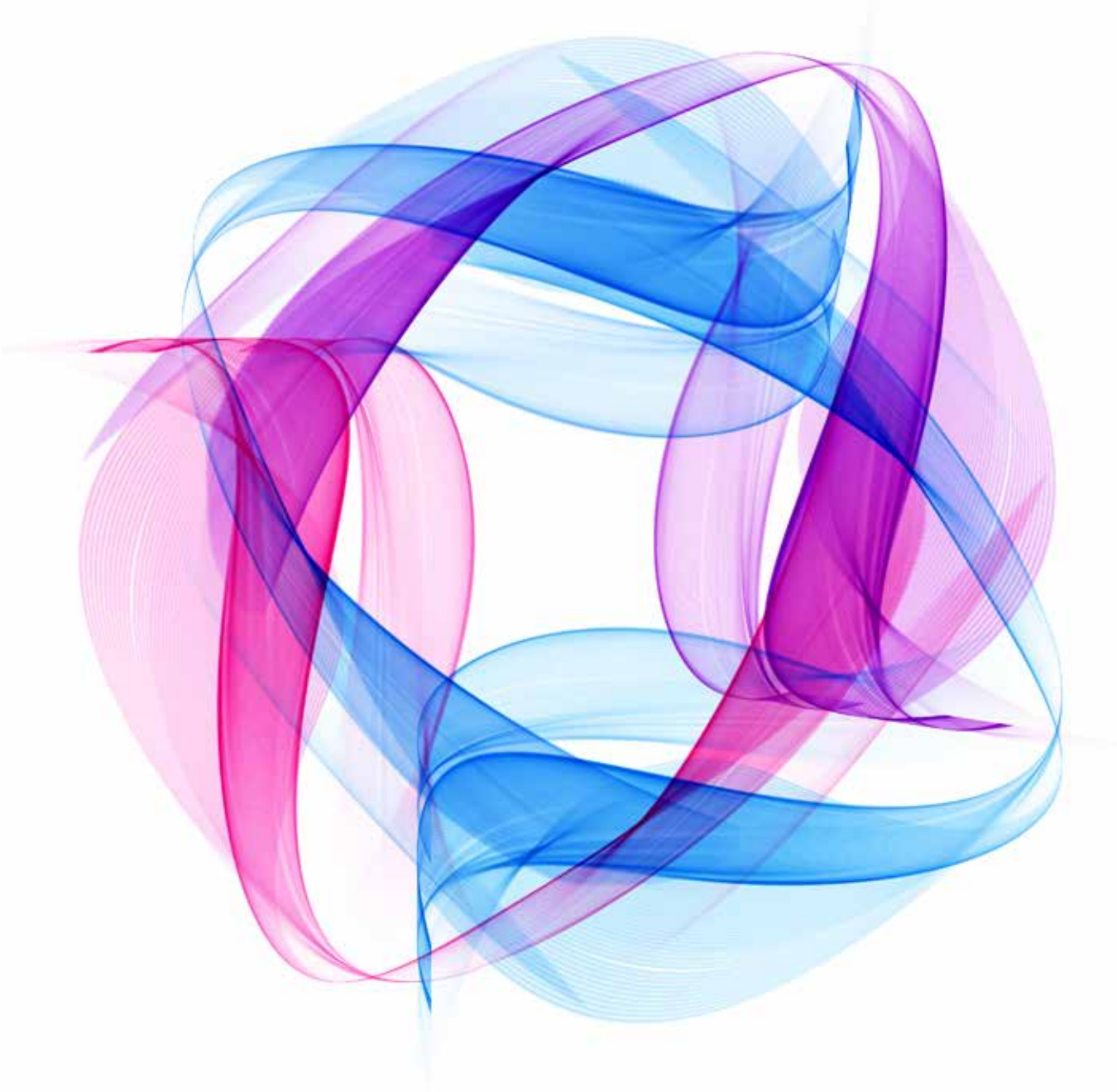
# TENDENCIAS SOBRE PREVENCIÓN Y GESTIÓN DEL FRAUDE

2018



ASOCIACIÓN ESPAÑOLA
DE **EMPRESAS**
**CONTRA EL FRAUDE**

# ÍNDICE

**Rita Estévez Luaña,** Presidenta de la AEECF

Un año más, la AEECF tiene la suerte de contar con la colaboración de sus prestigiosos asociados para elaborar un informe sobre la situación del fraude en nuestro país. Este hecho delictivo, que produce importantísimas pérdidas económicas, no ha menguado su incidencia en el mercado. Las empresas reciben cada vez más intentos de fraude, y como podemos ver en este estudio, la mayoría reconoce que los recursos dedicados a ponerle freno son insuficientes frente al inmenso desafío que se aproxima. Por otro lado, es positivo observar que los responsables no se han mantenido inmóviles y, además de tener relevancia dentro de las propias organizaciones, es una cuestión cada vez más presente en los medios y eventos especializados, que permiten una cooperación y divulgación necesaria.

El fraude siempre ha sido un escollo en la actividad de cualquier entidad, y el nuevo universo tecnológico ha multiplicado sus puntos vulnerables. Por suerte, el empresario es tan consciente del reto que supone protegerse en la era de la digitalización como de la exigencia de buscar apoyos en esta lucha. Las necesarias medidas tomadas por las compañías deben ser refrendadas por un apoyo constante del sector público, tercer vértice del sistema triangular promovido por la AEECF.

Para hacer frente a los desafíos que se nos avecinan, se incrementan las inversiones en fuentes de datos y en innovación tecnológica que proporcionan las soluciones más efectivas en prevención y verificación de identidad, así como en mecanismos de prevención y detección temprana. Empresas como Experian ofrecen soluciones activas durante todo el proceso de digitalización que permiten identificar no solo el fraude cometido por los estafadores, sino también a través de distintos dispositivos o identificando irregularidades.

A pesar del lance que se nos presenta, los progresos conseguidos en los últimos años dan cabida al optimismo. Los copartícipes de la actividad empresarial van asumiendo progresivamente la responsabilidad debida para evitar todo tipo de fraude, y a su impulso se suma la AEECF, que pone a su vez el foco en el crecimiento del número de asociados y en la promoción de iniciativas adaptadas al escenario actual para dar respuesta a la necesidad del tejido empresarial de España.

# ¿QUÉ ES LA AEECF?

Una entidad sin ánimo de lucro que, como en otros países del ámbito europeo, ayuda a establecer una plataforma colaborativa orientada a coordinar un sistema español antifraude para los asociados.



La **Asociación de Empresas Españolas Contra el Fraude** (AEECF) se constituye en 2014 como una entidad sin ánimo de lucro para dar respuesta a la necesidad de coordinar un sistema de prevención y lucha contra el fraude a través de una plataforma pionera de colaboración entre empresas. Ese mismo año, la Agencia Española de Protección de Datos avala la puesta en marcha de un sistema sectorial de lucha contra el fraude y, dos años después, su extensión para implantar un proyecto multisectorial entre estamentos y compañías que conforman el tejido empresarial español.

En la actualidad, la AEECF cuenta con asociados pertenecientes a los sectores que más sufren el impacto del fraude: Banca, Financieras de Automoción, Financieras de Consumo, Fintech y Telecomunicaciones.

## Objetivos de la AEECF

- Proteger los intereses de los asociados frente a la comisión o tentativa de actos fraudulentos.
- Promocionar y difundir sistemas y medidas para evitar el fraude, especialmente en lo referido a suplantación de identidad o falsificación de documentos y estafas digitales.
- Trabajar, en colaboración con las administraciones, para fomentar el establecimiento de políticas activas de previsión.
- Instaurar sistemas de participación tanto pública como privada para combatir el fraude en todas sus vertientes.
- Fomentar una cultura de prevención del fraude.

## Retos de las entidades asociadas

- La implantación de mecanismos de prevención del fraude en los procesos y sistemas de las organizaciones.
- La identificación de los delincuentes, especialmente de los reincidentes, y puesta en conocimiento de los Organismos adecuados.
- La detección temprana del fraude o prevención del mismo.
- Asegurar un correcto funcionamiento de los mecanismos de control y prevención del fraude sin impactar negativamente en la calidad del servicio y experiencia del cliente.

# EL ESCENARIO DEL FRAUDE EN 2017 SEGÚN NUESTROS ASOCIADOS

Cada año la AEECF acude a sus asociados para trazar un escenario del fraude en España. En 2017, estas empresas de altísimo nivel y presencia en el mercado relataron de esta forma los aspectos que más inquietaban a algunos de los sectores más castigados del mercado.

**Como cada año,** la AEECF acudió a sus asociados para trazar un escenario del fraude en España. Los resultados de la encuesta realizada por la Asociación evidenciaban un incremento de las actividades fraudulentas en España, circunstancia común a todos los sectores encuestados.

Las dificultades a las que se enfrentan las empresas a la hora de detectar el fraude interno y demostrar que ha existido por parte de un tercero van de la mano de una visión muy positiva sobre la gestión del riesgo en nuestro país. En concreto, más del 77% de los encuestados se mostraron satisfechos de los cauces abiertos para atajar las amenazas del fraude.

Si bien la cooperación y coordinación multisectorial es uno de los métodos más efectivos para desarrollar estrategias de lucha y prevención del fraude, la barrera legal fue señalada como el principal impedimento para compartir información entre diferentes sectores. Ante esta predisposición, la AEECF pide reformar las leyes de protección de datos y permitir la generación de espacios comunes, y promueve un sistema triangular que facilite el intercambio de información entre empresas del mismo sector, empresas de diferentes sectores afectadas por fraude en todas sus formas y entre el sector empresarial y el sector público.

Respecto a la localización del fraude, aunque casi el 60% de los encuestados coincide en que no es un fenómeno delimitado, sí señalan seis regiones como las más comunes en esta materia. Destacan Cataluña, Comunidad Valenciana y Andalucía como las tres donde más fraude se detecta, seguidas de cerca por la Comunidad de Madrid, reseñada principalmente por el sector de Automoción.

En un momento en el que la transformación tecnológica es clave en la evolución de los mercados, era imperativo incluir en esta encuesta preguntas para valorar el impacto de la digitalización en esta materia. La práctica totalidad de los participantes afirmaron que un aumento de sus negocios digitales va acompañado de una mayor exposición al riesgo, y sin embargo no consideran que conlleve necesariamente un impacto significativo sobre sus balances.

**77%** DE LOS ENCUESTADOS SE MOSTRARON SATISFECHOS DE LOS CAUCES ABIERTOS PARA ATAJAR LAS AMENAZAS DEL FRAUDE

# RGPD Y LA COMPARTICIÓN DE DATOS

Empresas pertenecientes a todo tipo de sectores llevan tiempo sufriendo casos de fraude, en los que es frecuente encontrar suplantaciones de identidad o falseamiento de datos que perjudican no solo a las empresas, sino también a otros individuos, víctimas de este tipo de actividades fraudulentas, cuyos nombres o datos se utilizan sin su conocimiento con la intención de cometer un fraude.

**El Sistema Nacional de Prevención del Fraude** o plataforma de compartición consiste en la aportación automática de datos de solicitudes a un sistema común entre entidades de diferentes sectores. Dicho sistema está configurado a través de una serie de "reglas" que permiten que se generen alertas en los casos en los que se detecta alguna incongruencia en el cruce de datos entre las distintas solicitudes. Así, estas alertas tienen un único fin: identificar posibles fraudes. Cada entidad deberá decidir cómo gestionar las solicitudes en las que se genere alguna alerta.

Dicho esto, las entidades, como responsables del tratamiento de datos, tienen la obligación de informar a los afectados indicando específicamente que los datos de la solicitud serán cruzados con los que figuran en las solicitudes de otras entidades de otros sectores. Así mismo, tienen que informarles de que la finalidad del tratamiento es la prevención del fraude.

¿Afecta el nuevo Reglamento General de Protección de Datos a la compartición de los mismos? A esta pregunta podemos responder de manera breve: el Sistema Nacional de Prevención del Fraude, o plataforma de compartición de datos, no se ve limitada para intercambiar información entre entidades bajo el nuevo RGPD. Esto es así porque la finalidad del tratamiento sigue siendo la misma: prevenir el fraude sobre el derecho de los interesados. No obstante, las entidades deberán tener en cuenta el nuevo marco regulatorio para adaptar todos sus procesos internos.

Bajo el nuevo RGPD, las entidades deberán observar los nuevos requerimientos de la normativa para garantizar que cumplen con los principios de la misma.

## NUEVOS REQUERIMIENTOS DE LA NORMATIVA

- **Licitud, lealtad y transparencia**
  Basado en el interés legítimo y en cómo informan a los interesados.
- **Minimización de datos**
  En este caso, no se comparten todos los campos entre todas las entidades; solo los comunes. De esa manera únicamente es posible visualizar los campos en los que puede haber algún tipo de incongruencia.
- **Limitación en el plazo de conservación**
  Los datos de los interesados no se pueden mantener más tiempo del necesario. Los períodos de retención se han establecido de la siguiente manera: 1 año para los datos correctos y 5 años para los inexactos.
- **Exactitud**
  Las entidades deberán establecer medidas y procesos para rectificar los datos que no sean exactos.
- **Integridad y confidencialidad**
  Asegurar el resguardo de los datos, incluyendo la protección contra el tratamiento no autorizado.
- **Limitación de la finalidad**
  En este caso, el único fin es prevenir el fraude.

# PSD2: CÓMO AFECTA LA NUEVA DIRECTIVA AL PROCESO DE DOBLE AUTENTICACIÓN

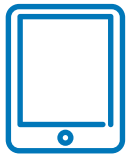
La nueva regulación europea relativa a los servicios de pago digitales PSD2 introduce cambios fundamentales en la industria de los medios de pago con el claro objetivo de potenciar el desarrollo de este mercado dentro de la UE, fomentando la innovación y la competencia, reduciendo los costes y, por supuesto, mejorando la seguridad de los pagos y la protección de los consumidores.



**Para incrementar la seguridad** de los pagos electrónicos esta Directiva promueve la creación de sistemas de autenticación reforzada SCA (Strong Customer Authentication) que, además, mitiguen la fricción en la experiencia de usuario dentro del proceso de pago.

Pero, ¿en qué consiste el sistema de autenticación reforzada o SCA? Según las recomendaciones de la nueva normativa, estos procesos de autenticación deberán contener, al menos, dos de los siguientes factores:

**> ALGO QUE SABE**
Passwords
Frases clave
PIN
Secuencia
Pregunta de seguridad



**> ALGO QUE POSEE**
Móvil
Dispositivo Wearable
Token

**> ALGO QUE ES**
Huella dactilar
Reconocimiento facial
Patrón de voz
Reconocimiento ocular

Sobre lo anterior, cabe destacar que la European Banking Authority (EBA) ha incorporado un requisito adicional: el 'Dynamic Linking'. Esto significa que la autenticación debe traducirse en un código de uso único, que está vinculado a una transacción con beneficiario e importe determinados, por lo que las modalidades quedan aún más acotadas. La consecuencia directa es que el factor de posesión siempre tendrá que estar presente.

Otro cambio fundamental es que estos mecanismos se aplicarán a los pagos electrónicos en los que, al menos, una de las partes intervinientes (ya sea beneficiario o pagador) esté dentro de Espacio Económico Europeo y no ambas, como era el caso anterior a la aplicación de esta

Directiva. Igualmente, afectará a todas las divisas oficiales, no incluyendo las criptomonedas.

Las tarjetas de crédito se han posicionado como el método estándar para realizar pagos electrónicos y las principales redes de tarjetas como Visa o Mastercard desarrollaron sus propios mecanismos de autenticación conocidos como 3D Secure, consistentes en introducir los datos de la tarjeta (número, fecha de caducidad y código de seguridad CCV o CVC) y posteriormente ser redirigidos al banco titular de la tarjeta para pasar por un segundo factor de autenticación tratándose, en la gran mayoría de los casos, de un One Time Password (OTP) enviado al titular de la tarjeta vía SMS y que deberá introducir en la página de autenticación del banco dentro de un plazo limitado de tiempo.

## Consecuencias de la implantación

Estos sistemas de autenticación y validación generan fricciones en la experiencia del cliente al introducir secuencias de control adicionales que reducen la tasa efectiva de compra. Adicionalmente, sobre todo en las aplicaciones para móviles, el proceso introduce otro tipo de distorsiones ya que 3D Secure puede redirigir al usuario de una aplicación nativa a una dirección web no optimizada para este tipo de dispositivos. En los últimos años, este protocolo de primera generación ha perdido su fortaleza inicial debido a debilidades inherentes al SMS, medio más común de intercambio de OTP. Las técnicas de intercepción del mensaje se han multiplicado (hack del sistema SS7, fraude en portabilidad), y se han democratizado (SIM Swap), observándose una cierta pérdida de confianza en este protocolo de uso muy extendido.

Otro de los cambios importantes en el enfoque de la UE fue la traslación de la responsabilidad en la decisión sobre el uso del SCA del banco adquiriente al banco emisor (o sus PSP -Payment System Provider- respectivos), ya que en una transacción remota el emisor tiene la información de su cliente, pero no sabe nada del contexto de la transacción ni de las informaciones comerciales que el adquiriente puede tener. Este tema fue fuente de gran controversia por parte de los comerciantes en línea, pero no pudieron cambiar el punto de vista de la Comisión Europea al respecto.

## Consecuencias

Todo lo anterior ha llevado a desarrollar una segunda versión conocida como 3D Secure 2 (3DS2) que promueve la adecuación a los sistemas de autenticación reforzada a la par que minimiza las fricciones que experimenta el cliente durante el proceso de pago, reforzando la información compartida con el banco emisor de la tarjeta. La clave está en facilitar al banco una información mucho más rica en cada pago (algo más de cien elementos de datos relativos a direcciones de envío, ID del dispositivo, historial de transacciones, patrones biométricos, etc.) para que evalúe el riesgo de la transacción y decida si considera identificado al cliente que realiza el pago, en cuyo caso su experiencia será sin fricciones al no sufrir redireccionamientos,  o bien requiere de un control adicional, tal y como en el proceso actual.

Igualmente, dentro del esquema SCA se han identificado ciertas transacciones que podrían quedar exentas para favorecer los flujos sin fricciones y que quedarían resumidas en la siguiente tabla:

<table>
<tr><th colspan="2">TRANSACCIONES QUE PODRÍAN QUEDAR EXENTAS PARA FAVORECER LOS FLUJOS SIN FRICCIONES</th></tr>
<tr><td>CONSULTA DE INFORMACIÓN DE CUENTA</td><td>Cuando no exista dato confidencial de pago. SCA será obligatorio solo en la primera conexión y posteriormente cada 90 días</td></tr>
<tr><td>PAGO CONTACTLESS EN TIENDA FÍSICA</td><td>Por importes inferiores a 50 euros, siempre que no se superen las 5 operaciones acumuladas o de más de 150 euros</td></tr>
<tr><td>PAGOS ESPECIALES</td><td>Tales como peajes, aparcamientos o accesos a transportes públicos</td></tr>
<tr><td>PAGOS RECURRENTES</td><td>El primer pago de la serie deberá cumplir con SCA, pero los siguientes quedarán exentos</td></tr>
<tr><td>PAGOS A BENEFICIARIO EN LISTA BLANCA</td><td>Listas establecidas por el pagador, si bien el primer pago deberá ser SCA</td></tr>
<tr><td>PAGOS PROPIOS</td><td>Cuando pagador y beneficiario sean la misma persona y coincida el proveedor de pagos</td></tr>
<tr><td>PAGOS ON-LINE</td><td>Pagos inferiores a 30 euros, siempre que no superen las 5 operaciones acumuladas o de más de 100 euros</td></tr>
<tr><td>PAGOS DE BAJO RIESGO</td><td>El proveedor de pago podrá quedar exento del SCA siempre que presente una tasa de fraude inferior a los siguientes niveles máximos por categoría de pago e importe:
<table>
<tr><th>IMPORTE</th><th>PAGO TARJETA CNP*</th><th>TRANSACCIONES ELECTRÓNICAS</th></tr>
<tr><td>Hasta 100€</td><td>0,13%</td><td>0,015%</td></tr>
<tr><td>Hasta 250€</td><td>0,06%</td><td>0,010%</td></tr>
<tr><td>Hasta 500€</td><td>0,01%</td><td>0,005%</td></tr>
</table>
(*) CNP: Card Not Present<br><br>En cualquier caso, los importes superiores a 500 euros no tendrán exención SCA</td></tr>
</table>

De la tabla anterior cabe destacar tanto las bajas tasas de fraude como el importe máximo para alcanzar las exenciones del SCA. En este caso, se plantea un límite máximo muy similar al observado en pagos ‘Chip & PIN’, por lo que será casi siempre necesario.

Está claro que todos estos cambios, retos y riesgos van a modificar en profundidad el paisaje de los servicios de pago, acelerar la innovación tecnológica y modificar sustancialmente las estrategias de prevención y gestión del fraude.

# TENDENCIAS Y PREOCUPACIONES DEL MERCADO

Para obtener una visión de las tendencias y preocupaciones del mercado en materia de fraude, la AEECF ha acudido a sus asociados para conocer de primera mano qué opinan sobre aspectos clave de esta actividad delictiva. En la encuesta han participado los directivos de algunas de las empresas más representativas de cinco sectores: Banca, Financieras de Automoción, Financieras de Consumo, Fintech y Telecomunicaciones.



## ¿Cómo perciben los asociados el fraude?

**Para elaborar este informe,** la AEECF ha recogido las opiniones de los asociados mediante un sondeo especialmente diseñado para entender la evolución del fraude en España. La consulta se realizó en febrero de 2019, y con los resultados se dibuja el escenario del fraude durante 2018. Esta encuesta continúa la línea de ejercicios anteriores, permitiendo realizar una comparativa sobre la evolución de los aspectos clave en materia de fraude.

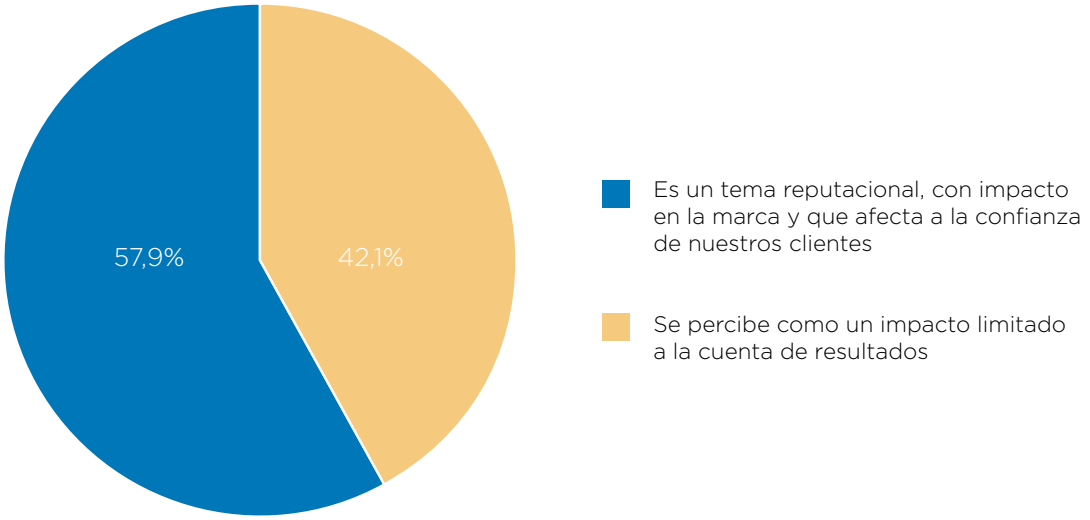
En esta ocasión, los encuestados pertenecen a los siguientes cinco sectores: Banca (15,8%), Financieras de Automoción (26,3%), Financieras de Consumo (36,8%), Fintech (10,5%) y Telecomunicaciones (10,5%).

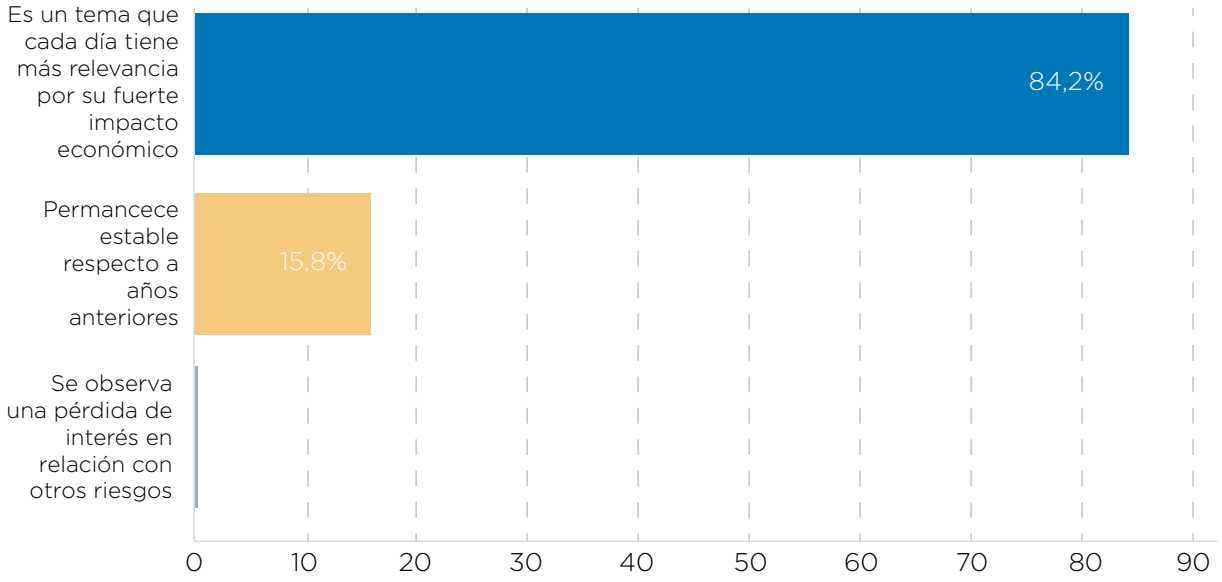
A tenor de los resultados, es indudable que el fraude sigue siendo una materia de suma importancia en el tejido empresarial de nuestro país, ya que cerca del 85% de los encuestados considera que es un tema que cada día tiene más relevancia por su impacto económico.

Aunque hay cierto consenso sobre la correcta divulgación que se hace en redes, medios y eventos especializados, existe un considerable número de empresas que opinan que tanto la dotación interna como las soluciones ofrecidas por el mercado para hacer frente al fraude son insuficientes dada su intensidad.

**¿Cómo percibe su organización el impacto de los casos de fraude?**

En materia de fraude, preocupa mayoritariamente el impacto que tiene sobre la marca y la confianza de los clientes, sobre todo para Banca y Financieras de Consumo. Las Financieras de Automoción y Telecomunicaciones reparten los pesos entre las dos visiones, mientras que las Fintech coinciden en señalar que el impacto se limita a la cuenta de resultados.



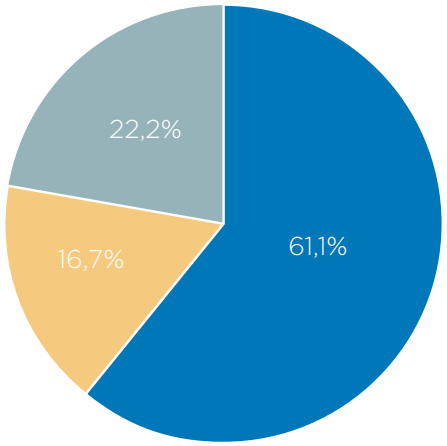




**¿Cómo valoraría la importancia que las organizaciones empresariales están dando a la prevención del fraude con respecto a los dos últimos años?**

Existe un amplio consenso en señalar que la prevención del fraude cobra una importancia creciente dentro de las organizaciones dado su impacto económico, si bien es cierto que más de un 15% de los encuestados consideran que esta actividad permanece estable respecto a años anteriores.

**La nueva directiva en materia de Servicios de Pagos Digitales (PSD2) introduce cambios significativos respecto a la compartición de información con los iniciadores de pagos o los agregadores de cuentas; en este sentido ¿cómo percibe su organización esta tendencia?**

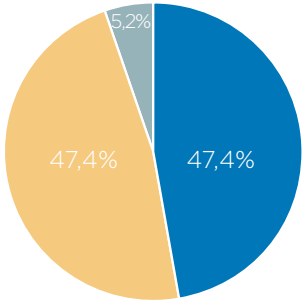
Si bien más del 60% de los encuestados considera que supone una oportunidad, existe una parte de los mismos (mayoritariamente del sector de Automoción) que ve un riesgo adicional en las nuevas vías que se abren para cometer fraude.




- Ofrece una clara oportunidad que es una apuesta hacia los esquemas de información completa
- No implica cambios significativos respecto a la situación anterior
- Supone un riesgo adicional puesto que introduce nuevas vías para los intentos de defraudara las organizaciones

**¿Cómo valora la calidad de los recursos dedicados en su organización a la prevención y gestión del fraude?**

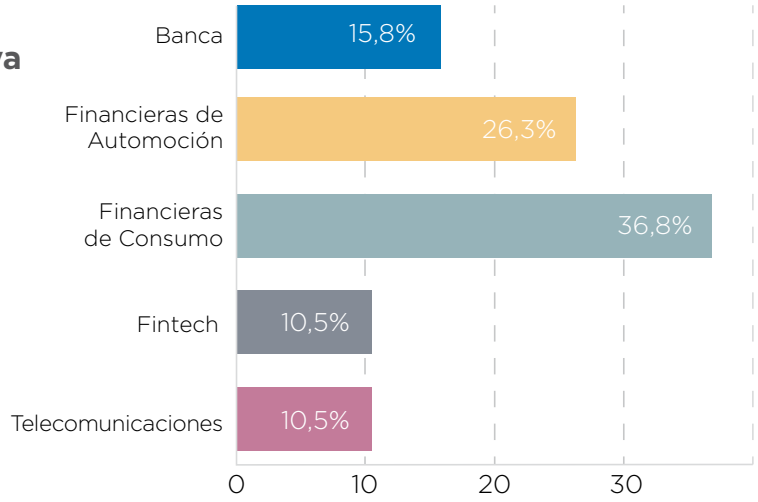
A tenor de los resultados de la encuesta, se aprecia que la cualificación de los recursos dedicados a la lucha contra el fraude es muy elevada, ya que solo un 5,2% de los encuestados identifica una necesidad de mejorar los perfiles de analistas.




- Nuestros recursos cuentan con una alta cualificación y especialización que permite anticipar y mitigar nuevas formas de fraude
- Necesitamos reforzar la capacitación, bien con formación adicional o mediante perfiles más especializados
- Cuentan con una calidad adecuada a las necesidades actuales

**¿Desde qué sectores nos dan su perspectiva del escenario del fraude?**

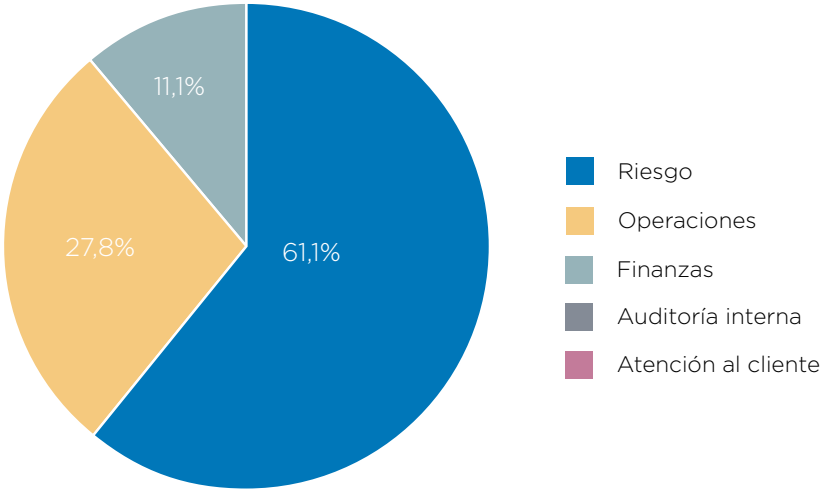
Los asociados que han colaborado en la elaboración de este informe pertenecen a algunas de las áreas empresariales más castigados por el impacto del fraude.

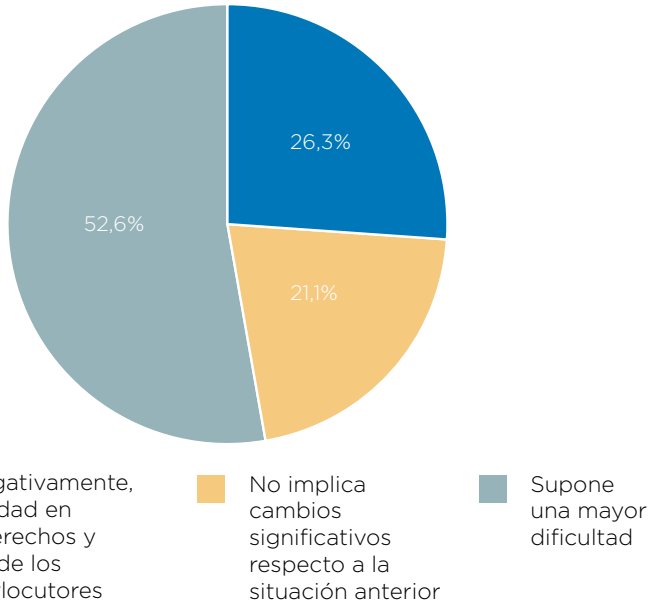


**¿Qué área de su organización tiene entre sus responsabilidades la prevención del fraude?**

Los encuestados atribuyen mayoritariamente la gestión del fraude al área de Riesgos, existiendo grandes diferencias entre sectores, donde el 90% de Banca y Financieras de Consumo presentan esta distribución, reduciéndose al 60% en Financieras de Automoción y al 50% en Fintech y Telecomunicaciones. El área de Operaciones se postula como la siguiente en peso relativo en todos los sectores.

Preguntados, además, sobre la involucración de otras áreas en la prevención del fraude, la totalidad de los encuestados coincide en que existe una cultura contra el fraude bien instaurada, o que al menos se va adoptando a buen ritmo .



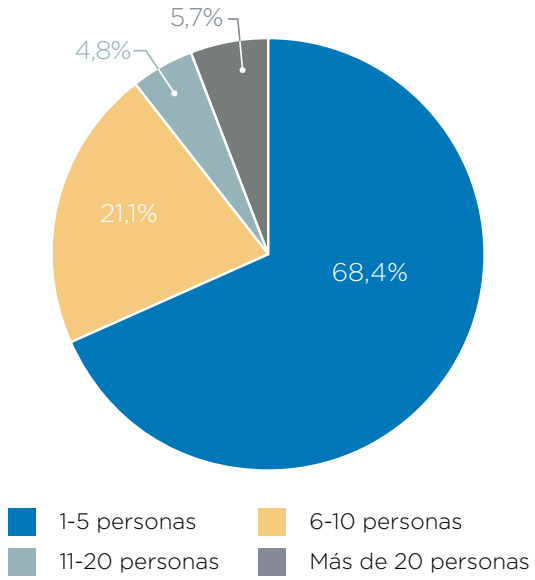




**En 2017, más del 77% de los encuestados señalaba como principal impedimento para compartir información la barrera legal. En este sentido, ¿cómo califica la nueva normativa RGPD?**

En el último informe sobre la visión del fraude desde la perspectiva de las empresas españolas, la barrera legal era percibida como el obstáculo más relevante. Desde entonces, ha entrado en vigor el nuevo Reglamento General de Protección de Datos, que divide la opinión de nuestros asociados sobre la incidencia de esta. Aunque gran parte de los encuestados afirma que la regulación no afecta negativamente o no supone cambios significativos (47,4%), una ligera mayoría reconoce que conlleva mayores dificultades.

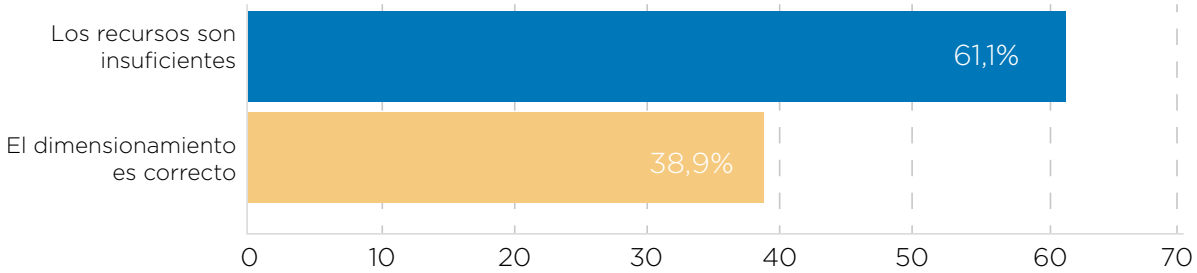
**¿Podría indicar aproximadamente la dotación de recursos dentro de su organización para el análisis y seguimiento de los casos de fraude?**

El número de personas destinadas a la gestión de todos los incidentes de esta materia delictiva no supera, en la mayoría de los casos, la decena. La excepción la marca, por unanimidad, el sector de Telecomunicaciones, que alcanza e incluso llega a superar la veintena.




**¿Considera que la dotación es acorde a los retos actuales?**

En este caso, una mayoría de encuestados opina que los recursos destinados a la gestión del fraude son insuficientes. De estos, un 70% opina así por el entorno de negocio creciente en complejidad, mientras que el resto señala a los volúmenes de actividad.




## TIPOLOGÍAS DE FRAUDE

Preguntados por las tipologías de fraude a las que más importancia otorgan entre los asociados, destaca claramente el fraude de admisión con más foco en canales digitales que presenciales. A continuación, se posiciona el fraude por Malware seguido muy de cerca por los fraudes de cuenta y fraude interno.

**1.** El fraude de admisión en puntos de venta digitales

**2.** El robo de datos (Malware, Ingeniería Social o Hacking)

**3**. El fraude admisión en puntos de venta presenciales

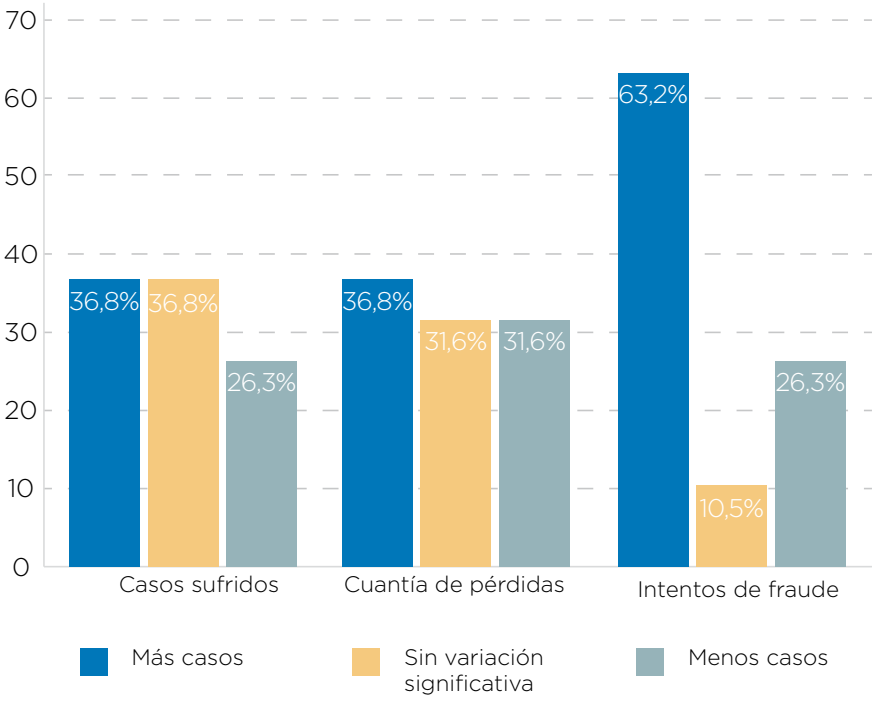
**4.** El fraude interno (empleado o vendedor)

**5.** El fraude de cuenta
(cambio de perfil o inicio de transacción tras un acceso fraudulento a la cuenta de un cliente)

**6.** Otros fraudes o estafas

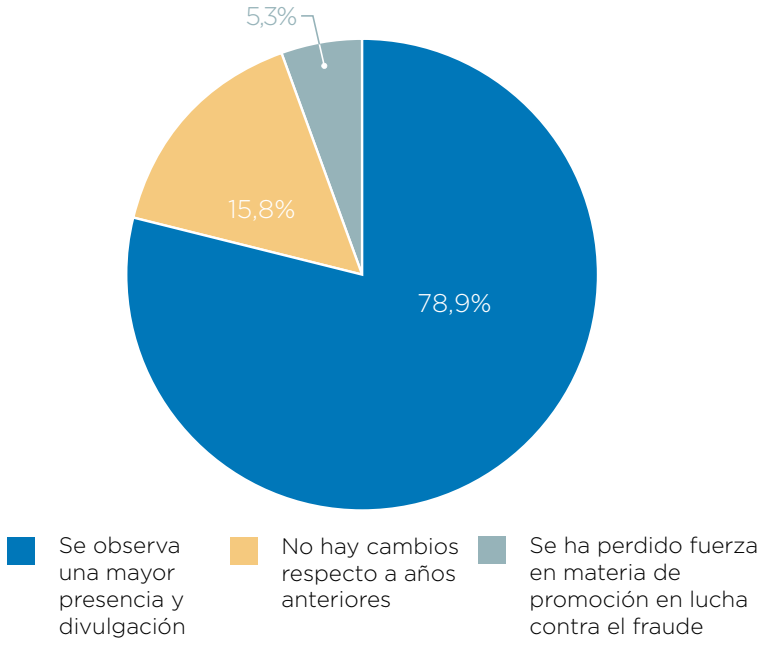
**Evolución e impacto del fraude.**

Se observa un incremento generalizado de los intentos de fraude. Un 63% de los encuestados han experimentado un mayor volumen respecto al año anterior, ratio que asciende al 100% si miramos solo a Banca y Financieras de Consumo. De la misma manera, el 74% de los encuestados alega haber sufrido un volumen mayor o similar de casos efectivos de fraude en sus organizaciones, siendo el 68,4% los que indican un impacto económico mayor o igual a los ejercicios anteriores.



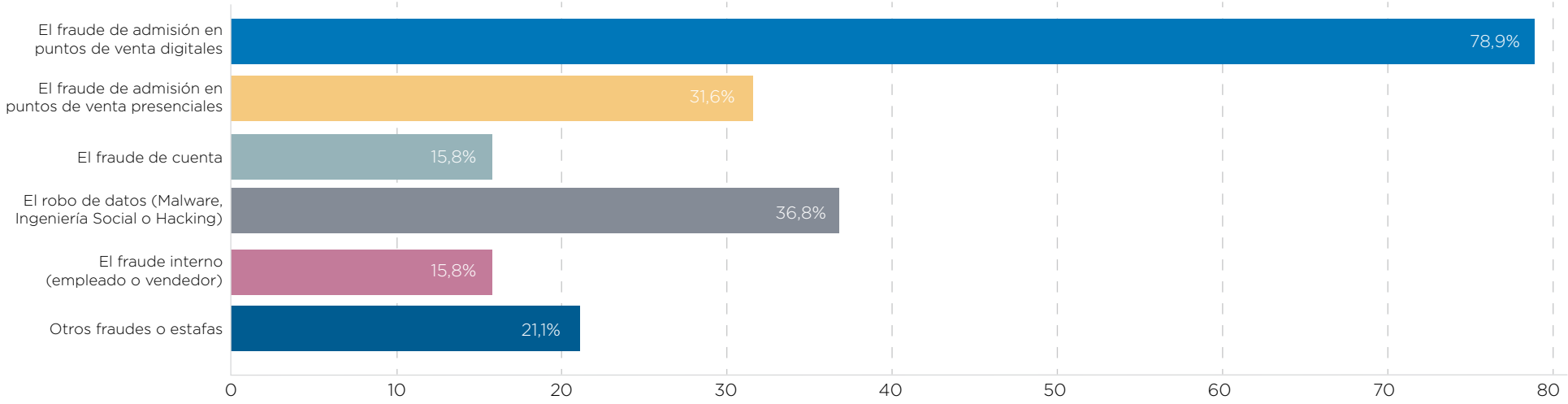

**¿Cómo calificaría la información y divulgación en redes, medios y eventos especializados en relación con los mecanismos y herramientas de detección en las organizaciones?**

La mayoría de los encuestados opina que cada vez hay más información y divulgación en la materia que nos ocupa. Nuevamente, Banca y Financieras de Consumo coinciden plenamente en esta visión, compartida también por las Fintech. Por su parte, las Financieras de Automoción están más divididas ya que el 40% consideran que no hay cambios respecto a años anteriores, subiendo al 50% en el caso de las operadoras de Telecomunicación.



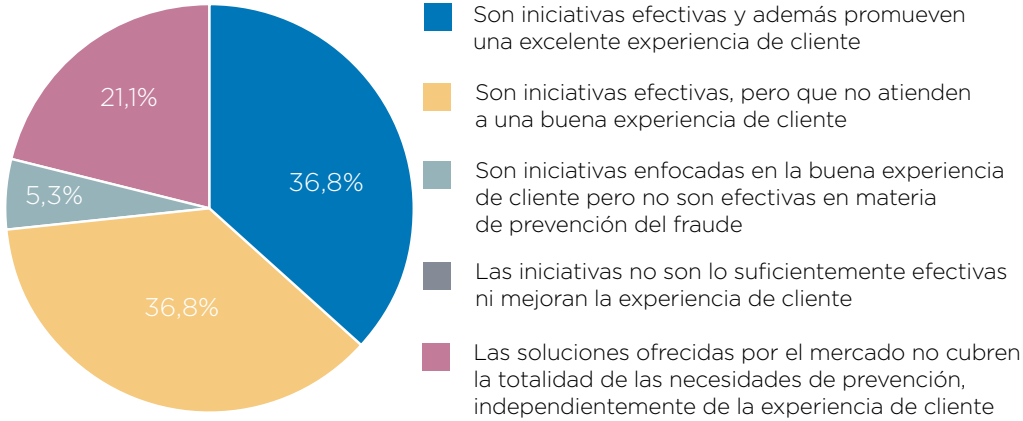
## Perspectivas para el próximo año

Esta misma estructura la encontramos al preguntar por las dos máximas prioridades del próximo año. Como primera opción se observa un amplio acuerdo en reforzar el fraude de admisión procedente de canales digitales, con un consenso del 78,9%. La segunda prioridad estaría más diversificada siendo el Malware la predilecta (36,8%) seguida en casi igual importancia por fraude en canales presenciales (31,6%), y en último lugar por variantes de fraude interno.




## ¿El mercado está aportando soluciones que realmente previenen el fraude, y que son consistentes con una buena experiencia de cliente?

Una mayoría (63,2%) no termina de estar cómoda con las soluciones del mercado, bien porque no cubren la totalidad de las necesidades de prevención del fraude o bien porque no atienden a la experiencia de cliente. El sector más conforme con la situación es el de Banca -un 66,7 % considera que son soluciones satisfactorias en ambos sentidos-.



# FUNDACIÓN UNIVERSITARIA BEHAVIOR & LAW

## RAFAEL LÓPEZ, PRESIDENTE

## DOCTOR EN PSICOLOGÍA Y ECONOMISTA

Formada por una sociedad y una fundación, tiene como objetivo principal contribuir a una sociedad más justa y segura, sobre el soporte de tres grandes pilares: la investigación científica, la formación y la divulgación en Ciencias del Comportamiento y Ciencias Forenses.

**La colaboración entre asociaciones y entidades** es imprescindible para enfrentarse al fraude, porque hace posible que se entrelacen diferentes visiones y objetivos, algo que enriquece los resultados. En concreto, desde nuestra perspectiva, es de interés un aporte desde la psicología. A continuación desgranaremos nuestra visión de la situación actual, de los riesgos y de las áreas de mejora en la lucha contra el fraude.

### Riesgos a los que se enfrentan las empresas

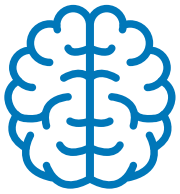
Globalización y ciberespacio. La repercusión del fraude sobre la reputación de una compañía puede ser trascendental. La existencia de un mercado global hace que inversores y clientes tengan acceso, prácticamente en tiempo real, a la información sobre una determinada entidad.

Un pequeño fraude cometido por los directivos de una empresa en un perdido punto del mapa puede tener una gran trascendencia en la confianza de inversores y clientes. Ahora más que nunca es imprescindible prevenir y detectar el fraude.

## SITUACIÓN ACTUAL

Desde nuestra perspectiva psicológica del fraude podemos ver una evolución positiva en España. Esta conducta delictiva emana de una serie de factores psicológicos y su desarrollo es fundamental para que no se llegue a cometer la conducta, el fraude.

### EMOCIONES



Es evidente que defraudar genera miedo y ansiedad por la posibilidad de ser cazado. Las consecuencias en la actualidad son mucho más duras que en el pasado, la presión por el cumplimiento es mucho mayor y no existe la sensación de impunidad que durante años existió.

# DESDE NUESTRA PERSPECTIVA PSICOLÓGICA DEL FRAUDE PODEMOS VER UNA EVOLUCIÓN POSITIVA EN ESPAÑA

La realidad de que el espacio físico y el ciberespacio conviven como mercados paralelos nos obliga a plantear nuevas estrategias en la lucha contra el fraude, que aún muchas empresas no tienen claras.

Al igual que en la actualidad hablamos del customer journey y se analiza la evolución del cliente tanto en el espacio físico como en su interacción online con nuestras compañías, deberíamos estar hablando del "defrauder journey" analizando también su interacción online.

En definitiva, el fraude online ha tenido en los últimos años una evolución exponencial y necesita estrategias concretas para el ciberespacio.

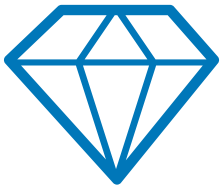
**Áreas de mejora en la lucha contra el fraude**

El error principal es no dar la importancia que se merece al fraude. En grandes compañías (por ejemplo, del sector asegurador o Retail) es habitual escuchar a los directivos afirmar que no les preocupa porque está repercutido en el precio, cuando esto solo sería aplicable en un mercado estable. Pero lo cierto es que estamos en un entorno muy competitivo, y muchas empresas consiguen bajar precios gracias a una gestión activa del fraude.

Por tanto, es imprescindible incluir el fraude como objetivo estratégico; no como algo circunscrito a un departamento, sino como una línea transversal a toda la compañía. Esto es algo que, en la actualidad, no muchas empresas hacen, y por eso existe una gran carencia de formación en concienciación, prevención y gestión de esta acción delictiva.

Como conclusión, es necesario intervenir desde una perspectiva multidisciplinar, con expertos en cumplimiento y en fraude, y con equipos de psicólogos y sociólogos que nos hagan entender la conducta de defraudador.

## VALORES



Movimientos como el Capitalismo Consciente o las Be Corporation ofrecen una visión mucho más esperanzadora de las empresas, en las cuales no solo se busca la justicia y honestidad, sino la contribución con la sociedad. Es decir, no solo se persigue un lícito objetivo económico sino también un objetivo social. Esto hará que las nuevas generaciones eviten el fraude por miedo y por convencimiento propio.

## FACTORES SOCIALES

Los factores sociales que influyen sobre la conducta de fraude, como sería el hecho de que esté bien o mal visto. Hace años no solo se cometía fraude: también se alardeaba de ello. Hoy en día esto ha cambiado de manera radical y, aunque pueda cometerse un fraude, no es algo que incremente el prestigio social.
Otro factor que incide sobre el fraude es el hecho de pensar que todo el mundo lo hace. Esto está cambiando y, sin duda, irá mermando nuestra tolerancia en términos de autoestima, de cómo nos sentimos cuando comentemos un fraude.

# WORLD COMPLIANCE ASSOCIATION

## ALBERT SALVADOR LAFUENTE, SECRETARIO GENERAL INTERNACIONAL

## AUDITOR Y ECONOMISTA

Asociación Internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del Compliance. Tiene entre sus objetivos la promoción y evaluación de las actividades de cumplimiento, además del desarrollo de herramientas de protección frente a determinados delitos cometidos por sus empleados o colaboradores.

**La lucha contra el fraude** es uno de los temas clave en la mayoría de los países; da lugar a muchas noticias y escándalos, y a pesar de ello existe poca efectividad en las políticas públicas y la gestión privada.

Del dicho al hecho, la nueva norma ISO 37001 y la UNE 19601 ofrecen herramientas concretas de lucha contra el soborno y de cumplimiento de la legalidad (y por extensión de la lucha contra el fraude). Esto supone un punto de inflexión y una oportunidad real, tanto para organizaciones públicas como privadas, de demostrar voluntad de transparencia y ética.

Muy conscientes de todo ello, desde el Comité antifraude de la WCA -integrado por miembros asociados especialistas en la lucha contra el fraude-

## SITUACIÓN ACTUAL

Desde nuestro punto de vista, y como asociación internacional en materia de cumplimiento, observamos que a nivel global, y a pesar de los esfuerzos adoptados por las organizaciones, aún queda mucho camino por recorrer.

Está sensación obtenida por la WCA, tanto en España como en los diversos países donde tenemos presencia, se refleja en los estudios publicados anualmente por otros organismos como Transparencia Internacional o ACFE.

Esta lacra social tiene ligado un coste muy elevado:

## EL FRAUDE TIENE LIGADO UN COSTE ECONÓMICO MUY IMPORTANTE, TANTO PARA LAS ORGANIZACIONES COMO PARA LA SOCIEDAD EN GENERAL

aportamos un conocimiento actualizado en materia de prevención del fraude, gestión del riesgo y valores éticos, que queremos aporten un crecimiento intelectual y personal.

Adicionalmente y de manera anual, la WCA convoca a través del menciona Comité el Congreso Nacional Antifraude, que tiene como objetivo dar a conocer todos los trabajos y estudios realizados en el último año, y que cuenta con la participación de distinguidos profesionales en esta materia, siendo una referencia nacional.

**Las organizaciones suman pérdidas del**

**5%**

**anuales (ACFE 2018)**

**La sociedad acumula**

**48.000**

**millones de euros**

**en sobrecostes en la contratación en España (CNMC 2015)**

### Riesgos a los que se enfrentan las empresas

Adicionalmente a los riesgos de fraude tradicionales, la globalización y la rápida evolución digital de las empresas han propiciado que el ciberfraude sea el mayor riesgo al que se van a enfrentar las empresas en el futuro.

Otro de los riesgos es la falsedad documental, fruto del incremento de la no presencia física en la realización de transacciones comerciales. Este elemento se debe tener muy en cuenta en el futuro.

### Áreas de mejora en la lucha contra el fraude

Si hubiera que destacar un área en el que se debe tratar de mejorar, desde WCA señalaríamos a los directivos y gerentes de la Administración Pública, que debe reconocer la existencia de fraude dentro de sus organizaciones.

Una vez conscientes de que esta realidad está ocurriendo -o puede ocurrir- dentro de cualquier ámbito, nuestro segundo paso se daría en la identificación de los posibles riesgos de fraude.

Un tercer área de mejora estaría circunscrito a la implementación de programas de prevención y detección de fraude, tomados siempre como una inversión y no como un gasto.

# CONCLUSIONES

En este informe 2018 de tendencias sobre prevención y gestión del fraude hemos podido constatar, de la mano de nuestros asociados, que se mantiene el incremento de los casos de fraude observado en años anteriores, así como su incidencia e impacto en términos económicos dentro del tejido empresarial español.

**Las empresas de distintos sectores** están cada vez más convencidas de la importancia estratégica de la prevención del fraude, por lo que invierten en recursos y mecanismos para impulsar esta lucha, si bien aún hay puntos de mejora y el dimensionamiento de los equipos no termina de adaptarse a los volúmenes crecientes de esta actividad delictiva. La nueva economía digital está incorporando mayor complejidad y necesidad de sofisticación en materia de prevención, algo que a su vez dificulta de forma importante la experiencia de cliente, exigiendo a las organizaciones revisitar sus procesos en busca de un equilibrio óptimo entre seguridad y efectividad en la gestión de los clientes. Existe un claro consenso en identificar este punto junto a la protección de datos como foco estratégico para los próximos ejercicios.

Los nuevos cambios normativos, como la Directiva Europea relativa a los servicios de pago digitales PSD2, ayudan a reforzar los mecanismos de control de las organizaciones mediante interesantes recomendaciones y exigencias adaptadas a la evolución de las nuevas tecnologías y obsolescencia de los controles ya implantados. No solo debemos velar por la seguridad de nuestras empresas, sino por la seguridad de nuestros clientes, quienes también sufren las consecuencias de estas actuaciones, todo ello bajo el más estricto control en la calidad y seguridad de la información.

LA NUEVA ECONOMÍA DIGITAL ESTÁ INCORPORANDO MAYOR COMPLEJIDAD Y NECESIDAD DE SOFISTICACIÓN EN MATERIA DE PREVENCIÓN

## UNA DE LAS HERRAMIENTAS MÁS POTENTES EN LA LUCHA CONTRA EL FRAUDE LA ENCONTRAMOS EN LOS ECOSISTEMAS DE COMPARTICIÓN DE INFORMACIÓN

Una de las herramientas más potentes en la lucha contra el fraude la encontramos en los ecosistemas de compartición de información, como el Sistema Nacional de Prevención del Fraude, donde no solo se cruzan datos de solicitudes, sino que se fomenta la colaboración entre empresas de diferentes sectores y con problemáticas muy dispares, enriqueciendo el pensamiento preventivo, favoreciendo la transición de un esquema reactivo a uno más proactivo y orientado a la anticipación.

En línea con lo anterior, la colaboración entre distintas Asociaciones orientadas a la lucha contra el fraude amplía de forma significativa la concepción del problema al aportar diferentes prismas para abordarlo. En este informe, Rafael López, Presidente de la Fundación Universitaria Behavior & Law, destaca la importancia de la dimensión psicológica en la motivación que favorece la acción fraudulenta, facilitando la comprensión de las conductas de un perfil defraudador. Por su parte, Albert Salvador Lafuente, Secretario General de World Compliance Association, incide en que la lucha contra el fraude es clave en la mayoría de los países, y nos habla del importante papel que cumplen en ella los directivos y gerentes de la Administración Pública, que deben reconocer la presencia de fraude dentro de sus organizaciones.

# ASOCIADOS

Este informe ha sido posible gracias a la colaboración de nuestros asociados, que comparten con nosotros el compromiso de hacer frente al fraude para proteger al tejido empresarial español. Para participar en la lucha activa contra el fraude y beneficiarse de todas las ventajas que tienen nuestros asociados, envíe un correo electrónico con sus datos a: **contacto@asociacioncontraelfraude.com**

www.asociacioncontraelfraude.com

www.linkedin.com/company/asociacion-espanola-de-empresas-contra-el-fraude

@aeecf_

contacto@asociacioncontraelfraude.com

ASOCIACIÓN ESPAÑOLA
DE **EMPRESAS**
**CONTRA EL FRAUDE**