

Encuesta mundial sobre fraude y delito económico 2011

*Resumen ejecutivo
España*





Índice

<i>Presentación</i>	4
<i>Situación en España</i>	6
Tipología del fraude en España	6
Perfil del defraudador	10
Acciones contra los defraudadores	12
Nuevo entorno regulatorio derivado de la Reforma del Código Penal	13
Medidas de detección	16
<i>El delito informático</i>	18
Origen del <i>cibercrimen</i>	22
El impacto de las redes sociales	27
<i>Conclusiones</i>	28
<i>Contactos</i>	30

Presentación

El fraude ha derivado en nuevas amenazas que afectan a las organizaciones de todo el mundo.

Nos encontramos en un entorno económico muy deteriorado como consecuencia de la larga y pronunciada crisis económica que estamos atravesando, donde las organizaciones se han visto obligadas a practicar ajustes en sus partidas presupuestarias viéndose fundamentalmente afectadas las áreas de *compliance* y control interno, áreas clave a la hora de prevenir los delitos económicos y tecnológicos. Todo ello ha dado origen a un aumento de las oportunidades para la comisión de delitos e irregularidades y es, en definitiva, una oportunidad para los potenciales defraudadores.

En este contexto, nos complace presentarles los resultados obtenidos en España de nuestra Encuesta mundial sobre el delito económico. Con casi 4.000 entrevistas a altos ejecutivos y mandos intermedios, y realizada en 72 países, este es el estudio mundial más completo sobre delitos y fraude empresarial disponible para las organizaciones. Del total de encuestados, el 53% eran miembros del Comité de Dirección o alta dirección, el 36% de organizaciones cotizadas y el

38% representantes de organizaciones con más de 1.000 empleados. Las respuestas recibidas de este amplio espectro de encuestados nos permite llevar a cabo un amplio y profundo análisis de la información obtenida en comparación con encuestas previas con el fin de establecer tendencias.

El objeto de este estudio es evaluar la actuación de las organizaciones frente al fraude en la actual coyuntura económica, y en particular:

- Analizar qué tipos de fraude son más frecuentes.
- Conocer qué medidas están acometiendo las organizaciones para prevenir y detectar el fraude.
- Analizar los efectos, impactos y percepciones del delito informático en España.

A lo largo de esta Encuesta hemos reflejado, de manera comparativa, los resultados que recogen las respuestas obtenidas en España con las obtenidas en Europa y en los 72 países participantes.

Como conclusión más relevante, nuestra Encuesta muestra que el fraude (en cualquiera de sus categorías: apropiación de activos, corrupción, manipulación contable, y muy en particular el *ciberdelito*) ha derivado en nuevas amenazas que afectan a las organizaciones de todo el mundo, como consecuencia de la irrupción con fuerza de las nuevas tecnologías y la dificultad de las organizaciones para adaptarse por sí solas a un entorno económico cambiante. Por ello, en este contexto (teniendo en cuenta la nueva explosión de Internet en el mundo empresarial), y ante el aumento de los casos de fraude detectados y su impacto, se hace aún más necesario invertir en medidas de prevención que minimicen los daños y eviten un aumento de la presencia de estos delitos en nuestras organizaciones.

Queremos agradecer la participación de todos los encuestados, sin los cuáles no habríamos podido realizar esta Encuesta. Esperamos que esta información ayude a los lectores en su lucha contra el fraude y el delito en todas sus facetas.



Se hace aún más necesario invertir en medidas de prevención que minimicen los daños y eviten un aumento de la presencia de estos delitos en nuestras organizaciones.

Determinados agentes ven que sus motivaciones y presiones para cometer fraude se incrementan.

Situación en España

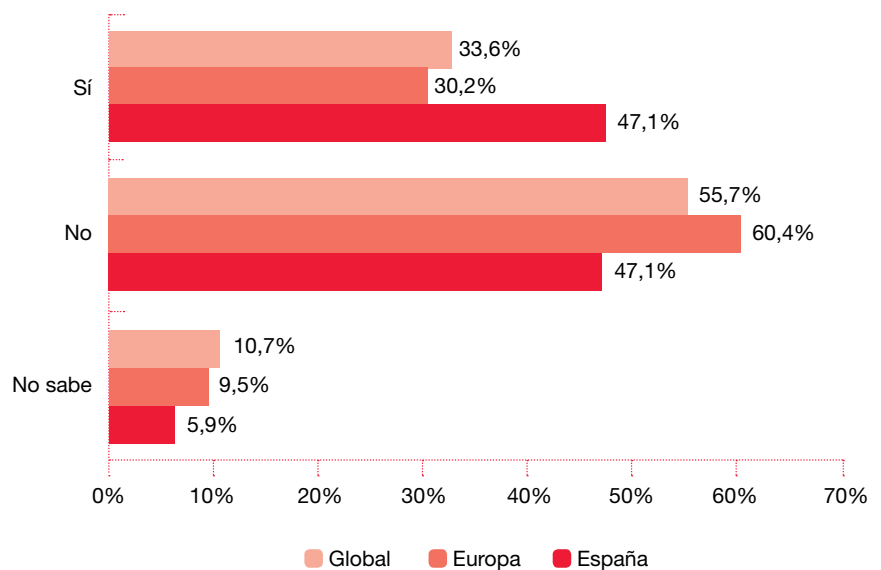
Tipología del fraude en España

En el momento actual de crisis económica, de variaciones en normativas y de la nueva explosión de Internet, contemplamos cómo determinados agentes ven que sus motivaciones y presiones para cometer fraude se incrementan. Nos encontramos con algunas organizaciones que no se encuentran preparadas para afrontar las nuevas normativas y vemos como la red puede

suponer una importante amenaza para las organizaciones.

De hecho, según los resultados de la Encuesta, un 47,1% de los encuestados españoles ha declarado haber sufrido, en sus respectivas organizaciones, al menos un tipo de fraude económico a lo largo de los últimos 12 meses, frente al 34,5% de la Encuesta del 2009. En concreto, de estas, un 80% de las organizaciones ha indicado que ha sufrido entre 1 y 10 delitos. Un incremento superior al que observamos a nivel global, donde el número de organizaciones que ha sufrido un fraude económico en el último año se incrementó en un 3,8%. Resaltar la enorme reducción de las contestaciones “no sabe” en España, que han disminuido del 23,6% de la Encuesta del 2009, a sólo un 5,9% en 2011, lo que indirectamente se puede relacionar con la creciente

Gráfico 1. ¿Ha sufrido su organización algún delito económico en los últimos 12 meses?



Un 47,1% de los encuestados españoles ha declarado haber sufrido, en sus respectivas organizaciones, al menos un tipo de fraude económico a lo largo de los últimos 12 meses, frente al 34,5% de la Encuesta del 2009.

Fuente: Encuesta mundial sobre el delito económico 2011.

Cuando una organización fortalezca los sistemas de prevención y detección de fraude, aumentará la probabilidad de prevenir y, en su caso, identificar y detectar la existencia de los mismos.

Existe una creciente preocupación por el fraude económico, así como una mayor implantación de medidas de prevención y detección.

preocupación de las organizaciones por el riesgo de fraude empresarial. Esta creciente preocupación se observa asimismo en otra vertiente: el incremento de las medidas destinadas a la detección del fraude, lo que parece indicar una cierta correlación entre ambas. Cuando una organización fortalezca los sistemas de prevención y detección de fraude, aumentará la probabilidad de prevenir y, en su caso, identificar y detectar la existencia de los mismos.

Por tanto, el incremento de las incidencias detectadas se debe, no sólo al incremento de casos sino también a un incremento de las medidas de prevención y detección. Es decir, desde nuestro punto de vista los datos obtenidos muestran conclusiones muy positivas: (i) existe una creciente preocupación por el fraude económico, (ii) así como una

mayor implantación de medidas de prevención y detección.

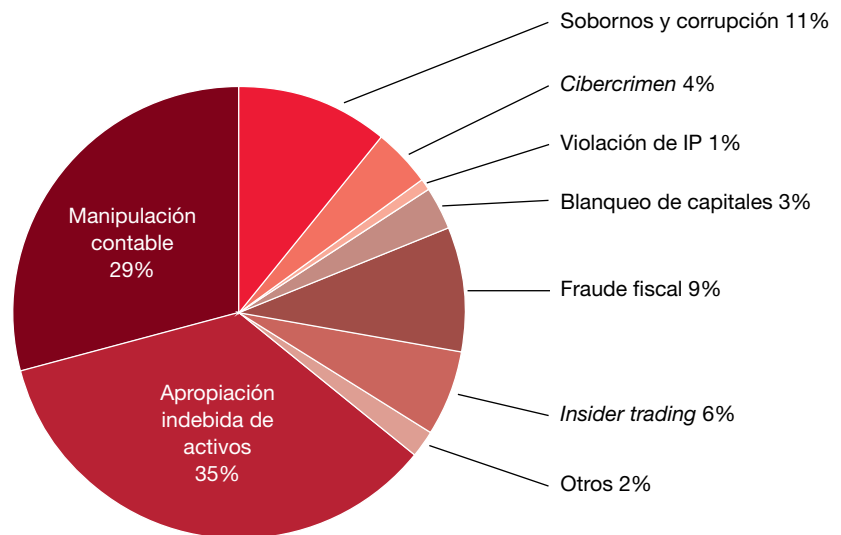
Del 47,1% de los participantes que ha declarado haber sufrido algún tipo de fraude, más de una tercera parte indicó haber sido objeto de algún caso de apropiación indebida de activos, seguidos por un 29% que reconoció haber sufrido manipulación contable.

La apropiación indebida se considera uno de los delitos económicos más habituales a nivel global, ya que abarca una amplia gama de delitos menores y, si bien es el más complicado de prevenir, es el más sencillo de detectar.

La enorme reducción de las contestaciones “no sabe” en España se puede relacionar con la creciente preocupación de las organizaciones por el riesgo de fraude empresarial.



Gráfico 2. ¿Qué tipo de delitos económicos ha sufrido su organización en los últimos 12 meses?



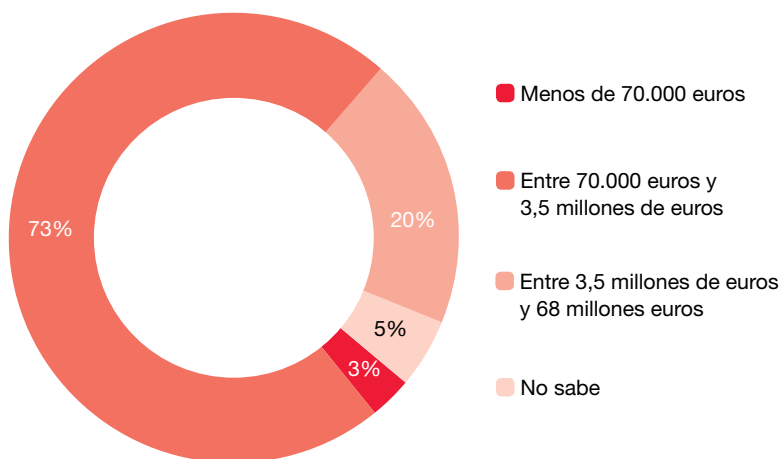
Fuente: Encuesta mundial sobre el delito económico 2011.

La normalización legislativa, el endurecimiento de los criterios contables a aplicar y, sobre todo, la creciente presión por resultados ha llevado a un importante incremento en los casos de manipulación contable: del 29% en 2011 al 11% en 2009.

En este sentido, la aplicación de medidas preventivas es la mejor manera de evitar (o al menos prevenir) este tipo de delitos, sistemas de control interno, programas de auditoría interna, segregación de funciones, etc., son medidas que ayudan a mitigar y controlar el riesgo de comisión de delitos

Destaca también la reducción que se ha producido en los delitos de corrupción y soborno disminuyendo de un 13% a un 11%. Estos son delitos claramente identificados en la Encuesta del 2009 y en especial en los ejercicios de la llamada burbuja inmobiliaria con el sector de la construcción. En este aspecto entendemos que la reducción se ha visto influida directamente por la crisis económica y su impacto en el citado sector, si bien, los casos de corrupción, cohecho, soborno, y malversación acontecidos en España en los últimos tiempos indican claramente la necesidad que existe de implantar medidas que eviten y persigan estos casos.

Gráfico 3. ¿Cuánto cree que ha sido el impacto económico para su organización derivado de los delitos económicos sufridos en los últimos 12 meses?



Fuente: Encuesta mundial sobre el delito económico 2011.

La mayor diferencia con la Encuesta del año 2009 se encuentra en el segmento inferior, menos de 70.000 euros, donde se ha producido una disminución en un 20%, pasando del 27% en 2009 al 3% en 2011. En contraposición el porcentaje del segmento 3,5 – 68 millones de euros- se multiplicó por cuatro con respecto a 2009, llegando al 20% de los delitos económicos en 2011. El segmento medio se ha incrementado en un 10%, entre 70.000 euros y 3,5 millones de euros. Los resultados muestran un dato alarmante para las organizaciones españolas: ha disminuido la importancia relativa del

segmento inferior, y ha aumentado la de los segmentos superiores. Es decir, que el coste económico medio del fraude por organización ha aumentado considerablemente.

Llama la atención, pese a este significativo incremento del coste medio de los delitos, cómo las organizaciones consideran como efecto más relevante el impacto que tiene el delito económico sobre la motivación de los empleados. Alrededor del 28% de las organizaciones encuestadas consideran este efecto como el más preocupante seguido de la reputación de la empresa con un 27%.

Ha disminuido la importancia relativa del segmento inferior, y ha aumentado la de los segmentos superiores. Es decir, que el coste económico medio del fraude por organización ha aumentado considerablemente.

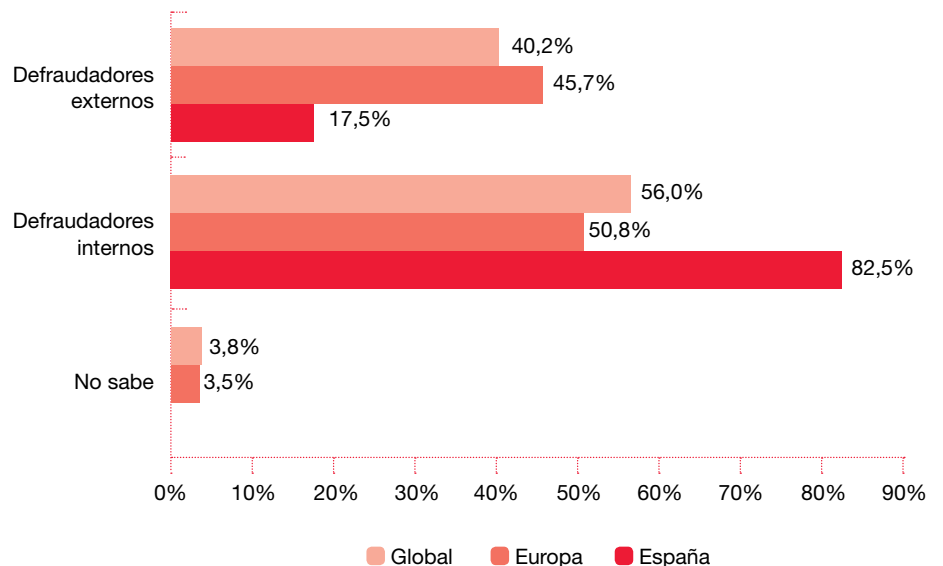
Perfil del defraudador

De acuerdo con los datos obtenidos en la Encuesta Global el diferencial entre la realización del fraude por empleados o representantes de la empresa o por terceros ajenos a la organización se ha incrementado ligeramente con respecto al 2009, aumentando del 10% al 16% actual.

En España, las cifras muestran una clara superioridad de los defraudadores internos, lo que

contrasta de forma significativa con la necesidad de incrementar las medidas de control y prevención establecidas para los mismos, ya que tradicionalmente las organizaciones se han centrado en las tareas de detección e identificación, fundamentalmente, del fraude externo¹ y en consecuencia, en los autores del mismo, dejando en muchos casos el fraude interno “olvidado” o relegado a una fase posterior de los programas de prevención.

Gráfico 4.: En relación con el delito económico de mayor gravedad que ha sufrido su organización en los últimos 12 meses, ¿quién fue el principal autor?



Fuente: Encuesta mundial sobre el delito económico 2011.

Las organizaciones se han centrado en las tareas de detección e identificación, fundamentalmente, del fraude externo y en consecuencia, en los autores del mismo, dejando en muchos casos el fraude interno “olvidado” o relegado a una fase posterior de los programas de prevención.

¹ En sectores como el financiero, el de distribución y retail, telecomunicaciones y seguros, la percepción por el riesgo de fraude externo es muy significativa por lo que muchas de las medidas de prevención están destinadas a mitigar la comisión de posibles delitos contra las propias organizaciones por parte de defraudadores externos.

El fraude interno es realizado fundamentalmente por la alta dirección y por los mandos intermedios. Por el contrario, en Europa y a nivel global, el 30% de delitos internos es cometido por los empleados más jóvenes o recién incorporados.

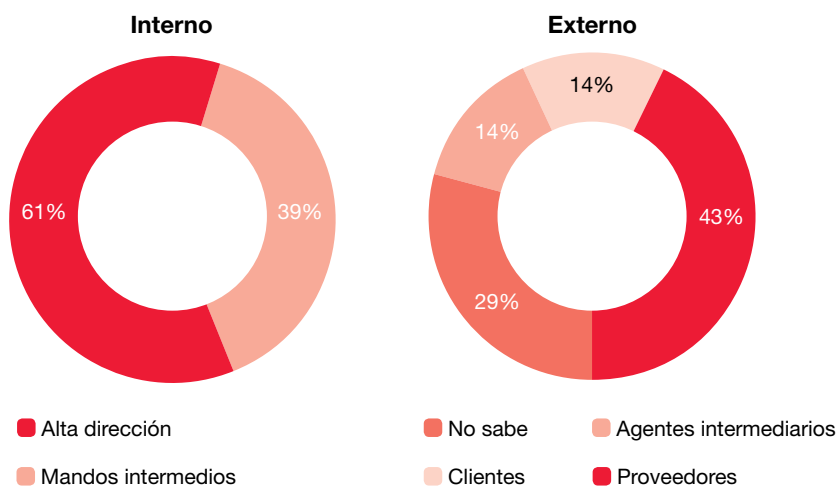
En España, el fraude interno es realizado fundamentalmente por la alta dirección y por los mandos intermedios. Por el contrario, en Europa y a nivel global, el 30% de delitos internos es cometido por los empleados más jóvenes o recién incorporados. Estos datos pueden directamente relacionarse con el hecho de que haya aumentado el coste medio de los delitos, ya que cuanto más alto es

el puesto del defraudador, más a su alcance está cometer un mayor fraude.

El fraude externo también difiere del europeo y del global, donde el principal perpetrador es el cliente (con un 35,1% a nivel global y un 32,6% en Europa).

En España, los proveedores abarcan un 43% del fraude externo, mientras que en Europa y global, este segmento no llega al 10%.

Gráfico 5. Teniendo en cuenta el delito económico más grave que ha experimentado su organización en los últimos 12 meses, ¿cuál era el puesto ocupado por el empleado autor del delito? O, ¿quién fue el principal autor externo del delito contra su organización?



Fuente: Encuesta mundial sobre el delito económico 2011.

Acciones contra los defraudadores

Debido a la crisis económica, a la reforma regulatoria y a la creciente sensibilización sobre la existencia de fraude, los patrones de respuesta ante el descubrimiento del mismo han cambiado en los últimos años.

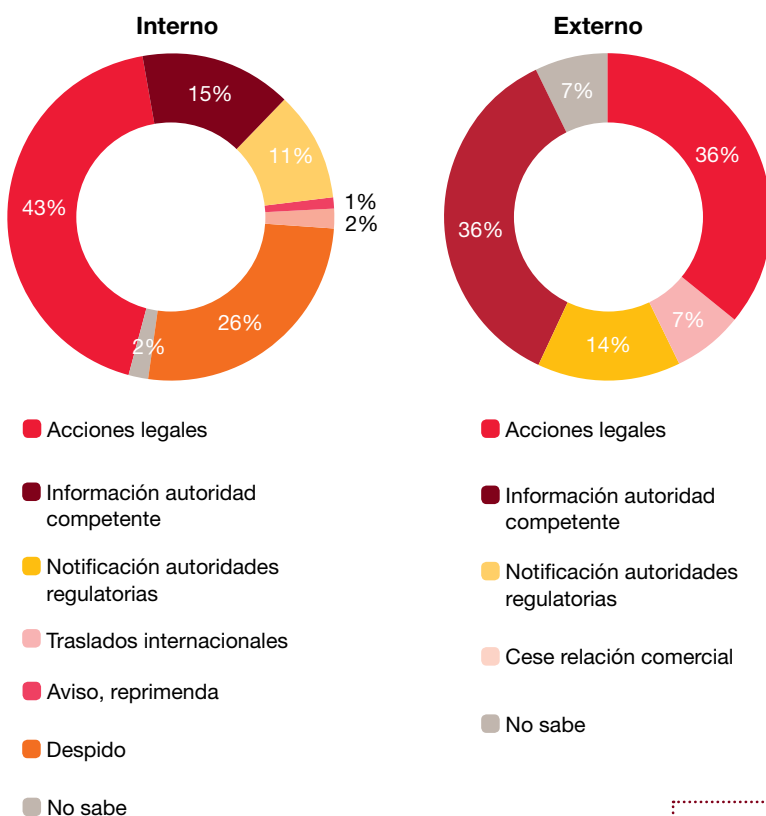
En el ámbito de fraude interno, se ha pasado del despido como medida en un 43% de los casos al 26%, mientras que las acciones legales han pasado del 26% en el 2009 al 43% en el 2011. Podemos interpretar que muchos de los encuestados han optado por elegir esta opción entre ambas al ser más grave

que el despido, por lo que entendemos que este 43% lleva implícito el despido del defraudador.

A medida que aumenta la preocupación por la existencia del fraude, las organizaciones comienzan a ser más conscientes de sus efectos, sobre todo en la motivación de los empleados, las medidas ejemplarizantes son cada vez más agresivas. No basta sólo con el despido, hay que demostrar que en una organización la cultura corporativa es contraria a la comisión de delitos, marcando unas pautas de conducta claras y unos valores concretos, estableciendo qué conductas no son tolerables y cuáles no son permitidas, para fomentar la colaboración de todos los empleados en la prevención y detección del fraude.

En cambio, desde el punto de vista del fraude externo destacar que las organizaciones no están tan predispuestas a interponer acciones legales, optando por el cese de las relaciones comerciales, esta opción ha aumentado del 33% en la Encuesta del 2009 al 36% en 2011. Y lo han hecho en detrimento del ejercicio de acciones legales, que ha disminuido del 40% al 36%.

Gráfico 6. Piense en el delito económico más serio que haya sufrido su organización en los últimos 12 meses, ¿qué acciones, si se tomó alguna, tomó su organización contra los defraudadores internos y / o externos?



Fuente: Encuesta mundial sobre el delito económico 2011.

Los patrones de respuesta ante el descubrimiento del fraude han cambiado en los últimos años.

Nuevo entorno regulatorio derivado de la Reforma del Código Penal

Debido a la nueva realidad financiera y como consecuencia de la globalización, asistimos a una normalización generalizada de las leyes. La rapidez con la que las organizaciones se adaptan a las nuevas reglas de juego será determinante tanto para aumentar sus beneficios, como para reducir posibles pérdidas por sanciones derivadas del incumplimiento de la ley.

La Reforma del Código Penal, que entró en vigor el 23 de diciembre del 2010, ha supuesto nuevas e importantes responsabilidades en el ámbito empresarial, como consecuencia de la tipificación de la comisión de delitos penales en los que puede incurrir una persona jurídica.

Esta reforma amplía de manera extraordinaria la responsabilidad de las personas jurídicas, haciéndolas responsables primarias de los perjuicios que pudieran ocasionar los representantes de las mismas o los trabajadores como consecuencia de actuaciones de los mismos o por defecto o insuficiencia de controles para prevenir este tipo de delitos.

Todo ello se traduce en que la organización podrá ser sancionada en el ámbito penal, hecho que hasta la fecha no era posible.

Los presupuestos objetivos para que una persona jurídica incurra en responsabilidad penal son:

- Que el delito se cometa en nombre o por cuenta de la misma y en su provecho.
- Que recaiga en una persona jurídica la comisión de alguno de los delitos tipificados en el Código Penal.
- Que en la comisión de delitos haya existido ausencia de mecanismos de control y/o prevención de las actividades irregulares llevadas a cabo.

La rapidez con la que las organizaciones se adaptan a las nuevas reglas de juego será determinante tanto para aumentar sus beneficios, como para reducir posibles pérdidas por sanciones derivadas del incumplimiento de la ley.

La Reforma del Código Penal, que entró en vigor el 23 de diciembre de 2010, ha supuesto nuevas e importantes responsabilidades en el ámbito empresarial, entre las que la organización podrá ser sancionada en el ámbito penal, hecho que hasta la fecha no era posible.



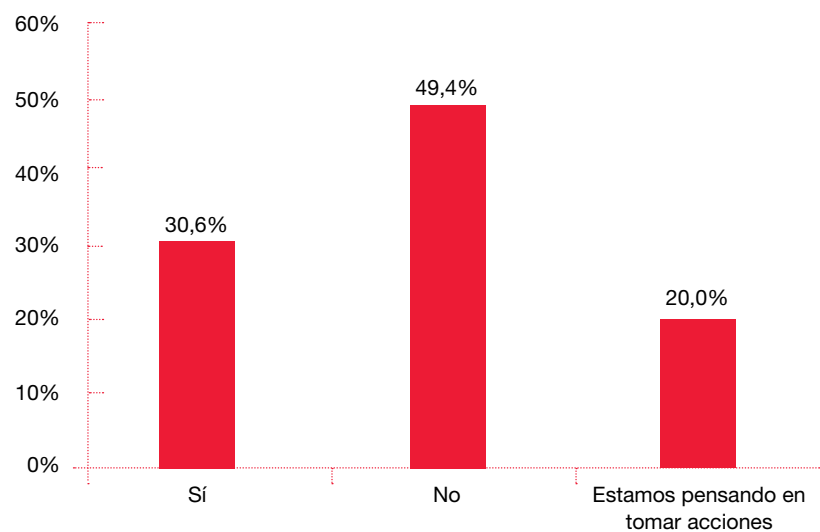
El 30% de las organizaciones ha adoptado medidas que responden a la modificación del entorno jurídico-penal, y el 20% de las organizaciones encuestadas está pensando adoptar acciones.



En base a los presupuestos se pone de manifiesto la necesidad de que toda persona jurídica adopte medidas para mitigar adecuadamente el riesgo de incurrir en una comisión de delito penal. Dichas medidas pueden, a nuestro juicio, resumirse en:

- Evaluación del riesgo al que están sometidas las personas jurídicas, determinando qué delitos de los tipificados en el Código Penal son aplicables y cuáles no.
- Evaluación de los controles implantados en la persona jurídica para mitigar el riesgo de incurrir en la comisión de algún delito penal.
- Implementación y mejora de aquellos controles que se consideren necesarios para ejercer “el debido control” por la organización con objeto de mitigar el riesgo de incurrir en la comisión de un delito penal.

Gráfico 7. ¿Ha tomado su organización alguna acción en respuesta a la reciente Reforma del Código Penal que establece por primera vez la responsabilidad penal de las personas jurídicas (aprobada el 23 de diciembre de 2010)?



Fuente: Encuesta mundial sobre el delito económico 2011.

De acuerdo con los resultados obtenidos, el 30 % de las organizaciones ha adoptado medidas² que responden a la modificación del entorno jurídico-penal, y el 20% de las organizaciones encuestadas está pensando adoptar acciones. Las organizaciones se preocupan por adaptarse al nuevo entorno regulatorio y adoptar las medidas necesarias para mitigar el riesgo legal de incurrir en un delito penal, y el riesgo de la comisión de un delito económico con su

consecuente pérdida económica y reputacional.

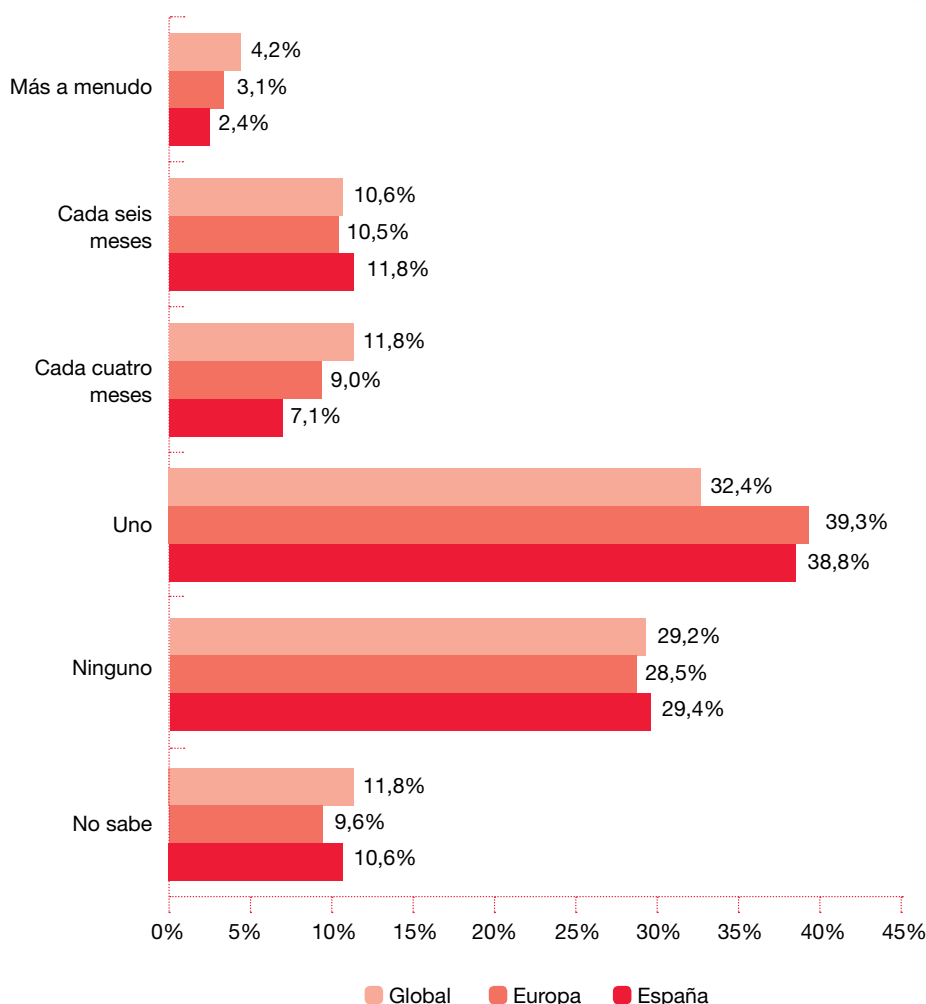
Dicha Reforma puede traer importantes sanciones a la empresa, que abarcan desde fuertes sanciones económicas, hasta la disolución de la misma. Por ello resulta vital, para evitar futuras complicaciones, que las organizaciones tomen acciones en este sentido y se preparen para cubrir sus responsabilidades.

Si bien de la pregunta anterior resulta que aproximadamente un 70% de las organizaciones encuestadas aún no ha tomado medidas en relación a la nueva Reforma del Código Penal, más de un 60% ha realizado una evaluación del riesgo de fraude en los últimos 12 meses. Esta medida es, a nuestro juicio, esencial para iniciar el camino hacia la reforma. Por tanto, podríamos decir que las organizaciones, poco a poco, están concienciándose sobre su exposición al riesgo de comisión de un delito económico.

No obstante, aún queda un cierto camino por recorrer: del 40% de organizaciones que ha contestado que no ha realizado una evaluación de riesgo, un 60% no lo ha realizado por razones de coste y un 28% alega desconocer lo que implica una evaluación del riesgo de fraude.

Estos datos ponen de manifiesto la necesidad de las organizaciones de establecer una cultura corporativa adecuada, con unos valores y unas conductas concretas, poniendo a disposición de los empleados los recursos necesarios y los medios formativos adecuados para evitar o mitigar la posible comisión de delitos económicos mediante un sistema eficaz de auditoría interna, así como de control interno y cumplimiento normativo, y una correcta implantación de un canal de denuncias.

Gráfico 8. En los últimos 12 meses, ¿cada cuánto ha realizado su organización una evaluación del riesgo de fraude?



Fuente: Encuesta mundial sobre el delito económico 2011.

² Entre otras medidas de prevención y detección de delitos se encuentran las siguientes:

- (i) **Organizativas:** Nombramiento de un responsable de cumplimiento penal, adaptación de códigos de conducta o códigos éticos, políticas de contratación, formación, etc.
- (ii) **Tecnología:** Adecuación de la segregación de funciones en los sistemas de información, implantación de programas de trabajo automatizados (data analysis), protocolo de utilización de evidencias digitales, etc.
- (iii) **Procesos:** Canal de denuncias o línea ética, protocolo de actuación/respuesta en caso de delito y revisión de controles preventivos o detectivos en procesos de negocio.

Medidas de detección

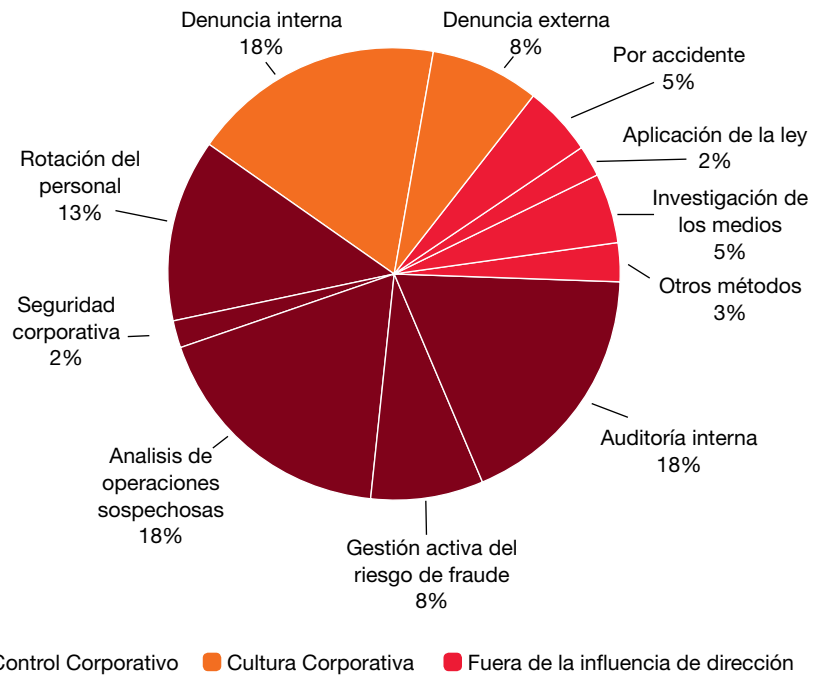
En este sentido, la Encuesta muestra que los medios de detección puestos a disposición por parte de las organizaciones a sus empleados, como los canales de denuncias internos y externos, continúan siendo identificados como los métodos de detección más eficaces, seguidos por las revisiones de auditoría interna, que han aumentado de un 5% a un 17%.

La gestión del riesgo de fraude ha representado en esta Encuesta en torno al 8% del total, que unido a la periodicidad de los controles pone de

manifiesto la iniciativa de las organizaciones para llevar a cabo una revisión interna de los controles implantados por las mismas, con objeto de adaptarlos a la nueva normativa derivada de la Reforma del Código Penal y a la voluntad de hacer frente a los delitos económicos de una manera más eficaz.

Asimismo, es necesario destacar que la identificación de delitos por accidente se ha reducido de un 11% en 2009 a sólo un 5% en 2011 en consonancia con el incremento de los controles e investigaciones realizados por las organizaciones.

Gráfico 9.: Piense en el delito económico más serio que haya sufrido su organización en los últimos 12 meses, ¿cómo fue el delito inicialmente detectado?



Fuente: Encuesta mundial sobre el delito económico 2011.



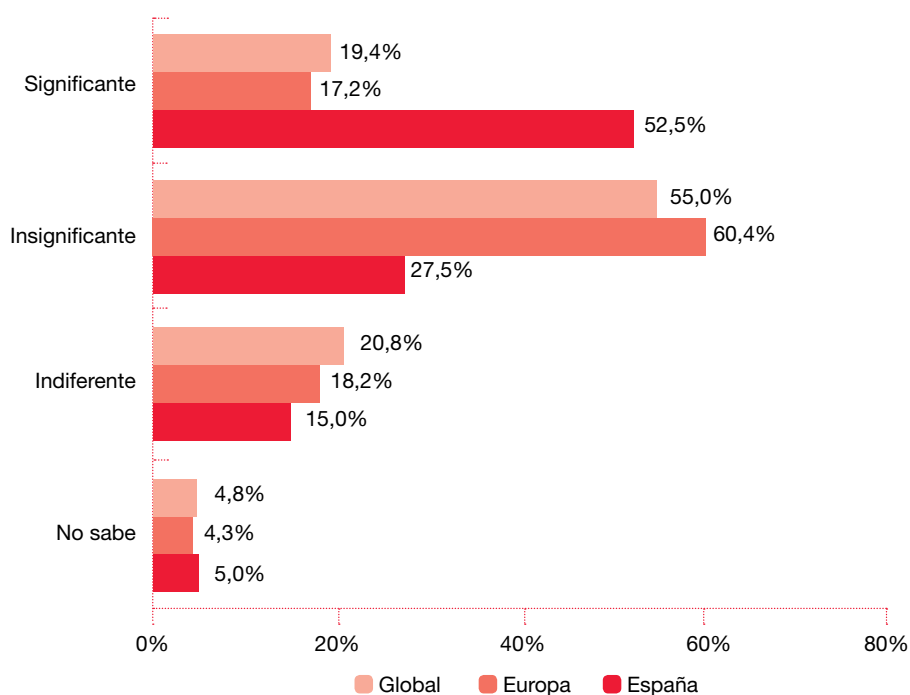
Los medios de detección puestos a disposición por parte de las organizaciones a sus empleados, como los canales de denuncias internos y externos, continúan siendo identificados como los métodos de detección más eficaces.

El delito informático

La creciente importancia de Internet en el mundo empresarial, la cada vez mayor interacción de las organizaciones en la red y sobre todo el incremento del valor del comercio electrónico en las organizaciones, se

traduce en la existencia de un nuevo riesgo potencial para las organizaciones, el riesgo de sufrir un delito informático también conocido como *ciberdelito*³. Esta realidad, que ha irrumpido con fuerza en el ámbito de los delitos económicos, abarca en la actualidad en torno al 4% de los delitos económicos, según los datos desprendidos de la Encuesta.

Gráfico 10. ¿Cómo ha sido de significativo el impacto del *ciberdelito* sufrido en los últimos meses por la organización en relación con la reputación de la misma?



Fuente: Encuesta mundial sobre el delito económico 2011.

Se trata de un riesgo cada vez mayor, que aún es difícil de cuantificar por las dimensiones que puede alcanzar. Esta Encuesta se ha centrado en estudiar el fraude cibernético con el fin de antepónernos a potenciales situaciones de riesgo.

La actual concepción de Internet hace que el efecto inmediato de este tipo de delitos afecte a la imagen de la organización, lo que se traduce en la existencia de un nivel significativo de riesgo reputacional con su consecuente impacto en los volúmenes de ventas de la organización y confianza en el sector.

A nivel europeo y global, el 17,2% y 19,4% de las organizaciones encuestadas, considera que el impacto de los casos de ciberdelito que han experimentado ha afectado significativamente a la reputación de la

³ Se entiende por delito informático o *ciberdelito* todo ataque usando como medio el ordenador y/o Internet. Las prácticas más típicas de *ciberdelito* son la distribución de virus, las descargas ilegales de información, *phishing*, *pharming*, y el robo de información personal como, por ejemplo, detalles de cuentas bancarias. Esta práctica excluye las pautas del fraude donde el ordenador es utilizado como un utensilio secundario e incluye las prácticas donde el ordenador, Internet o el uso de medios informáticos son el principal medio para acometer el fraude.

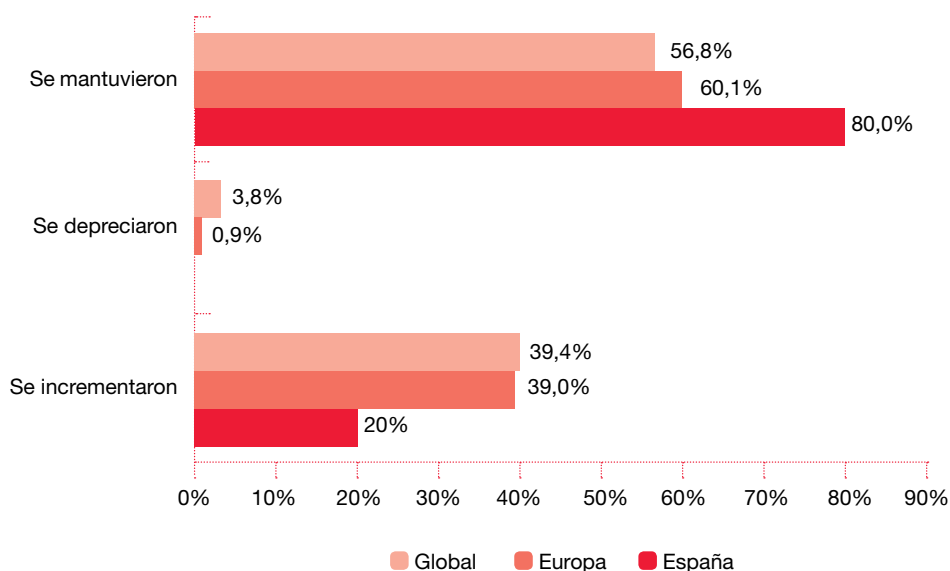
organización, mientras que en España este dato se eleva a un 52,5%.

La reputación de la organización es un factor clave para su posicionamiento empresarial en el mercado que unido al buen gobierno de la organización, transparencia, medio ambiente, derechos de los trabajadores, etc., constituyen motivos suficientes para “empujar” a las organizaciones a la adopción de medidas para hacer frente a este delito.

En los últimos 12 meses hemos visto la enorme repercusión mediática que han tenido determinados casos de *ciberdelitos*, sobre todo aquellos relacionados con el robo de información confidencial como algoritmos criptográficos, operaciones comerciales, documentación de alta dirección, etc.

Si analizamos los datos extraídos de la Encuesta se puede observar que, tanto a nivel europeo como global, existe un fuerte incremento de la percepción del riesgo de *ciberdelitos*. La Encuesta ha puesto de manifiesto el gap existente, en torno al 20%, entre el nivel de percepción de riesgo entre España y el nivel europeo y nivel global. La percepción mayoritaria en España, un 80% de las organizaciones encuestadas, es que el riesgo de *ciberdelitos* se mantuvo.

Gráfico 11. ¿Ha cambiado su percepción del riesgo de ciberdelitos en su organización durante los últimos 12 meses?



Fuente: Encuesta mundial sobre el delito económico 2011.





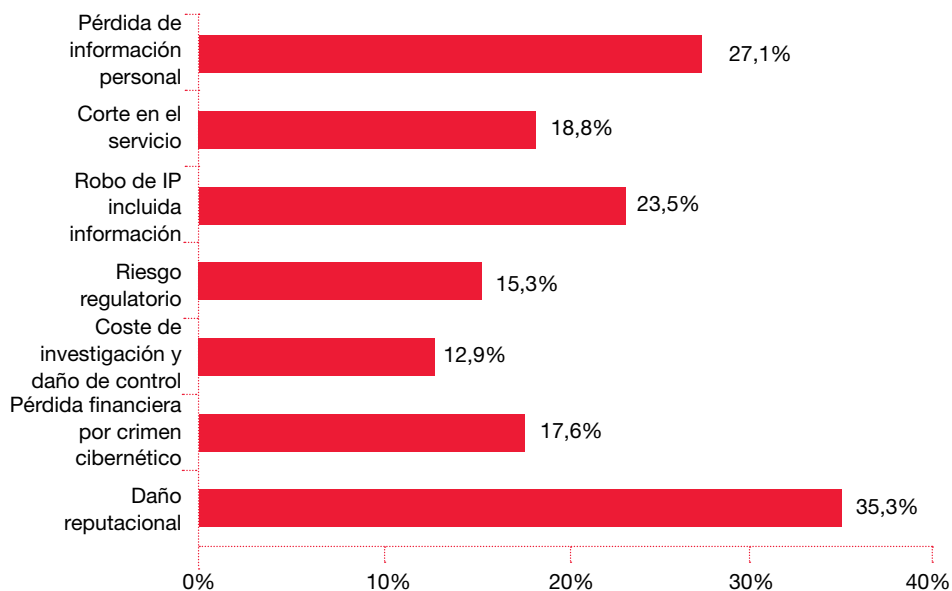
Las organizaciones que operan en España consideran que la reputación de la organización en el mercado es un activo estratégico, generador de valor y, por tanto, constituye una variable que puede hacer que las ventas de la organización se incrementen o disminuyan.

Esta percepción, para el caso de España, se fundamenta principalmente en dos factores importantes: (i) en una infravaloración de la repercusión que pudiera derivarse de este tipo de delitos y, por otro lado, (ii) en la asunción de los mismos debido al coste que supondría implantar medidas de control preventivo y correctivo. Los índices de percepción del riesgo en nuestro país chocan con el coste que estamos pagando por este tipo de delitos, lo cual arroja una conclusión importante: el fraude cibernético existe en España, tiene una repercusión significativa en las organizaciones y, sin embargo, aún no disponemos de la madurez suficiente para implantar los controles necesarios como modelo natural en los procesos de TI corporativos.

Por tanto, de los datos se obtiene una conclusión inmediata: en España, la madurez de los niveles de control preventivos y de monitorización, aún no son adecuados para la lucha contra el fraude cibernético y, por ello, estamos pagando un alto coste. En este sentido, es necesario destacar que el coste marginal de la ausencia de medidas preventivas en este tipo de delitos es mayor que en el resto de delitos económicos, como consecuencia de que el principal efecto del *ciberdelito* es la reputación de la organización.

Las organizaciones que operan en España consideran que la reputación de la organización en el mercado es un activo estratégico, generador de valor y, por tanto, constituye una variable que puede hacer que las ventas de la

Gráfico 12. ¿Cuál es el grado de preocupación de su organización ante cada uno de los siguientes efectos del *ciberdelito*? (Muy preocupado)



Fuente: Encuesta mundial sobre el delito económico 2011.

organización se incrementen o disminuyan.

El daño reputacional se considera por las organizaciones españolas como el principal efecto de los delitos informáticos seguido por la pérdida de información de carácter personal.

A nuestro juicio, la creciente preocupación por la pérdida de información de carácter personal puede directamente relacionarse con los efectos de la Ley Orgánica de Protección de Datos.

En España, la madurez de los niveles de control preventivos y de monitorización, aún no son adecuados para la lucha contra el fraude cibernético y, por ello, estamos pagando un alto coste. El coste marginal de la ausencia de medidas preventivas en este tipo de delitos es mayor que en el resto de delitos económicos, como consecuencia de que el principal efecto del ciberdelito es la reputación de la organización.

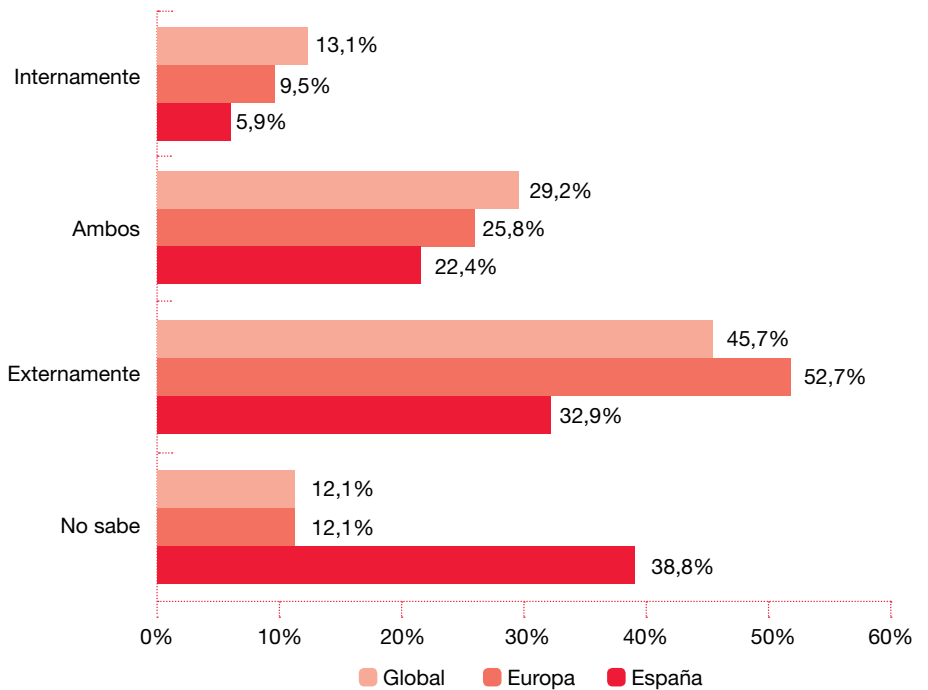
Origen del cibercrimen

El alto porcentaje de organizaciones que desconocen la fuente del cibercrimen en España está en correlación con sus niveles de iniciación en la prevención de este tipo de delitos

La baja importancia otorgada al cibercrimen puede entenderse que deriva

de su consideración como una amenaza primordialmente externa, lo cual transmite la impresión de que el daño a la organización es limitado, si bien sucesos acontecidos en años anteriores, han puesto nuevamente en evidencia cómo la fuga de información por parte de empleados de la organización es uno de los mayores riesgos de seguridad.

Gráfico 13. ¿Dónde ve usted la mayor amenaza de cibercrimen para su organización?



Fuente: Encuesta mundial sobre el delito económico 2011.

Los sucesos acontecidos en años anteriores, han puesto nuevamente en evidencia cómo la fuga de información por parte de empleados de la organización es uno de los mayores riesgos de seguridad.

Acciones llevadas a cabo para combatir el *cibercrimen*

Hasta hace muy poco la percepción del riesgo interno del *cibercrimen* se enmarcaba dentro del departamento de IT. Sin embargo, la creciente interacción de las distintas áreas de la organización con la red ha desplazado el foco del riesgo desde un solo departamento a distintos departamentos dentro de la organización. IT continúa abarcando un 25% del riesgo estimado, otros departamentos, como marketing y ventas u operaciones, han absorbido gran parte del riesgo de fraude. Esta tendencia a la diversificación dentro de los departamentos hace a la organización más vulnerable, no siendo suficiente con establecer fuertes controles a nivel de departamento, sino que la protección debe expandirse a la organización en su conjunto, siendo necesario el diseño e implementación de una política integral donde se incluyan entre otras:

- Medidas de control preventivas y detectivas.
- Protocolos de actuación y de respuesta ante una situación de *cibercrimen*.
- Adaptación del código ético corporativo.

Gráfico 14. ¿Cuáles son los departamentos que considera con mayor riesgo de *cibercrimen* dentro de su organización?

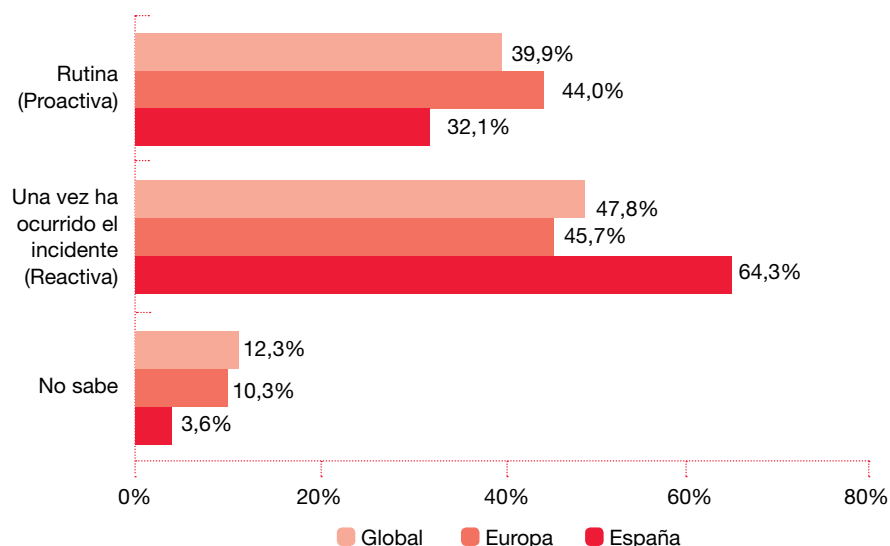
Departamento	Riesgo alto	Riesgo bajo	Sin riesgo	No sabe
Departamento de seguridad física/lógica	12,50%	58,33%	16,67%	12,50%
Departamento financiero	8,33%	70,83%	8,33%	12,50%
Departamento legal	-	50,00%	37,50%	12,50%
Alta dirección, consejo de administración	12,50%	37,50%	29,17%	20,83%
IT	25,00%	50,00%	8,33%	16,67%
Marketing y ventas	33,33%	37,50%	16,67%	12,50%
Operaciones	20,83%	33,33%	25,00%	20,83%
Recursos humanos	12,50%	41,67%	33,33%	12,50%

Fuente: Encuesta mundial sobre el delito económico 2011.



En España, en relación con los delitos económicos y, en particular, con el delito informático, continúa actuándose de manera reactiva en lugar de proactiva o preventiva. Mientras que en Europa y a nivel global se actúa con anterioridad a la comisión del delito, mediante la implementación de medidas tanto preventivas como detectivas que mitigan el riesgo de comisión de esta clase de delitos, en España el 64,3% de los encuestados manifiesta acudir a expertos externos una vez ha ocurrido el incidente.

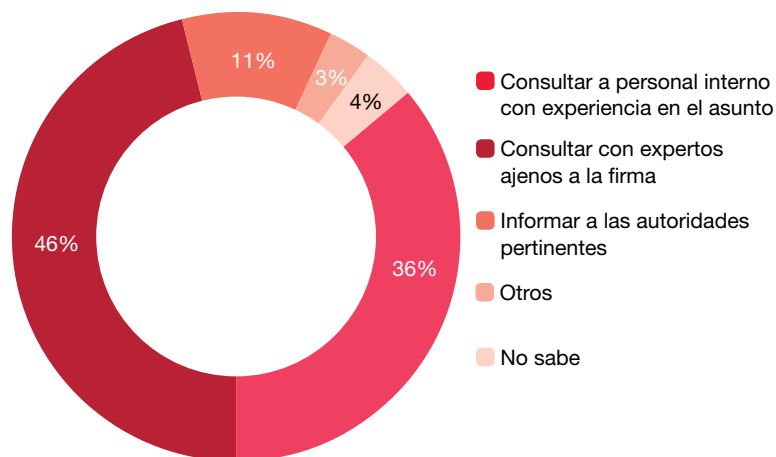
Gráfico 15.: ¿Cuándo acude su organización a expertos externos?



Fuente: Encuesta mundial sobre el delito económico 2011.

En este sentido, a la hora de investigar un *ciberdelito*, la mayoría de las organizaciones consultan directamente con expertos externos, un 46%, frente a un 36% de carácter interno. Tan sólo un 11% acude directamente a las autoridades pertinentes.

Gráfico 16. En caso de sufrir un *ciberdelito*, ¿cómo actúa su organización?



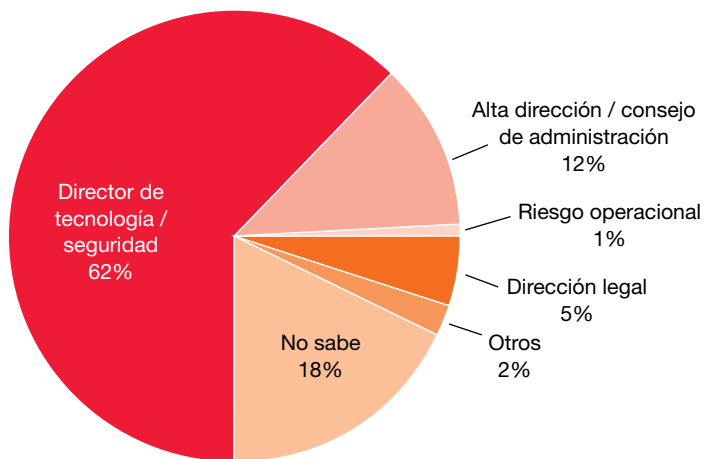
Fuente: Encuesta mundial sobre el delito económico 2011.

A la hora de investigar un ciberdelito, la mayoría de las organizaciones consultan directamente con expertos externos.

Los motivos fundamentales por los que una organización acude a expertos externos son los siguientes:

- El elevado coste de mantener un departamento de IT destinado a la investigación del *cibercrimen*.
- La rápida evolución de las tecnologías de la información.
- La alta especialización de organizaciones externas.

Gráfico 17.: Es común que la gestión diaria de la ciberseguridad resida en IT o en el departamento de seguridad. Sin embargo, ¿dónde reside la responsabilidad de prevenir el *cibercrimen* dentro de su organización?



Fuente: Encuesta mundial sobre el delito económico 2011.



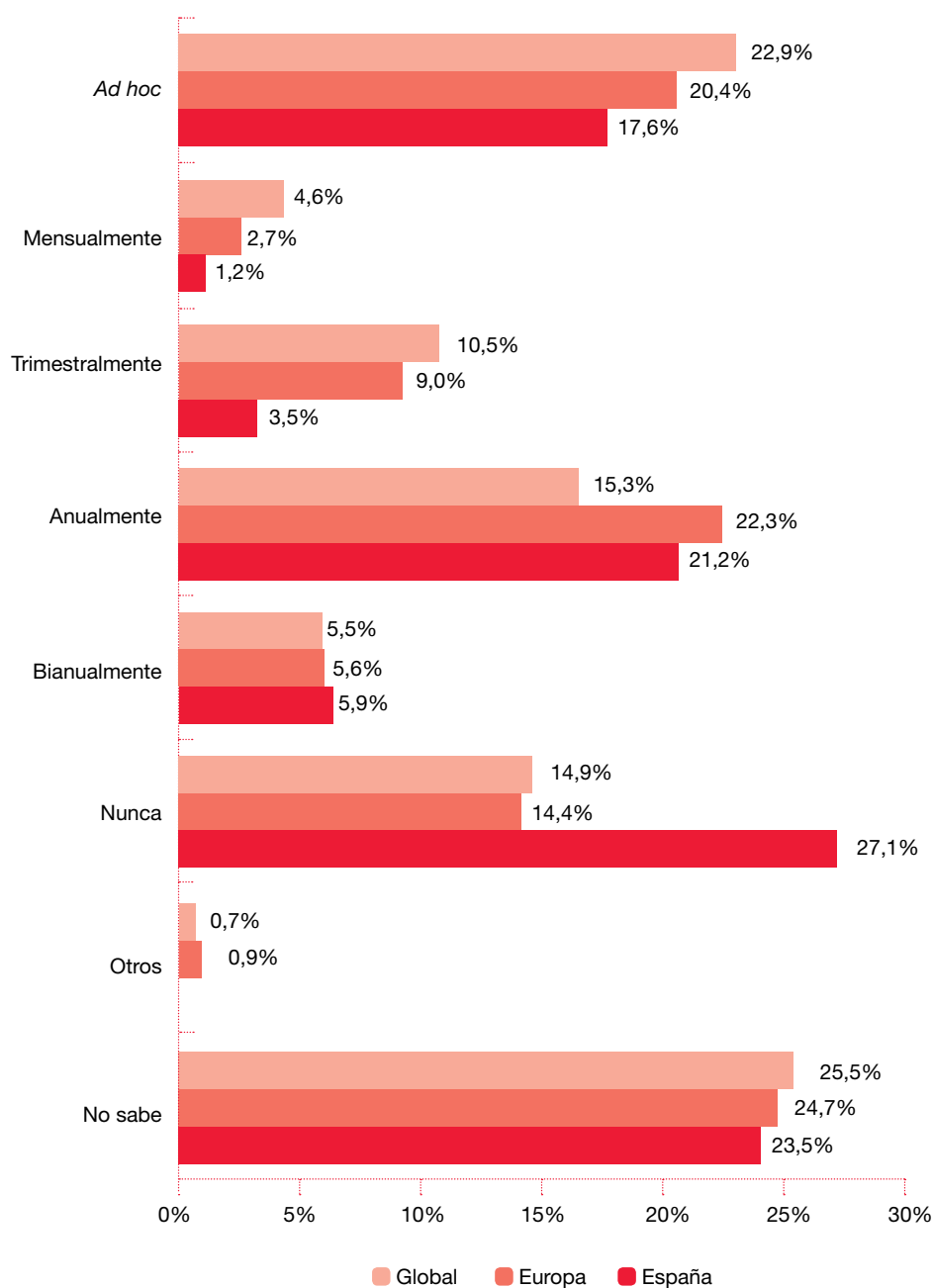
Los departamentos de IT y seguridad deben estar apoyados por la alta dirección ya que la cultura corporativa es el pilar para establecer los procedimientos, medidas y canales de comunicación al empleado sobre la adopción de medidas para prevenir estos delitos y actuar ante los mismos.

No obstante, parte de la responsabilidad de esta prevención debe también recaer en cada uno de los empleados y el uso que hace de la información corporativa. Los datos muestran que, a pesar de que la amenaza del *ciberdelito* puede afectar a todos los departamentos de una organización, en España aún se tiene una visión de que la responsabilidad de adoptar medidas preventivas contra el *ciberdelito* recae casi en exclusiva en los departamentos de IT y seguridad.

Así que, no es de extrañar que, de acuerdo con nuestra Encuesta, la alta dirección y el Consejo de Administración no suelen revisar las amenazas del riesgo de *ciberdelito*. Sólo el 25% de los encuestados manifestó que la alta dirección y el Consejo de Administración revisa la gestión de estos riesgos por lo menos una vez al año, y casi un 18% dijo que las revisiones se realizan *ad hoc*.

En el futuro, creemos que el liderazgo de una alta dirección que realmente entienda los riesgos y oportunidades del mundo cibernético constituirá una característica definitoria de las organizaciones - ya sean del sector público o privado - que dará cuenta de los beneficios que tiene llevar a cabo una gestión eficaz de este tipo de riesgos.

Gráfico 18.: ¿Cada cuanto revisa la alta dirección/ consejo de administración el riesgo del *ciberdelito* existente en su organización?



Fuente: Encuesta mundial sobre el delito económico 2011.

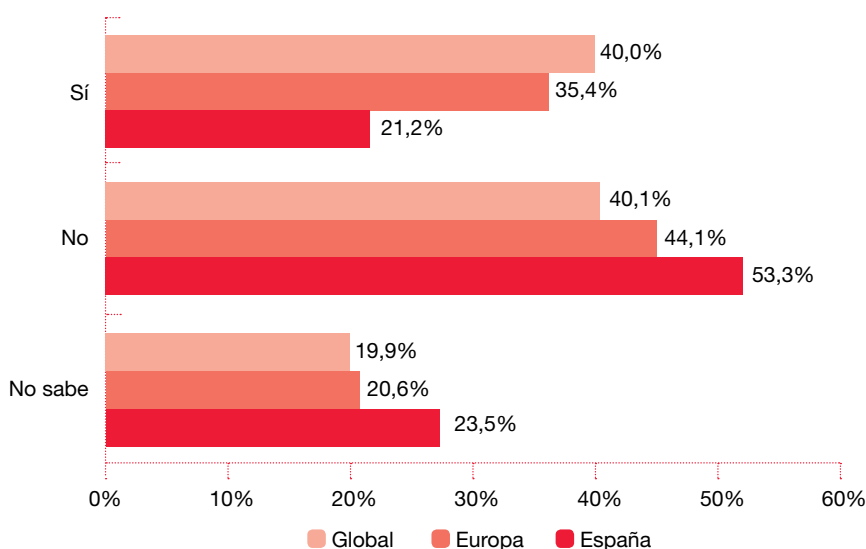
El impacto de las redes sociales

La irrupción de las redes sociales ha supuesto un fenómeno sin precedentes en el día a día de las personas, y las organizaciones no podían ser ajenas a ello. Hoy en día numerosas organizaciones tienen perfiles en redes sociales que utilizan para contactar con clientes, marketing, realizar estudios de mercado, etc.

Las ventajas de las redes sociales son de muy diversa índole, destacando, entre otras, la cercanía de la organización con la clientela pudiendo satisfacer las necesidades del consumidor final de una manera más óptima. Sin embargo, los riesgos inherentes derivados del empleo de las redes sociales aún no han sido valorados por las organizaciones de una manera adecuada.

La Encuesta muestra como en España las organizaciones aún no son conscientes de la necesidad de supervisar las redes sociales como medio de comunicación, sólo un 21,2% de las organizaciones controlan las redes sociales, frente al 35,4% y 40%, a nivel europeo y global.

Gráfico 19. ¿Controla su organización las redes sociales como Facebook o Twitter como factor de riesgo en su organización?

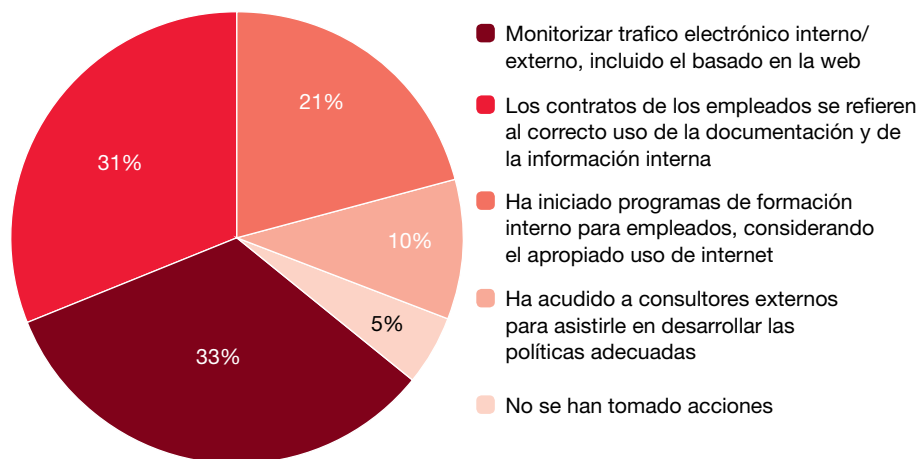


Fuente: Encuesta mundial sobre el delito económico 2011.

La Encuesta muestra como en España las organizaciones aún no son conscientes de la necesidad de supervisar las redes sociales como medio de comunicación.

De aquellas organizaciones que han contestado que ejercen medidas de control sobre las redes sociales el 33% ha optado por la monitorización del tráfico interno/externo; el 31% se ha decantado por informar a los empleados de la diligencia debida en el uso de información interna y del correcto uso de la documentación corporativa; mientras que el 21% ha impartido cursos de formación sobre la utilización de Internet.

Gráfico 20. ¿Qué acciones ha tomado su organización para combatir el riesgo de los medios sociales?



Fuente: Encuesta mundial sobre el delito económico 2011.

Conclusiones

Ante la grave y prolongada crisis económica en la que España se encuentra inmersa, con efectos devastadores en el núcleo de la sociedad, en una situación con elevadas tasas de paro, las organizaciones se ven avocadas a adoptar medidas tendentes a optimizar su estructura financiera, al aprovechamiento de recursos y a la minimización de costes. Medidas que constituyen en su conjunto un caldo de cultivo para el desarrollo de actividades delictivas, por lo que se erigen en una oportunidad y a su vez en un motivo para la comisión de actividades irregulares. De hecho un

41,7% de las empresas españolas encuestadas ha declarado haber sufrido algún tipo de delito económico o informático en los últimos 12 meses.

La (i) **apropiación indebida** de activos sigue siendo el delito económico más habitual, seguido de (ii) la **manipulación contable** y (iii) la **corrupción y el soborno**. Si bien, del estudio se desprende el importante incremento de los delitos informáticos, que han llegado a representar en torno al 4% sobre el total de los casos de fraude sufridos por las empresas españolas en los últimos 12 meses, y un incremento de aproximadamente el 130% en relación a los datos derivados de nuestro *Informe sobre delitos económicos y fraude empresarial* de 2009.

A este contexto de crisis, y de rápido desarrollo de las nuevas tecnologías y, por ende, del rápido y vertiginoso aumento de la amenaza del riesgo del delito informático o *ciberdelito*, se le une el nuevo entorno regulatorio derivado de la **Reforma del Código Penal** donde se hace extensiva la responsabilidad penal a las personas jurídicas.

Se hace fundamental implantar en las organizaciones una cultura corporativa adecuada, contraria a la comisión de



delitos, marcando unas pautas de conducta claras y unos valores concretos, estableciendo qué conductas no son tolerables y cuáles no son permitidas, para fomentar la colaboración de todos los empleados en la prevención y detección del fraude y minimizando el riesgo de comisión de delitos.

Más aún dada la especial relevancia de los casos de fraude identificados en los cuales los autores eran defraudadores internos, y de estos casi en su totalidad alta dirección y mandos intermedios, lo que claramente explica el aumento del coste medio del fraude respecto a nuestro estudio de 2009.

Por ello, la rapidez con la que las organizaciones se adapten a las nuevas reglas de juego será determinante tanto para aumentar sus ingresos y evitar costes económicos, como para reducir posibles pérdidas por sanciones derivadas del incumplimiento de la ley, ya que nuestras empresas se encuentran expuestas a diversos riesgos y amenazas:

- Un **riesgo de cumplimiento legal**: la Reforma del Código Penal puede traer importantes sanciones a la empresa, que abarcan desde fuertes sanciones económicas, a la disolución de la misma. Es por ello que resulta vital para evitar futuras complicaciones que las organizaciones tomen acciones en este sentido y se preparen

para cubrir sus responsabilidades. En este sentido, un 30,6% de las organizaciones ha adoptado medidas en respuesta a la modificación del entorno jurídico y un 20% de las organizaciones encuestadas está pensando adoptar acciones.

- Un **riesgo económico**: como hemos visto, el coste medio del fraude está en aumento dado que cada vez más los defraudadores forman parte de la alta dirección o son mandos intermedios, y cuanto más alto es el puesto del defraudador, más a su alcance está el cometer un mayor fraude.
- Un **riesgo reputacional** y de imagen, con su consecuente impacto en las ventas de la organización y, en su caso el coste de oportunidad que puede suponer la inviabilidad del desarrollo de nuevos canales de ventas, más rentables derivados como consecuencia de una minimización de los costes de venta, cercanía a la clientela e incremento potencial de la rotación de los productos.

Todo ello deberá ir unido a un análisis coste-beneficio, ya que una menor probabilidad de pérdida siempre se traduce en una mayor probabilidad de beneficio. El coste de implantar medidas de prevención y detección de fraude siempre deriva en un beneficio (a veces) difícil de cuantificar, pero sin duda es la única receta para gestionar estos riesgos.

Contactos



Javier López Andreo
Socio responsable de Forensic de PwC España
Tel.: +34 915 685 077
E-mail: javier.lopez.andreo@es.pwc.com



Sergio Aranda Morejudo
Director de Forensic
Tel.: +34 934 059 032
E-mail: sergio.aranda.morejudo@es.pwc.com



PwC ayuda a organizaciones y personas a crear el valor que están buscando. Somos una red de firmas presente en 158 países con cerca de 169.000 profesionales comprometidos en ofrecer servicios de calidad en auditoría, asesoramiento fiscal y legal y consultoría. Cuéntanos qué te preocupa y descubre cómo podemos ayudarte en www.pwc.com

© 2011 PricewaterhouseCoopers S.L. Todos los derechos reservados. "PwC" se refiere a PricewaterhouseCoopers S.L, firma miembro de PricewaterhouseCoopers International Limited; cada una de las cuales es una entidad legal separada e independiente.