www.pwc.com/ar

Combatiendo el fraude en el Sector Financiero

Encuesta Global sobre Delitos Económicos - Servicios Financieros

3.877 encuestados
en 78 países
Diciembre de 2011

pwc

La mitad de los ejecutivos del sector de SF percibe que el riesgo de ser víctima de un delito informático ha aumentado en los últimos 12 meses.

Contenido

Acerca del informe

Los datos de este informe surgen de la Encuesta Global sobre Delitos Económicos de PwC, y más específicamente de las respuestas de los ejecutivos del sector de Servicios Financieros[1] (SF) que participaron de la misma.

En ediciones anteriores, el análisis de nuestros especialistas giró en torno a aspectos tales como la incidencia que la crisis financiera global tuvo en el aumento de la cantidad de delitos económicos, y particularmente en los casos de fraude en los estados financieros.

Casi la mitad de las entidades financieras ha reportado un delito económico durante el último año a nivel global.

En el presente informe, en cambio, nos referimos a la tendencia global a enfatizar el marco normativo y regulatorio y los controles aplicados a las entidades financieras. Asimismo, nos enfocamos en la creciente amenaza que suponen los delitos informáticos y en su impacto en los negocios, ya que este tipo de fraude fue identificado como uno de los más recurrentes.

Teniendo en cuenta la relevancia de los temas tratados, consideramos que este informe será de gran utilidad para los ejecutivos del sector financiero, a los efectos de continuar en su esfuerzo por implementar las estrategias adecuadas y las mejores prácticas en materia de prevención y detección del fraude.

Acerca de la encuesta

La Encuesta Global sobre Delitos Económicos tiene como principal objetivo identificar los tipos de fraudes más reportados, el perfil de sus perpetradores y víctimas, las metodologías de detección utilizadas y las consecuencias que generaron, para definir estrategias eficaces para combatirlos.

En la sexta edición participaron ejecutivos de 3.877 organizaciones localizadas en 78 países, lo que permite un análisis de resultados por industrias. Específicamente, 878 ejecutivos de entidades financieras de 56 países contestaron la encuesta, representando al 23% de los respondientes.

1 Servicios financieros: incluye la banca minorista y de inversión, seguros, gestión de inversiones, corretaje de valores y fondos de capital de riesgo.

Resultados destacados

- *Las entidades financieras continúan siendo el principal blanco de los estafadores, principalmente en lo que respecta a la apropiación indebida de activos[2].*
- *El 45% de los ejecutivos de organizaciones del sector de SF ha reportado algún delito económico en los últimos 12 meses (en otras industrias, tan sólo el 30%).*
- *El delito informático es el segundo tipo de fraude más frecuente en la industria financiera.*
- *Casi un tercio de los empleados del sector financiero no ha recibido entrenamiento sobre seguridad informática.*
- *El fraude externo continúa siendo la principal amenaza para las entidades financieras. No obstante, los casos de fraude interno aumentaron en mayor proporción.*
- *En el sector de SF los delitos económicos que involucran a altos directivos han aumentado un 50% en los últimos 2 años.*
- *1 de cada 5 entidades financieras no llevó a cabo una evaluación de riesgo de fraude durante el último año.*
- *Los mecanismos de denuncia de irregularidades están infrautilizados y no son promovidos por las organizaciones de la industria financiera.*

Cómo proteger a su organización del fraude

- *Identificar y entender los riesgos informáticos y tomar las medidas de seguridad adecuadas.*
- *Establecer un plan de contingencia para proteger a la organización ante una eventual crisis informática.*
- *Liderar la lucha contra el fraude de manera proactiva, especialmente desde la alta gerencia.*
- *Realizar evaluaciones de riesgo de fraude regularmente, considerando que los riesgos pueden variar en función del contexto.*
- *Implementar, promover y dar soporte a mecanismos de denuncia de irregularidades.*

2 Apropiación indebida de activos (incluyendo la malversación/engaño por parte de los empleados): robo de activos (incluyendo activos monetarios o en efectivo o insumos y equipos) por los directores, fiduciarios o empleados para su propio beneficio.

38%

Porcentaje de delitos informáticos, entre el total de casos de fraude reportados por entidades financieras durante 2011.

Delitos informáticos

Durante los últimos años se ha incrementado la cantidad de víctimas de delitos informáticos, tales como robos de datos, pharming, phishing y virus, porque la mayoría de las personas y organizaciones confían en Internet y en las tecnologías y se exponen a los riesgos de ataques desde cualquier parte del mundo.

Por este motivo, consultamos a los ejecutivos qué acciones implementaron para prevenirlos, detectarlos y combatirlos, y por qué consideran que es una de las principales amenazas que enfrentan, y evaluamos sus impactos en las organizaciones de todo el mundo.

Tal vez el mayor desafío a la hora de analizar los riesgos de los delitos informáticos es que no existe una definición globalmente aceptada de este tipo de delito económico. Por ejemplo, si un ejecutivo de cualquier área roba información confidencial, la copia a un dispositivo USB y se la facilita a un competidor, puede tratarse de un caso de robo de propiedad intelectual, de un delito informático, o de ambos. Y debido a que no existe hoy en día una estándar a nivel internacional, muchas veces las organizaciones no tienen una verdadera noción del peligro que enfrentan, lo que las vuelve más vulnerables y hace que sea más difícil detectar y combatir este tipo de fraude.

A los efectos de la Encuesta Global de Delitos Económicos de PwC, hemos definido con el profesor Peter Sommer al delito informático como:

"Delitos económicos en los que se utilizan herramientas informáticas, tales como computadoras y/o Internet, que juegan un papel central, y no accidental o casual, en la comisión del delito. Incluye la distribución de virus, la descarga ilegal de archivos, el phishing y el pharming, y el robo de información personal".

Los ejecutivos de entidades financieras han destacado al delito informático con más énfasis que los encuestados de otras industrias, y los entes reguladores del sector están cada vez más enfocados en este tipo de fraude. Asimismo, es evidente que se espera que las organizaciones tengan sistemas de control adecuados. Por ejemplo, en el Reino Unido, la "Financial Services Authority" (F.S.A.) ha incluido a la "seguridad de los datos" como uno de los principales riesgos de fraude, y en una reciente conferencia en China[3] , el

3 Cuarta Conferencia Nacional de Trabajo Financiero, celebrada en Beijing en enero de 2012.

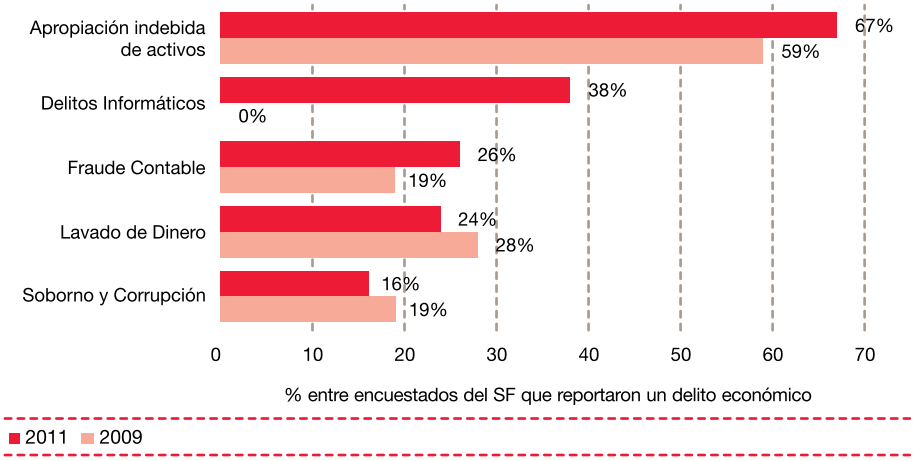
primer ministro, Wen Jiabao, declaró que es necesario enfatizar la lucha contra este tipo de delito.

Los ejecutivos de la industria financiera señalaron que el fraude más frecuente del que han sido víctimas durante el último año fue la apropiación indebida de activos, con el 67% de sus respuestas (Gráfico 1). Asimismo, ubicaron a los delitos informáticos en segundo lugar (38%), dato que adquiere más relevancia si se toma en consideración que tan sólo el 16% de los reportados por organizaciones de otras industrias fueron de este tipo.

Estos porcentajes tienen sentido porque las entidades financieras manejan datos en los que los delincuentes informáticos están interesados, sobre todo teniendo en cuenta que existe un mercado negro dedicado a la provisión de los mismos.

Desde hace tiempo, las organizaciones de la industria financiera han tomado medidas para proteger los datos de sus clientes (por ejemplo, aplicando protocolos en call centers, deshabilitando puertos de las computadoras o sumando factores de identificación para el acceso a internet), pero los problemas no cesaron. De hecho, la mitad de los ejecutivos del sector de SF encuestados percibe que el riesgo de ser víctimas de un delito informático ha aumentado en los últimos 12 meses, en comparación con el 36% para otras industrias.

Gráfico 1. 5 tipos de delitos económicos más reportados en el sector de SF



Nota: Se permitió la selección de respuestas múltiples.

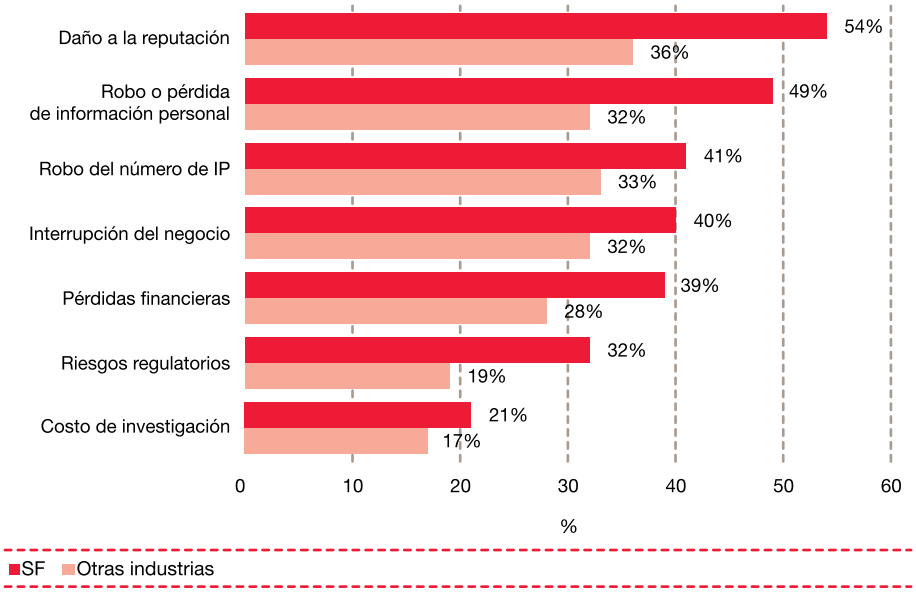
Gráfico 2: Departamentos internos que presentan el mayor riesgo de delito informático

Departamento	SF	Otras Industrias
1. Tecnología	63%	49%
2. Operaciones	47%	37%
3. Finanzas	39%	30%
4. Ventas y Marketing	33%	34%
5. Seguridad	31%	23%
6. Directorio / Ejecutivo Senior	19%	16%
7. Recursos Humanos	13%	15%
8. Legales	7%	8%

Nota: Se permitió la selección de respuestas múltiples.

La mayoría de los ejecutivos de la industria financiera cree que el Departamento de Tecnología es el más riesgoso en lo que respecta a los delitos informáticos.

Gráfico 3. Preocupación por los daños colaterales ocasionados por los delitos informáticos



Nota: Se permitió la selección de respuestas múltiples.

"El daño a la reputación es el efecto colateral de los delitos informáticos que más preocupa a los ejecutivos del sector de SF."

Asimismo, es probable que ciertas innovaciones tecnológicas, como las aplicaciones (o 'Apps') para acceder a los servicios bancarios, o los smartphones que se utilizan como medios de pago, aumenten estos riesgos en lugar de disminuirlos.

¿Dónde surge la amenaza de delitos informáticos?

Los ejecutivos de la industria financiera consideran que el delito informático es una amenaza predominantemente externa.

No obstante, están empezando a reconocer que a veces tiene procedencia interna, es decir, que es cometido por uno o más empleados de su staff.

Los líderes del sector de SF tienden a creer que el riesgo de delito informático es menor para los departamentos de Recursos Humanos (13%) y Legales (7%), lo cual es consistente con los resultados de otras industrias (Gráfico 2). Sin embargo, la información confidencial que se encuentra guardada en los sistemas informáticos de dichos sectores, como en los de cualquier otro, podría ser de interés para los delincuentes informáticos. Por ello, es importante que las entidades financieras reconozcan que la amenaza puede provenir de cualquier área de la organización, y que no debe ser considerada sólo como un riesgo del departamento de Tecnología.

Las entidades financieras deben identificar quién es responsable de afrontar la lucha contra los delitos informáticos, evaluar de dónde surge esta amenaza creciente, y tomar las medidas pertinentes cuando se identifica una amenaza de este tipo. Siguiendo esta línea, para que la gestión del riesgo sea eficaz, es fundamental que las medidas que tomen sean de carácter holístico e integral.

¿Qué preocupa a las entidades financieras en lo referido a los delitos informáticos?

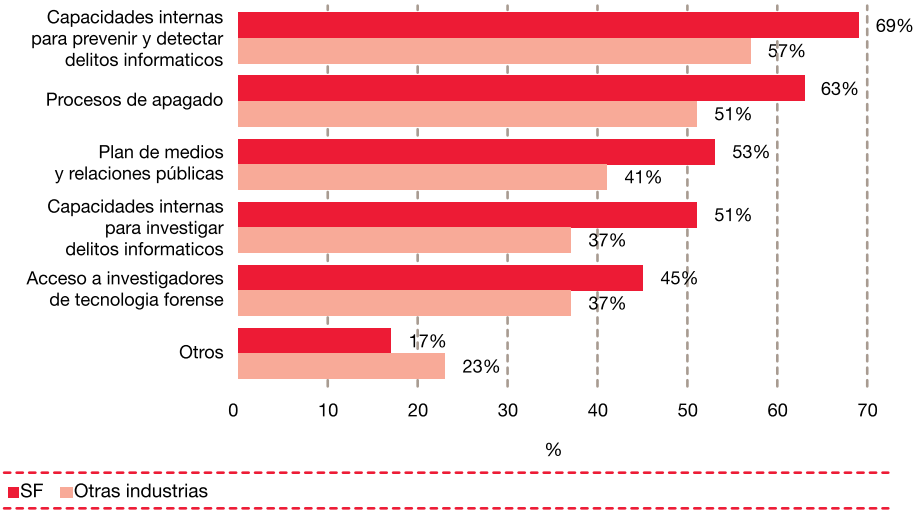
Para la Encuesta Global de Delitos Económicos de 2011 preguntamos cuáles son las consecuencias de los delitos informáticos a las que los ejecutivos más temen (Gráfico 3). Más de la mitad de los representantes de entidades financieras señalaron el daño a la reputación debido al impacto negativo que los medios de comunicación pueden ejercer sobre la percepción de una marca. Un dato que se destaca es que, en todas las categorías, el nivel de preocupación de los ejecutivos de entidades financieras es mayor en comparación con otras industrias, aspecto comprensible si se toma en cuenta que los riesgos son más significativos en dicho sector.

Las organizaciones, ¿están preparadas para combatir los delitos informáticos?

Las horas que transcurren luego de que se produce un delito informático son cruciales. Por este motivo, es fundamental reaccionar con rapidez y decisión, sobre todo teniendo en cuenta las consecuencias, incluidas aquellas referidas a la imagen de la organización afectada.

Teniendo en cuenta esto, era previsible que la mayoría de las entidades financieras tuviera mecanismos de respuesta a los delitos informáticos. Sin embargo, sólo el 18% de los ejecutivos del sector implementa los 5 principales mecanismos sugeridos para combatir este tipo de delitos (Gráfico 4).

Gráfico 4. Mecanismos aplicados para prevenir y/o combatir los delitos informáticos



Nota: Se permitió la selección de respuestas múltiples.

¿Quién debería ser el responsable de prevenir los delitos informáticos?

Los resultados de la encuesta muestran que los ejecutivos del sector de SF, al igual que los representantes de otras industrias, ven a los delitos informáticos como un asunto específico del departamento de Tecnología.

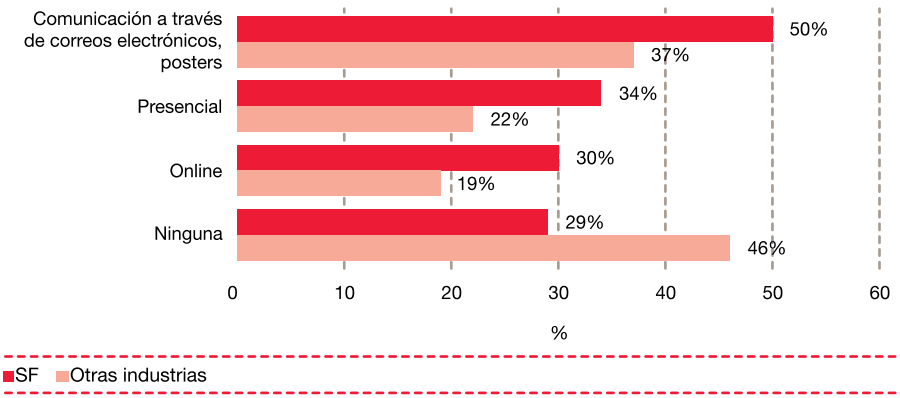
En nuestra opinión, la responsabilidad general de la gestión de fraudes recae en la alta gerencia, y por ello es esencial que sus representantes entiendan los potenciales riesgos y las oportunidades que el mundo informático presenta. Asimismo, todas las líneas de negocio deberían comprometerse con la lucha contra los delitos informáticos, ya que es una responsabilidad que trasciende al departamento de Tecnología.

Las entidades financieras han puesto bastante énfasis en la seguridad informática y tan sólo el 29% no ha recibido capacitación alguna sobre el tema, mientras que en el resto de las industrias respondieron lo mismo el 46% de los encuestados (Gráfico 5).

Este dato es alentador y sugiere que las organizaciones de la industria financiera están siendo proactivas. Sin embargo, también es cierto que es un problema que casi un tercio del personal no haya recibido ninguna capacitación sobre este tema, que se suma a la ambigüedad que existe en torno a la definición del delito informático y a la falta general de claridad sobre las responsabilidades de la gestión de riesgo de los mismos.

Por todo esto, es importante que las organizaciones financieras aseguren que su personal, sobre todo la alta gerencia, conozca las consecuencias de los delitos informáticos y cuenten con las herramientas para prevenir y combatir este tipo de fraude.

Gráfico 5. Tipo de capacitación que brindan sobre seguridad de la información



Nota: Se permitió la selección de respuestas múltiples.

Aumento contemplado en fraudes de alta gerencia en las organizaciones de SF.

50%

Delitos económicos

La industria financiera continúa siendo el blanco preferido de los estafadores.

Desde siempre, el sector de SF es un blanco para los estafadores, principalmente debido a la cantidad de dinero en efectivo, activos y datos confidenciales de clientes disponibles, así como por la naturaleza misma de la industria.

El 45% de los ejecutivos de entidades financieras encuestados ha reportado casos de fraude en los últimos 12 meses. Esta cifra es significativa en comparación con la de otras industrias (30%), pero es cierto que la diferencia también se debe a que las organizaciones del sector financiero poseen controles efectivos destinados a detectar los fraudes, factor que conlleva un aumento en el número de delitos económicos reportados.

¿Cuáles son los fraudes más recurrentes reportados por las entidades financieras?

El gráfico 1 muestra los 5 tipos de delitos económicos más reportados por los ejecutivos de la industria financiera en los últimos 12 meses. La apropiación indebida de activos y el fraude contable aumentaron con respecto a 2009, y como se destacó anteriormente en este informe, el delito informático ocupa el segundo lugar.

El fraude contable en el sector financiero aumentó de 19% en 2009 a 26% en 2011, mientras que en otras industrias cayó significativamente (de 38% en 2009 a 22% en el 2011). Este descenso podría ser consecuencia de que las organizaciones estén implementando controles y sanciones al personal más estrictos, o porque actualmente hay más oportunidades de que el fraude pase desapercibido y, por lo tanto, no sea reportado.

Por su parte, el aumento del fraude contable en el sector de SF podría estar relacionado con las mayores presiones que sufren los empleados que trabajan por objetivos, junto con otros factores, tales como el orgullo personal de tener una reputación exitosa o el incentivo de satisfacer las expectativas de los inversores y otros terceros interesados.

En lo que respecta al lavado de dinero, continúa siendo un fraude recurrente en la industria financiera (el 24% de las organizaciones del sector reportó este tipo de delito económico, mientras que en otras industrias tan sólo el 3% lo hizo). Por último, el soborno y la corrupción se mantienen dentro de los 5 tipos de fraude más recurrentes (16% en el sector de servicios financieros; 27% para otras industrias).

Los casos de lavado de dinero y de soborno y corrupción reportados han disminuido ligeramente con respecto a

2009. Sin embargo, este descenso se puede atribuir a que las entidades financieras cumplen con requisitos normativos y aplican sistemas y controles rigurosos para prevenir fraudes. Por estos motivos, podemos afirmar que ambos delitos económicos continúan siendo un riesgo importante para el sector de SF.

Las leyes contra el soborno y la corrupción, ¿deberían ser una preocupación primordial?

Hay un concepto erróneo de que la industria financiera es afectada en menor medida por el soborno y la corrupción, pero nuestra encuesta demuestra lo contrario, ya fue uno de los 5 tipos de fraude más reportados por el sector durante los últimos 12 meses.

La abundancia de leyes destinadas a combatir el soborno y la corrupción, incluyendo la "Foreign Corrupt Practices Act" o "FCPA" de Estados Unidos, la "UK Bribery Act " de Reino Unido y la "Canadian Corruption of Foreign Public Officials Act" de Canadá, ponen en evidencia la importancia de que las entidades financieras tomen las medidas adecuadas para prevenir y combatir este tipo de delito.

A pesar de que se debe reconocer que los niveles de ejecución de las mencionadas leyes pueden variar según la jurisdicción, el interés regulatorio está creciendo y es probable que surjan más sanciones reglamentarias para la lucha contra estos delitos. En este sentido, algunos ejemplos recientes son las sanciones impuestas a Siemens (USD 800 millones) y Daimler (USD 185 millones) bajo la FCPA, y dos multas por parte de la FSA del Reino Unido contra Willis Limited (7 millones de libras) y Aon (5 millones de libras).

¿Quién está cometiendo fraude?

El sector de SF suele ser percibido como el blanco de los estafadores externos, y los resultados de nuestra encuesta confirman este punto. No obstante, hubo una reducción con respecto a la edición de 2009 (del 71% al 60%), lo que sugiere que mejoraron los controles o que existen nuevos tipos de fraude externo que no se están detectando.

Gráfico 6. Principales autores de los fraudes externos reportados en organizaciones del sector de SF

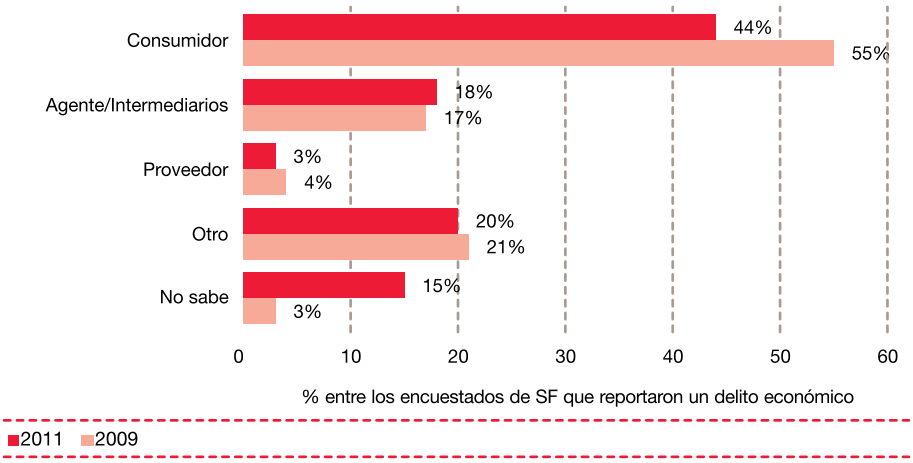
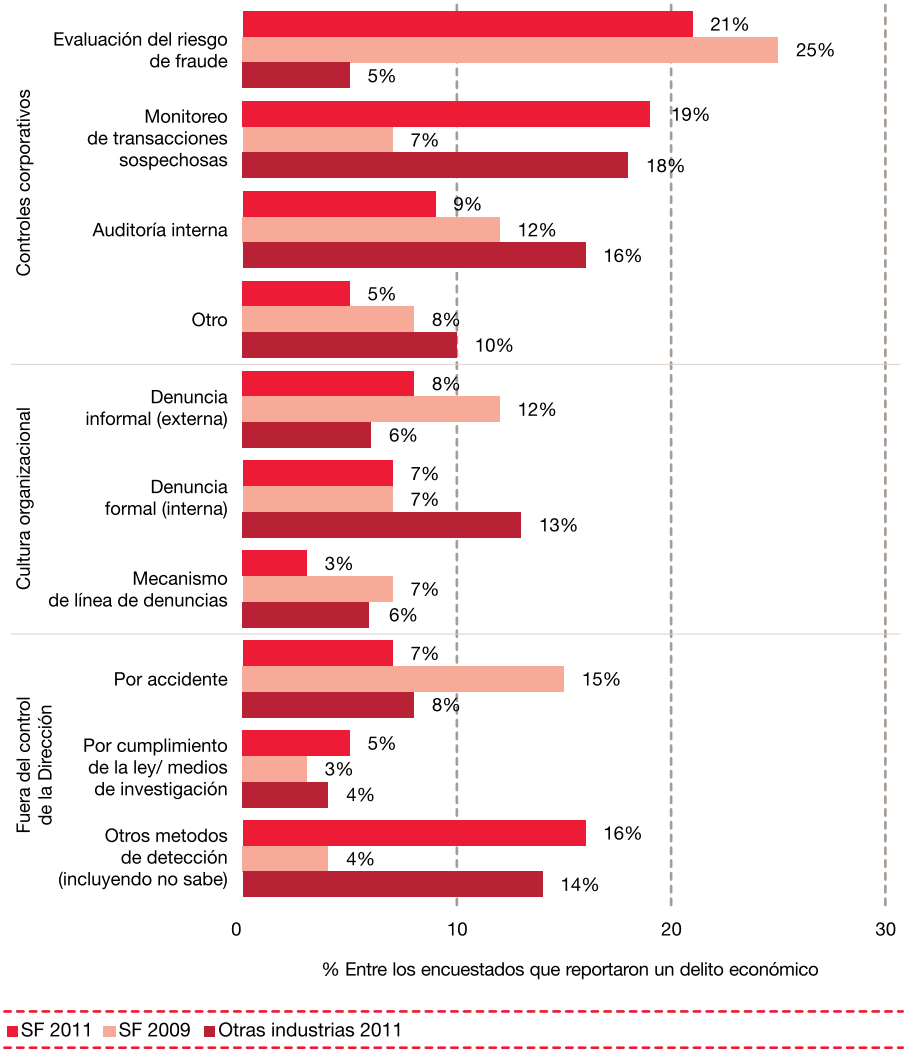


Gráfico 7. Métodos que han utilizado para detectar los delitos económicos reportados



La evaluación de riesgo fue el método de detección de casos de fraude más utilizado por las entidades financieras.

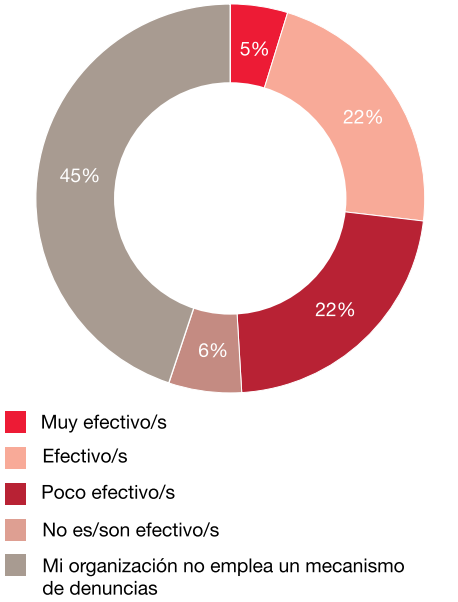
Asimismo, se han incrementado en un 50% los fraudes cometidos por la alta gerencia de entidades financieras (del 12% en 2009 al 18% en 2011), factor que podría impactar negativamente en la capacidad de las organizaciones para prevenirlos y detectarlos.

El 44% de los ejecutivos de entidades financieras encuestados considera que sus clientes fueron los principales perpetradores de fraude externo en los últimos 12 meses (Gráfico 6). No obstante, en 2009 el 55% se expresó de la misma forma y aumentaron las respuestas 'Otro' y 'No sabe'. Estos cambios pueden deberse al aumento de casos de delitos informáticos reportados por las entidades financieras, que raramente son perpetrados por los clientes, y también sugieren que las metodologías de detección utilizadas no son útiles a la hora de identificar a los autores de los delitos.

¿Qué métodos de detección de fraudes utilizan las entidades financieras?

Las entidades financieras han realizado más evaluaciones de riesgo que las organizaciones de otras industrias, y seguramente por ello han reportado más casos de fraude (45%, frente al 30%). Esto se debe a que existe una correlación directa entre la cantidad de fraudes reportados y la cantidad de evaluaciones de riesgo de fraude que se llevan a cabo. Siguiendo esta línea, la evaluación del riesgo de fraude fue el método de detección más eficaz en las entidades financieras: a través de la misma, se identificaron el 21% de los

Gráfico 8. Eficacia de los mecanismos de denuncia de fraude utilizados en las organizaciones de SF



delitos económicos reportados por el sector (Gráfico 7). Sin embargo, 1 de cada 5 ejecutivos de la industria financiera no llevó a cabo evaluaciones de riesgo durante los últimos 12 meses, y si la hubieran implementado, seguramente la cantidad de fraudes reportados sería superior a la registrada.

A los que respondieron que no la llevaron a cabo se les preguntó el motivo, y el 36% de los ejecutivos del sector de SF manifestó que fue porque no estaba seguro de lo que implicaba (en comparación con el 29% de los encuestados de otras industrias). Este desconocimiento es preocupante, y pone en evidencia la necesidad de que las entidades financieras evalúen y determinen los riesgos y costos asociados a los delitos económicos.

El segundo método de detección reportado por los respondientes del sector de SF fue el monitoreo de transacciones sospechosas, el cual ascendió de 7% en 2009, a 19% en 2011. Siendo esto consistente con otras industrias, es sorprendente que estas cifras hayan sido tan bajas en 2009, ya que las organizaciones financieras han utilizado el monitoreo de transacciones sospechosas por muchos años, sobre todo en lo que a lavado de dinero se refiere. Quizás sea porque las entidades suelen reportar transacciones sospechosas a entes reguladores sin saber si los delitos se llevaron realmente a cabo.

"Las estadísticas recientes muestran que las entidades financieras son particularmente vulnerables cuando los delincuentes utilizan los canales y sistemas existentes para estafarlas, o para blanquear el producto del delito. Los controles efectivos, como el monitoreo de transacciones, pueden ayudarlas a proteger a sus clientes, y a sí mismas, contra estas actividades. Sin embargo, esto también obliga a los entes reguladores a garantizar que se hayan implementado los controles necesarios para limitar estos riesgos" -Murray Michell, Director del South African Financial Intelligence Centre.

¿Se subestima la denuncia de irregularidades como método de detección?

A pesar de que muchas entidades financieras poseen mecanismos de denuncia de irregularidades, esta herramienta no ha sido muy eficaz en la detección de delitos económicos. Entre las posibles causas, podemos mencionar las siguientes:

- No se realizaron programas de capacitación y concientización sobre los mecanismos de denuncias existentes.
- La alta gerencia no promueve la importancia de los mecanismos de denuncias.
- No se han protegido los intereses de un denunciante, lo que generó desconfianza en el proceso.
- Hay resistencia cultural a denunciar a un compañero de trabajo.

Algunos de los datos más sorprendentes que se desprenden de nuestra encuesta son los siguientes: el 45% de los ejecutivos del sector de SF declaró que su organización no emplea un mecanismo de denuncia de irregularidades y el 28% dijo que el mecanismo de denuncia que utiliza no es eficaz o que es sólo ligeramente efectivo (Gráfico 8).

Las entidades financieras no confían en la eficacia de los mecanismos de denuncia de irregularidades, pero no comprenden que para que sea una

Organizaciones del sector de SF que no emplean mecanismos de denuncia de irregularidades o fraudes.

45%

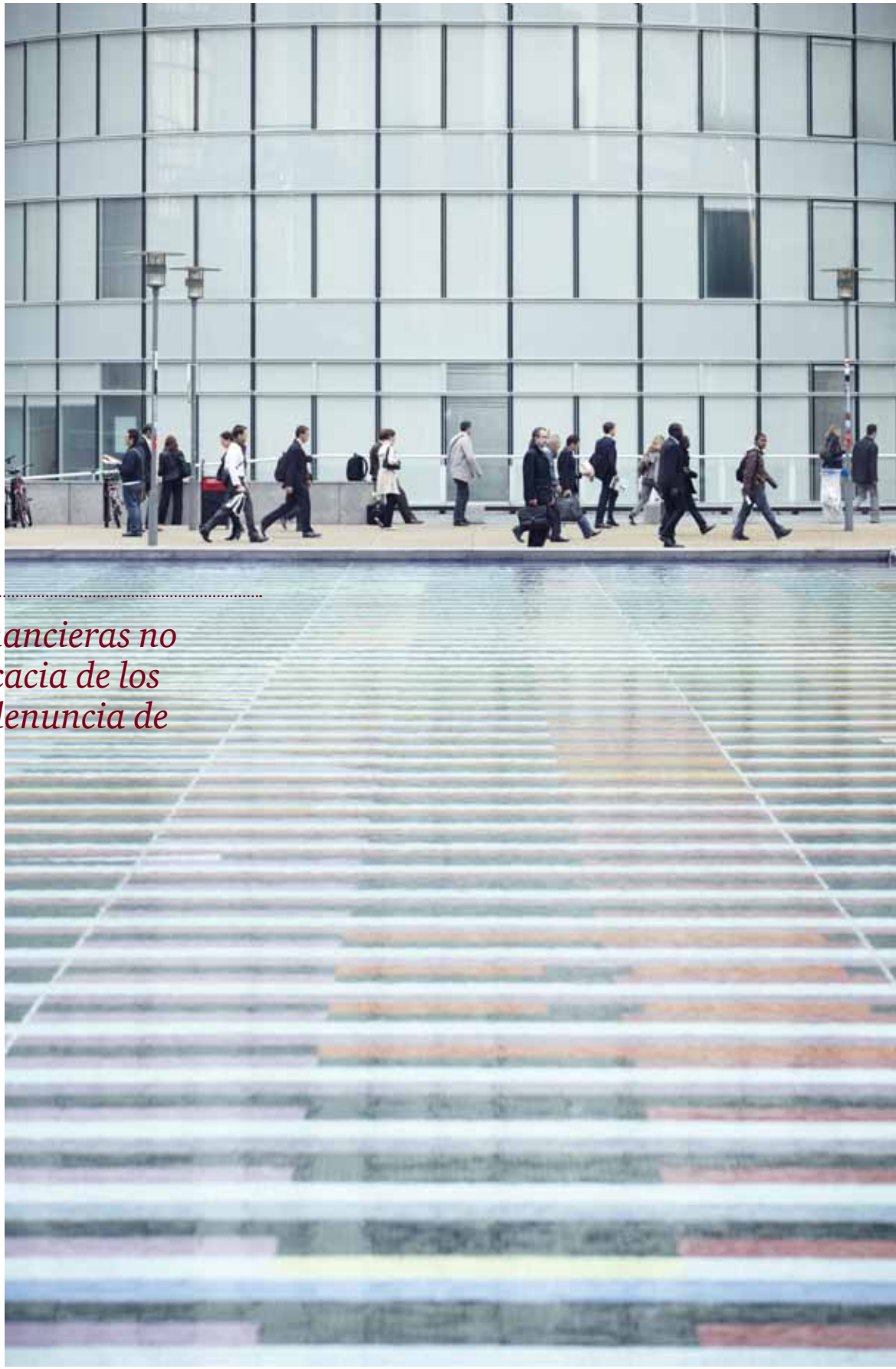
36%

Ejecutivos del sector de SF que no llevaron a cabo evaluaciones de riesgo porque desconocían lo que implicaban.

herramienta eficaz es indispensable que la alta gerencia se comprometa con la lucha contra el fraude y que promueva una cultura corporativa consistente con dicho fin. Asimismo, sus representantes deben tomar en consideración que la actitud hacia esta herramienta variará en los distintos países.

Pasos para desarrollar un mecanismo efectivo de denuncia de irregularidades:

1. Conseguir compromiso de todo el staff, especialmente de la alta gerencia;
2. Desarrollar una política de denuncia de irregularidades;
3. Diseñar su mecanismo;
4. Implementarlo; y
5. Realizar el monitoreo, seguimiento y evaluación del mismo.



Las entidades financieras no confían en la eficacia de los mecanismos de denuncia de irregularidades.

Es tiempo de que las entidades financieras asuman el desafío de prevenir, detectar y combatir los delitos económicos.

Conclusión

La industria financiera continúa siendo un blanco muy atractivo para los estafadores y es indispensable que las organizaciones del sector asuman un papel proactivo en la lucha contra el fraude.

Los delitos económicos tradicionales fueron los más reportados por los ejecutivos del sector financiero en los últimos 12 meses, pero también emergieron "nuevas" amenazas: el fraude informático fue identificado como el segundo más recurrente durante el período contemplado. Las entidades financieras están muy preocupadas por el daño a la reputación que conllevan, pero podrían hacer mucho más para prevenir éste y otros riesgos asociados.

Con los rápidos cambios que existen en la prestación de servicios bancarios y otros servicios financieros, y la dependencia cada vez mayor en la tecnología para la prestación de esos servicios, es de vital importancia tener la seguridad informática efectivamente incorporada en los procedimientos de rutina, así como mecanismos de detección y prevención de fraude informático, y un plan de respuesta frente a crisis asociadas.

La denuncia de irregularidades parece estar infrautilizada como método de detección de fraude, factor que puede estar relacionado con la cultura de las organizaciones. La promoción de este mecanismo debe incrementarse, y así la alta gerencia demostraría su compromiso con la lucha contra el fraude.

De acuerdo a nuestra opinión, las entidades financieras deberían tomar en consideración estas 5 sugerencias para prevenir el fraude:

1. Incorporar la seguridad informática al negocio, definir y entender los riesgos asociados, y planificar la gestión de acuerdo al impacto que se prevé que los cambios tecnológicos tendrán en el mercado.

2. Definir un plan de respuesta frente a una crisis informática, para proteger a la organización de pérdidas financieras o de otro tipo, como por ejemplo, a su reputación.

3. Liderar la lucha contra el fraude desde la alta gerencia.

4. Realizar evaluaciones de fraude regularmente, ya que hay delitos económicos que varían constantemente.

5. Utilizar mecanismos de denuncias de irregularidades.

La alta gerencia debe focalizarse en los controles y mecanismos de prevención y detección de delitos económicos y asegurar que se realicen regularmente evaluaciones de riesgo de fraude. Asimismo, es indispensable que exista un enfoque integral en toda la organización, en todas las líneas de negocios y en los procesos de rutina.

El fraude no es un problema que se restringe al departamento de Tecnología y puede afectar gravemente a las entidades financieras si no toman las medidas adecuadas para prevenirlos y combatirlos. En este sentido, cabe destacar que la tecnología avanza rápidamente, y con ella los defraudadores, pero las organizaciones están un paso atrás y muy pocas asumen la responsabilidad de conocer los riesgos y oportunidades del entorno. Por ello, es imprescindible que reconozcan las nuevas variables y que adapten sus mecanismos de respuesta y detección en consecuencia para enfrentar los delitos económicos. En definitiva, sólo las que asuman este desafío obtendrán una ventaja competitiva en el actual contexto.

Si desea conocer la metodología utilizada para la Encuesta Global sobre Delitos Económicos, por favor ingrese a: www.pwc.com/ar.

Contactos

Jorge C. Bacher
Socio
(+54 11) 4850-6814
jorge.c.bacher@ar.pwc.com

Ignacio Aquino
Socio
(+54 11) 4850-6816
ignacio.aquino@ar.pwc.com

Diego Taich
Director
(+54 11) 4850-6887
diego.taich@ar.pwc.com

Andrés Sarcuno
Gerente
(+54 11) 4850-0000 Int. 4141
andres.sarcuno@ar.pwc.com