entidades destina más de 5.000 € a la **formación de empleados propios**, indica que algunas compañías empiezan a reconocer que **la ciberresiliencia** se construye desde dentro, especialmente en sectores críticos.

Los **ejercicios de simulación** (continuidad de negocio o gestión de incidentes cibernéticos) también muestran una tendencia hacia presupuestos medios-altos: un 24% de las empresas invierte entre 10.000 y 25.000 €, y un 19% adicional entre 25.000 y 50.000 €. Esto evidencia que **las organizaciones más maduras están empezando a adoptar estrategias de ciberentrenamiento operativo**, alineadas con los estándares de resiliencia exigidos por normativas como DORA o NIS2.

En cambio, otras áreas clave como la **formación en puntos de venta** siguen estando desatendidas: un 33% **no realiza ninguna inversión** y otro 33% se limita a presupuestos por debajo de los 5.000 €. Esta debilidad es preocupante, especialmente para sectores con presencia física o interacción directa con el cliente, donde los fraudes presenciales, la **manipulación documental** o las **identidades ficticias** siguen siendo frecuentes.

De forma similar, **las campañas de concienciación al cliente** presentan un contraste marcado: mientras el 29% de las entidades no invierte nada en ellas, otro 29% sí lo hace en rangos de 5.000 a 10.000 €. Esta disparidad es sintomática de que aún muchas empresas **no han interiorizado la formación del cliente como parte del perímetro de seguridad**, a pesar de que la mayoría de fraudes requiere algún grado de participación (consciente o no) del usuario final.

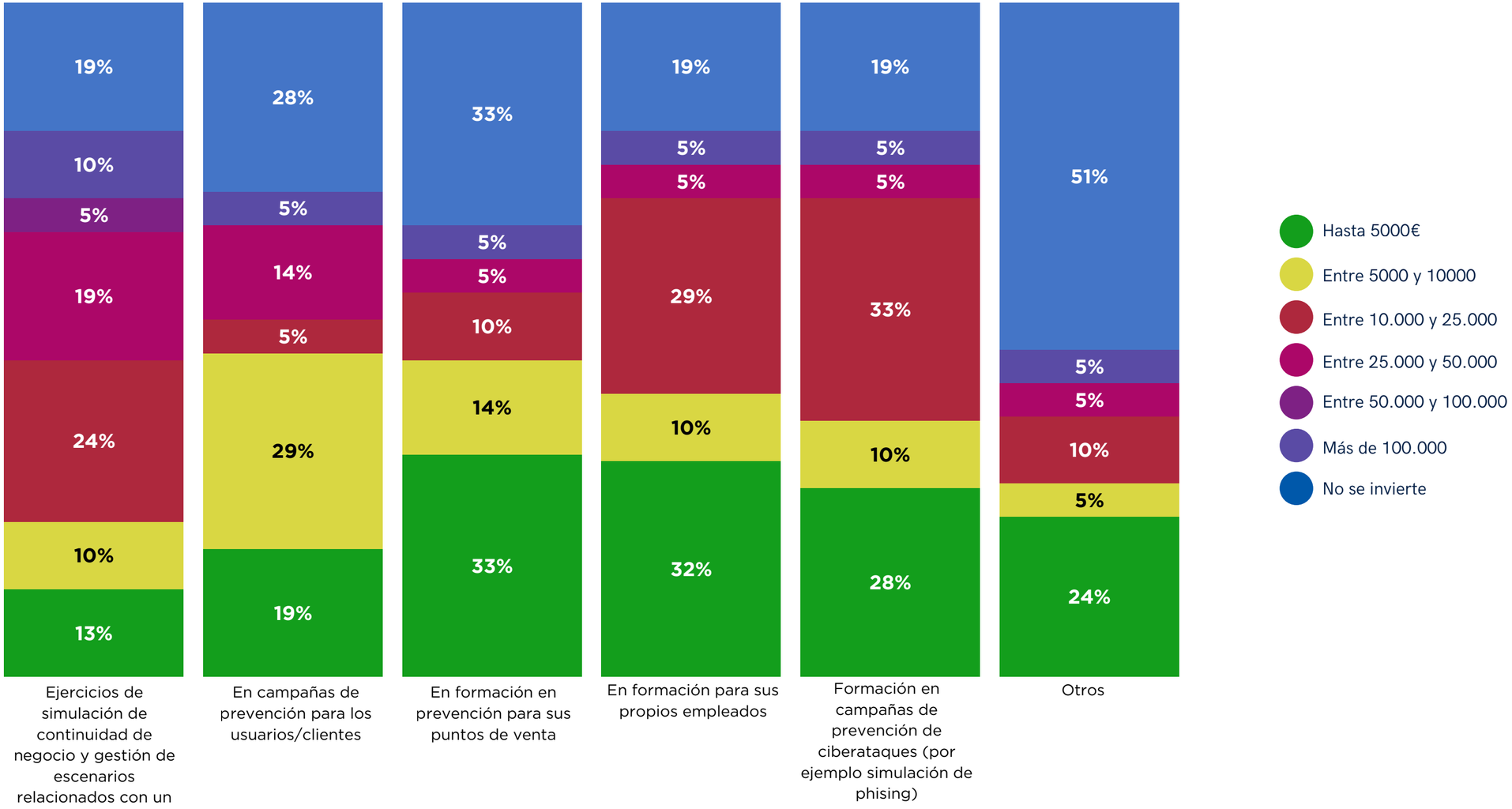
Por último, destaca que **más de la mitad de las empresas (52%) no invierten en acciones formativas alternativas** ("otras"), lo que confirma que el **modelo formativo actual es conservador**.

En conjunto, los datos revelan un compromiso parcial con la formación antifraude: aunque algunas organizaciones están evolucionando hacia esquemas más robustos, una parte significativa sigue operando con presupuestos bajos o inexistentes. Esta brecha presupuestaria es especialmente preocupante en un contexto donde el 82% del fraude empresarial accede por canales no presenciales, y donde el error humano sigue siendo el principal vector de ataque, como ha documentado el Verizon Data Breach Investigations Report 2024.

Para que la inversión sea efectiva, no basta con incrementar los presupuestos. Es necesario redefinir el modelo formativo, pasando de sesiones pasivas a entornos activos, simulados, interactivos y adaptados a roles concretos. Además, integrar estas acciones en la estrategia global de gestión del fraude y no tratarlas como iniciativas aisladas, será clave para reforzar la cultura organizativa frente a las ciberestafas.

«Puntos de venta, el eslabón olvidado: un tercio de las empresas no invierte en su capacitación frente al fraude.»

7.2 Importe aproximado de inversión en concienciación/prevención/formación



GRAF. 7.2 Inversiones en prevención y concienciación

7.3 Canales de atención a víctimas de fraude

La presencia de canales específicos para la atención de víctimas de fraude sigue siendo una asignatura pendiente para muchas organizaciones. Aunque se observan esfuerzos en establecer vías de contacto, el panorama sigue evidenciando claras oportunidades de mejora.

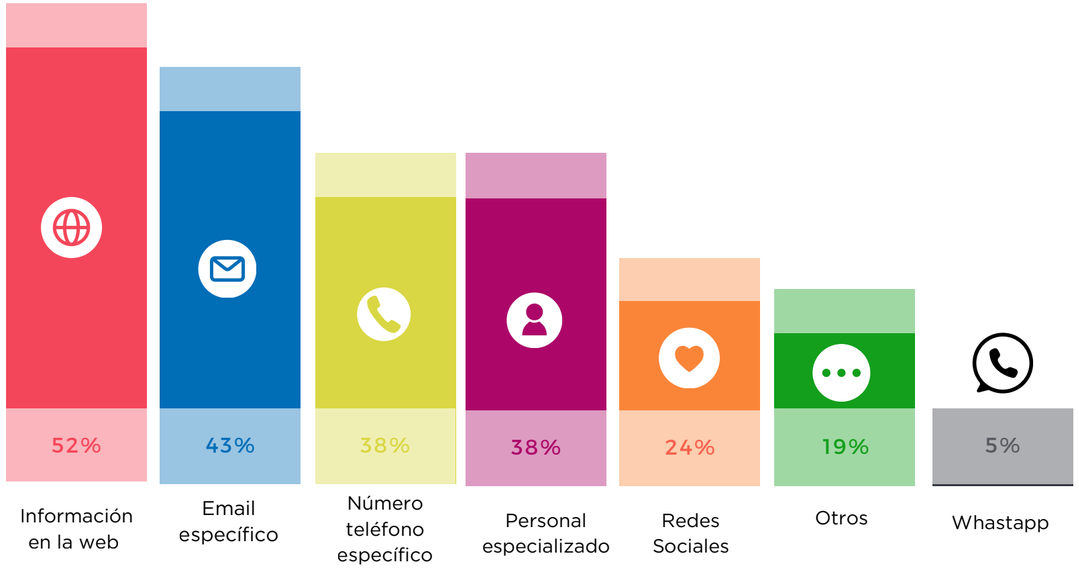
La opción más común es la publicación de **información en la web (52%)**, una acción importante pero pasiva, que requiere que el usuario sepa buscar y actuar. La **atención proactiva** es más limitada: solo el **38%** de las entidades dispone de **personal especializado** para gestionar fraudes, y la misma proporción ofrece un **teléfono específico** de atención al usuario, lo cual es relevante, dado que el fraude suele generar situaciones de urgencia y estrés en las víctimas.

El **correo electrónico específico (43%)** es un canal útil aunque insuficiente si no está integrado en un proceso ágil de gestión. Llama también la atención el **escaso uso de WhatsApp (5%) y redes sociales (24%)** como vías de contacto, a pesar de que estos canales son cada vez más utilizados por los clientes. En el contexto actual, donde el fraude suele propagarse a través de **canales digitales y móviles**, la **ausencia de respuesta omnicanal** deja expuestos a muchos usuarios.

Además, apenas un **19%** de las empresas menciona otros mecanismos alternativos, lo cual refleja una **limitada innovación en la experiencia de atención al cliente víctima de fraude**. En contraste, entidades punteras están implementando ya **chatbots especializados, portales seguros de autogestión**, e incluso **asistentes virtuales de respuesta emocional** ante fraudes severos, prácticas que aún no se observan en la mayoría de las compañías encuestadas.

En comparación con el informe anterior, los canales de atención al fraude **no han evolucionado significativamente**. Se mantienen niveles similares en el uso de email y teléfono, mientras que la atención con personal especializado sigue sin despegar**.** Además, canales digitales como WhatsApp o redes sociales continúan prácticamente sin uso, lo que refleja una falta de avance hacia una atención omnicanal más moderna y eficaz.

La atención al cliente víctima de fraude no solo es una obligación operativa, sino una herramienta clave para mantener su confianza. La baja implantación de canales activos y personalizados muestra una nula o pobre estrategia post-incidente de muchas empresas.
Las compañías que consigan responder de forma rápida, empática y multicanal no solo mitigarán el impacto reputacional del fraude, sino que fortalecerán la fidelidad del cliente y el valor de su marca.



GRAF. 7.3 Canales específicos para atención al fraude

«WhatsApp y redes sociales, ausentes en la atención al cliente víctima de fraude en el 90% de las empresas.»

BLOQUE VIII

Conclusiones

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

8.1 Conclusiones

El análisis del fraude corporativo en España durante 2025 confirma una realidad compleja: **la sofisticación de los ataques crece a mayor velocidad que la madurez de los sistemas de defensa**. Si bien sectores como banca y telecomunicaciones lideran en inversión y estructura, persisten lagunas críticas en trazabilidad, formación, tecnología y cultura antifraude.

Uno de los principales hallazgos es que el protagonismo del **onboarding digital** sigue siendo el punto de entrada prioritario para los defraudadores. El 72% de los ataques se dirigen a nuevos clientes persona física, revelando una fragilidad estructural en la verificación de identidad y autenticación temprana. Esta exposición inicial se ve amplificada por la falta de herramientas avanzadas y la baja adopción de tecnologías como machine learning o análisis del comportamiento digital, aún infrautilizadas pese a su potencial comprobado.

El **factor humano** sigue siendo el eslabón más débil. Aunque ha mejorado la formación interna, un tercio de las empresas no invierte en capacitar a sus puntos de venta —un canal todavía vulnerable al fraude documental y presencial—. Del mismo modo, los canales de atención a víctimas continúan rezagados, con un 90% de las organizaciones sin presencia en redes sociales o WhatsApp para gestionar incidentes de fraude.

Por otro lado, existe una **percepción positiva de eficacia**: el 76% de las empresas declara bloquear más del 75% de los intentos. Sin embargo, esta cifra podría enmascarar una peligrosa zona de confort, ya que muchos indicadores no se actualizan para captar los nuevos tipos de fraude híbrido que combinan ingeniería social, brechas digitales y manipulación de datos.

Preocupante aún es la **carencia de trazabilidad** del perfil del defraudador. Casi la mitad de las organizaciones no dispone de datos clave como sexo, nacionalidad, edad o ingresos de los implicados, lo que debilita la capacidad predictiva de los sistemas y compromete el desarrollo de estrategias segmentadas.

Y a pesar de que se observa una **mejora general en los ratios de fraude consumado** y en la reducción de pérdidas económicas respecto al año anterior, el **nivel de denuncia sigue siendo bajo** y selectivo. Solo el 6% de las empresas denuncia sistemáticamente más del 75% de los casos, lo que refleja una cultura de tolerancia parcial al fraude, con criterios reactivos y poco sistemáticos.

Finalmente, los principales retos tecnológicos se centran en el equilibrio entre seguridad y experiencia de cliente. Los falsos positivos siguen siendo el mayor dolor de cabeza, afectando tanto la eficiencia operativa como la percepción del usuario final.

8.2 Recomendaciones

1. **Reforzar el onboarding digital** con autenticación biométrica, validación documental automatizada y análisis de comportamiento para evitar fraudes desde el primer contacto.

2. **Construir una trazabilidad completa del defraudador**, incorporando variables como edad, género, nivel de ingresos y nacionalidad para optimizar modelos predictivos y machine learning.

3. **Incorporar tecnologías avanzadas** como inteligencia artificial, open data y scoring adaptativo, alineando la detección con la velocidad de evolución de los ataques.

4. **Actualizar periódicamente los KPIs antifraude** y las métricas de éxito, adaptándolos a nuevos vectores como el fraude sintético, APP o suplantación de clientes conocidos.

5. **Invertir en formación innovadora** utilizando gamificación, microlearning o simulacros interactivos, especialmente en puntos de venta y canales híbridos.

6. **Diseñar una atención post-fraude multicanal** que incluya soporte especializado por redes sociales, WhatsApp, chatbots y canales directos, generando confianza y contención reputacional.

7. **Fomentar la cultura de denuncia sistemática**, estableciendo políticas claras, procesos simples y reconociendo públicamente a las organizaciones comprometidas con la lucha activa contra el fraude.

8. **Participar en ecosistemas de inteligencia colaborativa**, integrando bases de datos compartidas sectoriales y alianzas público-privadas para anticipar amenazas emergentes.

9. **Elevar el fraude a una prioridad de la agenda directiva**, integrándolo en los comités de riesgo, compliance y estrategia corporativa como una función transversal y crítica.

10. **Utilizar como estrategia antifraude** utilizar las distintas herramientas que cada una de las entidades tienen a su disposición.

www.asociacioncontraelfraude.com

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

contacto@asociacioncontraelfraude.com