Prevenir el fraude en tiempos difíciles

INFORME SOBRE FRAUDE 2020 en EMEA

experian™

Índice

Introducción

Este año ha puesto de manifiesto lo adaptables, pertinaces, indiscriminados y oportunistas que pueden llegar a ser los estafadores.

Si bien la pandemia global y la consiguiente ralentización social y comercial se han traducido en obstáculos de consecuencias impredecibles para todos, las actividades fraudulentas se han mantenido intactas, especialmente en canales digitales, donde muchos usuarios realizan actualmente sus transacciones diarias.

Mientras que los delincuentes se han adaptado rápidamente a la nueva situación, es evidente que sigue habiendo carencias considerables en las capacidades de muchas empresas para reaccionar y afrontar los retos que plantea el futuro, como ya se destacó en el informe del año pasado. En esta ocasión, nos adentramos en las tendencias emergentes y destacamos aquellos puntos débiles que exponen peligrosamente a las empresas, muchas de las cuales se declaran desbordadas por la escala inabarcable, la complejidad y la diversidad de los métodos que emplean actualmente los delincuentes.

A pesar de los típicos retos relacionados con los presupuestos, los conocimientos, el talento, la contratación y la retención del personal, la pandemia ha reescrito las normas y su impacto seguirá dejándose notar durante algún tiempo.

ACERCA DEL AUTOR

Frédéric Dubout
Senior Consultant - Fraude e Identidad en Experian

Frédéric cuenta con 20 años de experiencia específica en el sector en los que ha trabajado para empresas multinacionales de telecomunicaciones, banca, automoción y servicios financieros en Europa, África y Oriente Medio. Ha trabajado con todos los sistemas de prevención del fraude, desde la aplicación de biometría y tecnologías emergentes hasta el fraude transaccional y de pagos, el fraude de aplicación y el fraude digital, móvil y sin presencia de la tarjeta. Sus ámbitos de experiencia incluyen también los recobros, la calidad y la administración de los datos y la gestión de proyectos.

METODOLOGÍA

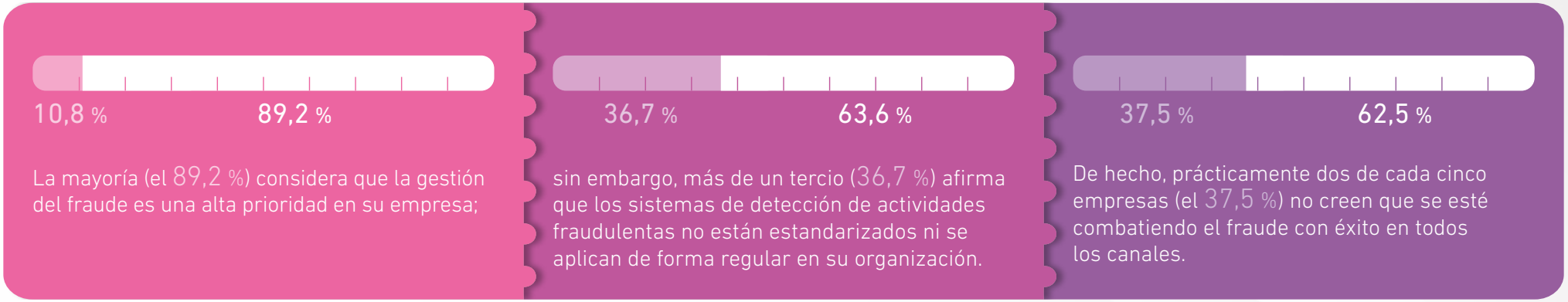
A lo largo del verano de 2020, entrevistamos a más de 150 altos cargos con responsabilidad o influencia en la estrategia de Riesgo y Fraude en empresas de toda Europa, Oriente Medio y África (EMEA).

Resumen ejecutivo

- La mayoría (un 89,2 %) de los encuestados considera que la gestión del fraude es una alta prioridad en su empresa.
- Sin embargo, cuando se abordan en profundidad los aspectos operativos, la confianza en el rendimiento general cae al 60 %.
- De hecho, prácticamente dos de cada cinco empresas (el 37,5 %) no creen que se esté combatiendo el fraude con éxito en todos los canales.
- Además, más de un tercio de ellas (el 36,7 %) tiene poca confianza en sus sistemas de detección de actividades fraudulentas.
- Los estafadores se han adaptado rápidamente para sacar provecho de la pandemia; aproximadamente dos de cada cinco encuestados (el 37,7 %) han notado un repunte de tres tipos de fraude, todos ellos relacionados con los canales digitales: se trata de la duplicación de tarjetas SIM («SIM swap»), la usurpación de identidad («mediante phishing») y los robos de cuentas.
- Todos los encuestados han comunicado un aumento de los porcentajes de alertas, la frecuencia de los ataques y un incremento de actividades fraudulentas residuales,
- Durante la pandemia, la continuidad del negocio ha sido la principal preocupación de casi una de cada seis empresas (el 16 %).
- Casi la mitad de los encuestados (el 42.6 %) considera que sus recursos de prevención del fraude son insuficientes.
- De hecho, la mayoría (el 54,5 %) atribuye el problema a que los tipos de fraude son cada vez más complejos.
- Además, prácticamente la mitad de los encuestados (el 49,1 %) reconoce que es preciso adoptar un enfoque más equilibrado de cara a la prevención del fraude.
- Sin embargo esto no resulta fácil cuando no se cuenta con los suficientes recursos dentro de la empresa
- Uno de cada tres encuestados (el 30,3 %) considera que el volumen de actividades fraudulentas ha aumentado con mayor rapidez que el personal en plantilla.
- Más de la mitad de ellos (el 51,2 %) afirma no ser capaz de gestionar las amenazas de fraude emergentes.
- Uno de cada trece (el 7,5 %) ya se enfrenta a dificultades para abarcar las amenazas actuales de fraude con los recursos existentes.
- Las mejoras en el análisis en tiempo real de las transacciones han sido clave para más de la mitad (50,9 %).
- Inversión en inteligencia de dispositivos, verificación de correos electrónicos, inteligencia artificial, aprendizaje automático y aumento de la automatización son prioridades para aproximadamente uno de cada cinco equipos expertos en fraude.

Contexto de mercado

Desde un primer momento, nos interesaba evaluar las opiniones relativas a la fiabilidad y la confianza en los sistemas contra el fraude. Se preguntó a los participantes por sus opiniones acerca del rendimiento a la hora de detectar y prevenir el fraude en sus compañías. A continuación se presentan algunos resultados clave.



Es evidente que la cuestión de la confianza tiene dos caras: por lo general, es bastante elevada en la mayoría de los encuestados; sin embargo, cuando se abordan en profundidad los aspectos operativos, la confianza en el rendimiento general cae notablemente (en torno al 60 %). Con un 36,7 % de empresas con escasa confianza en sus sistemas de detección de actividades fraudulentas y un porcentaje similar (37,5 %) que admite su incapacidad de hacer frente al fraude en todos los canales, llegamos a la conclusión de que hay un amplio margen para la mejora.

Variaciones regionales

La mitad de los encuestados (50 %) en Sudáfrica considera que los enfoques propuestos para la prevención del fraude en su mercado son demasiado costosos, lo que pone de manifiesto una clara necesidad de capacidades redimensionables y a medida, según las necesidades de la entidad.

VARIACIONES REGIONALES EN LA RESPONSABILIDAD DE LA GESTIÓN DEL FRAUDE

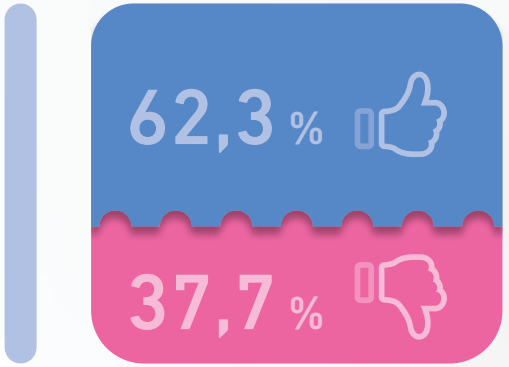
En la región EMEA, la mayoría de equipos antifraude se coordinan con los departamentos internos de riesgo.

Sin embargo, existen excepciones regionales: en Turquía y Sudáfrica, las empresas suelen decantarse por incluir sus equipos antifraude en el departamento de operaciones, mientras que en Francia prefieren integrarlos en el departamento financiero. En Dinamarca, se dispone de un enfoque claro y bien definido del fraude en el marco de las divisiones jurídicas comerciales y de cumplimiento.

Retos y tendencias emergentes

FRAUDES EMERGENTES EN EL ÚLTIMO AÑO

Los estafadores se han adaptado rápidamente para sacar provecho de la pandemia y el 37,7 % de los encuestados han notado un repunte de tres tipos de fraude; resulta sorprendente que todos ellos estén relacionados con la mayor dependencia de los canales digitales y que afecten particularmente a los usuarios menos acostumbrados al uso del canal digital.



1*

Duplicación de SIM (SIM swap)

Los ciberdelincuentes se apropian de números de teléfono para acceder a datos confidenciales y cuentas personales.

2*

Estafas relacionadas con la usurpación de identidad (Phishing)

Los estafadores tratan de obtener información y datos personales confidenciales (incluidos nombres de usuario, contraseñas y datos de tarjetas de crédito) haciéndose pasar por una entidad legítima y fiable por medio de una comunicación electrónica.

3*

Robo de cuentas (Account Takeover)

Los estafadores utilizan los datos legítimos de un cliente para tomar el control de sus cuentas digitales y robar dinero o realizar compras con la tarjeta de crédito. Ninguna de estas tendencias es nueva, pero todas ellas van en aumento y están directamente relacionadas con nuestra creciente dependencia de las interacciones digitales.

LA DUPLICACIÓN DE TARJETAS SIM VUELVE CON MÁS FUERZA QUE NUNCA

Entre las tendencias de fraude que han surgido con fuerza este año en la región EMEA, destaca la duplicación de tarjetas SIM, también conocida como *SIM swapping*. No es una tendencia nueva; de hecho, lleva existiendo tanto tiempo como los dispositivos móviles con acceso a la red. Sin embargo, la información facilitada por los participantes en la encuesta confirma que la duplicación fraudulenta de tarjetas SIM, al igual que otros tipos de fraude digital, ha vuelto con más fuerza que nunca; y no cabe duda de que se trata de un ámbito que requiere una mayor supervisión.

A primera vista, la duplicación de una tarjeta SIM puede parecer un método legítimo y práctico para cambiar de dispositivo móvil o actualizar un dispositivo sin perder los números de teléfono existentes en caso de daño, pérdida o robo de la tarjeta anterior. Tradicionalmente, este tipo de fraude tenía como objetivo simplemente dirigir el tráfico de llamadas a números de tarificación adicional, cargar costes inflados de *roaming* y actividades similares a fin de obtener dinero. Sin embargo, con la digitalización, se observa una tendencia general y cada vez más preferente hacia la autenticación por medio de contraseñas de un solo uso (también denominadas OTP, del inglés *one-time password*) que se envían por SMS a fin de demostrar la «posesión» en un proceso de autenticación de dos pasos. Así, el objetivo de este tipo de fraude con tarjetas SIM se ha orientado rápidamente al robo de activos financieros, principalmente a través del acceso a cuentas de banca en línea y del vaciado de las mismas mediante transferencias a otras cuentas bajo el control de los estafadores.

Evidentemente, el robo directo de dinero resulta mucho más atractivo y eficaz que tener que monetizar llamadas telefónicas a números de tarificación adicional. La normativa PSD2 está llamada a desfasar el proceso de OTP/SMS como método de autenticación de pagos. En su lugar, se fomenta la autenticación reforzada de clientes (conocida por sus siglas en inglés, SCA) por medio de métodos más estrictos que utilizan los factores combinados de posesión, herencia y conocimiento.

¿QUÉ POSIBILITA EL FRAUDE DE DUPLICACIÓN DE TARJETAS SIM?

No hay una única respuesta definitiva a esta pregunta; se trata más bien de una combinación de factores que ha evolucionado.

En primer lugar, constituye un elemento importante que las compañías se han apurado en adoptar el SMS como factor preferente de posesión del dispositivo para los procesos de autenticación en dos pasos. Paralelamente, la seguridad aplicada por los operadores ha sido tradicionalmente bastante pobre, lo que los hace vulnerables a tácticas de ingeniería social y robo de identidades. En segundo lugar, existe una falta de trazabilidad y rendición de cuentas en relación con las tarjetas SIM, que están insuficientemente controladas en la cadena de suministro.

Se espera que la llegada de la tarjeta SIM virtual (eSIM) tenga un impacto mínimo en el asunto, ya que los números de teléfono podrán seguir transfiriéndose de un terminal a otro por medio de procesos específicos para los que deberá garantizarse adecuadamente la seguridad.

Finalmente, como ocurre con la mayoría de actividades fraudulentas, el eslabón más débil de la cadena es inevitablemente el cliente, que continúa siendo vulnerable a las técnicas de ingeniería social. El reto es de dimensiones que abarcan mucho más que la duplicación de tarjetas SIM, que es solo uno de los muchos fraudes que existen en el entorno digital diseñados para evadir sin fisuras los procesos de autenticación, especialmente los de dos pasos.

Existen variaciones notables en las tendencias de fraude a nivel regional. Los encuestados españoles destacaron de forma unánime un repunte del fraude por duplicación de SIM. Sin embargo, en Alemania, donde la mayoría de encuestados (un **58 %**) provenían del sector bancario y de seguros, quedó clara la prevalencia de los ataques de *phishing* y *man in the middle* sobre la duplicación de tarjetas SIM.

Hoy por hoy, existen muchas alternativas al *SIM swap* más allá del duplicado fraudulento de tarjetas SIM físicas o virtuales (eSIM). Una de ellas es el fraude por medio de programas malignos conocidos como MitMo (del inglés *man in the mobile*, o *man in the browser*).

También son frecuentes los ataques al sistema de señalización por canal común n.º 7 (SS7), el protocolo que permite el intercambio de información entre redes telefónicas. Los ataques de SS7 permiten a los estafadores leer mensajes de texto, escuchar llamadas telefónicas y trazar las ubicaciones de los usuarios de teléfonos móviles solo con disponer del número de teléfono. Este fenómeno pone de manifiesto una vulnerabilidad de la infraestructura de la red mundial de telefonía móvil. No obstante, dado que se trata de un método de fraude dirigido, selectivo y relativamente laborioso, es improbable que se acabe empleando a gran escala.

Los programas maliciosos conocidos como *malware* continúan siendo prevalentes; entre ellos se encuentran los ataques con programas como Muraena y Necrobrowser, que se asemejan mucho en el sentido en que constituyen rutas prácticamente invisibles hacia el *phishing* automatizado y las actividades posteriores.

RUTAS HACIA RESPUESTAS EFECTIVAS

La amenaza de las técnicas de fraude requiere una combinación apropiada de niveles de detección y defensa. Existen también diversas medidas (que, no obstante, pueden ser muy irregulares) que pueden adaptarse para contribuir a prevenir pérdidas; por ejemplo, el aplazamiento de las transferencias hasta 72 horas antes de completar una transacción, lo que brinda una oportunidad de reaccionar cuando se alerta de una actividad sospechosa. Alternativamente, es posible limitar las transacciones a un número concreto de canales conocidos, debidamente identificados y bien protegidos. Las comprobaciones de identidad, hábitos y comportamiento (especialmente después de la pérdida, el robo o el cambio de un móvil o una tarjeta) son otra opción posible.

También pueden ser efectivos los controles en el punto de venta con comprobaciones obligatorias de validación de tarjetas SIM antiguas o de la identidad del usuario, así como los análisis de antigüedad de la tarjeta. Igualmente resultan de vital importancia las comprobaciones para garantizar la coherencia de la geolocalización; es evidente que un teléfono no puede pasar de encontrarse a una distancia de 500 km a una de 2000 km en cuestión de minutos.

Por supuesto, esto no resulta del todo favorable para los vendedores, dado que muchas de estas soluciones interfieren con la experiencia del cliente; sin embargo, ninguna de ellas debe considerarse como responsabilidad única de los operadores de telecomunicaciones.

Como se ha señalado, la duplicación de SIM es solo una de muchas técnicas de fraude que se ha vuelto, eso sí, más prevalente debido a nuestra mayor dependencia de los canales digitales. En todo caso, es evidente que, cuando existen múltiples vulnerabilidades y varios factores de riesgo, es necesario un enfoque sistemático para detectar, prevenir y abordar los riesgos de forma continua.

PHISHING Y MANERAS DE EVITAR QUE LOS CLIENTES MUERDAN "EL ANZUELO"

Los adeptos del *phishing* buscan sacar partido de las buenas relaciones que las empresas han consolidado con sus clientes. Los mayores ataques de *phishing* se basan en compromisos comerciales por correo electrónico. Estos estafadores envían correos electrónicos con una maquetación que al cliente le resulta familiar y le insta a completar una transacción en línea aparentemente legítima, como actualizar una cuenta, elegir un descuento por fidelidad o responder a una oferta personalizada.

Los clientes reaccionan porque quieren ayudar y, por lo general, apoyan a las empresas en las que confían, motivo por el cual este tipo de estafas continúa funcionando. Actualmente, los ataques se personalizan para asumir el aspecto de una empresa y dirigirse a un cliente específico; los adeptos al *phishing* suelen hacer uso de herramientas de automatización para obtener la mayor recompensa posible por sus esfuerzos.

Sirva de ejemplo una variante conocida como *spear phishing* o *phishing* «de lanza»: se trata de una estafa dirigida a personas con acceso a cuentas financieras o sistemas internos de una organización. Otra variante es la conocida como *whaling*, que se dirige a un individuo específico de alto valor simplemente porque tiene más dinero y se considera una oportunidad más lucrativa. También existe la práctica denominada *smishing*, que es una estafa que circula entre los clientes a través de mensajes de texto.

Las empresas no son las únicas que hacen uso del aprendizaje automático y la inteligencia artificial para crecer; los estafadores adeptos al *phishing* también saben sacarles partido. El uso de datos personales confidenciales es solo el primer paso; posteriormente, los estafadores recurren al aprendizaje automático y a la inteligencia artificial para crear perfiles detallados de los individuos, incluyendo sus preferencias de compra y detalles sobre su trayectoria laboral, su familia, su perfil social, etc. La información se utiliza para crear un mensaje a medida y extremadamente personalizado que tiene más posibilidades de conseguir que la víctima caiga en la estafa.

Los ataques de *phishing* están aquí para quedarse, pero existen medidas que las empresas pueden adoptar para ayudar a sus clientes a detectarlo. La clave radica en centrarse en la tecnología y la formación. Hasta las empresas más pequeñas pueden sacar provecho de las tecnologías disponibles de bloqueo o filtrado de correos electrónicos. Conviene formar a los empleados para que se lo piensen dos veces antes de reaccionar a solicitudes extrañas que puedan recibir. Pero, ante todo, es esencial mantener actualizada la formación del personal, porque los estafadores son incansables y siempre encuentran nuevas maneras de defraudar.

ROBO DE CUENTAS O “ACCOUNT TAKEOVER”

Al igual que ocurre con el *phishing*, los detalles de inicio de sesión de los clientes suelen obtenerse como consecuencia de violaciones masivas de datos. Los estafadores utilizan las credenciales robadas para comprobar los accesos a las cuentas y observar la actividad para comprender las fluctuaciones de los movimientos de las cuentas (también analizando los extractos financieros privados), a fin de determinar el momento óptimo para atacar y obtener el mayor beneficio posible.

La vigilancia y planificación del fraude son actividades transparentes en las cuentas de una persona; son acciones que los estafadores llevan a cabo antes de realizar cualquier ataque o movimiento. Las actividades incluyen la comprobación de extractos, la modificación de los ajustes para cubrir sus huellas con mayor eficacia y el establecimiento de enlaces a la cuenta para preparar el terreno y planificar transferencias fraudulentas.

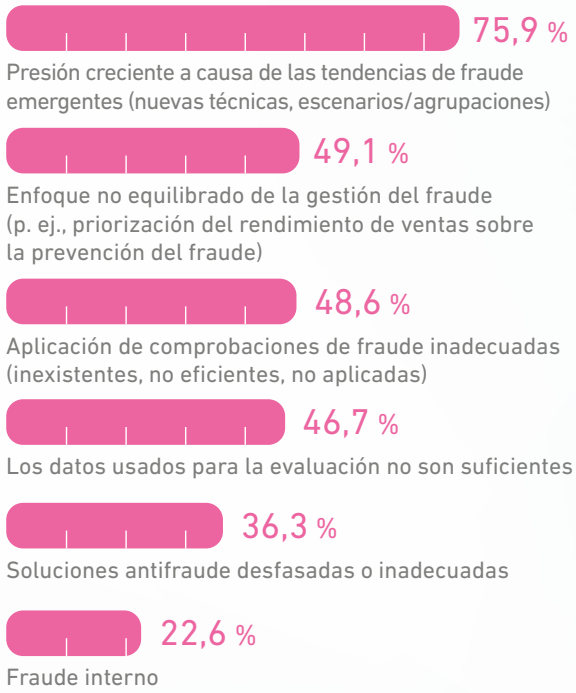
Desafortunadamente, el paso final suele ser la pérdida real de activos; es el final de una serie de actividades fraudulentas que, sencillamente, no se detectaron a tiempo. Este resultado puede socavar gravemente la confianza a largo plazo del cliente afectado y destruir la reputación de una marca.

Por otra parte, las medidas de seguridad resultan conflictivas; puede detectar actividades sospechosas o poco usuales, pero también puede ser una tremenda fuente de frustración para los clientes. Los estafadores se centran cada vez más en programas de fidelidad; utilizan los datos robados de las cuentas para acceder a ellos y bien usar los puntos acumulados por el cliente para realizar una compra directa o bien vender los puntos robados a un precio rebajado.

Por lo general, los clientes más fieles son los más atractivos para los estafadores, porque son los que acumulan mayores puntos. Resulta que estos clientes son también muy valiosos para las empresas, porque realizan y repiten compras periódicamente.
Se trata del tipo de clientes que ninguna empresa quiere perder, pero los problemas vinculados a un sistema de seguridad demasiado laxo o demasiado estricto pueden acabar empujándoles hacia la competencia.

El éxito se basa en sofisticadas herramientas de supervisión de cuentas capaces de detectar si se utiliza la sesión en línea de un cliente desde múltiples dispositivos. También resultan esenciales la capacidad de detectar las repeticiones de sesiones en línea anteriores y la capacidad de realizar un seguimiento de múltiples puntos de contacto a lo largo del ciclo de vida del cliente. El seguimiento debe incluir los inicios de sesión y las transacciones financieras y no financieras habituales, que conforman un perfil de comportamiento que puede usarse posteriormente para detectar las acciones maliciosas y bloquear las actividades sospechosas.

El porqué del éxito de las actividades fraudulentas



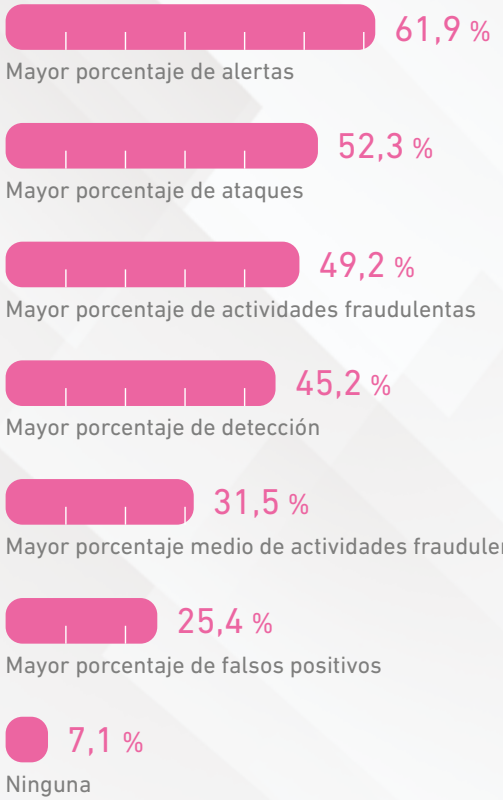
El estudio de este año arroja dos puntos esenciales en relación con los tipos de fraude. El motivo principal por el que funcionan los intentos de fraude radica en la creciente complejidad de estas actividades. Al mismo tiempo, la eficacia de la actuación contra las actividades sospechosas depende directamente de los recursos, los procesos y las capacidades de una empresa.

Tres cuartas partes de los encuestados admiten que necesitan ser capaces de reconocer y luchar contra las tendencias crecientes o cambiantes del fraude. Es de especial importancia que, a medida que surgen nuevos escenarios de fraude, las organizaciones sean capaces de unir piezas por todos los canales, a menudo entre actividades y comportamiento que parecen no tener relación entre sí.

En torno a la mitad de los encuestados (el 49,1 %) reconoce también una necesidad de garantizar un enfoque equilibrado entre la detección y la prevención del fraude. La inteligencia artificial respaldada por técnicas de aprendizaje automático comporta un beneficio total para las empresas, ya que los sistemas mejorados de detección del fraude ayudan a proteger a los clientes mejorando su experiencia, y por tanto, aumentar los beneficios para la empresa.

La capacidad de aprovechar al máximo los datos disponibles también resulta esencial para casi la mitad de los encuestados (el 46,7 %). Los análisis mediante inteligencia encubierta de dispositivos están demostrando ser muy eficaces a la hora de prevenir las transacciones sospechosas sin comprometer la fluidez de la experiencia en línea de los clientes.

El impacto de la pandemia en los sistemas de prevención y análisis de actividades fraudulentas



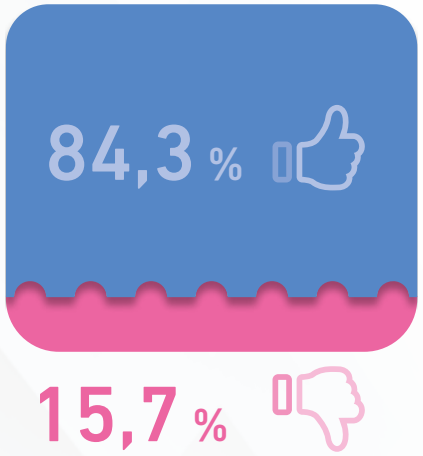
Al considerar el número total de transacciones como denominador común, los encuestados han señalado un mayor porcentaje de alertas y una mayor frecuencia de ataques, así como un incremento de las cifras de fraude residual.

El impacto de los confinamientos sobre la demanda de los clientes ha sido evidente: la actividad comercial se ha desplomado antes de verse posteriormente marcada por una transición a gran escala a los canales digitales. A medida que se han ido relajando las restricciones vinculadas a la pandemia, se ha apreciado un retorno gradual a los canales más «tradicionales».

Sin embargo, las empresas se han visto desbordadas por una sensación de urgencia: los ejecutivos no han tardado en darse cuenta de que tienen que adaptarse con rapidez para sobrevivir y migrar tantas actividades administrativas como sea posible a modalidades en línea.
Hay quienes han caído inevitablemente: algunas empresas más flexibles han logrado salir airosas, pero otras se han enfrentado a grandes dificultades y para algunas ha resultado imposible.

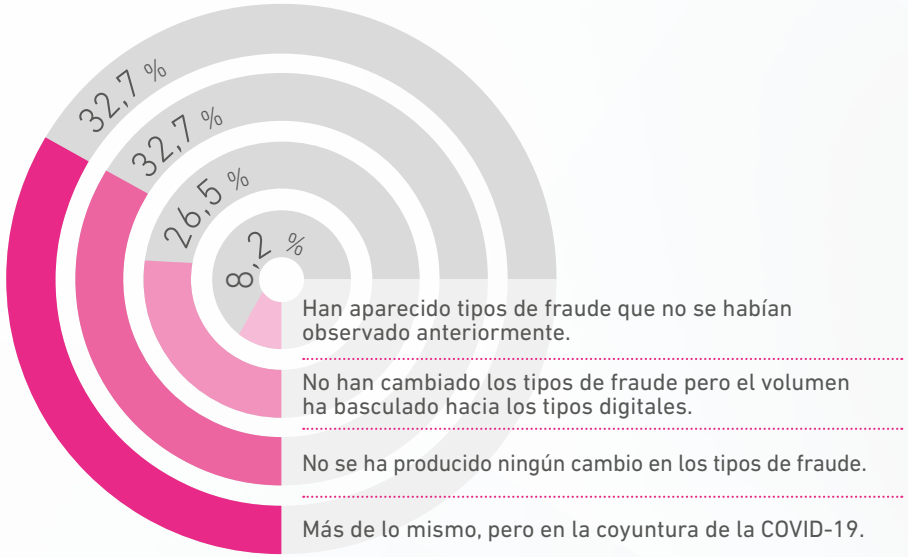
La continuidad del negocio se ha convertido en la principal preocupación de la de la mayoría de las empresas. De hecho, la principal angustia de los gestores antifraude fue la pérdida puntual de eficiencia que podía poner en peligro sus capacidades para prevenir, detectar y actuar contra el fraude con la misma rapidez y precisión que antes. Según los resultados del estudio, esta preocupación estaba justificada para prácticamente una de cada seis compañías encuestadas (un 16 %). En algunas de ellas, ha supuesto el punto de partida para una remodelación completa de su organización a largo plazo, su estructura, sus herramientas y su futura dependencia de la automatización, especialmente durante la segunda ola de la pandemia o de cara a mitigar los posibles rebrotes posteriores.

A consecuencia de los problemas relacionados con la **continuidad del negocio**, ¿se han **producido con éxito actividades fraudulentas** que se habrían podido evitar en las condiciones anteriores?



TIPOS DE FRAUDE MÁS DESTACADOS EN EL PUNTO ÁLGIDO DE LA PANDEMIA

Aproximadamente una de cada doce empresas notó el surgimiento de nuevas tendencias de fraude en el punto álgido de la primera ola de la pandemia, mientras que una de cada tres notó un repunte de los intentos directamente relacionado con el brote inicial.



TENDENCIAS EMERGENTES

Como es lógico, prácticamente todos los equipos antifraude intuían que el caos y la incertidumbre social derivados de la pandemia serían una motivación para los estafadores. Los resultados del estudio apoyan esta afirmación. Los encuestados admiten que los ataques inexorablemente adaptables de los estafadores resultaron evidentes desde el principio, a medida que fue aumentando la frecuencia, la cantidad y la variedad de intentos que, en circunstancias normales, habrían sido mucho más fáciles de detectar y combatir.

Entre los intentos de fraude más persistentes se encuentran ciertos tipos de ingeniería social, principalmente el *phishing*: correos y textos falsos se presentaban como mensajes oficiales procedentes de autoridades, instituciones o compañías. Se trataba de sacar provecho de los niveles disparados de ansiedad de la población, en un intento de aprovecharse de los clientes menos habituados al ámbito digital, muchos de los cuales se vieron obligados a cambiar a canales en línea con los que no estaban familiarizados durante los largos períodos de confinamiento.

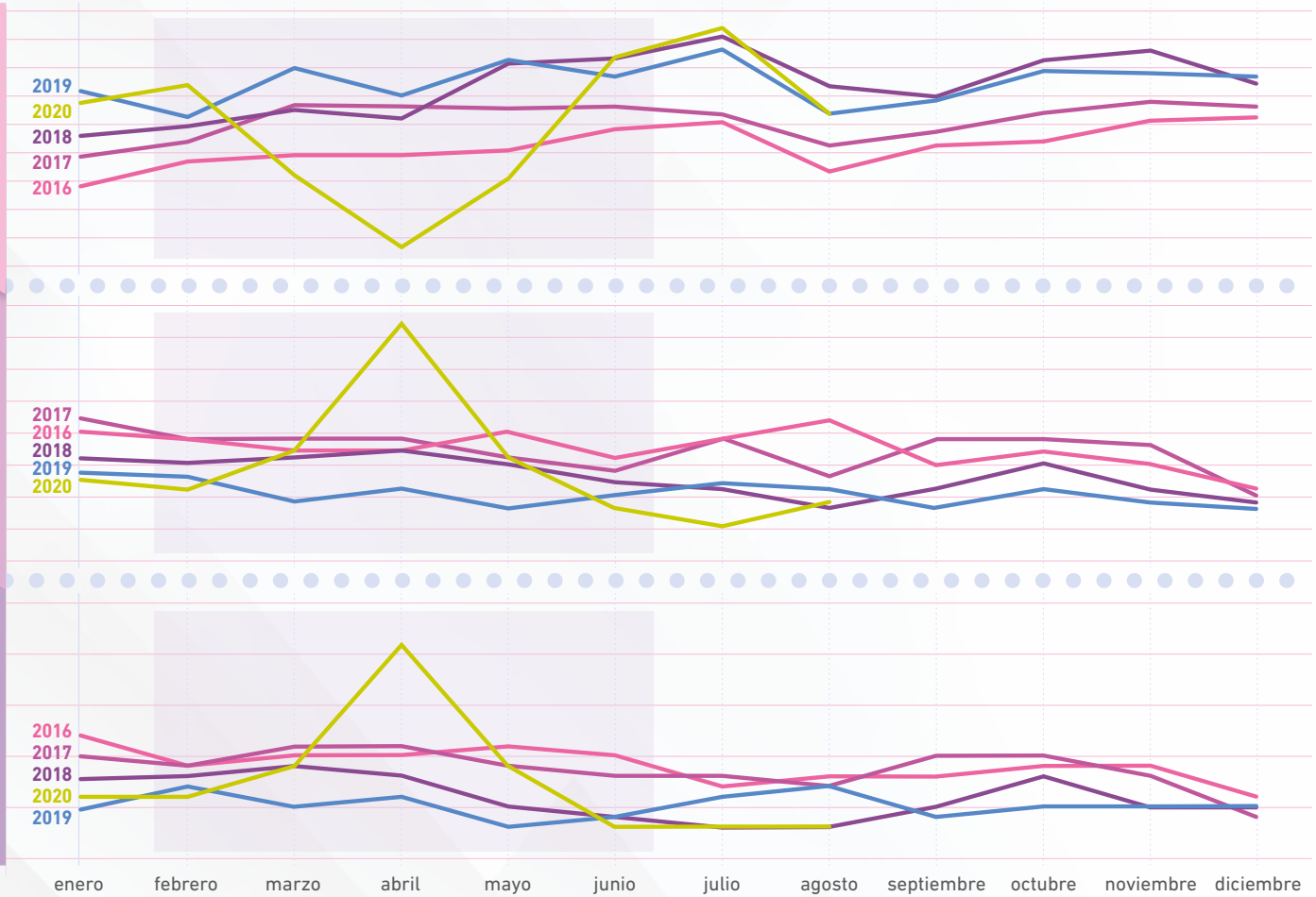
Un análisis realizado con un conjunto de clientes de EMEA implicados en uno de nuestros regímenes colaborativos a nivel regional de uso compartido de datos sobre el fraude muestra patrones interanuales de volúmenes de aplicaciones, cantidad de ataques y porcentaje de actividades fraudulentas. La comparación pone de manifiesto lo persistentes que fueron los estafadores en el punto álgido de la primera ola de la pandemia a la hora de buscar métodos para franquear las defensas de las compañías.

CÓMO LA PANDEMIA HA MOLDEADO LAS ACTIVIDADES COMERCIALES Y LOS COMPORTAMIENTOS FRAUDULENTOS

Un declive en V muy claro en la actividad empresarial

Un repunte del número de ataques

Un repunte también del porcentaje de actividades fraudulentas



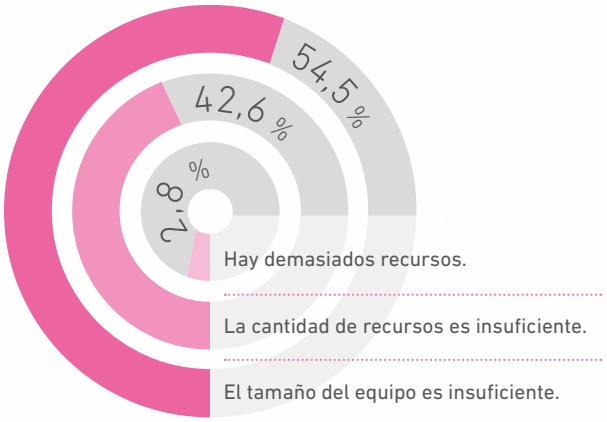
SISTEMAS DE MEDICIÓN E INDICADORES CLAVE DE RENDIMIENTO (KPI)

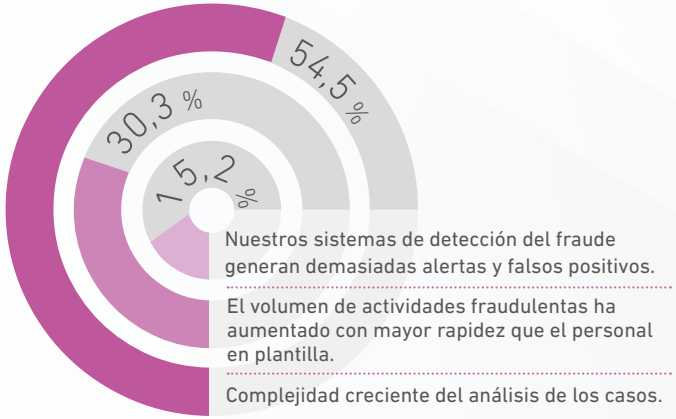
A partir de su experiencia y de los cambios en los comportamientos digitales típicos observados durante los cambios estacionales, muchos especialistas en fraude tenían una idea de qué esperar durante la pandemia. Los patrones de tendencias solían estar alineados con los altibajos de actividad propios de los períodos festivos y prenavideños, cuando los sistemas de detección del fraude suelen reflejar un aumento del volumen global de consumo acompañado de una ligera caída de los indicadores de fraude.

Durante el confinamiento, el desplome de la actividad comercial hacía esperar un aumento en los indicadores. Por lo general, los clientes atraviesan períodos de mayor consumo durante los días previos a las vacaciones y de menor consumo durante un confinamiento. Sin embargo, independientemente de estas tendencias, los estafadores han demostrado ser una constante incansable y no parecen encontrar motivos para reducir sus intentos de fraude.

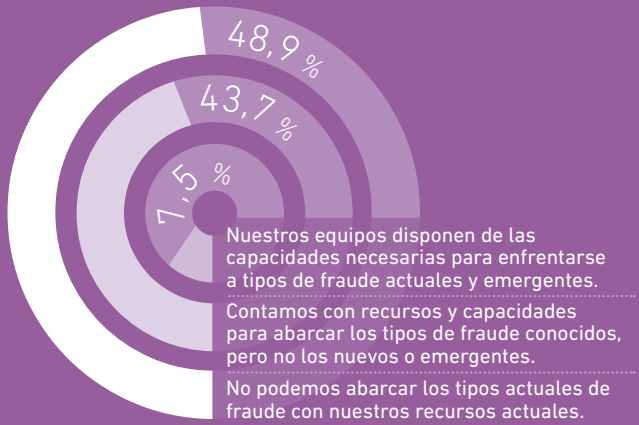
De nuevo, como hemos señalado, las cifras han reflejado en general las previsiones: mientras que los volúmenes de negocio adoptaban una forma de V (también denominada «palo de hockey») con un mínimo ubicado hacia el final del período de confinamiento, el fraude residual y el número de ataques vinculados adoptaron una forma de V simétrica invertida, sin caídas perceptibles en sus actividades. No obstante, cabe destacar que una lectura unidimensional de los datos puede llevar a interpretaciones erróneas; por eso, es de vital importancia garantizar análisis claros y bien diseñados e informes debidamente fundamentados.

Resolviendo el problema de la dotación de recursos





¿Qué opina acerca de la calidad de los recursos asignados a la gestión del fraude en su organización?



Casi la mitad de los encuestados (el 42.6 %) considera que sus recursos de prevención del fraude son insuficientes.

De hecho, la mayoría (el 54,5 %) atribuye el problema a que los tipos de fraude son cada vez más complejos. Uno de cada tres encuestados (el 30,3 %) considera que el volumen de actividades fraudulentas ha aumentado con mayor rapidez que el personal en plantilla, mientras que uno de cada seis ejecutivos admite que la frecuencia de falsos positivos constituye un problema.

En lo que respecta a las capacidades de los equipos, más de la mitad (el 51,2 %) afirma no ser capaz de gestionar las amenazas de fraude emergentes; de ellos, uno de cada trece (el 7,5 %) ya se enfrenta a dificultades para abarcar las amenazas actuales de fraude con los recursos existentes. Casi la mitad (el 48,9%) confía plenamente en las capacidades de sus equipos antifraude.

ANÁLISIS Y PRESENTACIÓN DE INFORMES

En lo que respecta a la gestión del fraude, hay voces que apuntan a que todo recae en el flujo prevención-detección-tratamiento. Sin embargo, la falta de un análisis adecuado de la tarea que se desee abordar complica enormemente la capacidad de adoptar las decisiones mejores o más apropiadas.

El «cuadro de mando» de un gestor antifraude debe abarcar indicadores muy diversos, incluyendo valores, cantidades y volúmenes absolutos, pero también valores relativos como porcentajes y medias. Por una parte, tiene que ofrecer un mínimo nivel de base para la supervisión; por otra, también debe ser capaz de ofrecer perspectivas y análisis estratégicos para alimentar políticas antifraude, aspiraciones y dotaciones de recursos más amplias.

Sin pretender ser una lista exhaustiva, las variables mencionadas a continuación se consideran imprescindibles: número de incidencias, número de alertas, número de actividades fraudulentas evitadas, fraude residual, intentos de fraude, falsos positivos y cantidades acumuladas relacionadas con el número de incidencias. También es aconsejable analizar la cantidad de pérdidas evitadas y sufridas. A partir de estos datos, es posible calcular de forma precisa porcentajes de prevención, de fraude residual, de ataques, de falsos positivos, cantidades medias de las transacciones y, lo que es más importante, la cuota media de fraude.

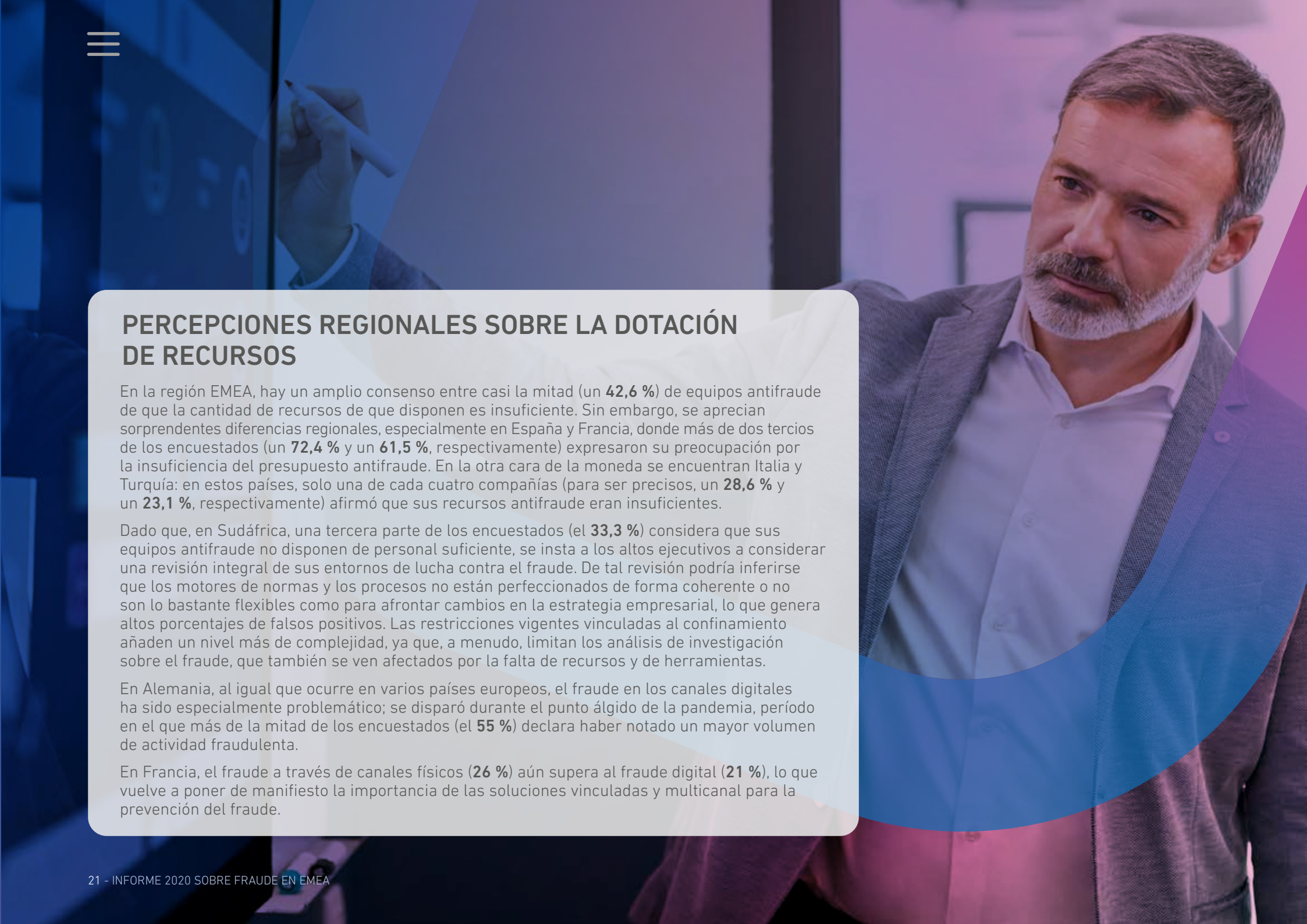
Es preciso determinar cada uno de estos indicadores a través de una serie de análisis que abarquen los canales, los productos, las ubicaciones geográficas, los puntos de venta, el segmento de clientes y el segmento de importes, entre otros factores.

Además, es preciso revisarlos con la periodicidad adecuada: algunos de ellos deben revisarse necesariamente a diario, sencillamente por motivos operativos y de cara a la adopción de decisiones tácticas inmediatas; otros son más apropiados para un análisis mensual encaminado a obtener una perspectiva estricta de las tendencias que permita reajustar las políticas como corresponda. Es aconsejable revisar también los indicadores mensuales en un contexto de análisis de todos los datos del año hasta la fecha. Los coeficientes son importantes porque ofrecen una interesante foto fija de la evolución del rendimiento a lo largo del año, así como útiles perspectivas sobre el impacto de los ajustes temporales e históricos.

La medición del rendimiento es una disciplina de gran dinamismo que se orienta claramente hacia la acción y la toma de decisiones. En la medida de lo posible, todos los coeficientes deberían constar de un aspecto volumétrico (a partir del número de casos) y un aspecto de valor (a partir del valor acumulado de casos idénticos).

No existe un valor correcto o incorrecto a la hora de juzgar el nivel de rendimiento para cada indicador; esta valoración es subjetiva y depende de un gran número de factores entre los que se encuentran la propensión y la tolerancia al riesgo, la capacidad operativa para efectuar revisiones manuales y los aspectos relacionados con la automatización, la digitalización y la reputación, entre otros muchos.

A modo de ejemplo, una proporción de alertas que requieren revisión manual del 10 % puede ser perfectamente viable si el máximo de casos que se procesan diariamente es de unos 200, ya que es un volumen que podría asumir fácilmente un empleado a tiempo completo; sin embargo, resultaría inconcebible para una empresa que genere 200 000 casos diarios, incluso con un centenar de empleados a tiempo completo.



PERCEPCIONES REGIONALES SOBRE LA DOTACIÓN DE RECURSOS

En la región EMEA, hay un amplio consenso entre casi la mitad (un **42,6 %**) de equipos antifraude de que la cantidad de recursos de que disponen es insuficiente. Sin embargo, se aprecian sorprendentes diferencias regionales, especialmente en España y Francia, donde más de dos tercios de los encuestados (un **72,4 %** y un **61,5 %**, respectivamente) expresaron su preocupación por la insuficiencia del presupuesto antifraude. En la otra cara de la moneda se encuentran Italia y Turquía: en estos países, solo una de cada cuatro compañías (para ser precisos, un **28,6 %** y un **23,1 %**, respectivamente) afirmó que sus recursos antifraude eran insuficientes.

Dado que, en Sudáfrica, una tercera parte de los encuestados (el **33,3 %**) considera que sus equipos antifraude no disponen de personal suficiente, se insta a los altos ejecutivos a considerar una revisión integral de sus entornos de lucha contra el fraude. De tal revisión podría inferirse que los motores de normas y los procesos no están perfeccionados de forma coherente o no son lo bastante flexibles como para afrontar cambios en la estrategia empresarial, lo que genera altos porcentajes de falsos positivos. Las restricciones vigentes vinculadas al confinamiento añaden un nivel más de complejidad, ya que, a menudo, limitan los análisis de investigación sobre el fraude, que también se ven afectados por la falta de recursos y de herramientas.

En Alemania, al igual que ocurre en varios países europeos, el fraude en los canales digitales ha sido especialmente problemático; se disparó durante el punto álgido de la pandemia, período en el que más de la mitad de los encuestados (el **55 %**) declara haber notado un mayor volumen de actividad fraudulenta.

En Francia, el fraude a través de canales físicos (**26 %**) aún supera al fraude digital (**21 %**), lo que vuelve a poner de manifiesto la importancia de las soluciones vinculadas y multicanal para la prevención del fraude.

UNA CUESTIÓN DE EQUILIBRIO

Los resultados muestran que casi la mitad de los encuestados (un 49,1%) reconocen la necesidad de adoptar un enfoque equilibrado. Es evidente que hay un problema cuando los recursos limitan la capacidad de remisión (especialmente con los ataques fraudulentos al alza), porque no parece probable que la tolerancia al riesgo vaya a cambiar de un día para otro.

También cabe señalar que el porcentaje de ataques fraudulentos suele ser el parámetro de medición más fácil de calcular pero, no obstante, se elude con frecuencia. Se trata simplemente de la proporción de intentos totales de fraude en relación con los volúmenes de negocio generales en un período de tiempo determinado.

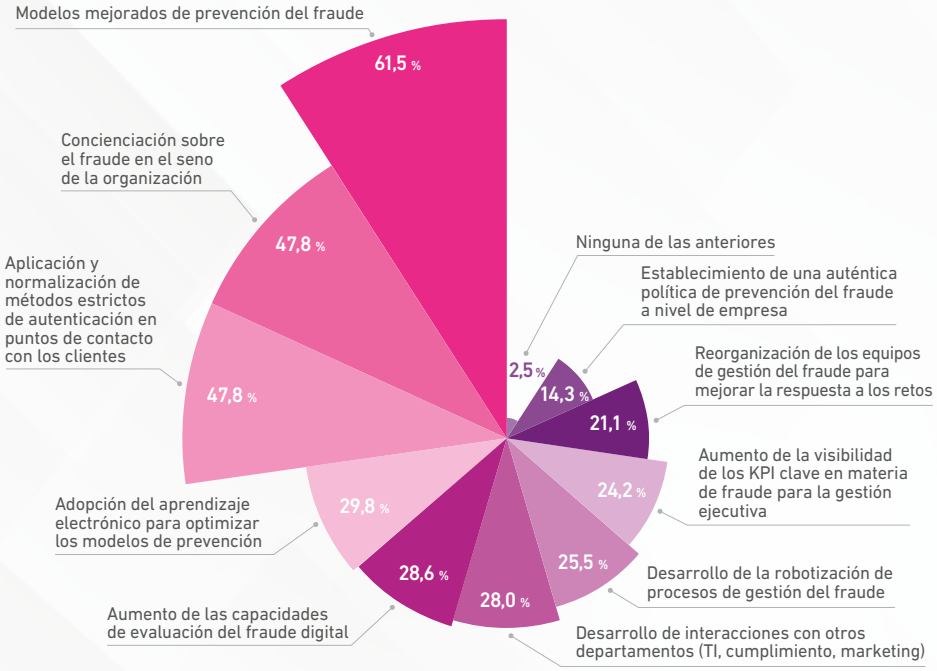
Sin embargo, dado que combina los ataques exitosos y no exitosos, se le concede menos atención a la hora de presentar informes porque toda la atención se centra en el número crítico de pérdidas totales vinculadas al fraude. Lamentablemente, incluso cuando se informa de este parámetro, suele quedarse al margen, porque muchas empresas aún consideran que solo obedece al capricho de delincuentes y grupos criminales.

MÉTODOS PARA REDUCIR LAS PÉRDIDAS E INCREMENTAR LA DETECCIÓN

Las soluciones de mitigación del fraude con varios niveles capaces de combinar el mayor número posible de datos disponibles con inteligencia artificial y técnicas de aprendizaje automático constituyen pasos rápidos hacia la reducción de las pérdidas asociadas al fraude. Prácticamente todas las empresas pueden adoptarlas, pero deben cumplir con los siguientes criterios mínimos de referencia:

- Deben contar con un sólido motor de riesgos que incluya un módulo preciso de información.
- Deben incluir tecnologías de identificación de dispositivos, ya que son muchos los puntos de contacto transaccional que pueden falsificarse (incluyendo la dirección IP, la información de identificación personal, etc.).
- Deben incluir indicadores de geolocalización que se puedan recopilar y aprovechar para la mitigación de riesgos y que permitan localizar el origen de la transacción, en vez de confiar ciegamente en los datos introducidos por el usuario.
- Deben incorporar modelos de aprendizaje automático que hagan uso de todos los datos disponibles para maximizar el porcentaje de detección de actividades fraudulentas.
- Deben ser capaces de integrar otras soluciones analíticas, como la biometría o la tecnología de verificación de documentos y de reputación del correo electrónico; se trata de que la solución integral antifraude sea tan difícil de traspasar como para que los estafadores se desmotiven y desistan, de modo que las organizaciones puedan centrarse en lo que mejor saben hacer, que es proporcionar sus servicios a sus clientes.

Aspiraciones y planificación de inversiones clave



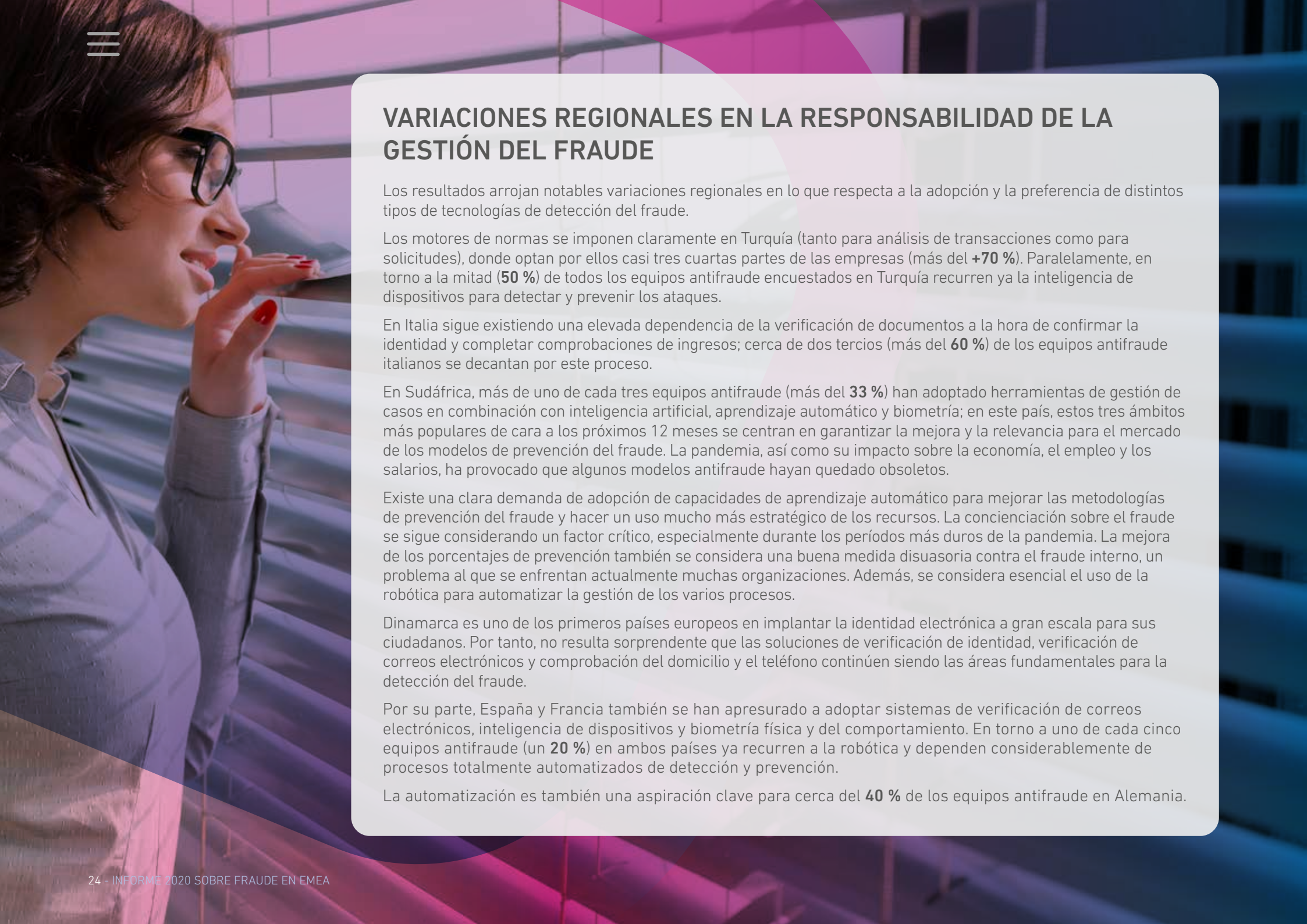
INICIATIVAS ANTIFRAUDE CUYA ADOPCIÓN ESTÁ PREVISTA EN LOS PRÓXIMOS 12 MESES

La mejora de la prevención del fraude (61,5%) y la adopción de sistemas de aprendizaje automático para seguir optimizando los modelos (47,8%) son las dos aspiraciones clave de los equipos antifraude de cara al próximo año. No obstante, se aprecia también una clara determinación de aumentar la concienciación y el perfil público de las actividades de prevención del fraude en casi la mitad (un 47,8%) de las empresas encuestadas. Además, se hace patente una evidente preocupación acerca del trabajo aislado: más de uno de cada cuatro equipos (un 28 %) se muestran a favor de mejorar la interacción con otros departamentos, incluyendo TI, *compliance* y marketing.

También hemos pedido a los encuestados que explicasen sus aspiraciones tecnológicas indicando en qué aspectos les gustaría que trabajaran sus equipos antifraude. Las mejoras de los motores de normas y el análisis en tiempo real de las transacciones han sido medidas clave para más de la mitad (50,9 %).

Cabe destacar también que la inteligencia de dispositivos, la verificación de correos electrónicos, la inteligencia artificial, el aprendizaje automático y el aumento de la automatización son prioritarios para aproximadamente uno de cada cinco equipos antifraude.

Las mejoras en la evaluación del fraude digital ya se hacen notar gracias a la combinación de inteligencia de dispositivos y calificación de correos electrónicos.



VARIACIONES REGIONALES EN LA RESPONSABILIDAD DE LA GESTIÓN DEL FRAUDE

Los resultados arrojan notables variaciones regionales en lo que respecta a la adopción y la preferencia de distintos tipos de tecnologías de detección del fraude.

Los motores de normas se imponen claramente en Turquía (tanto para análisis de transacciones como para solicitudes), donde optan por ellos casi tres cuartas partes de las empresas (más del **+70 %**). Paralelamente, en torno a la mitad (**50 %**) de todos los equipos antifraude encuestados en Turquía recurren ya la inteligencia de dispositivos para detectar y prevenir los ataques.

En Italia sigue existiendo una elevada dependencia de la verificación de documentos a la hora de confirmar la identidad y completar comprobaciones de ingresos; cerca de dos tercios (más del **60 %**) de los equipos antifraude italianos se decantan por este proceso.

En Sudáfrica, más de uno de cada tres equipos antifraude (más del **33 %**) han adoptado herramientas de gestión de casos en combinación con inteligencia artificial, aprendizaje automático y biometría; en este país, estos tres ámbitos más populares de cara a los próximos 12 meses se centran en garantizar la mejora y la relevancia para el mercado de los modelos de prevención del fraude. La pandemia, así como su impacto sobre la economía, el empleo y los salarios, ha provocado que algunos modelos antifraude hayan quedado obsoletos.

Existe una clara demanda de adopción de capacidades de aprendizaje automático para mejorar las metodologías de prevención del fraude y hacer un uso mucho más estratégico de los recursos. La concienciación sobre el fraude se sigue considerando un factor crítico, especialmente durante los períodos más duros de la pandemia. La mejora de los porcentajes de prevención también se considera una buena medida disuasoria contra el fraude interno, un problema al que se enfrentan actualmente muchas organizaciones. Además, se considera esencial el uso de la robótica para automatizar la gestión de los varios procesos.

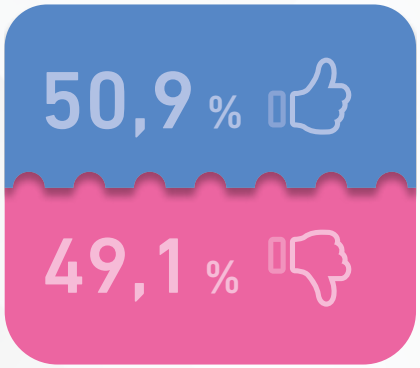
Dinamarca es uno de los primeros países europeos en implantar la identidad electrónica a gran escala para sus ciudadanos. Por tanto, no resulta sorprendente que las soluciones de verificación de identidad, verificación de correos electrónicos y comprobación del domicilio y el teléfono continúen siendo las áreas fundamentales para la detección del fraude.

Por su parte, España y Francia también se han apresurado a adoptar sistemas de verificación de correos electrónicos, inteligencia de dispositivos y biometría física y del comportamiento. En torno a uno de cada cinco equipos antifraude (un **20 %**) en ambos países ya recurren a la robótica y dependen considerablemente de procesos totalmente automatizados de detección y prevención.

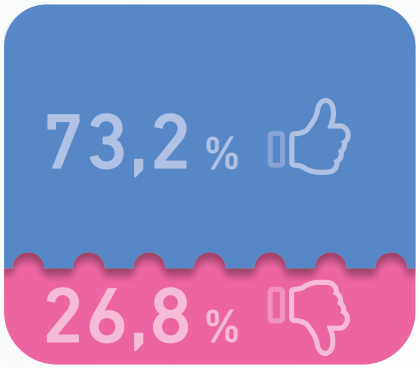
La automatización es también una aspiración clave para cerca del **40 %** de los equipos antifraude en Alemania.

Formar parte de un sistema multi-sectorial de lucha contra el fraude

¿Cree que sería beneficioso?



Entonces, ¿por qué no forma parte de uno de ellos?



Preguntamos a los entrevistados su opinión sobre el uso compartido, entre distintas entidades, de datos de fraudes ya conocidos, con el objetivo de fomentar la detección y la prevención. Con apenas un poco más de la mitad de los encuestados a favor (el 50,9 %), el éxito depende claramente de la superación de obstáculos normativos para garantizar la obtención de una solución coherente.

De entre los encuestados que declararon no formar aún parte de una iniciativa de uso compartido de datos, casi tres cuartas partes (el 73,2 %) se posicionaron a favor de asociarse a una y reconocieron sus beneficios abiertamente. Los motivos para no unirse a un sistema multi-sectorial de compartición de datos fraudulentos, se muestran en la sección de la derecha; casi la mitad de los encuestados considera que las normativas regionales son un impedimento clave.

24,6 %
Las normas locales nos lo impiden.

21,1 %
No existe un sistema así porque no hay suficiente oferta en el mercado.

15,8 %
La normativa ralentiza el proceso debido al estricto cumplimiento de los requisitos en materia de protección de datos.

10,5 %
Existe un sistema así, pero se ha tomado la decisión interna de no participar en él.

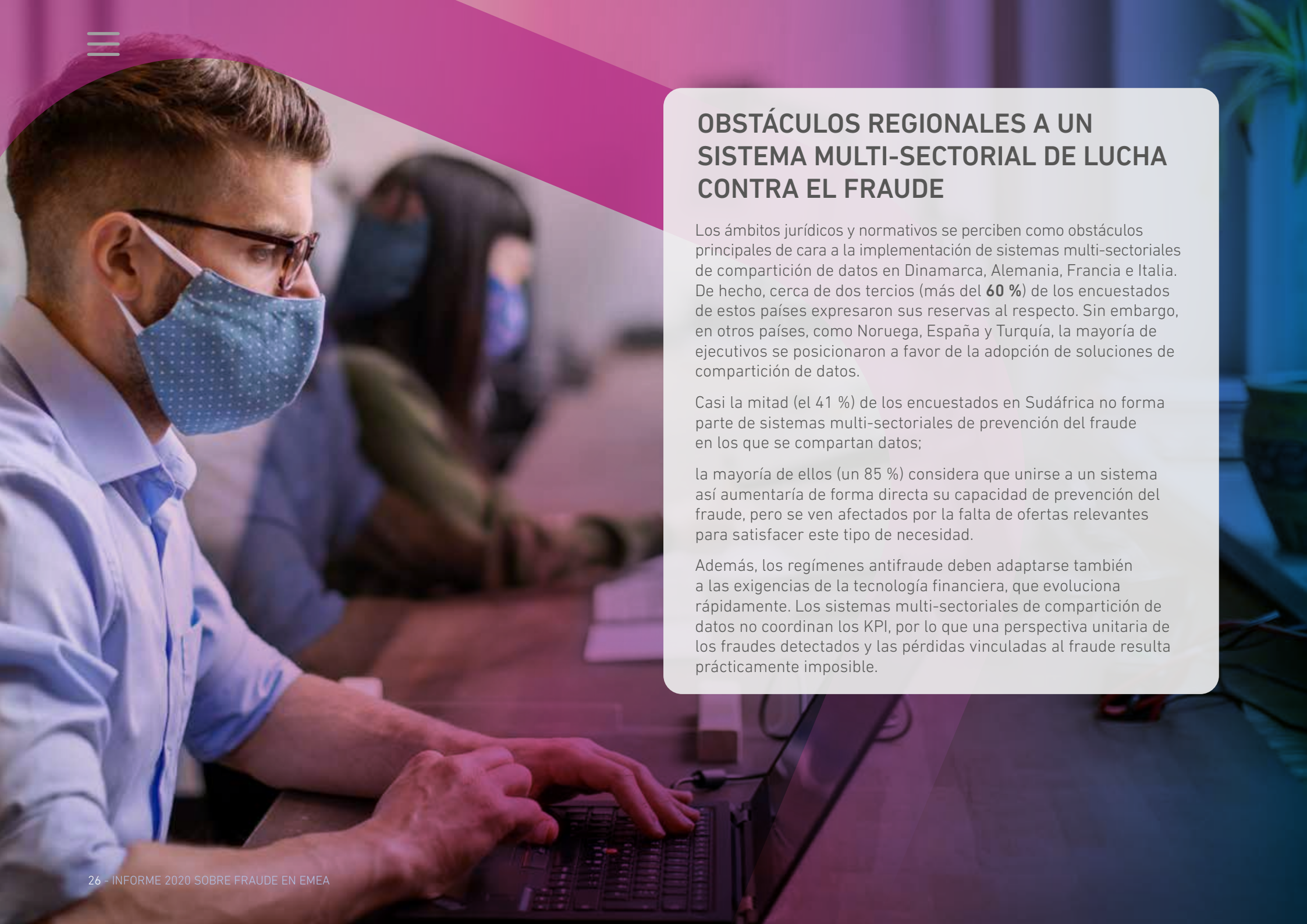
10,5 %
Aún no existe un sistema así, pero hay en marcha una iniciativa para establecerlo.

10,5 %
Aún no existe un sistema así porque no hay suficientes compañías dispuestas a participar.

7,0 %
Se planteó una iniciativa, pero fracasó por la falta de acuerdo entre los miembros potenciales.

+45 %

A lo largo de nuestra experiencia de más de 20 años de gestión de fraudes por todo el mundo, apreciamos que en general, las empresas pueden mejorar su gestión en la lucha contra el fraude perteneciendo a sistemas multi-sectoriales de compartición de datos fraudulentos entre todas las empresas que formen parte de la iniciativa.



OBSTÁCULOS REGIONALES A UN SISTEMA MULTI-SECTORIAL DE LUCHA CONTRA EL FRAUDE

Los ámbitos jurídicos y normativos se perciben como obstáculos principales de cara a la implementación de sistemas multi-sectoriales de compartición de datos en Dinamarca, Alemania, Francia e Italia. De hecho, cerca de dos tercios (más del **60 %**) de los encuestados de estos países expresaron sus reservas al respecto. Sin embargo, en otros países, como Noruega, España y Turquía, la mayoría de ejecutivos se posicionaron a favor de la adopción de soluciones de compartición de datos.

Casi la mitad (el 41 %) de los encuestados en Sudáfrica no forma parte de sistemas multi-sectoriales de prevención del fraude en los que se compartan datos;

la mayoría de ellos (un 85 %) considera que unirse a un sistema así aumentaría de forma directa su capacidad de prevención del fraude, pero se ven afectados por la falta de ofertas relevantes para satisfacer este tipo de necesidad.

Además, los regímenes antifraude deben adaptarse también a las exigencias de la tecnología financiera, que evoluciona rápidamente. Los sistemas multi-sectoriales de compartición de datos no coordinan los KPI, por lo que una perspectiva unitaria de los fraudes detectados y las pérdidas vinculadas al fraude resulta prácticamente imposible.

Conclusiones

Combatir el fraude es un reto global, y en Experian llevamos más de 20 años ayudando a nuestros clientes a prevenirlo, detectarlo y frenarlo.

Lo hacemos por medio de servicios de consultoría que incluyen estrategias de prevención, políticas antifraude, revisiones de procesos y, de forma más directa, por medio de soluciones diseñadas para detectar y prevenir diversos tipos de fraude.

Cabe destacar también que nuestra tecnología es transparente, de modo que los estafadores a menudo no son capaces de detectarla ni anticiparse a ella, con lo que la probabilidad de evadirla es muy baja. Además, nuestras soluciones ofrecen análisis en tiempo real de dispositivos y conexiones, así como análisis y biometría de comportamiento en el punto de inicio de sesión; a esto se suman la consideración del comportamiento típico de la cuenta y el análisis continuo de acontecimientos en puntos esenciales (como el IBAN, el número de teléfono, la dirección de correo electrónico, etc.), todo ello por medio de conjuntos de normas muy avanzados.

Desde el punto de vista de la experiencia del cliente, la tecnología es fluida y prácticamente imperceptible y, por lo tanto, no genera fricciones. La adopción de un enfoque holístico ofrece una protección más sólida para nuestros clientes y los usuarios.

El resurgimiento de las actividades de *phishing* y duplicación de tarjetas SIM y la amenaza actual del robo de cuentas han puesto de manifiesto que los estafadores son pertinaces y oportunistas, y que no cejan en su empeño de poner a prueba las defensas antifraude con todo tipo de técnicas. En todo caso, es evidente que, cuando entran en juego diversas vulnerabilidades y múltiples factores de riesgo, es preciso recurrir a enfoques sistemáticos y estratégicos: por una parte, para garantizar niveles máximos de detención y prevención y equilibrar la seguridad ofreciendo la mejor experiencia de cliente; por otra, para mantener la agilidad y la capacidad de respuesta para reaccionar a amenazas nuevas o emergentes.

Aumento de la confianza y el reconocimiento de los clientes

Mediante la optimización de la adquisición y el enriquecimiento de los datos.

Mejora de la detección y la prevención

Mediante la adopción de sistemas predictivos de análisis con aprendizaje automático capaces de ofrecer asistencia en tiempo real a los clientes, tratando el riesgo al que se exponen con cada interacción.

Lucha contra tipos de fraude nuevos y emergentes

Mediante la integración, la automatización y la armonización inteligente de soluciones de identidad y lucha contra el fraude a varios niveles.

Austria
Strozzigasse 10/14
1080 Vienna
www.experian.at

Bulgaria
Space Tower
86 Tsarigradsko Shosse Blvd
Sofia 1113
www.experian.bg

Dinamarca
Lyngbyvej 2
2100 Copenhague
www.experian.dk

Francia
Tour PB5
1 avenue du Général de Gaulle
La Défense 8
92074 Paris La Défense Cedex
www.experian.fr

Alemania
Rheinstraße 99
76532 Baden-Baden
www.experian.de

Grecia y Rumanía
65 Ag. Alexandrou Street
17561 Paleo Faliro Athens
www.experian.gr

Italia
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

Países Bajos
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

Noruega
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

Polonia
Metropolitan Complex
Plac Pilsudskiego 3
00-078 Warsaw
www.experian.com.pl

Rusia
5, bldg. 19, Nizhny Susalny lane
105064 Moscú
www.experian.ru.com

Sudáfrica
Ballyoaks Office Park
35 Ballyclare Drive
2191 Bryanston, Sandton
www.experian.co.za

España
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

Turquía
River Plaza
Buyukdere Cad. Bahar Sok.
No: 13 Kat: 8 Levent
34394 Estambul
www.experian.com.tr

Emiratos Árabes Unidos
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai Internet City
www.experian.ae

Dirección del domicilio social:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

T: 0844 481 5873
www.experian.co.uk

21-EMEA-0022