KPMG
cutting through complexity

Perfiles globales del defraudador

Presente y futuro de los delitos económicos

kpmg.com/fraudster

Introducción

Los especialistas en fraudes llevan mucho tiempo debatiendo si es posible desarrollar un perfil de defraudador que sea lo suficientemente preciso como para permitir a las organizaciones detectar a los autores durante la comisión del fraude o, incluso, con anterioridad al mismo. La completa predicción de un delito antes de que se produzca pertenece, al menos por el momento, al ámbito de la ciencia ficción. Sin embargo, un análisis de la naturaleza en constante cambio del fraude y del defraudador puede ayudar a las organizaciones a reforzar sus defensas contra estas actividades delictivas. Más vale prevenir que curar.

El presente informe contiene el análisis realizado por KPMG de 596 defraudadores que las firmas miembro han investigado entre 2011 y 2013. Su intención es proporcionar percepciones al lector sobre la relación entre los atributos de los defraudadores, sus motivaciones y el entorno en el que operan con más facilidad. Además, hemos entrevistado a responsables de investigación de firmas miembro de KPMG para recabar percepciones adicionales. Este estudio complementa a nuestra publicación de 2011, titulada Who is the typical fraudster? (¿cómo es el defraudador típico?) , que aborda 348 casos investigados, y a la de 2007, titulada El Perfil del Defraudador . El informe de 2011 se centró en la relación entre patrones globales de fraude, diversos atributos de los defraudadores y cómo puede ser su evolución en los próximos cinco años.

Entre los 596 incluidos en el estudio de 2013, el defraudador típico es muy similar al identificado en las investigaciones presentadas por las firmas de KPMG dos años antes. En el estudio de 2013, el defraudador típico tiene entre 36 y 45 años, generalmente actúa contra su propia organización y mayoritariamente trabaja en una función del área directiva , finanzas, operaciones o ventas/marketing. Ocupa un puesto de alta dirección, lleva en la organización más de seis años y, a la hora de cometer el fraude, suele actuar en complicidad con otros.

Entre los 596 incluidos en el estudio de 2013, el defraudador típico es muy similar al identificado en las investigaciones presentadas por las firmas de KPMG dos años antes.

Otras conclusiones, no obstante, son diferentes. En esta ocasión hemos desarrollado una serie de temas a fin de comprender la compleja relación entre el defraudador, su entorno y los fraudes cometidos. Después de tener en cuenta las percepciones de nuestros responsables de investigación de todo el mundo, hemos llegado a la conclusión de que el tipo de fraude y el tipo de defraudador están en constante cambio. "Lo desconcertante de los fraudes es que siempre están mutando, como el virus de la gripe. Puedes curar la cepa de hoy, pero el próximo año evolucionará a algo igual de dañino, o incluso peor", afirma Phil Ostwalt, coordinador global de investigaciones para la práctica global de Forensic de KPMG.

Un cambio destacado es el creciente uso de tecnología por parte de los defraudadores, y no solo en países tecnológicamente avanzados, como Estados Unidos. "Constituye una preocupación para todas las empresas el hecho de que estamos a punto de encontrarnos con una nueva generación capacitada para usar más tecnología y con acceso a mucha más información que las generaciones anteriores. Todo ello indica el inicio de una nueva era para el fraude y las actividades ilegales", comenta Arturo del Castillo, director gerente de Forensic, KPMG en Colombia.

Creemos que ser conscientes de esta fluidez permitirá a las organizaciones protegerse mejor contra el fraude, y puede mejorar su capacidad para identificar a los defraudadores, muchos de los cuales cometen sus delitos durante periodos prolongados. Muchos defraudadores se ocultan manteniéndose a plena

[1] Who is the typical fraudster? Análisis de patrones globales de fraude de KPMG, 2011
[2] Estudio El Perfil del Defraudador, 2007
[3] La función también se conoce como dirección general e incluye al director general (CEO).

vista. Puede que no llamen la atención al mantenerse en un segundo plano o que ocupen puestos destacados en la organización. Los tipos de fraude que cometen están en constante cambio, en el marco de un entorno de negocio en continuo cambio.

De forma permanente se crean nuevas técnicas de fraude, y las organizaciones han de reaccionar y poner al día sus defensas. "Las empresas no pueden quedarse de brazos cruzados y permitir que los controles de ayer detengan al defraudador de hoy o de mañana", dice Ostwalt. La tecnología no solo facilita las acciones del defraudador; también permite a la organización defenderse. "Las empresas tienen que pensar más detenidamente si siguen siendo válidas las viejas tecnologías de prevención del fraude. Enfoques más innovadores, como los análisis y la minería de datos, les proporcionan una oportunidad mucho mejor para atrapar al defraudador", declara Grant Jamieson, socio responsable de Servicios de Forensic para KPMG en Hong Kong.

A continuación ofrecemos más información sobre los fraudes investigados por las firmas miembro en todo el mundo desde el informe de 2011, nuestro análisis de las variaciones en el perfil del defraudador, cómo está relacionado dicho perfil con su entorno y los delitos cometidos, así como nuestra opinión sobre cómo podrían ser y cómo podrían comportarse en el futuro.

Tomando como referencia el análisis realizado por KPMG de los 596 defraudadores que han investigado sus firmas miembro, algunas de las principales características de su perfil son:

- Edad: La edad del 70 por ciento de los defraudadores está comprendida entre 36 y 55 años.
- Empleo: El 61 por ciento de los defraudadores trabajan para la organización afectada. De esta cifra, el 41 por ciento llevaba trabajando más de seis años.
- Colusión: En el 70 por ciento de los fraudes, el autor actuó en connivencia con otras personas.
- Tipo: El fraude más frecuente es la apropiación indebida de activos (56 por ciento), donde la malversación representa el 40 por ciento y el fraude en las compras representa el 27 por ciento.
- El segundo fraude más habitual es la obtención de ingresos o activos mediante actividades fraudulentas o ilegales (24 por ciento).
- En los casos en los que los defraudadores actuaron en solitario, el 69 por ciento de los delitos fueron cometidos a lo largo de un periodo de entre uno y cinco años. El 21 por ciento de estos fraudes supusieron un coste total para la organización afectada de entre 50.000 y 200.000 dólares estadounidenses, y el 16 por ciento, de entre 200.000 y 500.000 dólares. En el 32 por ciento de estos casos, el coste para la organización afectada excedió la cifra de 500.000 dólares, y superó la suma de 5.000.000 dólares en el 9 por ciento de los casos.
- En los casos en los que los defraudadores actuaron con cómplices, el 74 por ciento de los delitos fueron cometidos a lo largo de entre uno y cinco años. En lo que respecta a la cuantía, el 18 por ciento de los fraudes alcanzaron un total de entre 50.000 y 200.000 dólares, y el 16 por ciento superó la suma de 5.000.000 dólares. En el 43 por ciento de estos casos, el coste para la organización afectada excedió la cifra de 500.000 dólares, y superó la suma de 5.000.000 dólares en el 16 por ciento de los casos.
- El 93 por ciento de los fraudes fueron cometidos en múltiples transacciones. En el 42 por ciento de estos delitos, la cuantía media por cada transacción osciló entre 1.000 y 50.000 dólares.
- El 72 por ciento de todos los fraudes se cometieron durante un periodo de entre uno y cinco años (33 por ciento, entre uno y dos años, y 39 por ciento, entre tres y cinco años).

Metodología

A través de un estudio, KPMG recopiló datos de investigaciones sobre fraudes realizadas por profesionales especializados en el área de Forensic de las firmas miembro de KPMG en las regiones de Europa, Oriente Medio y África (EMA); América y Asia-Pacífico entre agosto de 2011 y febrero de 2013. Analizamos un total de 596 defraudadores implicados en actos cometidos en 78 países. En el estudio se examinaron investigaciones de delitos económicos perpetrados en las tres regiones, en los casos en que pudimos identificar al autor y pudimos aportar información contextual detallada sobre el delito.

En el análisis se identifican:

- Perfiles del defraudador y detalles sobre los tipos de fraude más habituales
- Condiciones del entorno que tienden a facilitar el fraude
- Sanciones aplicadas por la organización afectada o por la fiscalía pública

Las conclusiones de este informe se contrastan, siempre que es posible, con nuestros análisis de 2007 y 2011 para subrayar los cambios en los patrones y ofrecer una perspectiva sobre las tendencias emergentes.

En el presente informe no se revelan los nombres de ninguna de las partes implicadas para mantener la confidencialidad. Muchos de los casos incluidos no llegaron a ser de dominio público; otros fueron noticia, pero generalmente sin entrar en detalle. Todos los importes se reflejan en dólares estadounidenses.

Tres factores de fraude

A fin de comprender el perfil del defraudador es aconsejable tener en cuenta tres factores que incitan al fraude: oportunidad, motivación y racionalización. "Los fraudes se cometen cuando coinciden los tres elementos, la tormenta perfecta: motivación, oportunidad y capacidad para racionalizar el acto. En casi todos los casos, esto explica por qué se comete el fraude y por qué se convierte en defraudador un tipo específico de persona", declara la práctica de Forensic en China. Los tres factores forman parte de una metodología estándar desarrollada para investigadores de fraude en los años cincuenta. Incluimos la capacidad como componente de la oportunidad para crear una imagen más completa de la persona que comete un fraude. Una manera de comprender la imagen es pensar que el potencial defraudador ve una puerta abierta por la oportunidad. El motivo y la racionalización le conducen al umbral y la capacidad le impulsa a cruzarlo.

El triángulo del fraude

Fuente: Global profiles of a fraudster, KPMG International, 2013.

[4] Véase el artículo "Beyond the fraud triangle" (Más allá del triángulo del fraude), Fraud Magazine, septiembre/octubre de 2011.

> Tener buenos controles internos es importante, pero con cualquier control al final se depende del componente humano

Niamh Lambe
Director de KPMG, Responsable de KPMG Forensic en Ireland

Analicemos ahora por orden cada uno de los factores de fraude:

Oportunidad

Las personas no cometen fraudes si no se les presenta la oportunidad para ello. Un gran número de defraudadores en los casos investigados llevaban trabajando para la organización afectada más de seis años, y casi tres cuartas partes de los delitos fueron llevados a cabo en el transcurso de un periodo de uno a cinco años. Esto significa que los defraudadores no solicitan un puesto de trabajo en la organización con el objetivo de cometer un delito, pero los cambios en las circunstancias personales o las presiones para cumplir objetivos de negocio exigentes pueden crear las condiciones idóneas para el fraude. Posiblemente lo hacen cuando se sienten cómodos en su puesto y gozan de la confianza y del respeto de sus compañeros (véase recuadro).

¿Cómo se presenta la oportunidad? Según el estudio, la debilidad de los controles internos favoreció el 54 por ciento de los fraudes. Esto indica que si muchas organizaciones endurecieran los controles y la supervisión de los empleados, la oportunidad de cometer un fraude se reduciría visiblemente. Es muy frecuente que las organizaciones pasen por alto la prevención del fraude mediante la implantación de los controles adecuados y aprendan de sus errores cuando es demasiado tarde.

"Muchas empresas se plantean medidas antifraude proactivas como un seguro. Si es posible que no suceda nunca, ¿por qué gastar el dinero?", dice James McAuley, socio de Forensic para KPMG en Canadá. En otros lugares, las organizaciones carecen de los controles incluso más simples. "Los fraudes suelen producirse por el fallo de no haber implantado un control básico. Nuestras investigaciones demuestran, por ejemplo, que la dirección no siempre comprueba la documentación justificativa antes de autorizar una transacción. Esto proviene de la cultura de confianza sueca", afirma Martin Krüger, socio a cargo del área de Forensic para KPMG en Suecia. En zonas de Oriente Medio, muchas organizaciones no han hecho más que empezar a

> La dirección suele considerar el riesgo de fraude como un elemento más en el conjunto de riesgos, y no siempre valora plenamente su naturaleza y su alcance reales

Defraudador ocasional

- Características: no reincidente, de mediana edad, varón, casado con hijos, empleado de confianza, ocupa un puesto de responsabilidad, buen ciudadano en su comunidad.
- Generalmente tiene un problema que mantiene oculto que puede solucionarse con dinero y que le crea una tensión que se percibe.
- Cuando es descubierto, suele sorprender el supuesto comportamiento del autor del fraude.

Depredador

- Suele ser inicialmente un defraudador ocasional.
- En ocasiones, busca organizaciones donde pueda empezar a urdir un plan de acción casi inmediatamente después de su contratación.
- Defrauda deliberadamente a las organizaciones sin apenas atisbo de remordimiento.
- Está mejor organizado que el defraudador ocasional y utiliza mejores técnicas de ocultación.
- Está mejor preparado para esquivar a los auditores y otros mecanismos de supervisión.

entender la necesidad de los controles para prevenir el fraude. "Observamos que hay muchas empresas públicas y privadas expuestas a fraudes, con escasas defensas. Aunque los controles internos y la gestión del riesgo de fraude aún no se ha integrado en la cultura de la empresa, el diálogo ya está en marcha", comenta Arindam Ghosh, director asociado y responsable de Servicios de Forensic, Risk Consulting, KPMG en Baréin y Qatar.

Sin embargo, unos controles internos sólidos no impedirán todos los fraudes. El 20 por ciento de los defraudadores cometieron el delito de forma temeraria, haciendo caso omiso de los controles. En el 11 por ciento de los casos, actuaron en connivencia con otras personas para eludir los controles. En estos casos, el defraudador puede ser una persona que conoce los controles y sabe cómo manipularlos, o que encuentra un fallo en los mismos por accidente y se aprovecha de ello. Ningún sistema de control es inexpugnable; es necesaria la vigilancia de al menos una persona. Los investigadores de KPMG afirman que las organizaciones han de supervisar de forma permanente el entorno interno y externo, pero han detectado que la mayoría no lo hace. "La dirección suele considerar el riesgo de fraude como un elemento más en el conjunto de riesgos, y no siempre valora plenamente su naturaleza y su alcance reales. Por tanto, esto significa frecuentemente que no recibe la atención y el tratamiento necesarios para gestionarlo", afirma Mark Leishman, socio responsable de Servicios de Forensic, KPMG en Australia.

> En Singapur hay muy poca corrupción, en términos relativos, principalmente porque la aplicación de la ley es implacable y la actividad empresarial se desarrolla de forma transparente

Las sanciones, como, por ejemplo, las derivadas de una demanda o una querella, pueden servir de medida de disuasión del fraude, pero son pocas las empresas dispuestas a exponerse a un perjuicio para su reputación. La pena de cárcel solo se aplicó al 7 por ciento de los defraudadores, y el 35 por ciento se vio inmerso en procedimientos por la vía civil y penal. El 55 por ciento de los defraudadores fueron despedidos, por lo que se agrava el riesgo de que cometan delitos en otras empresas donde sean contratados posteriormente en caso de no haber tenido que afrontar un procedimiento judicial. Por tanto, es de la máxima importancia establecer reglamentos para controlar el comportamiento en la empresa y, a continuación, velar por su aplicación. "En Singapur hay muy poca corrupción, en términos relativos, principalmente porque la aplicación de la ley es implacable y la actividad empresarial se desarrolla de forma transparente", comenta Lem Chin Kok, socio de Servicios de Forensic, KPMG en Singapur.

Capacidad

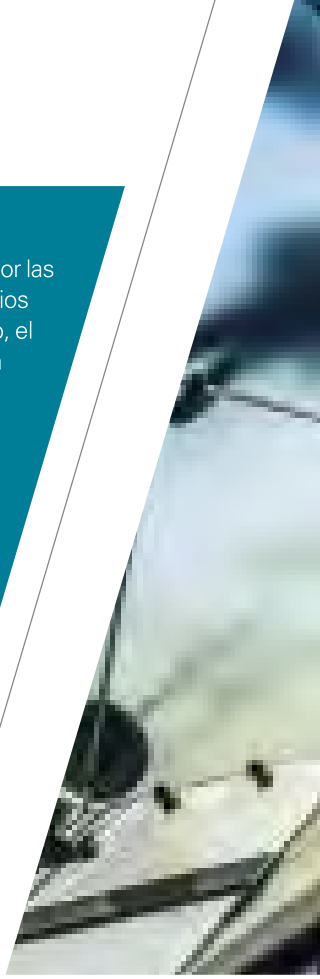
Como hemos indicado anteriormente, incluimos la capacidad como un elemento subordinado del factor oportunidad. La capacidad comprende aquellos atributos del defraudador que le permiten aprovechar la oportunidad cuando surge. Los atributos son los rasgos personales del defraudador y su habilidad para cometer el delito.

Así pues, la capacidad depende a menudo del nivel jerárquico que ocupa el defraudador en la empresa. Un gran número de ellos ocupan puestos directivos o ejecutivos (25 por ciento y 29 por ciento, respectivamente, de los contratados en la organización afectada). "En los próximos tres a cinco años quizás notemos que el defraudador en la región de África Oriental está cada vez más preparado y que tiene un nivel jerárquico más alto en la organización a medida que los controles de las empresas mejoran y más delincuentes son juzgados y condenados", dice Marion Barriskell,

[5] Como se ha indicado anteriormente, KPMG tiende a investigar fraudes cometidos por empleados de categoría senior, por lo que esta conclusión puede no ser válida para todos los defraudadores, ya que una gran parte de los delitos pueden ser cometidos por empleados de niveles inferiores.

Fraude por sectores

En todos los sectores, el fraude tiende a estar condicionado por las oportunidades de conducta irregular. En los sectores de servicios financieros, farmacéutico, mercados industriales y de consumo, el fraude más habitual es la malversación. Sin embargo, en energía y recursos naturales (ENR), el sector público y en información, comunicaciones y ocio, el fraude más frecuente es el fraude en las compras. En servicios financieros tuvo lugar el coste más elevado del fraude, usualmente más de 5 millones de dólares estadounidenses por infractor. En otros sectores los costes fueron menores, a menudo entre 200.000 y 500.000 dólares estadounidenses. La corrupción fue más generalizada en el sector farmacéutico, servicios financieros y ENR que en otros sectores. En el caso del sector farmacéutico y los servicios financieros, esto se produjo pese al hecho de que las organizaciones pertenecientes a estos sectores operan en un entorno muy regulado.



responsable de Investigaciones para KPMG en África Oriental. Cuanto mayor sea el nivel jerárquico del defraudador, mayor será su habilidad para esquivar los controles. "Generalmente el defraudador hace caso omiso de los controles. Aunque la mayoría de las empresas en Suiza disponen de controles internos estándar, una persona puede hacer aflorar oportunidades después de cuatro o cinco años", añade Anne van Heerden, socia responsable de las prácticas de Forensic y Consulting para KPMG en Suiza.

Los porcentajes respectivos de los directivos y ejecutivos que actúan en connivencia con otros empleados son del 24 y del 38 por ciento. En segundo lugar, el 46 por ciento de todos los defraudadores tenían conocimientos informáticos, lo cual se está convirtiendo gradualmente en un activo ahora que se almacena un volumen tan grande de datos en los ordenadores y es probable que aumente la frecuencia de los fraudes cibernéticos. En lo que respecta a rasgos personales, las características preponderantes no tienden a confirmar la imagen de una persona solitaria y aislada. El defraudador suele ser muy respetado (39 por ciento de todos los casos examinados), afable (35 por ciento) y/o extrovertido (33 por ciento).

Motivación

El fraude, como sucede con cualquier delito, requiere un motivo, y en los 596 casos analizados la razón predominante para cometerlo es la motivación económica. Se planteó a los participantes en la encuesta 14 posibles motivaciones, de las que podían elegir tantas como considerasen oportunas. Del total de 1.082 motivaciones mencionadas, 614 tenían que ver con la avaricia, el beneficio económico y las dificultades económicas, mientras que otras 114 estaban relacionadas con el cumplimiento de objetivos de negocio. El único motivo no financiero con una frecuencia similar es la simple voluntad de hacerlo (o "porque puedo") con 106 casos.

Estas 614 motivaciones abarcan una amplia gama de desencadenantes financieros. Por ejemplo, uno de ellos es mejorar el estilo de vida. "Generalmente, una persona comete un fraude para costearse un ritmo de vida extravagante, o al menos muy elevado. Rara vez la persona se convierte en defraudador para cubrir sus necesidades básicas. Ya tienen una buena posición, por lo que a menudo uno se pregunta por qué se arriesgan", señala Anne van Heerden, socia y responsable de Forensic para KPMG en Suiza. Otros factores financieros son el temor a incumplir un objetivo financiero o el deseo de obtener mayores incentivos. "Son más las empresas extranjeras que están aumentando los incentivos de la dirección local que están vinculados a su desempeño, al tiempo que recortan su salario base. Hemos notado que esto ha potenciado la manipulación de la cifra de beneficios y el fraude en los estados financieros, a causa de los objetivos que debe cumplir la dirección", declara Jimmy Helm, socio responsable de Forensic para KPMG en Europa Central y del Este.

Lo cierto es que varios responsables de investigación han observado un aumento en la manipulación de beneficios, sin duda relacionada con los efectos de la recesión económica. "A causa de las presiones económicas, varias empresas en riesgo de quiebra e incapaces de cumplir los estrictos objetivos establecidos por las entidades financieras, han recurrido al fraude en sus estados financieros o a la manipulación de beneficios para mostrar crecimiento", afirma Yvonne Vlasman, socia de Forensic para KPMG en Países Bajos.

No es habitual que la avaricia esté presente en los patrones observables de conducta. Tan solo el 18 por ciento de los defraudadores tenían aficiones caras y el 17 por ciento conducía vehículos de lujo, circunstancias que son difíciles de diferenciar cuando el defraudador es un alto directivo.

Racionalización

Los defraudadores, como otros tipos de delincuentes, aportarán con frecuencia argumentos para justificar sus actos. Motivaciones emocionales como la ira y el miedo fueron mencionadas en escasas ocasiones por los autores. La ira y el miedo fueron factores importantes en el 10 por ciento como máximo de los 596 casos. Incluso la sensación de estar mal remunerado solo fue mencionada como factor importante en el 16 por ciento de las investigaciones, algo sorprendente, en cierta medida, pues el beneficio económico es un factor predominante en el fraude.

La única emoción que parece significativa es la sensación de superioridad, que es importante para el 36 por ciento de los defraudadores. Es posible que se deba al hecho de que el 29 por ciento de los fraudes fueron cometidos por consejeros ejecutivos, el cargo más frecuente en relación con la comisión de estos actos. El 44 por ciento de los consejeros ejecutivos tenían una fuerte sensación de superioridad que, sin duda, les reafirmaba en su convicción de que no necesitaban someterse a las reglas que regulan el comportamiento del resto de los empleados.

Según observaron los investigadores de las firmas de KPMG, la razón del fraude viene determinada en gran medida por el contexto ético y cultural, y este varía según el país. La regulación gubernamental y el cumplimiento de las normas pueden reforzar a menudo las reglas éticas, porque un defraudador que es llevado ante la justicia tendrá más dificultad para racionalizar sus acciones aduciendo que el comportamiento está aceptado en el país. "Hace una década, en algunas zonas de Europa, las empresas podían deducirse los sobornos pagados en jurisdicciones extranjeras como coste útil. No obstante, lo que anteriormente estaba permitido y se consideraba un coste de hacer negocios ahora es ilegal. Será necesario un cambio de hábitos precedido, en lugar de seguido, por la legislación", argumenta Gert Weidinger, socio responsable de servicios de Forensic para KPMG en Austria.

En algunos países de África Oriental, las normas para las empresas se están endureciendo y se está invirtiendo más dinero en el enjuiciamiento del fraude. Además, las conductas irregulares son actos cada vez menos aceptables. "En estos últimos tiempos está disminuyendo la tolerancia al fraude a medida que los nuevos Gobiernos están fomentando la libertad de expresión y están invirtiendo en el marco de aplicación de la ley en el país. La actitud ante el fraude está cambiando; desde la sociedad hasta las empresas y los Gobiernos, el fraude está dejando de ser aceptable. En resumen, el margen para la corrupción endémica se está reduciendo paulatinamente", añade Barriskell. En Vietnam también hay señales de una mayor aplicación de la ley. "Las comisiones ilegales y los sobornos en el área de compras son generalizados; forman parte de la operativa de los negocios en Vietnam, y frecuentemente se consideran inofensivos en comparación con el fraude o el robo. Pero esperamos resultados visibles en los próximos tres a cinco años por el mayor empeño en reducir el fraude", comenta John Ditty, presidente de KPMG en Vietnam y Camboya.

El defraudador ¿nace o se hace?

El impacto relativo de factores personales y del entorno en la propensión a cometer fraude

Es importante saber si los factores personales o del entorno condicionan en mayor medida la conducta fraudulenta, pues este dato influirá en la forma de investigar el fraude y en cómo se gestiona dicho riesgo. Si predominan los factores personales, las investigaciones de fraude (y la gestión del riesgo de fraude) se centrarán en la personalidad del delincuente. Si predominan los factores del entorno, la investigación se centrará en los aspectos del entorno para determinar cómo se ha producido el fraude.

Hemos aislado los casos de fraude que han investigado las firmas miembro de KPMG y en los que estamos convencidos de que ha habido una conducta corrupta. La conducta corrupta en la comisión de un fraude aporta indicadores que han ayudado a crear un perfil para conocer cómo actúan los defraudadores, así como el modo en que interviene la corrupción en sus delitos. Estos indicadores consisten en determinados patrones de conducta de un tipo específico de defraudador y hacen posible la predicción de un comportamiento corrupto como elemento del perfil del defraudador. A la hora de analizar la conducta corrupta, las principales observaciones se agruparon en tres factores, y se añadió la capacidad como elemento subordinado de la oportunidad (oportunidad, motivación, racionalización y capacidad; las dos primeras categorías son factores del entorno y las dos últimas son atributos personales).

En el 53 por ciento de los 198 defraudadores que tuvieron una conducta corrupta, la debilidad de los controles internos favoreció la comisión del fraude. No obstante, el control interno no es un factor destacado que influye en el hecho de que una persona desarrolle un comportamiento corrupto. En el comportamiento corrupto intervienen, como mínimo, dos personas, y al menos una de ellas rara vez está sometida a controles internos. El aumento de la globalización de las organizaciones está dificultando cada vez más que la sede central pueda supervisar lo que están haciendo departamentos situados en lugares alejados. "En Reino Unido, más del 60 por ciento de las investigaciones de soborno y corrupción están relacionadas con problemas en otras jurisdicciones. No se trata de que haya más o menos corrupción en distintos países, sino del hecho de que cuanto más nos alejamos de la sede central, más se disipa el mensaje, especialmente teniendo en cuenta la presión significativa que se ejerce para que las personas obtengan resultados", afirma Alex Plavsic, responsable de Forensic para KPMG en Reino Unido.

Más relevante, quizás, es la naturaleza de la autoridad con que opera el defraudador. En el 62 por ciento de los 130 defraudadores analizados en los que pudimos observar el grado de autoridad de que disponían y que actuaban de manera corrupta, observamos que el infractor ejercía una autoridad ilimitada sobre el área donde se había producido el fraude (ya fuera dicha área el derecho a suscribir contratos, autorizar pagos, etcétera). "Seguimos encontrándonos que el defraudador arquetípico en la mayoría de las investigaciones en Europa Central y del Este es un gerente o directivo de categoría sénior con autoridad, que lleva trabajando en la empresa más de cuatro años, y que conoce el sistema y sus deficiencias. Lo que ha cambiado es que hay un aumento de la colusión y más temeridad", añade Helm.

En este sentido, la autoridad ilimitada refleja una ausencia de controles internos, aun en el caso de que el fraude se haya cometido en un entorno de buen gobierno. Observamos que en el 61 por ciento de los 214 defraudadores con autoridad ilimitada investigados por las firmas miembro de KPMG, los delitos se produjeron en un entorno regulado más débil. Así pues, los temas del entorno de controles y mecanismos de equilibrio de poderes son esenciales para tres de las cuatro categorías mencionadas anteriormente (oportunidad, motivación y racionalización; la cuarta es la capacidad). "El fraude es más habitual en empresas más pequeñas, de propiedad familiar, principalmente porque carecen de los controles que les permiten protegerse contra posibles fraudes. No obstante, este tipo de empresa compone el núcleo de la economía griega", declara Christian Thomas, socio, responsable de Forensic para KPMG en Grecia.

Tenemos en cuenta cuatro factores: la competencia en la empresa (esto es, la rivalidad entre compañeros de trabajo), la competencia en el mercado (es decir, una empresa que compite con otra), una cultura de ventas agresivas, y el deseo, por parte del defraudador, de ocultar las malas noticias. Estos factores hacen referencia, en parte, al entorno, pero nosotros consideramos que están más estrechamente relacionados con

En última instancia, es un reto difícil investigar casos e impedir el soborno y la corrupción en países extranjeros. Para muchas empresas es difícil llegar al otro lado del mundo y realmente entender los riesgos en entornos locales

Phil Ostwalt
Coordinador Global para investigaciones de la práctica Global de Forensic en KPMG

atributos personales de un comportamiento corrupto. Un defraudador elige si reacciona ante estos entornos y cómo lo hace, por ejemplo, al intentar superar a sus rivales para obtener la comisión de ventas más elevada. En determinados casos, la impresión de que "todo el mundo lo hace" puede favorecer el fraude. "Un estudio de KPMG demuestra que casi todas las empresas creían que sus competidores vulnerarían las normas éticas para hacer negocio", comenta Raul Saccani, senior manager del área de Forensic, KPMG en Argentina.

No obstante, basándonos en los datos, no pudimos afirmar taxativamente que alguno de los cuatro factores constituyera un elemento de motivación o de presión para los 198 defraudadores que actuaron de forma corrupta. La aparición de estos factores se especifica enel Gráfico 1.

Por lo tanto, los resultados de nuestro estudio indican que los factores relativos a la presión y la motivación tienen menos influencia en la propensión a que un defraudador se comporte de forma corrupta que los factores relativos a la oportunidad. Por ejemplo, si un defraudador necesita establecer una red de colusión para cometer un fraude, es posible que tenga que sobornar a directivos de la organización para lograrlo. En otras palabras, en los casos en que los defraudadores han tenido la oportunidad de comportarse de forma corrupta a la hora de cometer fraude, lo han hecho; no ha sido una cuestión de necesidad o motivación. Esto indica que los atributos personales podrían ser más importantes que el entorno del negocio como factor determinante para introducir el comportamiento corrupto en el perfil del defraudador.

Gráfico 1

Fuente: Global profiles of a fraudster, KPMG International, 2013.

[6] El Fraude Corporativo en Latinoamérica, 2008-2010, informe de KPMG publicado en 2011.

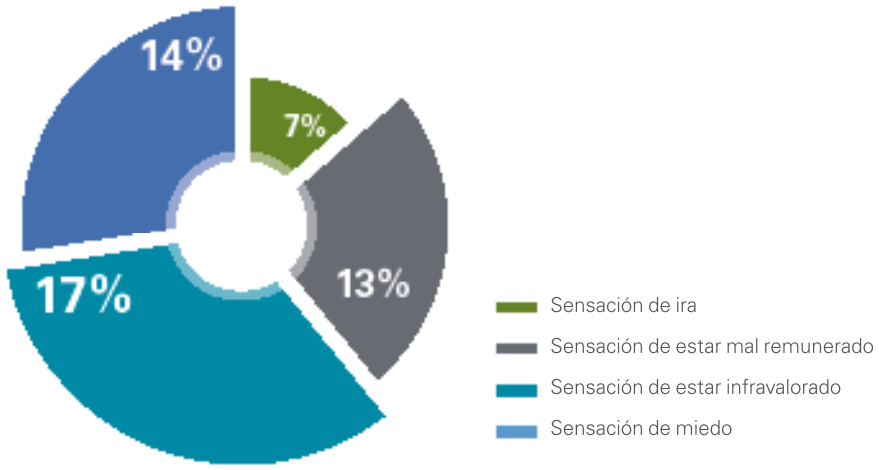
Personalidad y capacidad

A continuación, consideramos los aspectos de personalidad y capacidad del defraudador. Hemos analizado en primer lugar los factores relevantes para crear una racionalización de los fraudes en los que interviene un comportamiento corrupto y hemos observado que la motivación emocional (como, por ejemplo, ira, miedo y resentimiento) se mencionaba en raras ocasiones como razón que justificaba la conducta del defraudador (gráfico 2).

Volviendo a los rasgos personales y la habilidad de los defraudadores en los casos que hemos investigado, agrupamos en primer lugar las observaciones sobre su personalidad y presencia. Hemos notado que muchos de los defraudadores se ajustan a los elementos del perfil indicados en el gráfico 3.

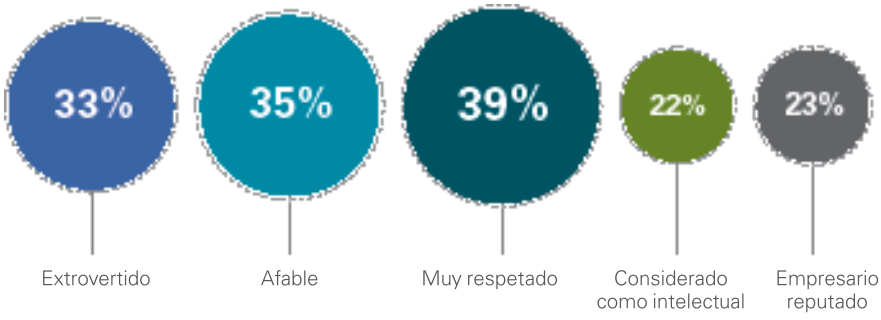
Dada la elevada proporción de defraudadores que son extrovertidos, afables, muy respetados, etcétera, cuesta imaginar que estos atributos puedan servir para identificar a quienes son propensos a la corrupción. Además, un gran porcentaje (39 por ciento) de los 596 defraudadores eran muy respetados por sus compañeros. "El defraudador que nos encontramos suele ser un gerente

Gráfico 2



Fuente: Global profiles of a fraudster, KPMG International, 2013.

Gráfico 3

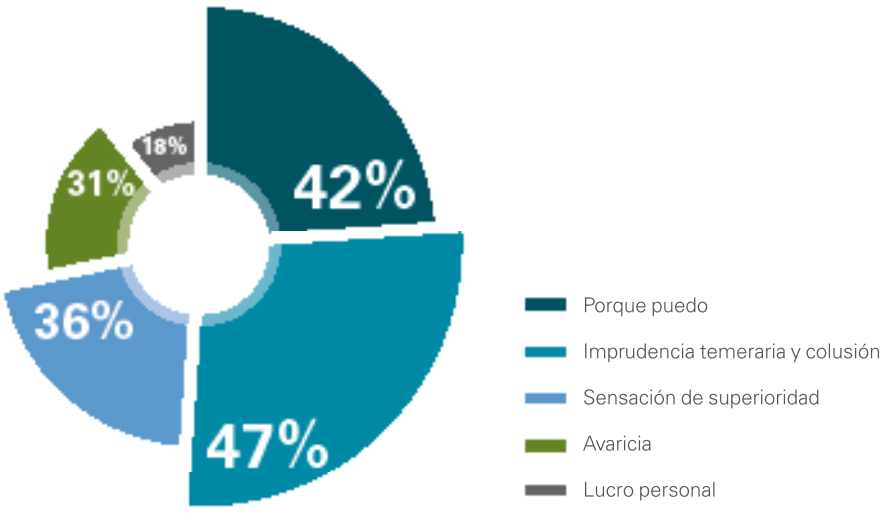


Fuente: Global profiles of a fraudster, KPMG International, 2013.

de confianza o empleado en el área de finanzas. Cuando queda al descubierto, la mayoría de las personas se sorprenden, y consideran que esa conducta es totalmente distinta a la habitual", comenta van Heerden. A continuación, de los dos gráficos siguientes hemos agrupado las observaciones de factores que describen la actitud de un defraudador.

Dada la elevada proporción de defraudadores que son extrovertidos, afables, muy respetados, etcétera, cuesta imaginar que estos atributos puedan servir para identificar a quienes son propensos a la corrupción. Además, un gran porcentaje (39 por ciento) de los 596 defraudadores eran muy respetados por sus compañeros. "El defraudador que nos encontramos suele ser un gerente de confianza o empleado en el área de finanzas. Cuando queda al descubierto, la mayoría de las personas se sorprenden, y consideran que esa conducta es totalmente distinta a la habitual", comenta van Heerden. A continuación, de los dos gráficos siguientes hemos agrupado las observaciones de factores que describen la actitud de un defraudador.

Gráfico 4



Fuente: Global profiles of a fraudster, KPMG International, 2013.

La avaricia, reflejo de un mayor nivel de bajeza moral, y el lucro personal, fueron los rasgos personales que más motivaron la conducta del defraudador en los casos en que hubo comportamiento corrupto. Al considerar los 596 defraudadores investigados por las firmas miembro de KPMG, se observó lucro personal en el 47 por ciento de los casos y avaricia en el 42 por ciento. Así pues, cuando hay un debilitamiento de los controles internos y del gobierno corporativo, las personas normales pueden ser susceptibles de caer en la avaricia y en el anhelo de lucrarse. Estas personas pueden llegar a estar un poco más dispuestas que otras a introducir un comportamiento corrupto en el fraude que cometen. "En definitiva, el fraude siempre tiene que ver con las personas, con lo que quieren y cuánta resistencia deben afrontar. Generalmente, suele tratarse de alcanzar un determinado estilo de vida, de lo que es culturalmente aceptable y de la calidad de las defensas de la empresa", manifiesta Sukdev Singh, director ejecutivo del área de Forensic para KPMG en Malasia.

Las mil caras del fraude

Las organizaciones deben adaptarse al cambiante perfil del defraudador

No existe un único modelo de fraude y no hay una cara única e inmutable del defraudador. El delito y el delincuente serán distintos dependiendo de la importancia relativa de los tres factores que incitan al fraude y de la capacidad del defraudador como se ha comentado anteriormente, y este suele ser el motivo de que generalmente sea difícil detectar el fraude. "No observamos un único perfil de personalidad en la comisión de un fraude; todos los tipos de personas pueden llegar a hacerlo si se presenta la oportunidad", dice Nigel Layton, socio, responsable de Forensic, Risk Consulting en KPMG en Rusia y la CEI. Lem lo expresa de otra manera: "Nuestra experiencia indica que la mayoría de las personas pueden cometer un fraude si se encuentran con el factor desencadenante adecuado."

Ante la desoladora conclusión de que la mayoría de las personas son capaces de cometer un fraude, corresponde a la organización intentar evitar en la medida de lo posible que se produzca el mismo. "Por el momento, no hay indicios de que el perfil del defraudador vaya a cambiar radicalmente en un futuro próximo; podría tratarse de cualquiera, dependiendo de quién tenga la oportunidad en un momento dado. La clave para mitigar el riesgo de fraude en una empresa consiste en encontrar medios para cambiar la conducta", añade Ghosh. Un cambio importante en el perfil es la creciente función que desempeña la colusión, como veremos en el siguiente apartado.

Complicidad, dentro y fuera de la organización

Las actuaciones en solitario son complicadas. Muchos defraudadores prefieren trabajar por su cuenta para no tener que confiar en el silencio de otros ni compartir el botín, pero la mayoría de los fraudes requieren actuar en complicidad. El fraude suele ser demasiado complejo para que lo ejecute una sola persona; es necesario que otros hagan la vista gorda, que se faciliten contraseñas o que se falsifiquen documentos. El 70 por ciento de los 596 defraudadores analizados por los profesionales de KPMG para este informe actuaron en connivencia con otros y, de ellos, el 56 por ciento involucró a entre dos y cinco personas más. Tres cuartas partes de los defraudadores investigados fueron el autor principal.

> El 70 por ciento de los 596 defraudadores analizados, actuaron en connivencia con otros y, de ellos, el 56 por ciento involucró a entre dos y cinco personas más. Tres cuartas partes de los defraudadores investigados fueron el autor principal

La colusión adopta muchas formas y se produce tanto dentro como fuera de las organizaciones. El fraude cometido por terceros puede ser especialmente difícil de descubrir. "Frecuentemente vemos cómo agentes o terceros, por ejemplo, agentes de aduanas, realizan un soborno en nombre de una empresa y, posteriormente, facturan servicios aparentemente legítimos para justificar el desembolso. La factura remitida a la empresa simula el pago de unos honorarios legítimos por servicios prestados, así que es difícil de detectar", argumenta Layton.

En los casos en los que el defraudador actuó en colusión, el 21 por ciento de los fraudes consistieron en malversación, en comparación con el 27 por ciento en los casos en los que el defraudador actuó en solitario. El fraude en las compras fue el segundo tipo más común donde intervino la colusión, con un 19 por ciento. Además, el fraude con colusión produce un mayor perjuicio económico. El 33 por ciento de los casos en los que se actuó en complicidad supusieron un coste total para la organización afectada de más de 1 millón de dólares estadounidenses. En el caso de actuaciones en solitario, se superó dicha cifra en el 24 por ciento de los casos.

La colusión parece estar al alza. La proporción de casos en los que ha habido colusión aumentó desde el 32 por ciento observado en el estudio de 2007 hasta el 61 por ciento registrado en 2011 y

el 70 por ciento de 2013. Por zonas geográficas, no obstante, la variación no es tan patente. Entre 2011 y 2013 se produjo un aumento en la proporción de casos en los que hubo colusión en las regiones EMA y Asia Pacífico, no así en América. La colusión tiende a ser mayor en países donde la actividad empresarial suele estar condicionada por las relaciones sociales, como, por ejemplo, en África y algunas zonas de Asia. Sin embargo, en lugares con estructuras más patriarcales, el fraude suele ser cometido por personal de categoría sénior que encarga a los empleados a su cargo que lleven a cabo transacciones ilegales. "Algunas personas ayudan a cometer un fraude por motivos no relacionados con el lucro personal, sino porque se les ha ordenado que lo hagan", añade Jamieson.

Cómplices dentro y fuera de la organización

Un método destacado de colusión se produce entre una persona que está dentro y otra que está fuera de la organización, especialmente en los casos de fraude en las compras como cuando se inflan facturas. La verdad es que muchas organizaciones no realizan un estudio de due diligence de sus proveedores y empresas clientes . "La defensa en última instancia en el entorno actual consiste en preguntarse si se está haciendo negocios con, y por medio de, personas en las que se puede confiar", dice Plavsic. En el 43 por ciento de los fraudes participaron en la colusión personas de dentro y de fuera de la organización, y en el 19 por ciento se actuó en complicidad con una única persona de la organización y una o más ajenas a la organización. Los investigadores de las firmas de KPMG manifiestan que en la mayoría de los casos en los que personas de la organización han trabajado con otras ajenas a la misma, fueron los empleados los que tomaron la iniciativa, puesto que suelen identificar la oportunidad y conocen los puntos débiles en las defensas de la empresa. Además, más del 42 por ciento de los defraudadores habían trabajado en la organización afectada durante más de seis años.

El fraude con colusión produce un mayor perjuicio económico. El 33 por ciento de los casos en los que se actuó en complicidad supusieron un coste total para la organización afectada de más de 1 millón de dólares estadounidenses

La corrupción fue un elemento común en los casos de colusión; hemos detectado que en el 29 por ciento de casos relacionados con la colusión hubo soborno (hecho que no puede producirse cuando el autor actúa en solitario). También hubo una disparidad en el método de detección. Las actuaciones en solitario fueron mayoritariamente detectadas mediante una revisión de la dirección (27 por ciento) y accidentalmente en una cuarta parte de los casos. En los casos de colusión, los principales métodos de detección del fraude consistieron en denuncias anónimas informales (22 por ciento) y a través de un mecanismo formal como una línea ética o whistle blowing (19 por ciento).

Si el fraude cibernético adquiere más importancia, como parece ser el caso, queda por ver si va a aumentar la función desempeñada por las personas ajenas a la organización. En teoría, serán más los piratas informáticos que busquen puntos débiles en las defensas de las organizaciones, pero puede tratarse tanto de empleados internos como de personas ajenas. "Es de prever que los empleados y los directivos que hacen uso de las oportunidades de fraude seguirán suponiendo una amenaza para las empresas en el futuro. No obstante, las organizaciones afrontarán más amenazas por parte de personas externas en el futuro, ya sea de terceros que actúan en colusión con empleados o piratas informáticos que actúan por su cuenta", comenta Torben Lange, socio, responsable de Risk Consulting y Forensic para KPMG en Dinamarca. Examinamos a continuación la función cada vez mayor que desempeña la tecnología en el fraude.

[7] *Third-party risk management: What you don't know about your business partners can hurt you (gestión de riesgos de terceros: lo que desconoce de sus socios de negocio puede perjudicarle), KPMG 2013*

Aventuras en el ciberespacio

Las nuevas tecnologías han creado nuevas conductas fraudulentas

La seguridad cibernética se ha convertido en un término de moda a una velocidad alarmante. Gran parte de la publicidad que rodea al término se ha centrado en informes de los intentos de los Gobiernos por impedir el desarrollo, por parte de otros Gobiernos, de armas nucleares y hechos estratégicos similares. Sin embargo, las empresas se sienten cada vez más vulnerables a los ataques cibernéticos, muchos de los cuales, hemos de reconocer, no son denunciados. "Lo preocupante sobre los ataques cibernéticos y el fraude de alta tecnología es la facilidad con la que los autores de estos actos logran el acceso; muchas empresas ni siquiera saben que está ocurriendo", comenta Vlasman.

Las organizaciones, empresas u otro tipo de entidades tienen dificultades para avanzar al ritmo de la sofisticación cada vez mayor de las tecnologías empleadas por los piratas informáticos. "Si bien algunos sectores están mejor preparados que otros para hacer frente a la ciberdelincuencia, las empresas que han sufrido incidentes cibernéticos de gran repercusión no parecen estar necesariamente en mejor posición para abordar ataques futuros. A estas empresas también les está costando gestionar este riesgo de forma proactiva", explica Ostwalt.

Hace unos años, los piratas informáticos actuaban motivados por objetivos políticos y provocaban interrupciones en las redes informáticas para reivindicar un planteamiento ideológico, pero solo es cuestión de tiempo que los defraudadores aprovechen todo el poder de las tecnologías para enriquecerse y beneficiar a organizaciones criminales, a menos que las organizaciones legítimas adopten medidas para defenderse."Las tecnologías de red e informáticas permiten que los delincuentes económicos operen de forma más eficiente y corran menos riesgos; facilitan el acceso y se reducen así los obstáculos para una nueva generación de defraudadores", señala Ödil Gürdil, responsable de Risk Consulting de KPMG en Turquía.

Qué depara el futuro

En este momento, la magnitud de los fraudes cibernéticos detectados parece escasa. De los delitos cibernéticos analizados, la mayoría se cometieron a través de métodos como la infección de sistemas informáticos con programas maliciosos (malware), ataques a redes informáticas, etc. La debilidad de los controles internos facilitó con frecuencia los fraudes que consistieron, entre otras actividades, en la presentación de información financiera fraudulenta y la apropiación indebida de activos. En la mayoría de casos, los defraudadores trabajaban para la organización donde cometieron el fraude, principalmente en TI, pero también en las áreas de finanzas y operaciones. Ocupaban diversos cargos en la jerarquía de la empresa, desde personal de nivel básico hasta directivos; tenían entre 18 y 55 años y llevaban en la organización entre uno y seis años. En la mayoría de los casos también actuaron en colusión con otros, que también eran, principalmente, empleados de la organización afectada.

Según las entrevistas con los investigadores de las firmas miembro, es probable que el fraude cibernético se convierta en un problema que aumentará rápidamente en las organizaciones y tendrá una amplitud geográfica mucho mayor que antes. "La ciberdelincuencia ha aumentado y cabe esperar que crezcan exponencialmente los ataques cibernéticos y el fraude de alta tecnología", comenta Lem.

Un método para defenderse contra los delitos informáticos consiste en desarrollar sistemas de TI sólidos diseñados para detectar a piratas informáticos e impedir que dañen la infraestructura interna o que roben datos. "En Italia, al igual que en otros sitios, los ataques cibernéticos han registrado un incremento vertiginoso", explica Pasquale Soccio, socio associate de Forensic, KPMG en Italia. "En un mundo empresarial que depende de la tecnología, la empresa que no disponga de un sistema de seguridad de TI sólido para protegerse frente a los ataques, incluso los internos, tiene un

[8] Stuxnet, por ejemplo, es un gusano informático que se descubrió ya en junio de 2010 y que, según se ha informado, fue desarrollado por Estados Unidos y por Israel para atacar las instalaciones nucleares de Irán.

[9] No existe una definición comúnmente aceptada de fraude cibernético. Los defraudadores llevan décadas utilizando ordenadores para cometer delitos. Estos actos se consideran fraude asistido por ordenador. El fraude cibernético exige dar un gran paso en la capacidad tecnológica del defraudador, incluida la capacidad de descifrar datos extremadamente cifrados y atravesar cortafuegos muy sofisticados.

> Muchas empresas dicen tener los sistemas adecuados, pero las infiltraciones solo necesitan un por dos fallos en el sistema y años de innovación se pierden o son robados por un competidor. No es posible poner precio por prevenir estas oportunidades perdidas

Alex Plavsic
Responsable de KPMG Forensic en UK

problema realmente grave. Un sistema de seguridad de TI sólido es un requisito previo imprescindible para hacer negocios". Sin embargo, muchas organizaciones han tardado en reforzar sus defensas. "Muchas empresas no desarrollan informes de alerta o detección adecuados para alertar sobre transacciones inusuales en el sistema, por lo que resulta difícil detectar y hacer un seguimiento de actividades inusuales", indica Rex Chu, director de Forensic en KPMG en Taiwán.

Teniendo en cuenta que se tarda una media de tres a cinco años en detectar un fraude y que los delitos informáticos son tan novedosos, es posible que tenga que transcurrir aún cierto tiempo antes de que el fraude cibernético tenga un efecto significativo sobre nuestras estadísticas. "Si bien las investigaciones aún no muestran niveles elevados de fraude de alta tecnología o de ciberdelincuencia organizada en mercados extraterritoriales, las tendencias globales apuntan a que se trata solo de una cuestión de tiempo", explica Charles Thresh, director gerente de KPMG en las Bermudas. "Es de prever que la tecnología móvil no solo cambie la forma de cometer fraude, sino también el modo de blanquear capitales". Este hecho dificulta la creación de un perfil de defraudadores cibernéticos. El pirata informático típico podría tener veintipocos años, pero este hecho guarda poca relación con la edad de los defraudadores internos que son expertos en infiltrarse en redes informáticas. Puede suceder que los defraudadores cibernéticos tengan una edad media inferior a la de otro tipo de defraudadores. O podrían encontrarse miembros de la alta dirección que actúan en colusión con jóvenes piratas informáticos que trabajan desde fuera.

Ostwalt señala que "en última instancia, el defraudador del futuro dependerá de las oportunidades del día". Hace dos décadas, sacar dinero de manera ilícita de, digamos, un banco solía llevarse a cabo con una banda bien organizada que a veces recurría a la violencia o falsificaba firmas para lograr sus propósitos. Actualmente, las oportunidades de sacar dinero de un banco se han transformado con Internet, los dispositivos inteligentes y la capacidad de analizar enormes cantidades de datos.

En el futuro, seguirá siendo necesario un grupo de personas que actúen en connivencia para cometer un fraude, pero cambiarán las herramientas tecnológicas. Ya no es necesario un falsificador en tal grupo, sino una persona que pueda redactar un mensaje electrónico fraudulento para suplantar la identidad (phising). Tampoco se necesita una persona creíble para que presente un cheque robado al cajero de un banco, sino un pirata informático que pueda acceder a una red informática protegida. Es posible que las emociones y la apariencia ya no formen una parte significativa del perfil; en su lugar, puede que una organización afectada solo llegue a conocer la identidad electrónica, las firmas y las conductas del defraudador cibernético. "Para desentrañar los fraudes del futuro, los mejores investigadores serán aquellos que puedan reducir grandes cantidades de datos a incidentes identificables con buenas soluciones tecnológicas, que trabajen de manera uniforme a través de las fronteras y que cuenten con una buena capacidad de inteligencia empresarial que les proporcione un alcance histórico y geográfico rápido", señala Dean Friedman, responsable de la red de investigaciones de KPMG en la región de Europa, Oriente Medio y África.

El delincuente cibernético puede atacar de lleno a la protección adoptada por las organizaciones y utilizar quizás esas mismas contraseñas y técnicas de cifrado para cometer el delito. "El principal cambio derivado de la tecnología es la facilidad con la que la propiedad intelectual puede 'desvanecerse' de la organización. Las empresas no parecen darse cuenta de lo expuestos que están sus sistemas a la pérdida de información sensible", explica Niamh Lambe, director y responsable de Forensic de KPMG en Irlanda.

Gracias al entorno de los ordenadores, la nube e Internet, los defraudadores cibernéticos son incluso más esquivos que antes. Esta conducta difiere de lo que los investigadores están acostumbrados a observar y, por tanto, tendrán que adaptar sus métodos para adecuarse. No obstante, incluso los delitos cibernéticos siguen estando probablemente motivados por los mismos perfiles psicológicos que los observados anteriormente; es posible que lo único que haya cambiado sea la conducta. "En los próximos tres a cinco años, el riesgo de fraude se verá afectado por la dependencia cada vez mayor de TI y de nuevas tecnologías como los pagos móviles para todos los aspectos del negocio. Los riesgos de fraude anteriores seguirán

persistiendo; lo único que sucede es que se están añadiendo más áreas de riesgo", comenta McAuley.

Organizaciones criminales modernas

La ciberdelincuencia se convertirá probablemente en un área de creciente interés para las organizaciones criminales; ya son cada vez más sofisticadas en lo que a tecnología se refiere, dice Oswalt. Señala que existe un mercado negro de propiedad intelectual robada en el que operan grupos de delincuentes. "El crimen organizado está mejorando su capacidad de apropiarse de dinero de grandes empresas. En los últimos meses, las firmas miembro han observado un aumento de fraudes mediante desvío de fondos, donde el defraudador recurre a empleados recién contratados o relativamente ingenuos para cambiar datos de pago a proveedores con el fin de desviar los pagos a destinos en el extranjero", explica Plavsic.

El fraude cibernético parecería ser el siguiente paso lógico. "Los delincuentes organizados cometen delitos económicos de un modo algo diferente, ya que utilizan tecnología sofisticada e introducen a personas en las organizaciones para obtener información y cometer el fraude. El defraudador interno por excelencia está ahora respaldado por el crimen organizado", comenta del Castillo. Lamentablemente, la magnitud de la participación de organizaciones criminales en todo tipo de fraude es difícil de medir porque no es fácil de detectar. Solo 15 de los 596 defraudadores actuaron en colusión con bandas criminales, 13 de los cuales contaron con ayuda de cómplices tanto internos como externos.

Además, 13 de ellos participaron en la apropiación indebida de activos. Los grupos de delincuentes organizados siguen secuestrando a directivos de grandes empresas, especialmente en Latinoamérica y en África, pero existen razones justificadas para creer que en muchas partes del mundo ampliarán su ámbito de actuación al participar en fraudes cibernéticos.

La ciberdelincuencia clandestina: un modelo de servicios

Los avances en la tecnología, unidos al uso de servicios electrónicos por parte de empresas y consumidores, están generando beneficios significativos para los delincuentes organizados y no organizados. Los delitos cometidos recientemente en todo el mundo ilustran cómo el robo tradicional de bancos está evolucionando hacia un enfoque basado exclusivamente en la ciberdelincuencia, por lo que se reducen los riesgos, se mantiene el anonimato y se logran beneficios económicos significativamente más cuantiosos. En la mayoría de los casos, los delincuentes organizados centran su atención en el uso de servicios diversificados que se ofrecen en la clandestinidad cibernética. Entre los servicios clandestinos se incluyen los siguientes: alquiler de redes botnets (ISP ilegales que se componen de cientos de miles de ordenadores infectados) que permiten a los usuarios ocultar su verdadera identidad y aparecer en casi cualquier ciudad del mundo; programas maliciosos (malware) diseñados por delincuentes para delincuentes que están codificados para ejecutarse sin ser detectados por los programas antivirus y por los cortafuegos, y se centran en robar credenciales de identidad (como nombres de usuario y contraseñas, y tarjetas de crédito; piratas informáticos contratados para objetivos específicos como empresas o dispositivos; servicios delictivos en la nube (alojamiento a prueba de fallos) alquilados por delincuentes para almacenar identidades robadas o campañas de suplantación de identidad de sitios web con propiedad intelectual falsa, etc., además de servicios de tráfico de dinero en efectivo ("mulas" de dinero) y de blanqueo de capitales.

En el caso de entidades financieras, el objetivo principal son las cuentas bancarias y las tarjetas de crédito. En un delito cometido casi en tiempo real en varias ubicaciones de todo el mundo simultáneamente, los delincuentes se basaron en una combinación singular de conocimientos del sistema de cajeros automáticos, procesos y la pericia tecnológica que se encuentra en los servicios clandestinos mencionados anteriormente.

Los piratas informáticos accedieron a las bases de datos del banco y quedó comprometida la seguridad de 100 tarjetas de crédito vinculadas a cuentas bancarias aparentemente legítimas. Los piratas, que parecen haber contado con la ayuda de alguien desde dentro, fueron capaces de acceder de forma remota a una terminal para aumentar el límite diario de retirada de efectivo de los cajeros automáticos en cada una de las tarjetas hasta superar los 100.000 dólares estadounidenses. Al sacar partido de esta deficiencia en la seguridad de TI del banco, los piratas crearon básicamente la disponibilidad de "dinero falso" que podía obtenerse posteriormente con tarjetas de banda magnética codificadas de forma adecuada en cajeros automáticos de todo el mundo. La fase final exigió que la banda criminal utilizase "mulas de dinero" para retirar dinero en efectivo de las cuentas en más de 100 cajeros de todo el mundo. En pocas horas se retiraron más de 45.000.000 de dólares de forma inadvertida. En el momento de redactar el presente informe las pérdidas reales superan los 100.000.000 de dólares. El conocimiento de la tecnología y los recursos del mundo clandestino de la ciberdelincuencia organizada hizo posible que se cometiese este delito a escala global.

¿Estamos asistiendo a un preludio de lo que nos espera? Sí, y más. Los delincuentes están actuando unilateralmente y en grupo al comprar y alquilar servicios de la ciberdelincuencia clandestina, lo que permite una menor implicación en la cadena delictiva y una mayor ubicuidad. Los piratas informáticos, extremadamente competentes, que se pueden contratar trabajan probablemente con torres de servidores alquilados de gama alta con una potencia informática aparentemente ilimitada. En un futuro próximo o incluso ya mismo es probable que se creen seeker bots ("bots buscadores"), mejorados por inteligencia artificial que les permite aprender y reproducirse, para poner a prueba constantemente la infraestructura cibernética de las organizaciones con el fin de encontrar "un hueco para colarse". Cuando encuentran un hueco, los bots podrían transformarse en "agentes" que hacen un reconocimiento del terreno del sitio en el que acaban de entrar para determinar las posibilidades de cometer fraude. A continuación, podrían lanzar un attack bot ("bot de ataque") muy especializado, adaptado al tipo y al tamaño de la organización afectada, a la infraestructura establecida, al volumen de datos y a otros parámetros. Los bots podrían entonces trasladar activos de contenedores ocultos o cifrados a una ubicación virtual, anónima y de un solo uso, donde la red de delincuentes organizados puede recoger el botín. El delincuente se vuelve invisible.

Cultura de corrupción

El impacto de los rasgos nacionales en el fraude y en la detección

En algunos países, ofrecer regalos constituye una práctica habitual en los negocios, mientras que, en otros, se considera un soborno. La cultura influye en gran medida en nuestras acciones y determina lo que se considera una conducta ética y correcta. Debido a los distintos parámetros establecidos en las diferentes culturas nacionales, una persona en China, por ejemplo, puede entender el fraude de un modo distinto a otra de Norteamérica. "Los socios de negocios y los empleados locales suelen tener una perspectiva diferente sobre la ética. Si bien los regalos y los agasajos relacionados pueden presentar riesgos en otros lugares, para muchos países de la región de Asia-Pacífico constituyen una parte importante a la hora de establecer relaciones y hacer negocios", según la práctica de Forensic de KPMG en China. Por lo tanto, es interesante analizar el perfil de un defraudador desde una perspectiva cultural. Para examinar las diferencias nacionales entre los patrones de fraude, analizamos los resultados de seis países donde se informó de 20 o más casos de fraude: Alemania, Reino Unido, República Checa, Sudáfrica, India y Canadá.

En general, las variables relativas al perfil de los defraudadores investigados fueron, en líneas generales, similares en los diferentes países. La mayoría de los defraudadores suelen tener de 36 a 45 años en India, Canadá, Sudáfrica y Alemania, y de 46 a 55 años en República Checa y Reino Unido. La mayoría de los defraudadores de todos los países habían completado estudios universitarios y llevaban más de seis años trabajando para la organización afectada, salvo en el caso de la República Checa donde los defraudadores se dividieron casi por igual entre los que tenían una antigüedad de entre uno y cuatro años, entre cuatro y seis años, y más de seis años. En India, en cambio, la mayoría de los defraudadores habían trabajado durante un periodo de entre uno y cuatro años. No obstante, en el Reino Unido, Canadá, República Checa e India se registraron más casos de fraude cometido por empleados que llevaban trabajando para la organización afectada de uno a cuatro años que en Sudáfrica y Alemania. Podría deberse a que en los primeros cuatro países se otorga a la persona un grado mayor de confianza.

Los resultados mostraron que el departamento donde se cometieron más fraudes en Sudáfrica, India y Canadá fue en el de operaciones, mientras que se registró un número elevado de casos de fraude cometidos en finanzas y en el área de compras, así como en el órgano de dirección, en Reino Unido, Alemania y República Checa. De modo similar, las áreas de finanzas, operaciones y el órgano de dirección son tres de los departamentos donde actúan con más frecuencia los defraudadores en los seis países. El nivel jerárquico parece tener un efecto desigual en la incidencia del fraude. En Reino Unido, Canadá, Alemania y República Checa, la mayoría de defraudadores eran consejeros ejecutivos. Es posible que haya menos controles internos sobre los consejeros ya que se deposita mayor responsabilidad y confianza en ellos. En Canadá, se observa una distribución bastante equitativa del fraude, algo que implica que es posible que el nivel jerárquico no influya en gran medida en la capacidad para cometer fraude, mientras que en Sudáfrica y en India la mayoría de defraudadores pertenecían al área de dirección.

Tipo de fraude

En todos los países se cometieron más fraudes en múltiples transacciones que en una única transacción; esta última opción solo fue seleccionada como máximo dos veces por país. De los seis países, Canadá fue el único donde todos los fraudes se cometieron en múltiples transacciones. En los casos en los que los fraudes se cometen en varias transacciones hay más probabilidades de capturar al defraudador, algo que podría indicar un sesgo en los resultados, ya que los fraudes cometidos en una única transacción podrían pasar inadvertidos. El periodo durante el que se cometen fraudes en múltiples transacciones suele ser de uno a cinco años en todos los países. En este periodo, el coste total medio para la organización afectada fue de 50.000 a 200.000 dólares estadounidenses en todos los países, salvo en Sudáfrica, Canadá y Reino Unido, donde fue más elevado.

La apropiación indebida de activos fue el tipo de fraude cometido más habitual en todos los países por un amplio margen, y los métodos empleados con más frecuencia fueron malversación y fraude en las compras y en las nóminas. La cantidad de ingresos

> Las empresas españolas deberían considerar los posibles riesgos legislativos y de fraude a la hora de invertir en nuevos mercados. No conocer cómo las diferentes culturas y prácticas empresariales pueden afectar las operaciones de la compañía, códigos de conducta y responsabilidades normativas puede ser letal

Angel Requena
Socio Forensic, KPMG en España

o activos obtenidos, información financiera fraudulenta presentada y gastos o pasivos fue moderada o elevada en todos los países. El hecho de que los defraudadores actuasen en complicidad con otros u operasen solos varió desde una diferencia de 91-9 en República Checa hasta una diferencia de 48-52 en Canadá. Esto supone que los defraudadores de Canadá, más que en otros países, intentan evitar los riesgos de tener un cómplice.

En la mayoría de los seis países se actuó en complicidad con un grupo heterogéneo, salvo en Reino Unido y Canadá. En Reino Unido, el mayor número de cómplices pertenecía al personal interno, mientras que en Canadá eran agentes externos. En Alemania, Reino Unido y Sudáfrica, en segundo lugar se encuentra la actuación en complicidad con partes externas, mientras que en República Checa y en Canadá, el segundo lugar lo ocupa la actuación en complicidad con partes internas. Los resultados mostraron que en Canadá la proporción entre cómplices internos y externos fue la misma. La proporción de cómplices que fueron solo hombres, solo mujeres y de ambos sexos también fue similar en todos los países, salvo en Alemania donde no se denunciaron casos donde los cómplices fuesen solo mujeres. En los seis países, las motivaciones más comunes fueron la avaricia y el beneficio económico personal. Los resultados mostraron también que las dificultades económicas personales fueron uno de los motivos habituales para cometer fraude en Canadá, Reino Unido y Alemania, mientras que los infractores de India, República Checa y Sudáfrica tendieron a aprovechar las oportunidades que se presentaron para cometer fraude en lugar de planificarlo con antelación.

Detección y consecuencias

El factor citado con más frecuencia que facilitó el fraude fue la debilidad de los controles internos, dato que coincide en todos los países. Asimismo, la deshonestidad temeraria independientemente de los controles fue el factor mencionado con más frecuencia en todos los países salvo en Alemania. La colusión para eludir los controles eficaces se considera un factor que facilitó el fraude en los seis países excepto en Alemania. En todos los países, salvo en Alemania y Canadá, se cometió una cantidad significativa de fraudes que se detectaron mediante un mecanismo formal de línea ética (whistle-blowing). Sin embargo, Alemania, República Checa, India y Canadá registraron un número considerable de denuncias anónimas informales. Entre otros medios de detección habituales se incluye la revisión de la dirección, así como la auditoría interna y externa, que se consideran métodos más proactivos para detectar el fraude y reducir las pérdidas derivadas.

En general, las consecuencias del fraude son similares en los seis países y el despido es la consecuencia mencionada más veces que recae sobre el defraudador. Las empresas suelen evitar los litigios penales por temor a la publicidad, aunque denunciar a los infractores ante la policía puede ser un elemento muy disuasorio. En Alemania, el riesgo de reputación para la organización fue menor que en otros países.

Matizaciones

Al comparar diversos aspectos del fraude en República Checa, Alemania, Reino Unido, Sudáfrica, India y Canadá, se observa que, aunque las características nacionales sean similares, existen algunas diferencias significativas que podrían ser debidas a variaciones culturales. Como resultado, podría ser conveniente que las empresas internacionales adaptasen sus programas de gestión del riesgo de fraude a las condiciones de los distintos países. Por ejemplo, el mecanismo de línea ética podría no resultar ser eficaz en las culturas donde revelar información sobre los demás está mal visto. De modo similar, podría resultar beneficioso centrar las medidas disuasorias en igual medida entre la dirección y el resto del personal en India y, más concretamente, en los consejeros ejecutivos de Alemania. En Reino Unido, la atención podría dividirse en igual proporción entre los miembros del órgano de dirección y el área de finanzas. Al adaptar las medidas antifraude a las diferentes culturas, las organizaciones podrían mejorar sus medidas de disuasión y detección de delitos.

Teoría de la relatividad

Cómo influye el contexto moral en el perfil de un defraudador

En este tema estudiamos si el contexto ético en el que el defraudador comete un delito o actúa de manera irregular influye en su perfil. La bajeza moral del infractor de delitos comerciales y económicos es mayor cuando tales actos delictivos coinciden con, o son favorecidos por, el soborno y la corrupción. El soborno y la corrupción, por tanto, influyen en el perfil del defraudador. Preguntamos si estaban presentes elementos de corrupción en los fraudes analizados en el presente informe y, en el 14 por ciento de los defraudadores que afirmaron que existía un elemento de corrupción notable en sus respuestas a esta pregunta, descubrimos que el soborno y la corrupción habían sido los delitos cometidos.

Cuando analizamos a escala global los factores del entorno que explicarían la presencia de soborno y corrupción, no se observó ninguna tendencia clara. Sin embargo, cuando comparamos los casos investigados por las firmas miembro de KPMG en Estados Unidos, China, la Comunidad de Estados Independientes (CEI, antigua Unión Soviética) y África Occidental, parecieron surgir tendencias más definitivas. En los cuatro países (o regiones en el caso de la CEI y de África Occidental), los elementos de soborno y corrupción en los fraudes investigados guardaron relación con la media global del 33 por ciento, de la siguiente manera: Estados Unidos (24 por ciento), China (48 por ciento), CEI (64 por ciento) y África Occidental (67 por ciento).

Regulación

Nuestro estudio no fue diseñado para medir normas eticas reales, sino que preguntamos si (en los casos en los que estuvieron presentes el soborno y la corrupción en los fraudes observados en los cuatro países objeto de estudio) los fraudes marcados por la corrupción se produjeron en entornos muy regulados. Descubrimos que el 50 por ciento de los casos investigados en Estados Unidos se produjeron en un entorno muy regulado, el 50 por ciento en China, el 33 por ciento en la CEI y ningún caso en África Occidental.

La relación inversamente proporcional entre los dos factores del cuadro anterior (cuanto mayor es el elemento de corrupción en los fraudes, menor es el nivel de regulación) indica que la institucionalización de valores éticos, incorporados, digamos, en un marco de regulación, podría influir en el perfil de un defraudador. Este podría ser el caso al menos con respecto a la propensión hacia la introducción de la corrupción en actos fraudulentos. "La inversión va ligada a la solidez de las entidades financieras y la calidad del gobierno corporativo. Contar con un código de conducta de la empresa para establecer normas éticas y promover una cultura de negocios transparentes no reside solo en la disuasión del fraude, sino que se trata de un imperativo de crecimiento a largo plazo", comenta Ditty.

	Región				
	Global	EEUU	China	CEI	África Occ.
Elemento de corrupción en los fraudes	33%	24%	48%	64%	67%
Nivel de regulación	38%	50%	50%	33%	0%

Fuente: Global profiles of a fraudster, KPMG International, 2013.

Entorno

A continuación comprobamos el mismo atributo del defraudador que observamos en los cuatro países y lo contrastamos con los factores del entorno más estrechamente relacionados con la organización afectada. Consideramos los siguientes factores que se sabe que son sensibles a contextos éticos y morales: competencia en la empresa, competencia en el mercado y autoridad ilimitada del defraudador. Los resultados que figuran a continuación muestran la incidencia de estos tres factores del entorno en los casos de fraude que incluyeron corrupción.

	Región				
	Global	EEUU	China	CEI	África
Competencia en la empresa	23%	25%	43%	33%	25%
Competencia en el mercado	29%	0%	50%	39%	33%
Entorno de ventas agresivas	31%	25%	43%	28%	8%
Deseo de ocultar malas noticias	22%	25%	7%	11%	8%
Autoridad ilimitada	40%	50%	36%	33%	17%

Fuente: Global profiles of a fraudster, KPMG International, 2013.

Los resultados señalan que existe una relación inversamente proporcional entre el entorno de la competencia en la empresa y la prevalencia de la corrupción en los perfiles de los defraudadores con referencia a la CEI y África Occidental, mientras que en Estados Unidos y en China la relación es directamente proporcional. Los indicadores sobre un entorno de competencia en el mercado son los mismos que en el caso de la competencia en la empresa, salvo en Estados Unidos donde se observa una relación inversamente proporcional. Parece existir una relación inversamente proporcional entre los entornos de autoridad ilimitada y la prevalencia de la propensión a la corrupción en los perfiles de los defraudadores. A escala global, se observa que el 40 por ciento de los autores de fraude que habían introducido elementos de corrupción en sus fraudes lo habían hecho en un entorno de autoridad ilimitada.

Estas observaciones indican que existen correlaciones entre elementos de conducta de los perfiles de los defraudadores y algunos factores del entorno que pueden influir en el contexto ético del defraudador. Sin embargo, los vínculos no parecen encontrarse en todos los países y en algunos de ellos es posible que no haya ninguno. Analizamos también los casos desde un punto de vista personal sin relación con el entorno. A este respecto, estudiamos si los defraudadores transmitieron una sensación de superioridad, que es un factor que no tiene nada que ver con el entorno (véase a continuación).

No se observa ningún patrón claro. Parece probable que la sensación de superioridad sea un atributo personal de los defraudadores encuestados, más que un atributo del entorno que podría configurar el propio perfil.

Valores y normas

Dado que no existe un perfil único e invariable de los autores de fraude, nos mostramos escépticos con el hecho de que la tendencia identificada anteriormente (entre la propensión a introducir la corrupción en actos fraudulentos y los entornos regulados observados en Estados Unidos, China, la CEI y África Occidental) resistirá el paso del tiempo.

El fraude parece variar en espacio y en tiempo en función de la intensidad de los diferentes factores que lo motivan. Parece que los impulsos creados por las normas y los valores institucionalizados configuran el perfil del defraudador y que la falta de coherencia con respecto al tiempo y al espacio resalta la inestabilidad del perfil de los autores de fraude.

	Región			
	EEUU	China	CEI	África Occ.
Elemento de corrupción en los fraudes	24%	48%	64%	67%
Sensación de superioridad	50%	43%	67%	50%

Fuente: Global profiles of a fraudster, KPMG International, 2013.

España

Angel Requena
Socio Forensic, KPMG en España

- **El fraude está en auge en todos los sectores y las empresas disponen de escasas defensas**
- **El Sector Público es uno de los afectados**
- **Las empresas españolas que operan en países extranjeros y que desconocen los nuevos riesgos de fraude y la nueva legislación se enfrentan a pérdidas, multas cuantiosas y sanciones penales**
- **Los ataques cibernéticos amenazan a las empresas, y los peores daños siguen siendo los causados por personal dentro de la propia empresa**

La situación económica de España no es buena y, en este clima, las organizaciones se replantean sus prioridades; para reducir el fraude, es necesario que consideren la implantación de normas eficientes, tecnologías y sistemas avanzados de prevención

"En la mayoría de los casos, las investigaciones de KPMG revelan que los defraudadores son personas con poder para tomar decisiones y con la oportunidad de cometer el fraude: ejecutivos y altos directivos"

Las investigaciones de KPMG muestran que los altos ejecutivos continúan aprovechando las oportunidades para cometer fraudes en las empresas en las que trabajan por importes muy elevados. Sin embargo, en España el fraude se comete sin exceptuar ningún sector o categoría profesional.

El Sector Público es uno de los afectado. Los defraudadores internos y externos, aprovechan las deficiencias de los controles internos y la escasa disuasión del fraude. Atraídos por las oportunidades de la cadena de suministro y de otras áreas con acceso rápido a efectivo como las subvenciones o las cotizaciones a la Seguridad Social, los defraudadores suponen una amenaza para todos los niveles del Sector Público en época de dificultades económicas.

Las Cajas de Ahorros españolas también se han enfrentado a problemas significativos puesto que se han generalizado las crisis y las investigaciones de decisiones de inversiones dudosas. Algunos bancos también han sido víctimas de fraude por haber confiado en información financiera o planes de negocios manipulados.

La ausencia de elementos disuasorios del fraude y de controles internos no es una simple cuestión económica, sino también una cuestión cultural. Este rasgo no es exclusivo del Sector Público: la mayoría de empresas españolas disponen de sistemas de defensa inadecuados contra el fraude, con la posible excepción del sector financiero, que se ha visto obligado a reforzar sus defensas a golpe de regulación. No obstante, algunas organizaciones están empezando a tomar medidas.

KPMG en España está trabajando actualmente con varias empresas importantes para implantar medidas y técnicas contra el fraude, mediante la activación de señales de detección preventiva de fraude y de otras irregularidades

Tras una época de enorme crecimiento, los sectores de la construcción e inmobiliario viven su peor momento; los recortes drásticos de inversión local de los últimos tres a cuatro años han obligado a muchas empresas a buscar trabajo en otros lugares, por ejemplo, en Latinoamérica. Con todo, es posible que salgan a la luz más fraudes en estos sectores ya que las grandes inversiones en infraestructuras proporcionaron numerosas oportunidades para el fraude. El fraude cometido por terceros suele ser un área en la que se centran las investigaciones de KPMG pues las empresas no verifican lo suficiente la

integridad de proveedores y socios con los que realizan sus negocios.

El fraude en el sector financiero español no siempre es el fraude típico observado en otros lugares, sino más bien el resultado de decisiones de inversión cuestionables que tras un análisis minucioso han acarreado pérdidas muy relevantes para las entidades, para sus accionistas y para sus clientes.

Los medios tecnológicos son imprescindibles en las investigaciones de KPMG puesto que se observa que los defraudadores utilizan frecuentemente tecnologías sofisticadas, especialmente en los sectores de banca, seguros y telecomunicaciones.

En un caso, los empleados manipularon las comunicaciones digitales de la empresa para simular tanto la decisión como la autorización de pagos automáticos. Se retiraron sumas muy elevadas de la cuenta bancaria de la empresa y se ingresaron en una cuenta bancaria en el extranjero, para que fuese imposible recuperar los fondos: este es un ejemplo del tipo de fraude que se está imponiendo, con la utilización sofisticada de tecnología

En el pasado, el fraude se concentraba en mayor medida en los sectores de mayor tamaño, como el sector financiero, infraestructuras e inmobiliario. Ahora, no sorprende encontrar fraudes relevantes en otros sectores. En cuanto a los fraudes relacionados con la alteración de la información financiera, la presión sobre la dirección y sobre los consejos de administración para obtener buenos resultados financieros y para cumplir las expectativas de los accionistas, son una de las causas más observadas.

"Nuestras investigaciones incluyen fraudes en estados financieros en los que están implicadas importantes sociedades, donde los estados financieros son manipulados para cumplir determinadas expectativas de crecimiento. Es obvio que el fraude en la información financiera presentada no se limita a ningún sector en particular"

Las empresas españolas tienen que evitar los problemas de fraude tanto en el extranjero como en el propio país. La inversión española en Latinoamérica y en otras áreas exteriores se ha intensificado y ya muchas de las mayores empresas realizan la mayor parte de sus operaciones en el extranjero.

"Las empresas españolas deberían considerar los posibles riesgos legislativos y de fraude a la hora de invertir en nuevos mercados. No conocer cómo las diferentes culturas y prácticas empresariales pueden afectar las operaciones de la compañía, códigos de conducta y responsabilidades normativas puede ser letal"

Para mitigar el riesgo de fraude al operar en un país extranjero, las empresas deben garantizar que el personal recibe una formación clara orientaciones sobre ética a través del código de conducta de la empresa, así como formación de concienciación sobre las medidas de prevención y detección del fraude.

Las empresas españolas con operaciones conectadas con Estados Unidos y Reino Unido en particular tendrán que ser conscientes del gran alcance de la legislación contra la corrupción de estos dos países que se aplica de forma muy rigurosa.

Visión de futuro

A medida que aumenta el riesgo legislativo en España en áreas como soborno, corrupción y fraude fiscal, es posible que la dirección tenga que volver a establecer sus prioridades en cuanto a controles internos y defensas contra el riesgo de fraude. Se espera una aplicación más rigurosa de las leyes a escala internacional por lo que las empresas se verán obligadas a vigilar cada vez más el cumplimiento normativo global.

La tecnología seguirá influyendo en quién puede acceder a los activos de una empresa. A pesar de vivir tiempos difíciles, la seguridad de las tecnologías de la información (TI) y las pruebas para detectar el fraude se han convertido en un componente irrenunciable para la mayoría de las organizaciones, especialmente para las que operan en jurisdicciones de alto riesgo.

"Si bien los ataques cibernéticos introducen la amenaza del defraudador externo, seguimos observando que en las organizaciones españolas, el peor daño lo sigue causando el defraudador interno. Parece que las personas con más oportunidades de defraudar seguirán constituyendo un riesgo de fraude predominante y, en la actualidad, aparentemente son los ejecutivos y los altos directivos"

Como consecuencia del actual clima económico, los consejos de administración y la dirección dan prioridad a los resultados y, en segundo

lugar y con gran diferencia, a los controles y al cumplimiento , incluyendo la gestión del riesgo de fraude, por lo que las organizaciones están más expuestas que nunca.

Sin embargo, unas simples medidas de disuasión del fraude, como programas de concienciación sobre el fraude y verificación exhaustiva de los principales riesgos, serían relativamente baratas en comparación con el coste que supone el fraude.

Ángel, censor jurado de cuentas y especializado en el área de Forensic, tiene 25 años de experiencia en proyectos de prevención y detección del fraude en diversos sectores. Ha dirigido una variedad de investigaciones de fraude, en algunas incluyendo el análisis de pruebas digitales, investigaciones complejas nacionales e internacionales.

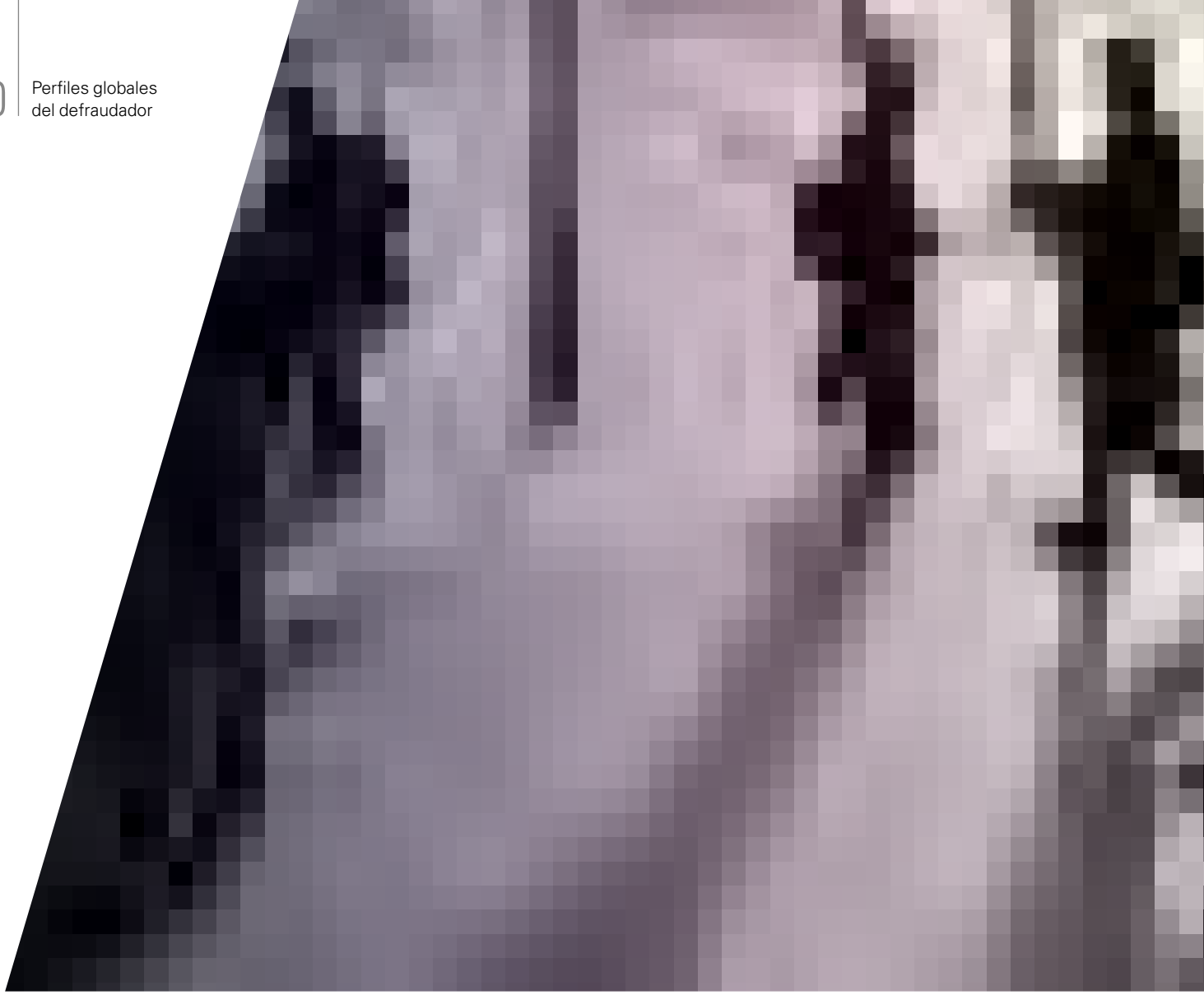
Ha cursado estudios de posgrado en Tecnologías y Fraude, y ayuda a los clientes a implantar sistemas sofisticados para la prevención del fraude y la supervisión continua, así como herramientas de predicción del fraude.

Conclusión

Quizás sea necesario hacer hincapié en los siguientes puntos principales extraídos de las percepciones de los responsables de investigación de las firmas de KPMG en la labor que han realizado y en las tendencias que prevén:

1	Aumenta la vulnerabilidad frente a amenazas externas de "hackers" (piratas informáticos activistas) que dirigen su atención a obtener un beneficio económico con ayuda de organizaciones criminales, dotadas de tecnologías, cuyo objetivo es interrumpir las operaciones y ganar un beneficio económico.
2	La tendencia al alza uniforme y sostenible en la colusión entre empleados que trabajan dentro de la propia empresa y con personas externas, unida al efecto que causa el punto mencionado inmediatamente antes, exige que las organizaciones no se centren únicamente en los sistemas y controles internos y que amplíen sus medidas defensivas para alejar la atención y librarse de la amenaza de los defraudadores.
3	La corrupción y el soborno ya no son hechos aislados. Ahora es más frecuente observarlos durante la comisión de otros delitos económicos, se están convirtiendo en una parte persistente y consolidada del perfil del defraudador contemporáneo y contribuyen a mejorar la capacidad del defraudador para establecer relaciones de colusión con un impacto económico sobre las víctimas relativamente mayor que en los casos en los que el defraudador actúa en solitario.
4	La inestabilidad económica, la volatilidad de los mercados de capitales, las nuevas tecnologías y la innovación, los nuevos sistemas contables, el incremento de la conectividad del mundo en el espacio cibernético y un entorno de transacciones sin soporte de papel brindan oportunidades a las personas con las razones y los motivos delictivos suficientes para aplicar las capacidades necesarias con el fin de beneficiarse de dichos cambios por la vía delictiva.

Si bien es cierto que algunas cosas cambiarán sin duda, y que nos preocupa la invisibilidad del defraudador cibernético, no debemos olvidar que es probable que el defraudador típico siga siendo el empleado de confianza con antigüedad en la entidad. Ese del que nunca se ha sospechado... el que está justo delante, pero que pasa desapercibido.



Agradecimientos

Agradecemos a las siguientes personas su ayuda para elaborar este informe:

Elizabeth Cain
Nigel Holloway
Alecia Hope
Victoria Malloy
Theresa Mayer
Lissa Mitchell
Ron Plesco
Kajen Subramoney
Tracey Walker
Estelle Wickham

Responsables Regionales del equipo Global de Forensic de KPMG

Petrus Marais
Responsable Global de Forensic
T: +27 795159469
E: petrus.marais@kpmg.co.za

Richard H. Girgenti
Responsable de Forensic en la Región de Américas
T: 212 872 6953
E: rgirgenti@kpmg.com

Jack DeRaad
Responsable de Forensic en EMA
T: +31206 567774
E: deraad.jack@kpmg.nl

Grant Jamieson
Responsible de Forensic en AsPAC
T: +85 221402804
E: grant.jamieson@kpmg.com

Red Internacional de Investigaciones Globales de Forensic de KPMG

Phillip Ostwalt
Responsable Global & Américas de Investigaciones
T: 404 222 3327
E: postwalt@kpmg.com

Dean Friedman
Responsable de Investigaciones en EMA
T: +27 116478033
E: dean.friedman@kpmg.co.za

Mark Leishman
Responsable de Investigaciones en AsPAC
T: +61 7 3233 9683
E: mleishman@kpmg.com.au

EQUIPO DE KPMG FORENSIC EN ESPAÑA:

Pablo Bernad
Socio responsable de Risk Consulting en Europa, Oriente Medio, África y Sudeste asiático de KPMG

Rocio Campos
Socia de KPMG Forensic

Fernando Cuñado
Socio de KPMG Forensic

Enric Olcina
Socio de KPMG Forensic

Ángel Requena
Socio de KPMG Forensic

Carlos Solé
Socio de KPMG Forensic

Alfonso Bravo
Director de KPMG Forensic

Dunia Florenciano
Directora de KPMG Forensic

Marisa Yepes
Directora de KPMG Forensic

CONTACTO:

Tel. 91 456 34 00

kpmg.es

kpmg.com/fraudster

kpmg.com/socialmedia

kpmg.com/app