INFORME SOBRE
TENDENCIAS DE FRAUDE EN EMPRESAS 2024-2025

AEECF
ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

Bienvenida

INFORME DE **TENDENCIAS DE FRAUDE** EN EMPRESAS 2024-25

Desde el comienzo de nuestra andadura en la AEECF, hemos estado firmemente dedicados a la tarea de resguardar a las empresas frente a las amenazas emergentes del fraude en el ámbito digital.

A lo largo de estos años, una de nuestras prioridades es la recopilación de datos, el análisis de tendencias y la adaptación a los nuevos desafíos que surgen en el campo del fraude. Y este esfuerzo se materializa en nuestros informes anuales, el Informe de Fraude a Empresas y el Informe de Fraude entre Consumidores.

Hoy, es un honor para nosotros presentar la VIII edición del Informe Anual sobre Tendencias de Fraude en Empresas. Esta nueva entrega no solo incorpora nuevos vértices de estudio, sino que también incluye por primera vez algunas perspectivas sectoriales de nuestras empresas asociadas y los profesionales que las representan, expertos altamente comprometidos con la defensa contra el fraude digital.

Seguiremos explorando áreas de gran relevancia en el panorama del fraude digital y mejorando cada año nuestro estudio, con la convicción de que este informe se convierta en una herramienta de referencia para la estrategia de las empresas que forman parte de nuestra red.

Como presidente de la AEECF, quisiera extender mi agradecimiento a todas las empresas asociadas por su valiosa colaboración y la calidad de los datos aportados, y a cada persona que ha contribuido a la realización de este informe.

Invito a todas las organizaciones a integrarse en nuestra comunidad. A nuestros eventos, a nuestras formaciones, a nuestros estudios. La colaboración y el compromiso mutuo nos permitirán alcanzar nuevos logros y seguir innovando en la protección de los intereses empresariales en un entorno digital en constante expansión.

Saludos cordiales,

Jorge Hernández

Presidente de la AEECF

Índice

BIENVENIDA [2]

ÍNDICE [3]

BLOQUE I. ANALISIS DEMOGRAFICO [5]

1.1. Sectores
1.2. Departamentos
1.3. Roles

BLOQUE II. RECURSOS DEDICADOS AL FRAUDE [8]

2.1. Tamaño del departamento de fraude
2.2. Externalización de las funciones de Fraude

BLOQUE III. PERCEPCIÓN DEL FRAUDE [10]

3.1. Percepción del fraude
3.2. Distribución geográfica
3.3. Distribución por edad
3.4. Clasificación por sexo
3.5. Nacionalidad del defraudador
3.6. Perfil de empleo de la víctima de Fraude
3.7 Nivel de ingresos de víctimas de fraude
3.8. Niveles formativos de las víctimas de fraude

BLOQUE IV. EVOLUCION DEL FRAUDE [17]

4.1. Intentos de fraude respecto a solicitudes
4.2. Incremento de los casos de fraude
4.3. Casos de fraude consumados
4.4 Pérdidas económicas a causa del Fraude

Índice

BLOQUE V. CANALES Y TIPOLOGÍAS DE FRAUDE [20]

5.1. Canales de fraude
5.2. Distribución entre tipologías de clientes
5.3. Tipos de fraude
5.4. Frecuencia de los tipos de fraude a su organización
5.5. Denuncias de los casos de fraude denunciados y destinatarios

BLOQUE VI. HERRAMIENTAS CONTRA EL FRAUDE [26]

7.1 Herramientas contra el fraude
7.2. Satisfacción de las herramientas
7.3. Problemas con las herramientas
7.4. Herramientas a futuro

BLOQUE VII. INVERSIÓN EN PREVENCIÓN DEL FRAUDE [31]

8.1. Inversiones en prevención de fraude
8.2. Importes destinados a prevención del fraude
8.3. Canales de atención a víctimas de fraude

CONCLUSIONES [37]

BLOQUE I

Análisis Demográfico

1.1. Sectores

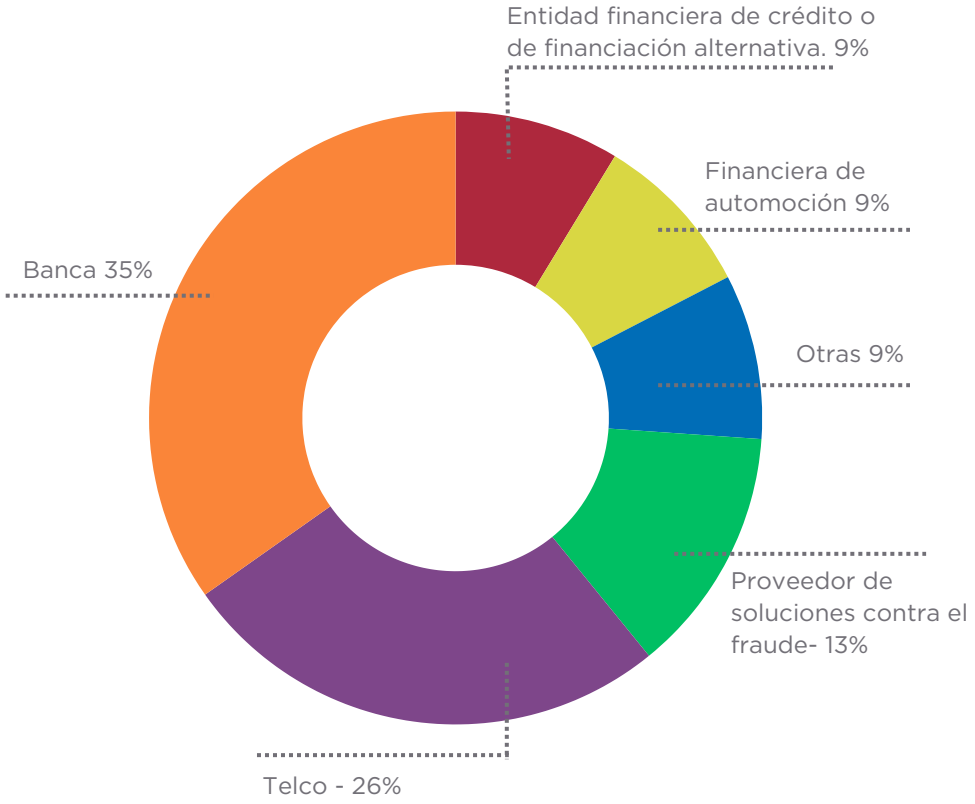
El *Informe de Fraude a Empresas 2024* representa la opinión de diferentes sectores.

La **Banca** está representada con un **34,8%** de las respuestas. Se trata de un sector que tradicionalmente es el principal o 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 sigue el sector **Telecomunicaciones** con un **26,1**% de las respuestas. Se trata de un sector expuesto a diferentes riesgos , especialmente financiación de terminales e identificación online de sus clientes y que ha sido objeto del aumento de los ciberdelitos y estafas a ciudadanos.

Por otro lado las **entidades financieras de crédito, entidades de financiación alternativa y las financeras de marca de automoción** están representadas en un **8,7%** respectivamente. Se trata de sectores que afrontan riesgo de fraude significativo dado que realizan operaciones de crédito normalmente con nuevos clientes y mayoritariamente online.

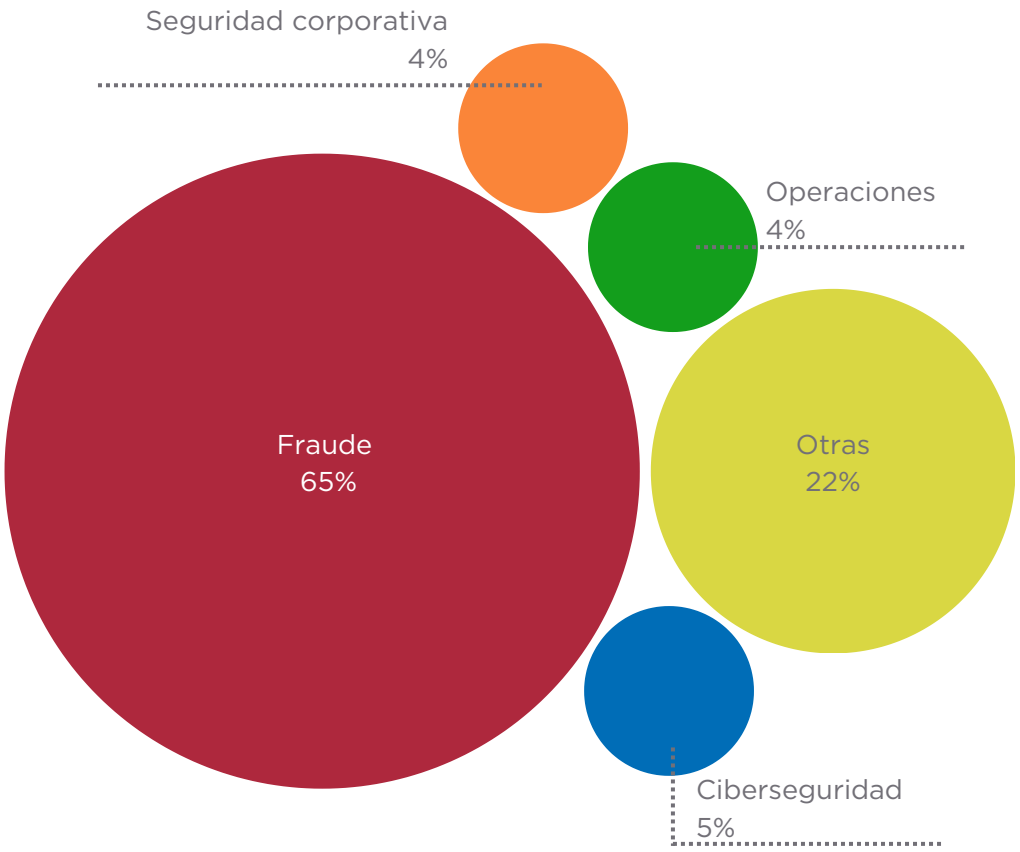
La participación de empresas **proveedoras de soluciones contra el fraude** es del **13%**, se trata de un sector que muestra su interés en comprender las tendencias y desafíos actuales en la prevención del fraude para ofrecer soluciones adaptadas a las necesidades de los clientes, como se refleja posteriormente en este estudio.



«La muestra representa en más de un 80% a nuestras empresas asociadas.»

Análisis Demográfico

1.2. Departamentos



En lo que se refiere al **área responsable** en la gestión del fraude dentro de las organizaciones, sigue ostentando el primer lugar, con un notable **65,22%, el departamento de Fraude.** Esto subraya el papel central que este departamento asume en la identificación y mitigación de riesgos de fraude, apuntando a una alta especialización y enfoque en la gestión de este problema específico.

El **sector de Ciberseguridad** emerge con un **4,35%**, reflejando su papel complementario en la protección contra ataques cibernéticos y fraudes digitales, pues la colaboración entre ciberseguridad y gestión de fraude es esencial para la implementación de estrategias integrales de prevención y respuesta.

Por su parte, **las áreas de Seguridad Corporativa** también representan un **4,35%** de la muestra estudiada, lo que sugiere un enfoque en la protección de activos y la prevención de riesgos físicos y operacionales que podrían estar relacionados con el fraude.

La participación de **"Otras áreas",** con un **21,74%,** señala la diversidad de áreas, roles y perspectivas adicionales que pueden contribuir a la comprensión y manejo del fraude en las empresas.

Los departamentos de **auditoría interna**, **compliance** y **riesgos no están presentes en este estudio**. Se trata de áreas que si que eran responsables de fraude en anteriores estudios, lo cual muestra la importancia creciente del área de riesgos como departamento independiente para la gestión del fraude.

Por primera vez aparecen reflejados en el Informe los departamentos de **ciberseguridad y seguridad corporativa**.

Análisis Demográfico

1.3. Roles

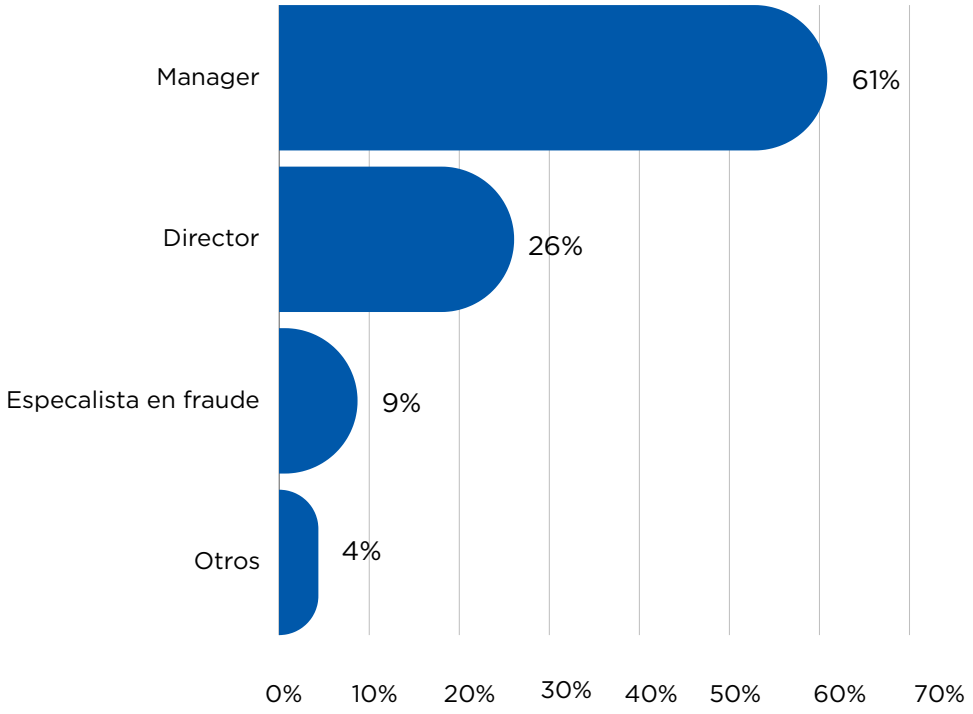
Los datos reflejan una predominancia clara de los **managers y mandos intermedios en la gestión de fraude, con un notable 60,87%**. La mayoría de los encuestados, son quienes están encargados de aplicar las políticas establecidas por la dirección, gestionar la implementación diaria y de la supervisión directa de las actividades que pueden estar expuestas a riesgos de fraude.

El rol de **Director** y la importancia de la toma de decisiones a nivel ejecutivo para abordar y mitigar los riesgos de fraude en toda la organización ocupa el segundo lugar, con un **26,09%** de representación en este estudio.

Los **especialistas en fraude, representan el 8,70%** de la muestra. Los especialistas aportan un nivel de expertise técnico y conocimiento específico en el análisis y la investigación de casos de fraude, y su papel es indispensable para la identificación y resolución de incidentes.

El **4,35%** de participación en la categoría **"Otras"** refleja la variedad de roles adicionales que pueden estar implicados en la gestión del fraude, como personal de auditoría, cumplimiento normativo, o seguridad corporativa, que también pueden tener responsabilidades relacionadas con la detección y prevención del fraude.

Esta distribución viene a destacar la importancia de una colaboración estrecha entre los diferentes niveles de la organización para abordar eficazmente el desafío del fraude.



BLOQUE II

Recursos dedicados al fraude

2.1. Tamaño del departamento de Fraude

El análisis de los datos sobre el **tamaño de los departamentos** dedicados a la gestión del fraude revela una distribución relativamente equilibrada entre diferentes rangos.

Un **17,39%** de las empresas tiene departamentos de fraude con **más de 50 personas**. Este grupo representa sobretodo a las **grandes corporaciones o entidades con una alta exposición al riesgo de fraude**, que han escalado sus esfuerzos de prevención y detección en respuesta a la creciente sofisticación y frecuencia de los incidentes de fraude.

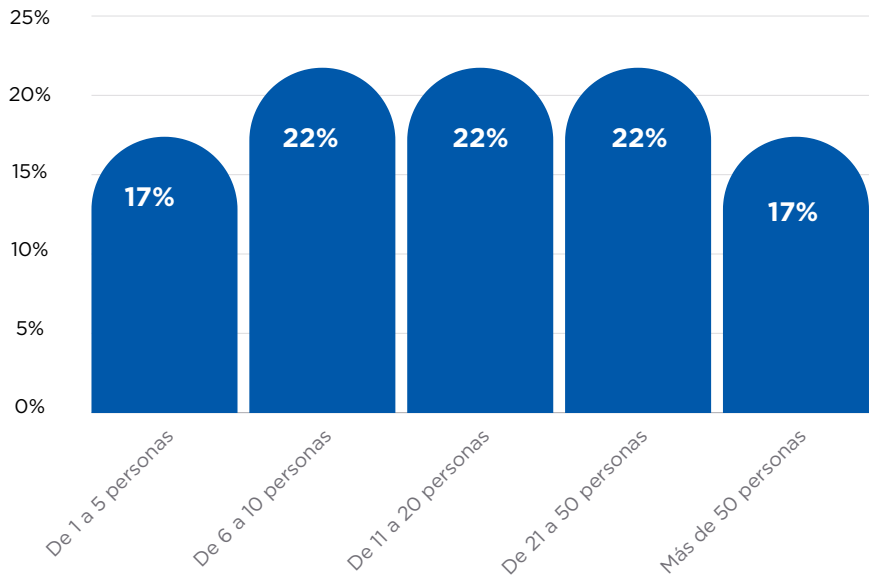
Un 21,74% de las empresas encuestadas tiene **equipos de entre 21 y 50 personas**, reflejando una capacidad amplia para abordar y gestionar problemas complejos de fraude a una escala considerable, mientras que **otro 21,74%** reporta tener departamentos de fraude con **equipos de entre 11 y 20 personas.**

El hecho de que un número tan significativo de organizaciones **(casi un 44%)** mantenga departamentos de fraude de **entre 11 y 50 personas,** destaca la creciente importancia de inversión para protegerse contra amenazas y ciberestafas cada vez más complejas.

Otro 21,7% de las empresas declara tener **entre 6 y 10 personas** en el departamento de fraude. En nuestro anterior estudio este segmento representaba un 5% lo cual el crecimiento de los departamentos de fraude de hasta 10 personas.

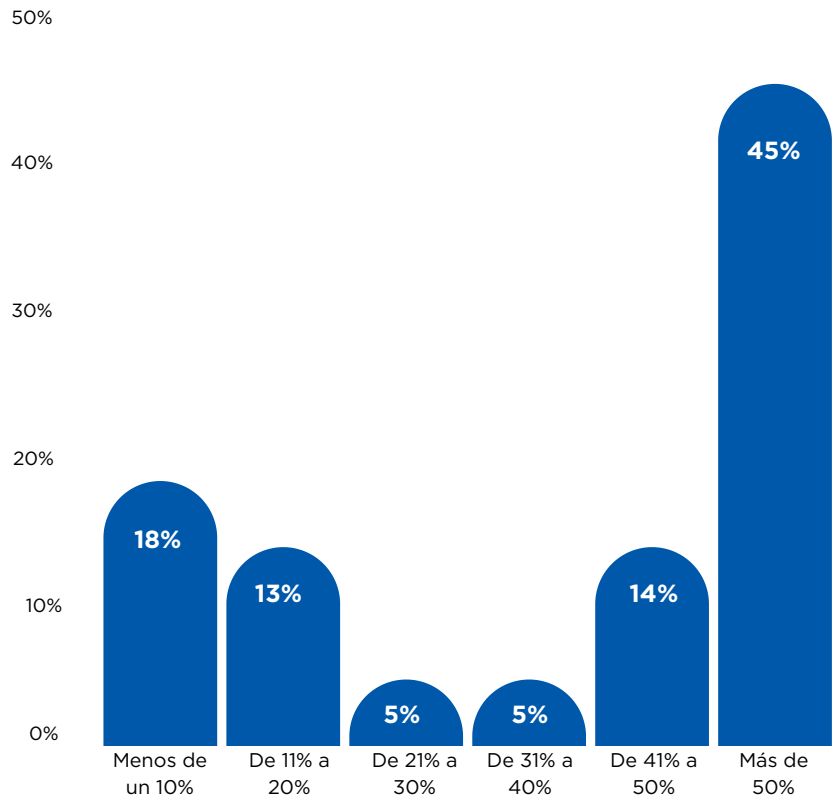
El **17,39%** de las empresas restantes cuenta con equipos de **entre 1 y 5 personas**, con una estructura dedicada al fraude más limitada y que puede suponer un verdadero desafío, ya que equipos reducidos deben enfrentar un volumen creciente y cada vez más diversificado de casos de fraude.

«El crecimiento y la expansión de los departamentos de fraude ,es una tendencia notable, con un claro aumento de la dotación de personal respecto a años anteriores. »



Recursos dedicados al fraude

2.2. Externalización de las funciones de Fraude



Miembros externos del equipo de Fraude

Se trata de una **novedad en este estudio respecto a informes anteriores**. Será interesante observar la evolución de este parámetro en los siguientes años.

El análisis de la composición de los departamentos de fraude revela una **significativa tendencia hacia la externalización en la gestión de funciones relacionadas con el fraude** que se manifiesta claramente en las entidades que dedican más personal al control del fraude.

De acuerdo a los datos recopilados, un notable **45,45%** de las empresas indica que **más del 50% de su personal dedicado al fraude es externo**. Esta alta proporción de personal externo refleja una creciente dependencia en consultores y proveedores de servicios para gestionar y mitigar el riesgo de fraude existente en la organización.

El **13,64%** de las empresas cuenta con una proporción de **entre el 41% y el 50% de personal externo,** lo que confirma esta tendencia hacia una mayor integración de recursos externos en la estructura de gestión del fraude. Este enfoque puede estar impulsado también por la necesidad de talento experto o tecnologías avanzadas que no siempre están disponibles internamente.

En el rango de **21% a 40%,** ambos con una representación del 4,55% respectivamente**, se observa un mayor equilibrio entre recursos internos y externos** y una estrategia de externalización moderada, buscando complementar las capacidades internas sin depender en exceso de servicios externos.

Un **18,18%** de las empresas señala que **menos del 10%** de su equipo de fraude está compuesto por personal externo**,** mientras que **el 13,64% tiene entre un 11% y un 20% de su personal en esta modalidad**. Son las organizaciones que optan por equipos mayoritariamente internos para una gestión más directa del fraude.

La estrategia de externalización permite a las empresas acceder a talento y conocimiento experto sin la necesidad de mantener una estructura interna de gran tamaño. Sin embargo, esta dependencia también plantea desafíos en términos de integración y coordinación con los equipos internos para asegurar una estrategia de prevención de fraude efectiva y cohesionada.

Percepción del fraude

3.1. Percepción del fraude

Un **33,93%** de las empresas considera el fraude principalmente como un **asunto reputacional** que compromete la credibilidad y la confianza de los clientes, poniendo el foco en la imagen pública de la entidad y en la relación con sus clientes.

Por otro lado, el **21,43**% de las empresas percibe el fraude como una **pérdida provisionada en la cuenta de resultados**. Este porcentaje **ha bajado respecto a estudios anteriores donde representaba hasta el 40%** de las respuestas, lo cual demuestra la mayor concienciación respecto a la percepción del problema del fraude por las entidades.

Han aparecido **nuevas respuestas, fruto del feedback dado por los asociados**, como relacionados con la consideración del fraude como fuente de información para la toma de decisiones. A consecuencia de esto han surgido dos respuestas interesantes:

- Un **16,07%** de los encuestados declara utilizar los casos de fraude como una fuente para la mejora de procesos futuros
- El **10,71**% de las empresas considera sus casos de fraude como una fuente de información para futuras tomas de decisiones en procesos de machine learning

Este enfoque refleja cómo las organizaciones están integrando tecnologías avanzadas para analizar patrones de fraude y mejorar sus estrategias preventivas, pues poder entrenar algoritmos de machine learning puede ayudar a anticipar y prevenir fraudes de manera más efectiva.

Un **16,07%** de los encuestados declara utilizar los casos de fraude como una **fuente para la mejora de procesos futuros**. Esta perspectiva constructiva, analiza los casos de fraude para optimizar los controles internos y los procesos operativos.

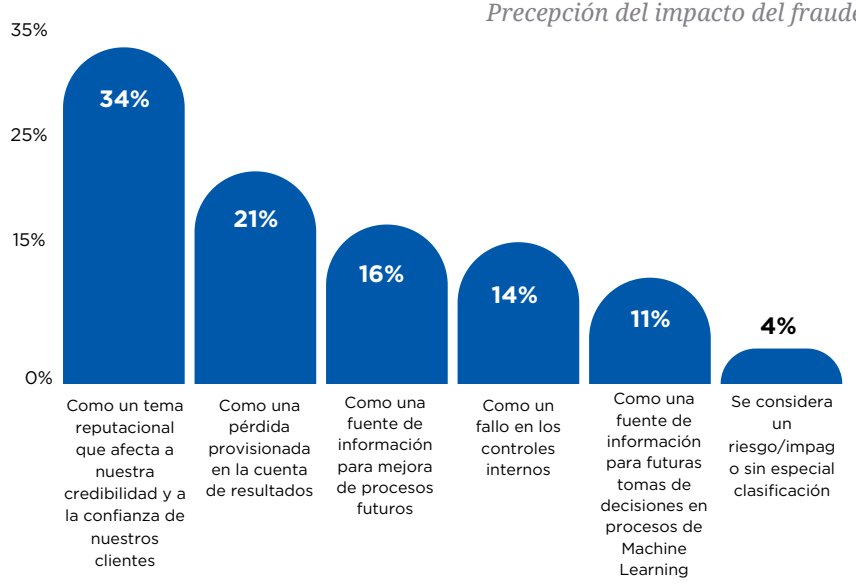
El **14,29%** de las empresas encuestadas considera que el fraude como **un fallo en los controles internos**, lo que indica la percepción de que es la debilidad en los mecanismos de control lo que facilita estos incidentes.

El **10,71%** de las empresas ve el fraude desde un prisma más innovador, como una **fuente de información para futuras tomas de decisiones en procesos de machine learning**. Este enfoque refleja cómo las organizaciones están integrando tecnologías avanzadas para analizar patrones de fraude y mejorar sus estrategias preventivas, pues poder entrenar algoritmos de machine learning puede ayudar a anticipar y prevenir fraudes de manera más efectiva.

Un **3,57%** de las empresas trata los casos de fraude como **riesgos o impagos sin una clasificación especial**, lo que sugiere una visión menos profesionalizada del fraude en comparación con otros tipos de riesgos.

Finalmente**, ningún encuestado** clasifica el fraude exclusivamente basándose en **dictámenes judiciales** o en la definición del departamento legal**,** indicando este dato que las empresas tienden a considerar el fraude desde una perspectiva más amplia y multidimensional.

Precepción del impacto del fraude



Percepción del fraude

3.2. Distribución geográfica

«Más del 60% de las empresas opinan que hay mayor incidencia de fraude en algunas regiones concretas.»

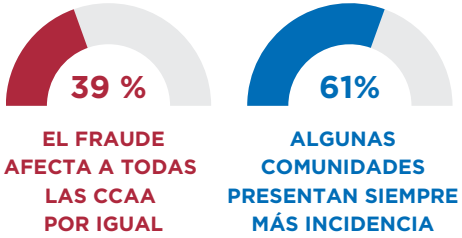
Cataluña sigue siendo, como en años anteriores, la **región con la mayor proporción de casos de fraude**, representando un **33%** del total.

A continuación, la **Comunidad Valenciana asciende al segundo puesto** con un **17%** de las respuestas y en el **tercer puesto** comparten el pódium del fraude la **Comunidad de Madrid** y **Andalucía** con un **13%** de las respuestas.

Canarias vuelve a aparecer en el **cuarto puesto**, como en el anterior estudio, con un **7%** de las respuestas.

El **resto de las regiones** que aparecen mencionadas, aunque con menor incidencia, son Galicia ,Aragón, Canarias, Castilla y León, País Vasco, y Región de Murcia, donde un **3%** de las respuestas indican que son las regiones con mayor proporción de fraude.

El **fraude** lógicamente está más **concentrado en los centros económicos, turísticos o financieros** pero aparecen menciones a 10 Comunidades Autónomas y no olvidemos que **el 40% de las respuestas indican que el fraude afecta a todas las CC.AA**. En próximas ediciones se realizará un estudio más detallado para mostrar la proporción entre número de solicitudes y número de fraudes.



Distribución geográfica del Fraude

Cataluña 33%

Comunidad Valenciana 17%

Adalucia y Comunidad de Madrid 13%

Canarias 7%

Aragón, Castilla y León. Galicia. País Vasco y Región de Murcia - 3%

Percepción del fraude

3.3. Distribución por edad

EL FRAUDE AFECTA A TODAS LAS FRANJAS DE EDADES

OTRAS

Si tenemos en cuenta la pirámide poblacional española, **el análisis de los datos arroja una clara desproporción entre representatividad e incidencia de fraude en ciertos grupos etarios**.

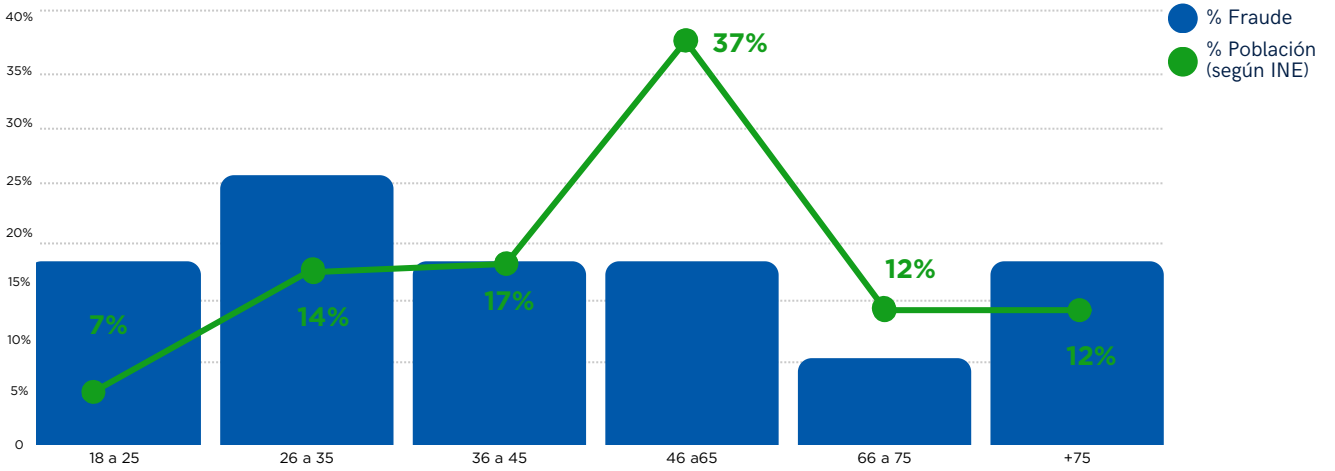
Los **grupos de menor edad presentan una incidencia de fraude notablemente superior** a su representación poblacional, lo que indica una mayor exposición o susceptibilidad a fraudes en estas edades, posiblemente por su alta interacción con tecnologías y transacciones digitales. Un **42% de los casos de fraude afectan a las personas menores de 35 años** (que solo representan un 21% de la población).

A partir de los **46 años, y hasta los 75, la incidencia de fraude es significativamente menor** que su proporción poblacional, lo que podría responder a una mayor prudencia y concienciación ante situaciones de fraude. Sin embargo, es preocupante que las personas mayores de 75 años, a pesar de asociarse a una menor interacción con entornos de riesgo, presentan una incidencia de fraude muy elevada y probablemente asociada a la suplantación de identidad.

«Las poblaciones de menor edad están claramente sobrerepresentados en los casos de fraude respecto a su peso en la pirámide poblacional: hasta 35 años hay un 42% de casos de fraude, aún representando tan solo el 21% de la población adulta.»

Este análisis sugiere que las **estrategias** de prevención del fraude deben ser **diferenciadas por franjas de edad**, con un enfoque especial en los grupos más jóvenes (hasta 35 años) y los mayores de 75 años, quienes parecen estar en mayor riesgo en relación con su tamaño poblacional.

Además, estos hallazgos podrían indicar la **necesidad de una mayor educación financiera y tecnológica** para todos los grupos, con el objetivo de mitigar las oportunidades de fraude.

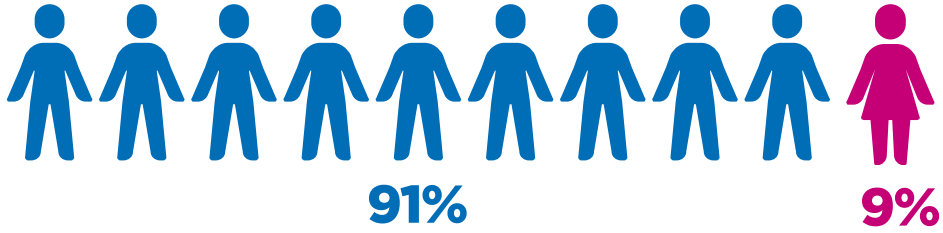


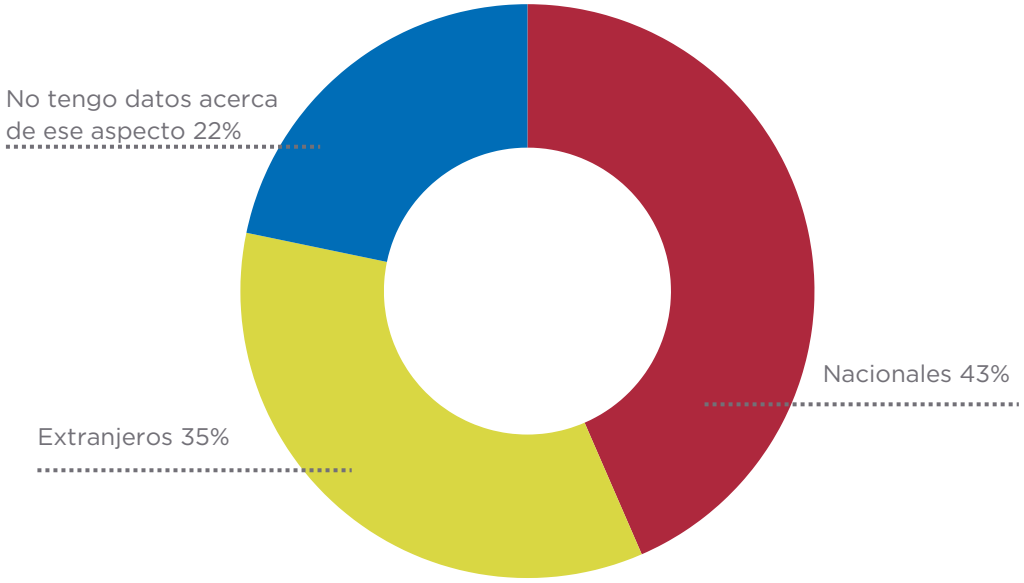
«Los mayores de 75 años representan el 12% de la población adulta pero casi un 17% de los casos de fraude.»

Percepción del fraude

3.4. Clasificación por Sexo

El análisis de la distribución por sexo de las víctimas de fraude percibida en esta muestra, revela una notable disparidad, con una representación significativamente mayor de hombres en comparación con mujeres. Según los datos recogidos en la presente muestra, la percepción es que el **91,30%** de las víctimas de fraude son **hombres**, mientras que el **8,70% son mujeres.**





Distribución por nacionalidad

3.5. Nacionalidad del defraudador

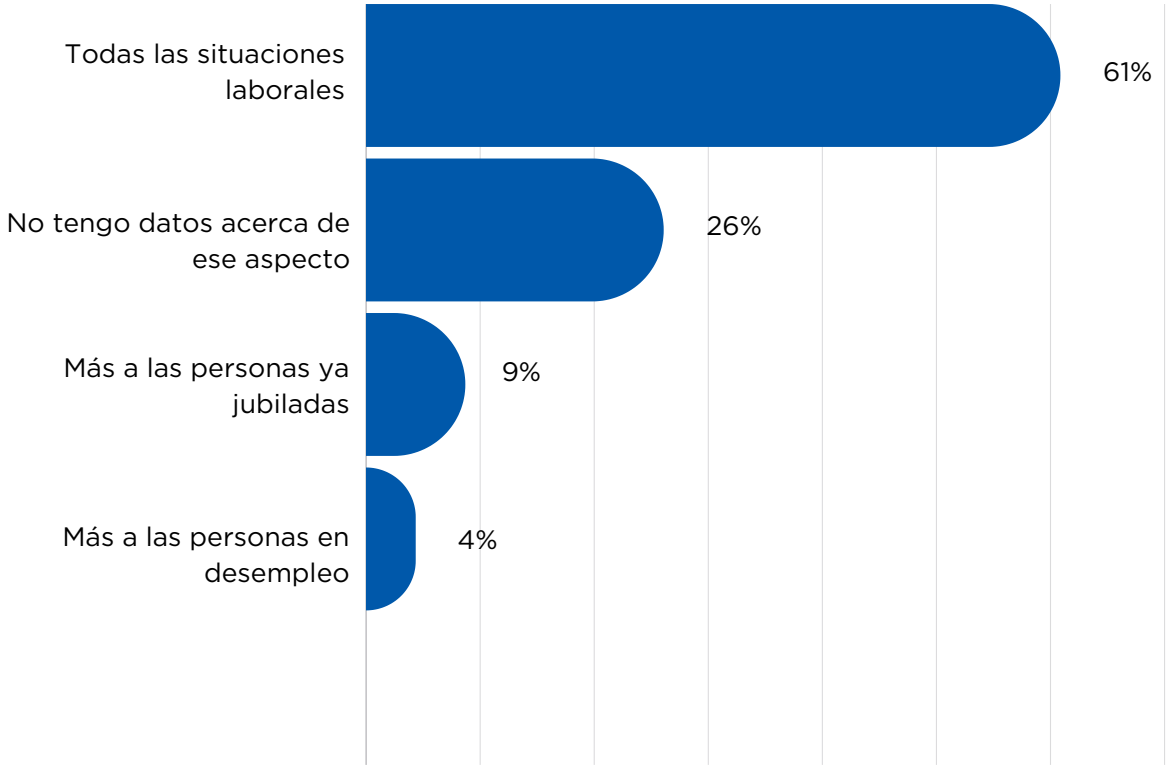
El análisis de la distribución por nacionalidad de los defraudadores en España muestra una combinación notable entre defraudadores nacionales y extranjeros.

Según los datos analizados, **el 43,48% de los defraudadores identificados son nacionales,** mientras que **34,78% son extranjeros.**

Este patrón sugiere que, aunque una parte significativa de los defraudadores proviene del ámbito nacional, una proporción considerable también involucra a individuos de otras nacionalidades.

Esto evidencia la importancia de implementar estrategias de prevención y detección de fraude que no solo se enfoquen en las particularidades del entorno local, sino que también consideren el riesgo asociado a actores internacionales que actúan de forma deslocalizada por la creciente globalización de las actividades comerciales y financieras.

Percepción del fraude



«El fraude afecta a todo tipo de situaciones laborales y a cualquier edad.»

3.6. Perfil de empleo de la víctima de Fraude

El análisis de la situación laboral de las víctimas revela una **distribución amplia y diversa.**

Según los datos recopilados, el **60,87%** de **las víctimas de fraude se encuentra en una variedad de situaciones laborales**, abarcando múltiples sectores y condiciones de empleabilidad.

Un 26,09% de las empresas declara que carece de información sobre la situación laboral de las víctimas**,** lo que limita la comprensión completa del perfil de las personas afectadas por el fraude.

Al margen, un **8,70%** de las empresas apunta a individuos ya **jubilados** como víctimas principales, mientras que el **4,35%** señala a personas en situación de **desempleo**.

La amplitud en la situación laboral de las víctimas sugiere que las estrategias de prevención y mitigación del fraude deben ser inclusivas y adaptativas, considerando tanto a trabajadores activos en diversas posiciones como a aquellos en condiciones no laborales, como jubilados o desempleados.

Percepción del fraude

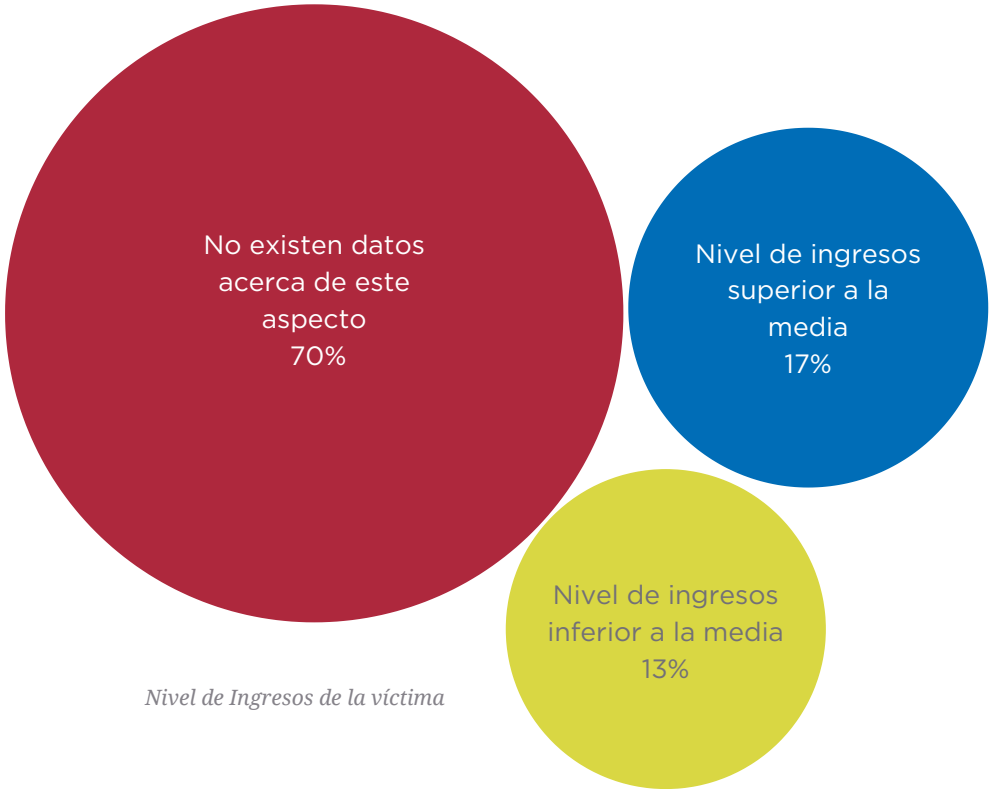
3.7. Nivel de ingresos de las víctimas de Fraude

El análisis de los niveles de ingresos de las víctimas de fraude arroja una distribución notablemente variada. Un **17,39%** de las empresas apunta a que las víctimas tienen un **nivel de ingresos superior a la media.**

En contraste, un **13,04%** se posiciona en el polo opuesto, percibiendo que el fraude impacta a **individuos con menos recursos financieros.**

En resumen, los datos disponibles sugieren que **el fraude no discrimina** exclusivamente en función del nivel de ingresos, afectando tanto a personas con ingresos superiores como inferiores a la media.

Un amplísimo porcentaje de las empresas encuestadas, **un 69,57%, no cuenta con información** detallada sobre el nivel de ingresos de las víctimas. Llama la atención la ausencia de datos en este aspecto aun tratándose de un parámetro fundamental a la hora de concesión de créditos. Se profundizará en estos datos en próximas ediciones.



Nivel de Ingresos de la víctima

«El 70% de las entidades no tienen datos acerca del nivel de ingresos de las víctimas del fraude cuando habitualmente se indica que es un parámetro que tiene incidencia en el fraude.»

Percepción del fraude

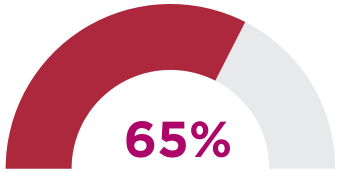
3.8. Niveles formativos de las víctimas de Fraude

Poniendo el foco en el nivel formativo de las víctimas de fraude, **un 65,22%** de las empresas defienden que las víctimas **provienen de diversos niveles formativos** y que el fraude afecta a cualquier individuo independientemente de su formación académica.

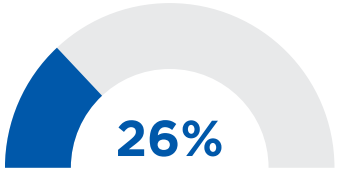
En contraste, **8,70%** defiende que las víctimas corresponden a **perfiles con escasa formación**, destacando una mayor vulnerabilidad de aquellos con menor nivel educativo ante prácticas fraudulentas.

Ninguna respuesta apunta a los perfiles con formación superior, lo que podría sugerir que, al menos en la muestra de datos disponible, las personas con un nivel educativo alto no están sobrerrepresentadas entre las víctimas de fraude.

Un **26,09% de los casos no cuenta con información suficiente** sobre el nivel formativo de las víctimas, lo que de nuevo, al igual que en análisis anteriores, limita la capacidad de comprensión del perfil de las víctimas.



A TODOS LOS NIVELES FORMATIVOS



NO CUENTO CON LA INFORMACIÓN SUFICIENTE

PERFILES CON ESCASA FORMACION

Evolución del Fraude

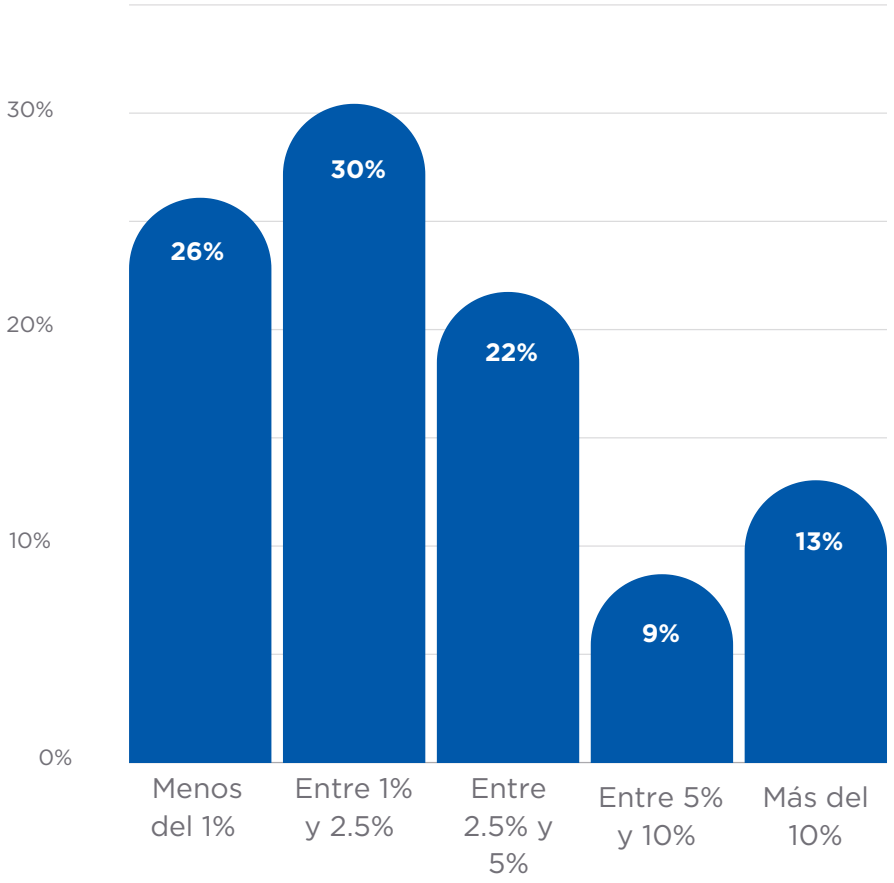
«Un notable 78% de las empresas encuestadas ha experimentado un incremento en los **intentos de fraude**, intensificándose la actividad fraudulenta que enfrentan»

4.1. Intentos de fraude respecto a solicitudes

Un **26.09%** de las organizaciones reporta que los intentos de fraude representan **menos del 1% de sus solicitudes totales**, seguido de **un 30.43%** de empresas que declara una incidencia de intento de fraude situada **entre el 1% y el 2.5% del total** de solicitudes.

Un **21.74%** de las empresas enfrenta intentos de fraude que **constituyen entre el 2.5% y el 5% del total de sus solicitudes**, reflejando un desafío considerable que podría impactar significativamente en sus operaciones. Un **8.70%** de las empresas reporta que los intentos de fraude se encuentran **en el rango del 5% al 10%**, y finalmente el **13.04%** de las empresas enfrenta una **situación más crítica, con intentos de fraude que superan el 10%** de sus solicitudes, lo que demanda una acción robusta para proteger la integridad de sus operaciones.

Un notable **44%** de las empresas **manifiestan que tienen intentos de fraude superiores al 2,5% de su cartera**, lo que pone de manifiesto la importancia de los controles, medidas y herramientas antifraude en las políticas de admisión para evitar cifras tan significativas.



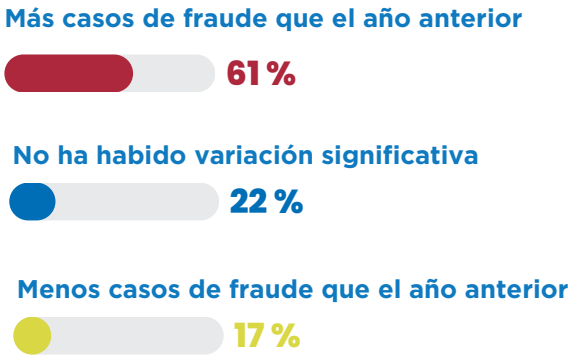
Porcentaje de intentos de fraude respecto al total de solicitudes

Evolución del Fraude

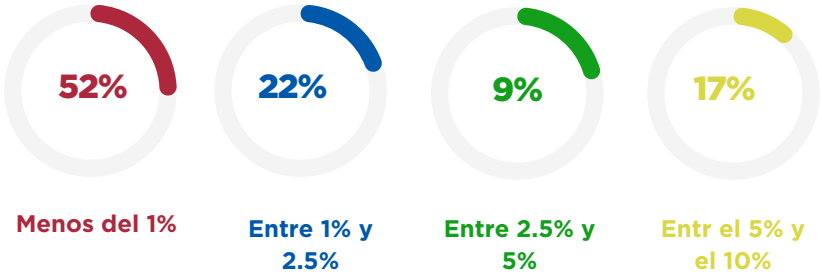
4.2. Incremento de los casos de fraude

Un **60,87%** de las empresas reportan un **aumento en los casos consumados de fraude**, lo que indica una intensificación de las actividades fraudulentas y sugiere una necesidad urgente de fortalecer las medidas de prevención y control.

En contraste, **21,74% de las empresas observan que no ha habido una variación significativa** en los intentos de fraude, indicando una estabilidad en la incidencia de estos eventos, mientras que el **17,39%** de las empresas reportan una **disminución en los casos de fraude** en comparación con el año anterior.



Casos de fraude consumados



4.3. Casos de fraude consumados

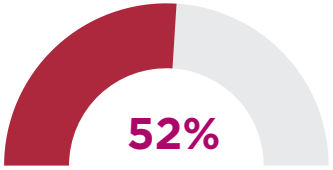
En cuanto a la proporción de casos de fraude consumados en las empresas, un **52,17%** de las empresas reportan que representa **menos del 1% de los casos**, lo que sugiere que, aunque el fraude está presente, el nivel de control y detección en la organización es efectivo.

Un **21,74%** de las empresas experimentan que el fraude consumado se sitúa **entre el 1% y el 2,5%** de sus operaciones, mientras que el **8,70%** de las empresas indican que el fraude consumado oscila **entre el 2,5% y el 5%** de sus operaciones.

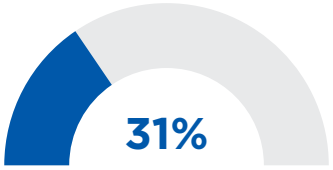
Finalmente, un porcentaje nada desdeñable, **17,39%,** reportan que el fraude consumado representa **entre el 5% y el 10%** de los intentos de fraude. Este dato, resalta la necesidad de estrategias más efectivas y adaptativas para proteger los activos y garantizar la integridad operativa.

«A pesar del aumento de casos de fraude consumados, este es inferior a la intensificación de los intentos de fraude y con un impacto inferior respecto al total de solicitudes»

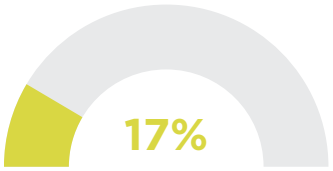
Evolución del Fraude



HA GENERADO MÁS PÉRDIDAS QUE EN EL AÑO ANTERIOR



NO HA HABIDO VARIACIÓN SIGNIFICATIVA



MENOS PÉRDIDAS GENERADAS QUE EN EL EJERCICIO ANTERIOR

«La tendencia hacia un aumento de las pérdidas por fraude en más de la mitad de las empresas destaca la necesidad de una adaptación continua de las medidas de seguridad y un enfoque proactivo para minimizar los riesgos y proteger los activos »

4.4. Pérdidas económicas a causa del Fraude

En el análisis de la evolución de las pérdidas económicas causadas por fraude en las empresas, se observa una tendencia preocupante en la mayoría de los casos.

Un **52,17%** de las empresas reportan que el fraude **ha generado más pérdidas** económicas en el año actual en comparación con el anterior, lo que sugiere un agravamiento del problema y una posible insuficiencia en las medidas de prevención y control antifraude.

Un **30,43%** de las empresas informan que no ha habido **una variación significativa en las pérdidas económica**s por fraude con respecto al año anterior. La situación, aunque estancada, no mejora, lo que requiere mantenerse alerta para abordar las amenazas emergentes.

Finalmente, el **17,39%** de las empresas indican que las **pérdidas por fraude han disminuido** en comparación con el ejercicio anterior. Una buena noticia posiblemente atribuible a la implementación de medidas más robustas de prevención y respuesta ante el fraude, y a una mejora en los procesos internos de gestión de riesgos.

Canales del fraude

5.1. Canales de fraude

El análisis de los canales a través de los cuales el fraude accede a las empresas viene a confirmar la tendencia de los últimos años.

El **43,59%** de las empresas reporta que el **canal directo online es el principal** punto de acceso para actividades fraudulentas. El entorno por excelencia que los defraudadores explotan para llevar a cabo sus ataques. La proliferación de técnicas de phishing, malware y fraudes en plataformas digitales subraya la necesidad urgente de fortalecer las medidas de seguridad cibernética y adoptar soluciones avanzadas para proteger los sistemas empresariales.

El **20,51%** de los fraudes, apuntan al **canal telefónico**, indicando que los defraudadores aún recurren a técnicas más tradicionales como la estafa telefónica y el uso indebido de información compartida a través de llamadas. Este canal puede ser vulnerable a prácticas como el vishing (phishing por voz), lo que sugiere la importancia de implementar procedimientos de verificación adicionales y capacitación para el personal que gestiona las interacciones telefónicas.

Tanto el **17,95%** de los casos atribuidos a **prescriptores o sucursales presenciales** como el **17,95%** relacionados con **prescriptores online** indican que los fraudes también pueden surgir de interacciones y transacciones a través de estos canales, aunque en menor medida que los anteriores. Estos datos destacan la necesidad de controles rigurosos para mitigar el riesgo asociado con intermediarios y representantes externos.

Sin duda, la predominancia del canal directo online en los incidentes de fraude apunta a la **criticidad a la hora reforzar las medidas de seguridad digital**. Las empresas deben centrarse en mejorar la ciberseguridad, implementar herramientas avanzadas de detección y respuesta ante amenazas, y mantener una vigilancia constante sobre todas las interacciones digitales para reducir las vulnerabilidades y proteger la integridad de sus operaciones

«El fraude online representa el 62% del total del fraude que junto al 20% del canal telefónico ofrece un 82% de fraude no presencial»

Canales del fraude

5.2. Distribución entre tipologías de clientes

El análisis de la distribución de intentos de fraude en relación con diferentes tipos de clientes revela patrones diferenciados según la naturaleza del negocio.

Para **clientes nuevos persona física,** se observa que el **78,3%** considera que los intentos de fraude son entre **frecuentes y muy frecuentes**.

En el caso de **clientes nuevos persona jurídica**, el **42,7%** de las empresas reportan que los intentos de fraude son entre infrecuentes y muy infrecuentes.

Para los **clientes conocidos persona física**, la percepción es mixta. Mientras que **43,5%** reportan que los intentos de fraude son **entre infrecuentes y muy infrecuentes,** un **47,8%** consideran que estos intentos son **bastante normales o frecuentes**. Esto indica que los intentos de fraude pueden ser más comunes cuando implican a los clientes que ya tienen una relación establecida con la empresa.

La distribución es igualmente equilibrada para **clientes conocidos persona jurídica**. Un **43,4%** considera los intentos de fraude son entre **infrecuentes y muy infrecuentes**, mientras que **30,4%** los ve como algo **normal o frecuente**. Esto puede depender de diversos factores como la industria en cuestión.

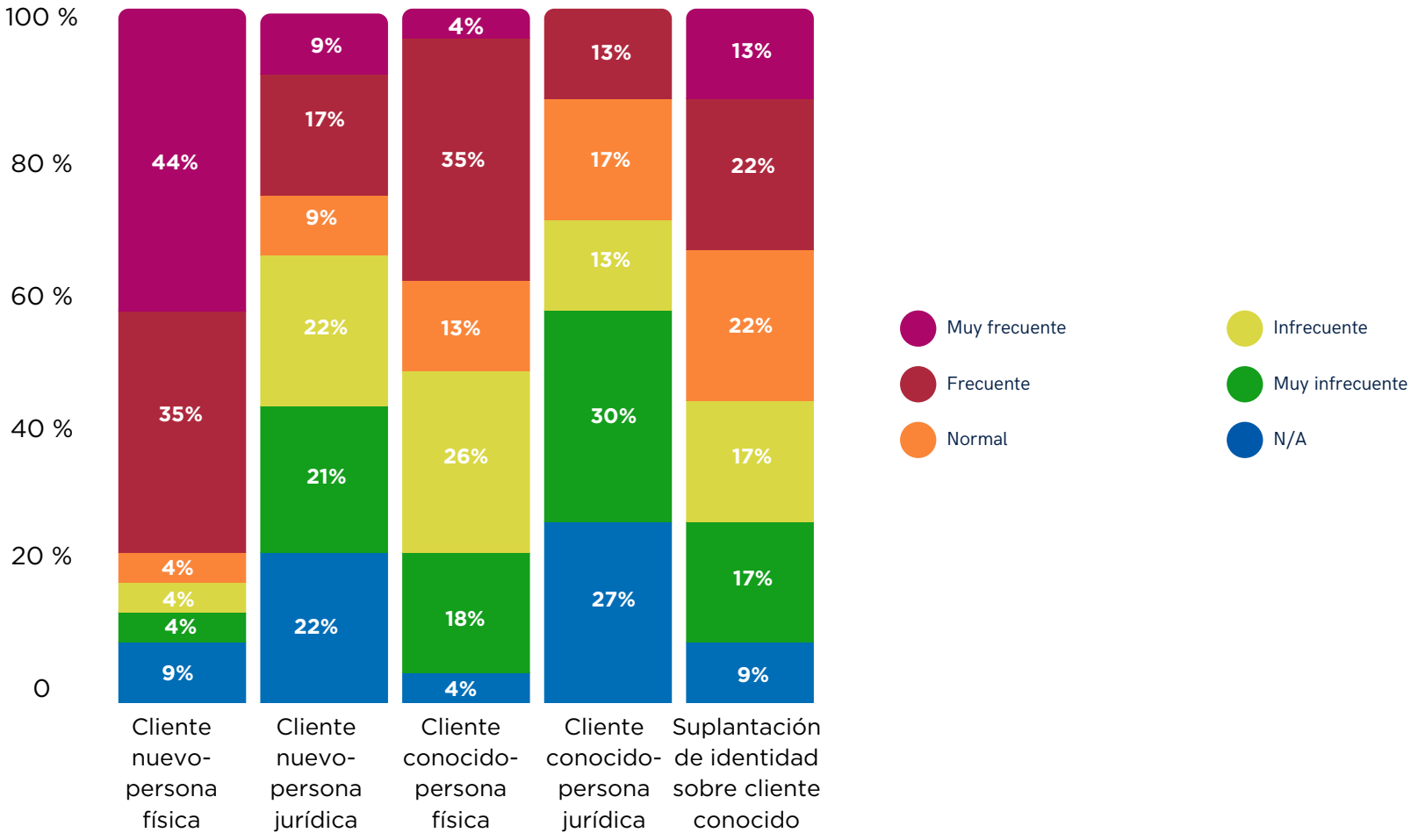
En cuanto a la **suplantación de identidad sobre clientes conocidos**, se presenta una distribución bastante equilibrada. **Un 43,4% de las empresas indican que esta modalidad de fraude es normal o frecuente, mientras que 34,8% consideran que es infrecuente o muy infrecuente**. Esto pone de relieve que la suplantación de identidad es una preocupación existente a nivel general, más o menos significativa según el modelo de negocio.

Los datos recogidos sugieren que las empresas deben adaptar sus estrategias de prevención de fraude en función de la categoría del cliente. Para los **clientes nuevos**, las medidas pueden centrarse en la **verificación rigurosa** desde el inicio de la relación. Para los **clientes conocidos**, es crucial fortalecer los **controles y la monitorización continua**. La **suplantación de identidad**, en particular, debería ser un foco clave en la seguridad de la información, dada su prevalencia en los intentos de fraude.

.

Canales del fraude

5.2. Distribución entre tipologías de clientes



Canales del fraude

5.3. Tipos de fraude

En el análisis de los tipos de fraude que afectan a las empresas, se observa una cada vez más variada gama de técnicas utilizadas por los defraudadores, cada una con implicaciones específicas para la seguridad corporativa.

El **19,35%** de los casos de fraude se atribuye al fraude de suscripción en **canales digitales**, , donde los atacantes explotan vulnerabilidades en las plataformas en línea para realizar sus actividades fraudulentas.

El **17,74%** de los fraudes se relaciona con el **robo de datos a través de malware**, **ingeniería social o hacking** para obtener información sensible. Esta categoría destaca la importancia de implementar soluciones avanzadas de ciberseguridad y formación continua para el personal sobre las mejores prácticas para evitar ser víctima de técnicas de ingeniería social.

El **14,52%** de los casos apunta al **fraude documental**, que puede incluir la falsificación de documentos y la manipulación de registros, y enfatiza la necesidad de procesos robustos de verificación y autenticación para garantizar la integridad de la documentación.

El **12,90%** de los incidentes se debe a la **apertura de cuentas mula y a estafas**, para facilitar actividades fraudulentas y blanqueo de dinero. Esto precisa una vigilancia estricta y mecanismos de control para prevenir la apertura indebida de cuentas y detectar estafas antes de que se materialicen.

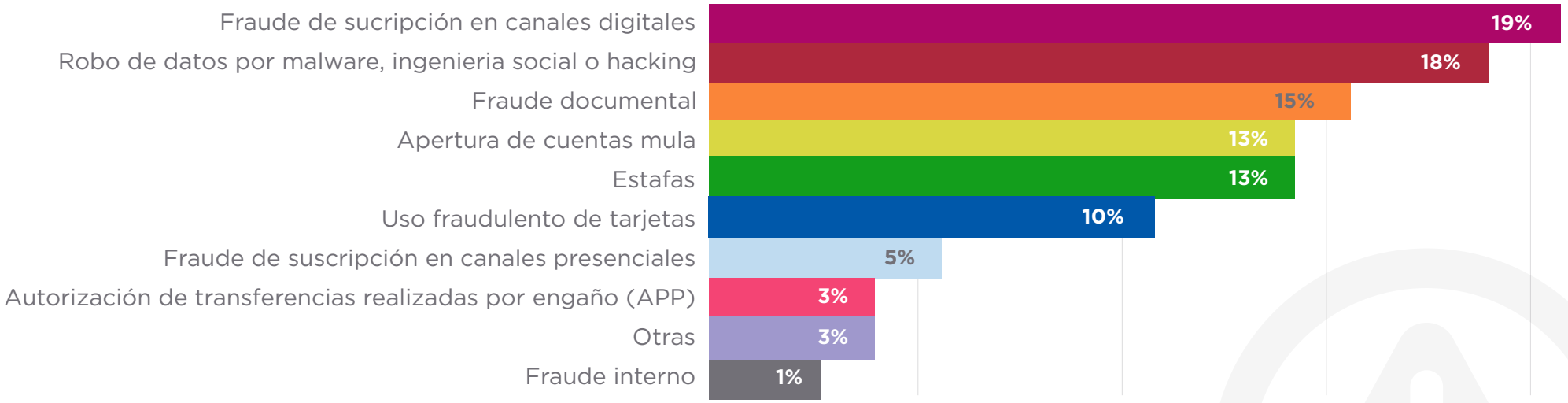
El **9,68%** de los fraudes involucra el **uso fraudulento de tarjetas**, destacando la relevancia de contar con sistemas efectivos de detección y prevención de fraudes en transacciones financieras.

El **4,84%** de los fraudes corresponde a **fraude de suscripción en canales presenciales**, mientras que el **3,23%** se refiere a **autorización de transferencias realizadas por engaño (APP)**, indicando que, aunque menos frecuentes, estos métodos también representan un riesgo significativo para las empresas.

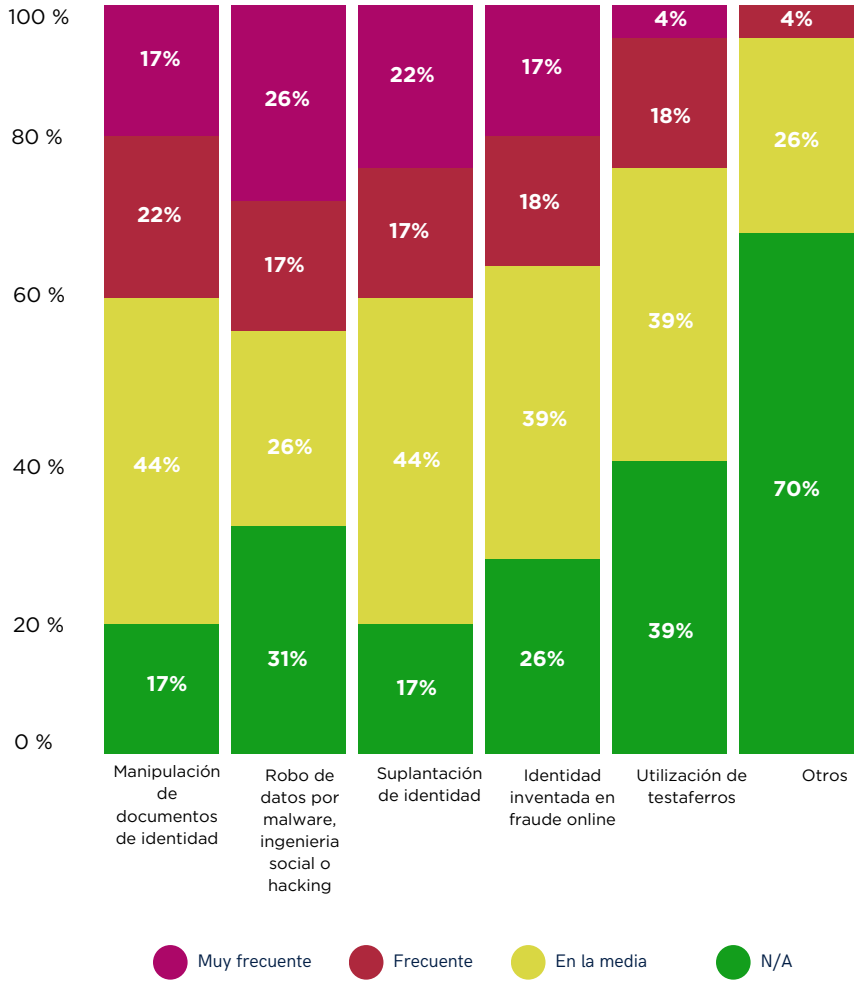
El **1,61%** de fraude interno subraya la **importancia de fortalecer los controles internos** y fomentar una cultura de **ética y transparencia** dentro de las organizaciones**.**

Canales del fraude

5.3. Tipos de fraude



Canales del fraude



5.4. Frecuencia de los tipos de Fraude a su organización

El análisis revela que las empresas enfrentan con alta frecuencia varias formas de manipulación y ataque.

La **manipulación de documentos de identidad** es percibida como un problema de **frecuente a muy frecuente** por un **39%** de las empresas encuestadas, indicando que la autenticación de identidad sigue siendo una preocupación crítica.

De igual manera, **el robo de datos mediante malware, ingeniería social o hacking afecta a un 43%** de las organizaciones con la misma frecuencia, reflejando la creciente sofisticación de los ciberataques y la vulnerabilidad de las infraestructuras digitales.

La **suplantación de identidad** también representa un desafío significativo, para el **39%**, sugiriendo que la protección contra identidades falsas sigue siendo insuficiente en muchas entidades.

Por otro lado, **la identidad inventada en fraude online afecta al 35%** de las empresas encuestadas con una frecuencia similar (frecuente o muy frecuente) , lo que resalta los riesgos asociados con el registro y verificación de identidades en entornos digitales.

La utilización de testaferros es reportada **de frecuente a muy frecuente** por el **22%** de las empresas, aunque casi un **40% de las entidades no enfrenta este tipo de fraude,** lo que podría sugerir una variabilidad en la prevalencia de este fenómeno según el sector o tipo de operaciones.

Herramientas contra el fraude

7.1. Herramientas contra el fraude

El **perfilado interno de clientes (65,2%)**, como en anteriores estudios, es la herramienta más utilizada por la mayoría de empresas para identificar fraudes basados en su propia experiencia.

La **validación del documento identificativo (60,9%)** y la **verificación de identidad/prueba de vida (60,9%)** son ampliamente utilizadas como principal herramienta de validación de identidad online de clientes nuevos, aunque con un grado de satisfacción medio, como veremos a continuación.

Por su parte, las **bases de datos de fraude compartido (56,52%)** y las **bases de datos externas (52,17%)** son también herramientas clave, lo que indica una tendencia a utilizar información de terceros para complementar y reforzar las medidas internas de seguridad.

El análisis o **verificación del dispositivo (43,48%)** y el **análisis del comportamiento online (30,43%)** son menos utilizadas en comparación con las anteriores. Sin embargo, su uso es crucial para detectar fraudes más sofisticados que podrían no ser identificados a través de métodos más tradicionales.

Herramientas de **Machine Learning (21,74%) y Openbanking (21,74%)** aún son utilizadas por un porcentaje menor de empresas. Así como otras herramientas como el **análisis de la reputación del email (13,04%), la información del número de teléfono (8,70%), Opendata (4,35%), y Otras (4,35%)**. Estas herramientas son menos comunes y probablemente son utilizadas en escenarios específicos o como complementos a las herramientas principales.

El uso del **análisis de titularidad del teléfono no es reportado por ninguna empresa encuestada**, lo que podría indicar la preferencia por alternativas más eficientes.

Herramientas contra el fraude

7.2. Satisfacción de las herramientas

En base al actual análisis, las **bases de datos en general,** las herramientas de **Machine Learning**, y la **verificación del dispositivo** utilizado por el cliente, son las herramientas que obtienen mayor satisfacción entre los usuarios.

El **análisis o verificación del dispositivo utilizado por el cliente encabeza el ranking, con un 75%** de satisfacción, y se erige como una herramienta crucial como barrera antifraude de primer nivel en las empresas.

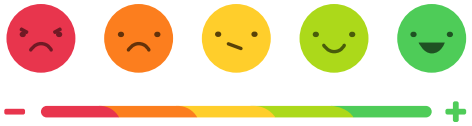
«El perfilado interno de clientes es una de las herramientas más utilizadas (78% de las entidades) y que mayor satisfacción producen (72%) y el análisis/verificación del dispositivo, aún siendo utilizada sólo por el 52% de las entidades, es la que goza de mayor reconocimiento (el 75% está muy satisfecho o satisfecho)..»

Utilizadas por el **78,2%** de las empresas encuestadas, el **perfilado interno de clientes** recibe también un **72%** de satisfacción, lo que refleja su efectividad y confiabilidad en la lucha contra el fraude. Y las herramientas de **Machine Learning** irrumpen con una aplicación del **56,5%** y una **satisfacción del 69%** de satisfacción, ayudando a detectar patrones complejos y a predecir comportamientos fraudulentos de manera más efectiva.

Las **bases de datos externas y bases de datos de fraude** compartido cuentan con una consolidada posición en las organizaciones y con un elevado reconocimiento y grado de satisfacción (**65% y 61%** respectivamente).

El **Openbanking y la validación del documento identificativo son evaluados con un aprobado** (50% de satisfacción), aunque la segunda tiene un uso mucho más extendido. Y el **análisis del comportamiento online del cliente** , aunque se aplica e

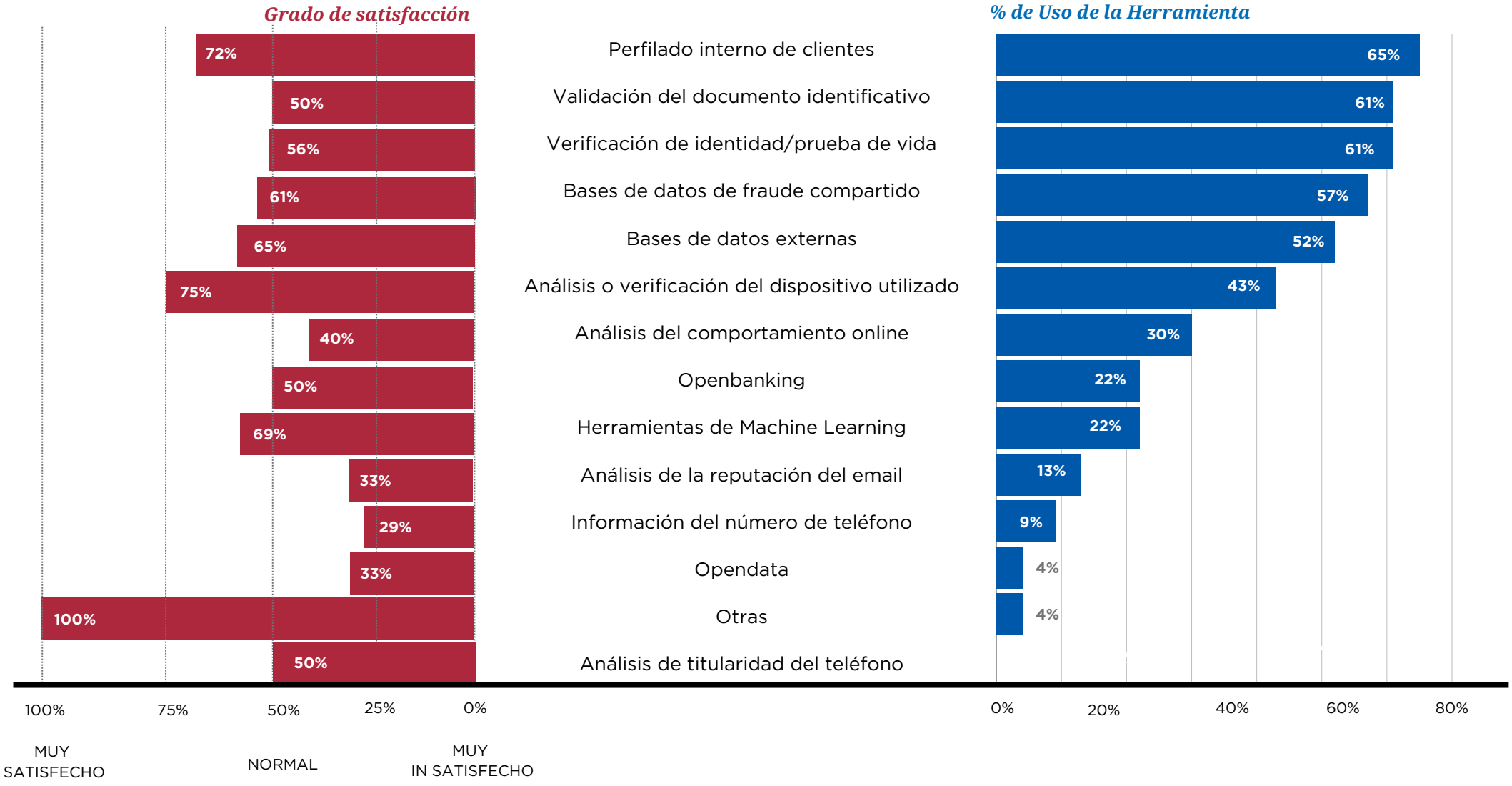
Por otro lado, herramientas como el **Análisis de la reputación del email** (**33%** de satisfacción), **Opendata** (**33%** de satisfacción), y la Información del **número de teléfono** (**29%** de satisfacción) muestran un menor reconocimiento, lo que sugiere que pueden no cumplir con las expectativas de las empresas o no ser lo suficientemente efectivas en la detección y prevención de fraudes.



«EL Opendata, el análisis de la información del número de teléfono y de la reputación del email, son utilizadas por menos de un tercio de las entidades, y señaladas con insatisfacción por el 67% de las entidades.»

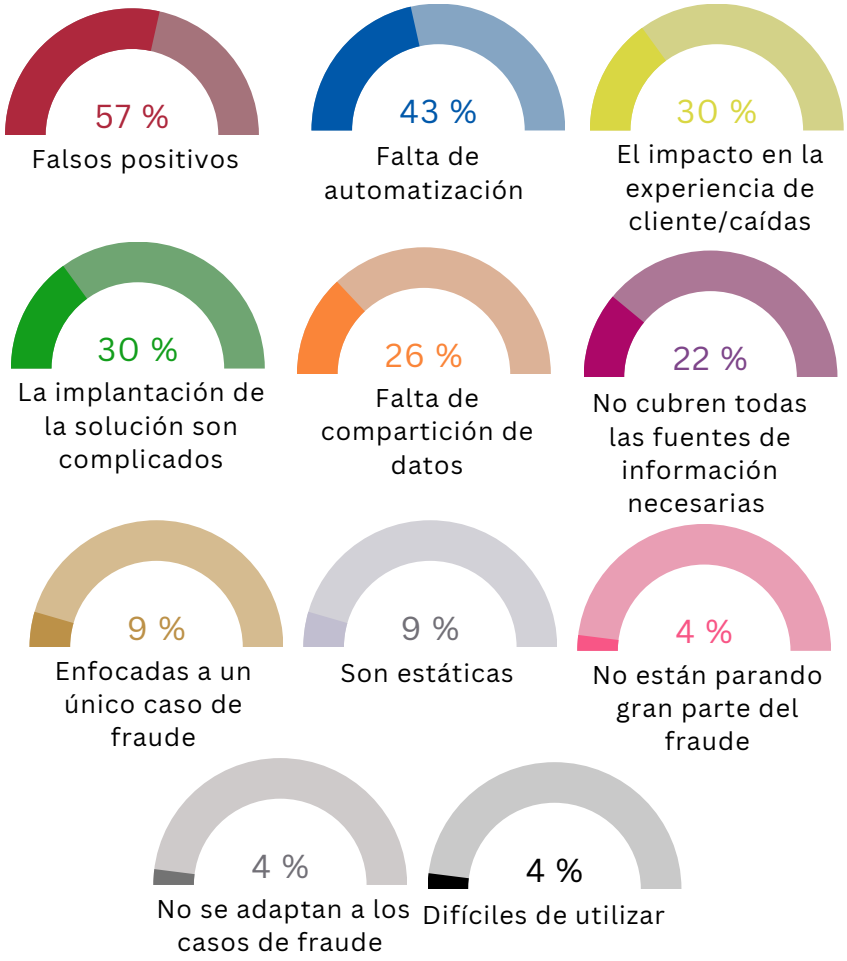
Herramientas contra el fraude

7.2. Satisfacción y % de utilización de las herramientas antifraude



Herramientas contra el fraude

7.3. Problemas con las herramientas



Los datos reflejan que las herramientas necesitan mejoras y seguir evolucionando para maximizar su efectividad y minimizar sus impactos negativos.

La alta incidencia de **falsos positivos** es un problema crítico para el **57%** de las empresas encuestadas, lo que no solo afecta la eficiencia operativa, sino que también compromete la experiencia del cliente, un aspecto clave para la fidelización.

Además, la **falta de automatización** y requerir una supervisión constante por parte de gestores es una preocupación para el **43%** de las empresas, pues puede ralentizar el proceso de detección y respuesta ante fraudes, dejando a las empresas más vulnerables.

El impacto en la **experiencia de cliente/caídas de clientes** es reportado como un problema importante por el **30%**, por cómo puede comprometer la satisfacción del cliente. Asimismo las **complicaciones en la implantación** y evolución de soluciones tienen el mismo peso en la preocupación de las empresas (**30%**). Un 30% de las empresas encuentra que la implementación de estas herramientas, o sus evoluciones, es complicada, lo que puede retrasar la mejora de las capacidades antifraude y hacer que la empresa quede desfasada frente a nuevas amenazas.

El **26%** de las empresas señala la **falta de compartición de datos** como una barrera importante y el **22%** señala el problema de la c**obertura insuficiente de fuentes de información** y la necesidad de poder analizar una mayor diversidad de datos.
Por último, las empresas indican que las herramientas están demasiado enfocadas a determinado fraude o son **demasiado estáticas (9% respectivamente)** , lo que dificulta la adaptación a nuevos tipos de fraude o a las reglas del negocio.

Además, de forma minoritaria se reporta que las herramientas actuales son complicadas en su utilización, no están deteniendo gran parte del fraude que están sufriendo, o no se adaptan a los casos de su entidad, lo que subraya la necesidad de innovación continua y de adaptación de las soluciones.

Herramientas contra el fraude

7.4. Herramientas a futuro

Los datos indican que las empresas están planeando adoptar herramientas más avanzadas y automatizadas para la prevención del fraude, con un fuerte enfoque en la **verificación biométrica de identidad (26%)**, **el análisis de comportamiento online (26%)**, y el **Machine Learning (26%)**. Estas herramientas ofrecen la capacidad de adaptarse y evolucionar frente a nuevas amenazas, lo que es crucial en el entorno digital actual.

Verificar el dispositivo del cliente es otra opción presente para las empresas, con un **22%** de ellas planeando utilizar esta herramienta en el futuro.

Con menor nivel de atención, se encuentran la **validación del documento identificativo (17%)**, el **Opendata (17%)**, el **perfilado interno de clientes, las bases de datos externas y de fraude** compartido, así como el **análisis de la reputación del email**, **información del número de teléfono**, y otras (9% respectivamente).

Aunque importantes y efectivas, al poner el foco en futuras apuestas, estas últimas herramientas mencionadas tienen menos protagonismo, quizá por estar ya en la categoría de "tradicionales" o por estar también más consolidadas y muy presentes en la estrategia global de prevención de fraudes.

Inversión en prevención del fraude

8.1. Inversiones en prevención del fraude

El análisis de la **inversión en prevención de fraude** revela una fuerte dedicación de las empresas hacia la protección y la preparación frente a posibles incidentes.

En particular, un notable **86.8%** de las empresas destina recursos significativos a **campañas de concienciación para usuarios y clientes.** En contraste, un 13% de las empresas todavía muestra una inversión insuficiente en esta área.

En cuanto a los **ejercicios de simulación de continuidad de negocio y gestión de escenarios** relacionados con ciberataques, el **82.6%** de las empresas reporta una inversión significativa, destacando el compromiso con la preparación ante posibles crisis. Sin embargo, un 17.4% no alcanza el nivel de inversión deseado.

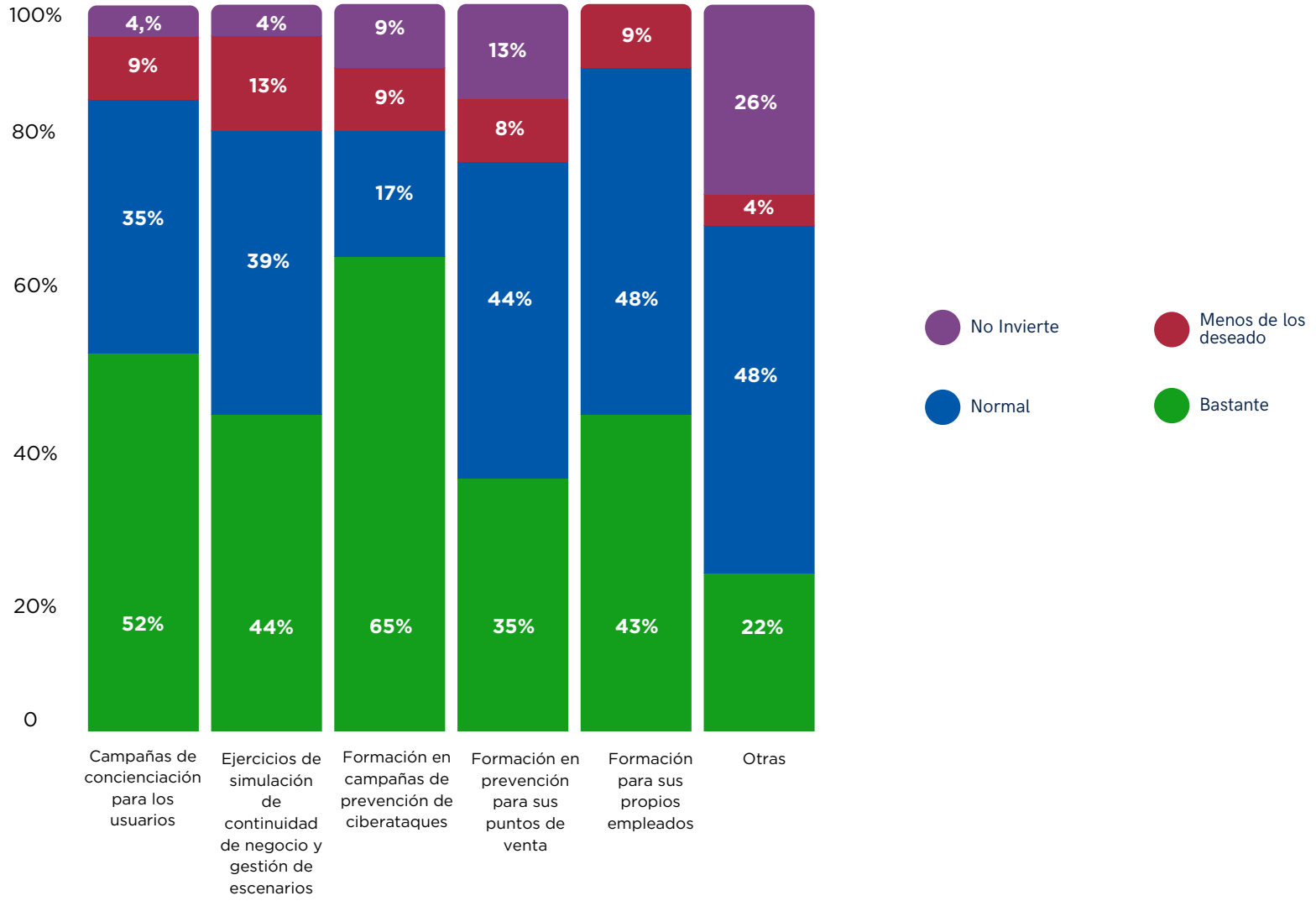
La **inversión en formación para campañas de prevención de ciberataques**, como la simulación de phishing, también es alta, con un **82.6%** de las empresas invirtiendo por encima de lo normal. No obstante, el 17.4% restante revela una brecha en la formación en ciberseguridad.

En el ámbito de la **formación en prevención para puntos de venta**, un **34.8%** de las empresas muestra una inversión considerable, mientras que un **43.5% realiza una inversión estándar.** El **21.7%** restante **no invierte o lo hace por debajo de lo necesario**, comprometiendo la prevención de fraudes en entornos físicos.

«La formación para empleados se destaca como una prioridad para el **91.3%** de las empresas, con una inversión que supera lo normal y reconoce la importancia de capacitar al personal como *primera línea* de defensa contra fraudes.»

Inversión en prevención del fraude

Inversiones en prevención del fraude

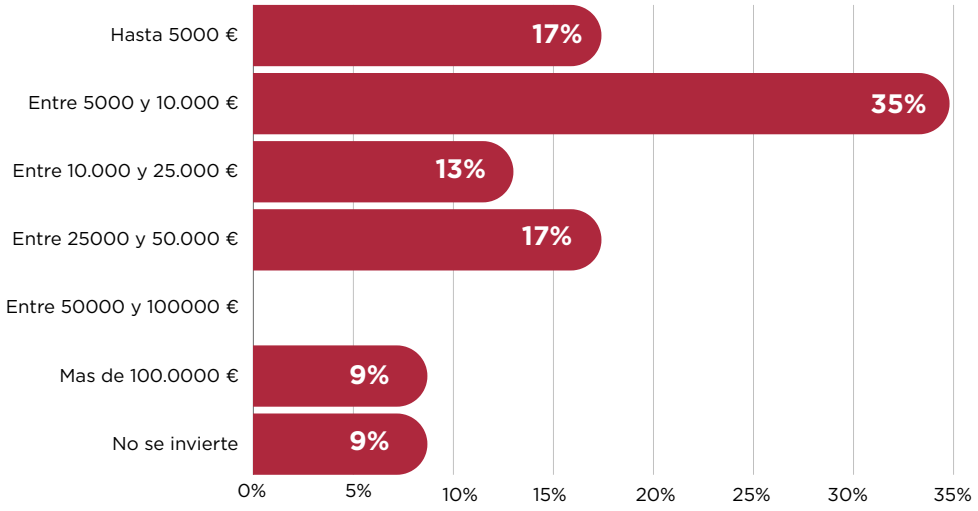


Inversión en prevención del fraude

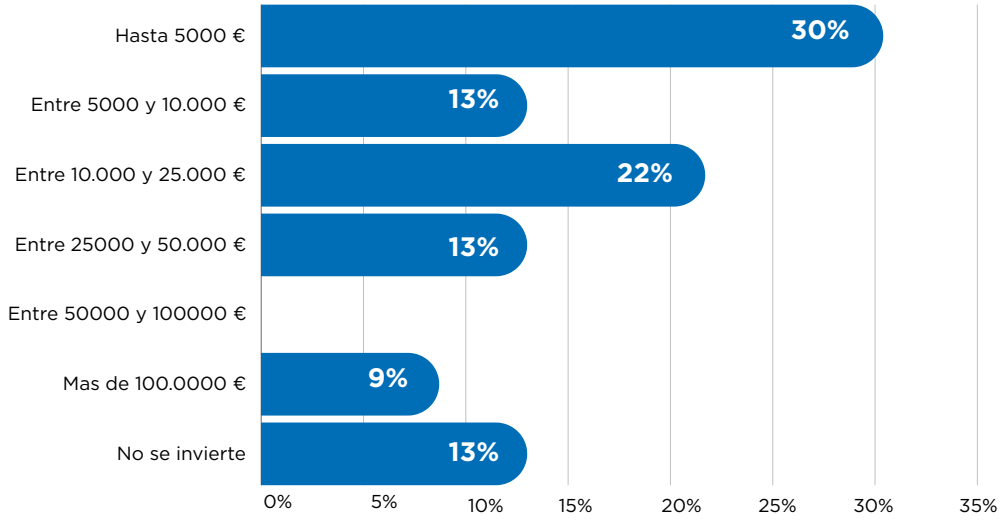
8.2. Importes destinados a prevención del Fraude

El análisis de las inversiones en acciones preventivas contra el fraude revela un panorama mixto en cuanto a los esfuerzos y recursos asignados por las empresas.

En los ejercicios de **simulación de continuidad de negocio** y gestión de escenarios de ciberataques, se observa una fuerte inclinación hacia las inversiones en rangos intermedios. Mientras que un 34.8% de las empresas invierte entre 5,000 y 10,000 euros, y un 17.4% destina entre 25,000 y 50,000 euros, solo un 8.7% de las empresas realiza inversiones superiores a 100,000 euros.



En el ámbito de la **prevención de fraude dirigida a usuarios y clientes**, las inversiones son variadas, con un 30.4% de las empresas destinando hasta 5,000 euros y un 21.7% invirtiendo entre 10,000 y 25,000 euros.

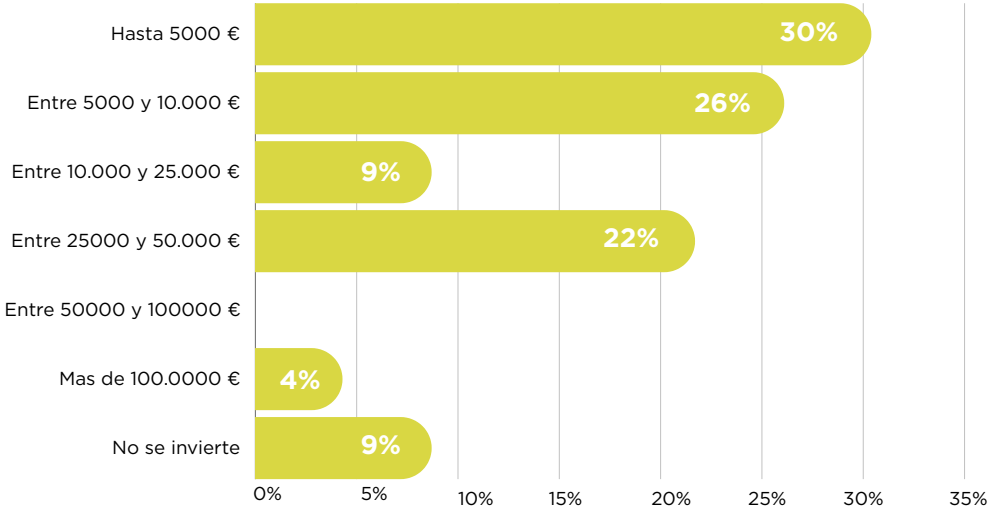


Inversión en prevención del fraude

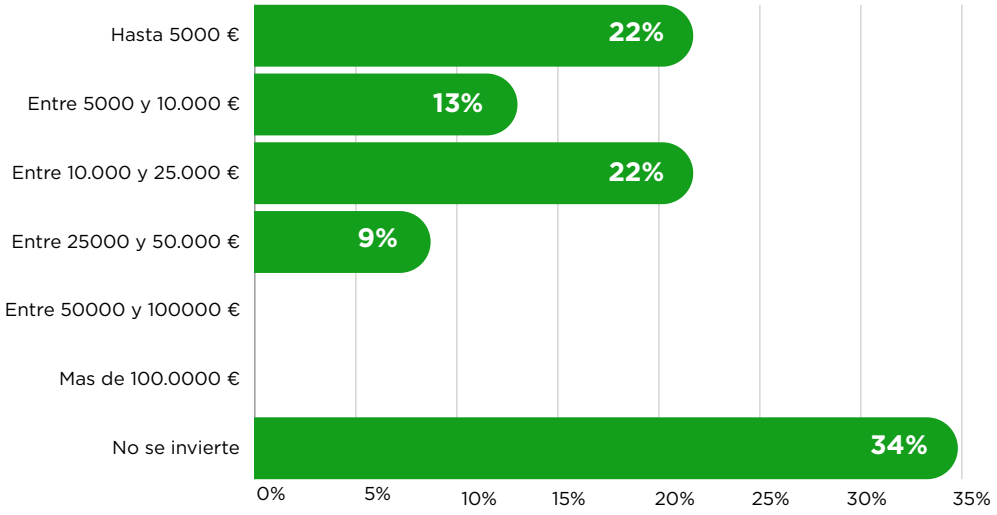
Importes destinados a prevención del Fraude

En cuanto a la **formación en prevención de fraude para empleados**, el patrón de inversión varía, con un 30.4% de las empresas destinando hasta 5,000 euros y un 26.1% entre 5,000 y 10,000 euros. Aunque una porción significativa invierte en formación, solo un 4.3% dedica más de 100,000 euros, y un 8.7% no realiza ninguna inversión.

.



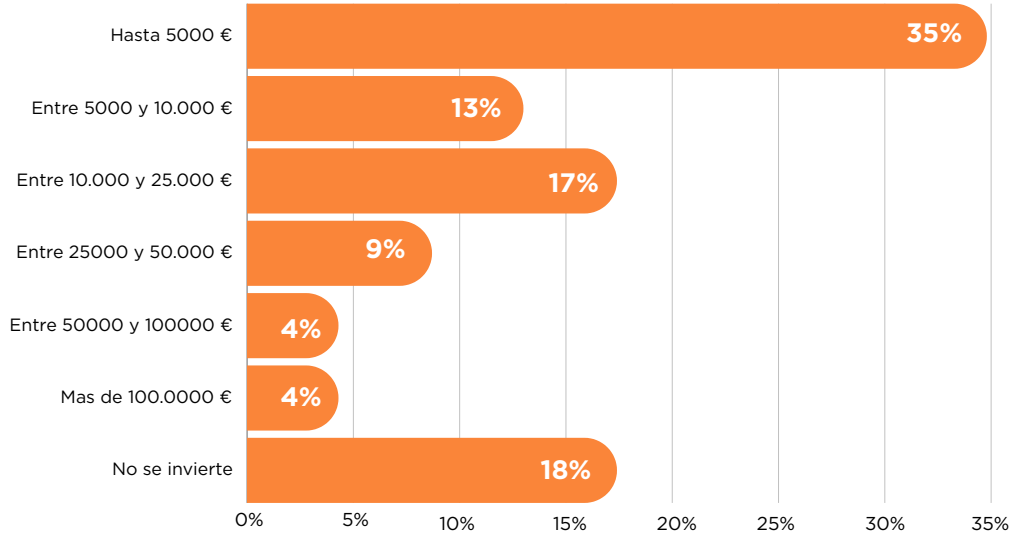
El análisis de la inversión en **formación preventiva para puntos de venta** muestra que una proporción considerable de empresas (34.8%) no realiza ninguna inversión en este ámbito, lo que es preocupante dado el potencial impacto del fraude en el punto de venta. Los porcentajes de inversión en rangos inferiores a 5,000 euros y entre 10,000 y 25,000 euros son iguales (21.7%),.



Inversión en prevención del fraude

Importes destinados a prevención del fraude

Finalmente, las **campañas de prevención de ciberataques** presentan una alta variabilidad en la inversión. Un 34.8% invierte hasta 5,000 euros, mientras que solo un 8.7% realiza inversiones en los rangos superiores a 25,000 euros. La falta de inversión en este tipo de formación por parte del 17.4% de las empresas es una área crítica que podría incrementar su vulnerabilidad ante ataques cibernéticos.



«Cabe destacar que casi el 35% de los encuestados declaran no invertir nada en formación en sus puntos de venta para prevenir el fraude. Y el 18% tampoco invierte todavía en formación a sus empleados»

Inversión en prevención del fraude

8.3. Canales de atención a víctimas de fraude

Las empresas han establecido diversos canales para facilitar la atención y resolución de los incidentes de fraude, algo muy valorado por clientes y usuarios.

Un **61,00%** de las empresas han dispuesto un **email específico** para la notificación y gestión de casos de fraude. Este canal proporciona un medio estructurado y documentado para recibir y manejar incidencias, asegurando que las solicitudes se gestionen de manera eficaz y organizada.

El **43,00%** ofrecen información en **su sitio web** sobre cómo actuar en caso de fraude, un recurso más focalizado en educar sobre los pasos a seguir.

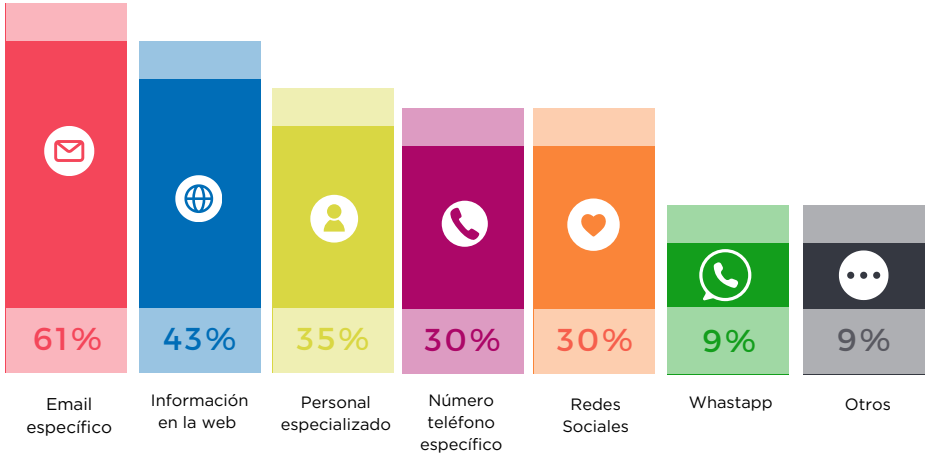
El **35,00%** de las empresas cuentan con **personal especializado** dedicado a atender a las víctimas de fraude y hacer un seguimiento exhaustivo de cada caso, mejorando tanto la resolución de los casos como la satisfacción de las víctimas.

El **30,00%** facilitan un **número de teléfono específico** para la atención de fraude, brindando una opción directa y personalizada para la comunicación con el equipo encargado de gestionar los incidentes. Y un **30,00%** utilizan además las **redes sociales** como un canal adicional para recibir reportes y proporcionar actualizaciones sobre el estado de los casos de fraude.

Solo el **9,00%** han habilitado un **WhatsApp** de la entidad, un canal rápido de comunicación, aunque menos formal que los anteriores canales mencionados.

Solo el **9,00%** han habilitado un **WhatsApp** de la entidad, un canal rápido de comunicación, aunque menos formal que los anteriores canales mencionados.

Combinar métodos tradicionales con plataformas digitales para abordar los casos de fraude, mejora la accesibilidad para la diversidad de los afectados, y permite un intercambio de información eficiente y una respuesta más ágil y efectiva frente a los incidentes de fraude.



Canales específicos para atención al fraude

Conclusiones

El informe **subraya una creciente preocupación por el fraude y su impacto en las empresas**, con una tendencia ascendente en el aumento de intentos de fraude y en consecuencia riesgo de pérdidas económicas.

Ha habido un **78% más de intentos de fraude y un 61% más de fraude consumado**. Estas cifras son muy significativas pero comparadas con el estudio anterior (84% y 68% respectivamente) nos hacen ver que las estrategias contra el fraude están funcionando.

Sin embargo, el fraude ya no se considera como algo inevitable que se provisiona como pérdida, sino que de forma creciente **se muestra como un riesgo reputacional en las entidades y como una fuente de información para la mejora de procesos y decisiones.**

La **combinación de estrategias** avanzadas de ciberseguridad, **procedimientos rigurosos de verificación**, **optimización de canales de atención y una inversión continua en formación y tecnología** son cruciales para mitigar los riesgos y proteger la integridad de las operaciones empresariales.

Los recursos contra el fraude están creciendo. Hay más personal especializado que en años anteriores**. Además, más del 85% de las entidades realiza campañas de concienciación a usuarios y clientes frente a un 74% de 2023**. Aunque falta invertir en formación a puntos de venta.

El **fraude online** representa un **62% del total** que junto al **20% del canal telefónico,** representa un abrumador 82% de fraude no presencial. Por eso, la **adopción de herramientas avanzadas y el enfoque colaborativo son cruciales** para mejorar la detección y respuesta ante el fraude.

Es una **tendencia el incremento de las inversiones en formación avanzada y las simulaciones de ciberataques**, especialmente para aquellos segmentos en los que actualmente no disponen de grandes recursos para la lucha contra el fraude. Estas acciones son cruciales para preparar al personal y garantizar una respuesta efectiva ante incidentes, incluida la formación para puntos de venta, para fortalecer la protección en entornos físicos y reducir la vulnerabilidad al fraude

La **diversificación de los canales de atención a víctimas de fraude se torna clave y parte del servicio al cliente**, asegurando que cada canal, desde email hasta redes sociales, sea gestionado de manera efectiva para mejorar la accesibilidad y respuesta ante incidentes.

Fomentar **inversiones en tecnologías avanzadas como Machine Learning y biometría puede ser fundamental para fortalecer la seguridad** y la protección contra fraudes cada vez más sofisticados.

En resumen, mientras que las **empresas han demostrado un compromiso robusto en la prevención del fraude** a través de nuevas acciones y mayores inversiones en formación, herramientas y recursos internos, **existen todavía áreas críticas que requieren atención** adicional para cerrar brechas y mejorar la eficacia general de las estrategias integrales.

www.asociacioncontraelfraude.com

AEECF

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS CONTRA EL FRAUDE

join us

contacto@asociacioncontraelfraude.com