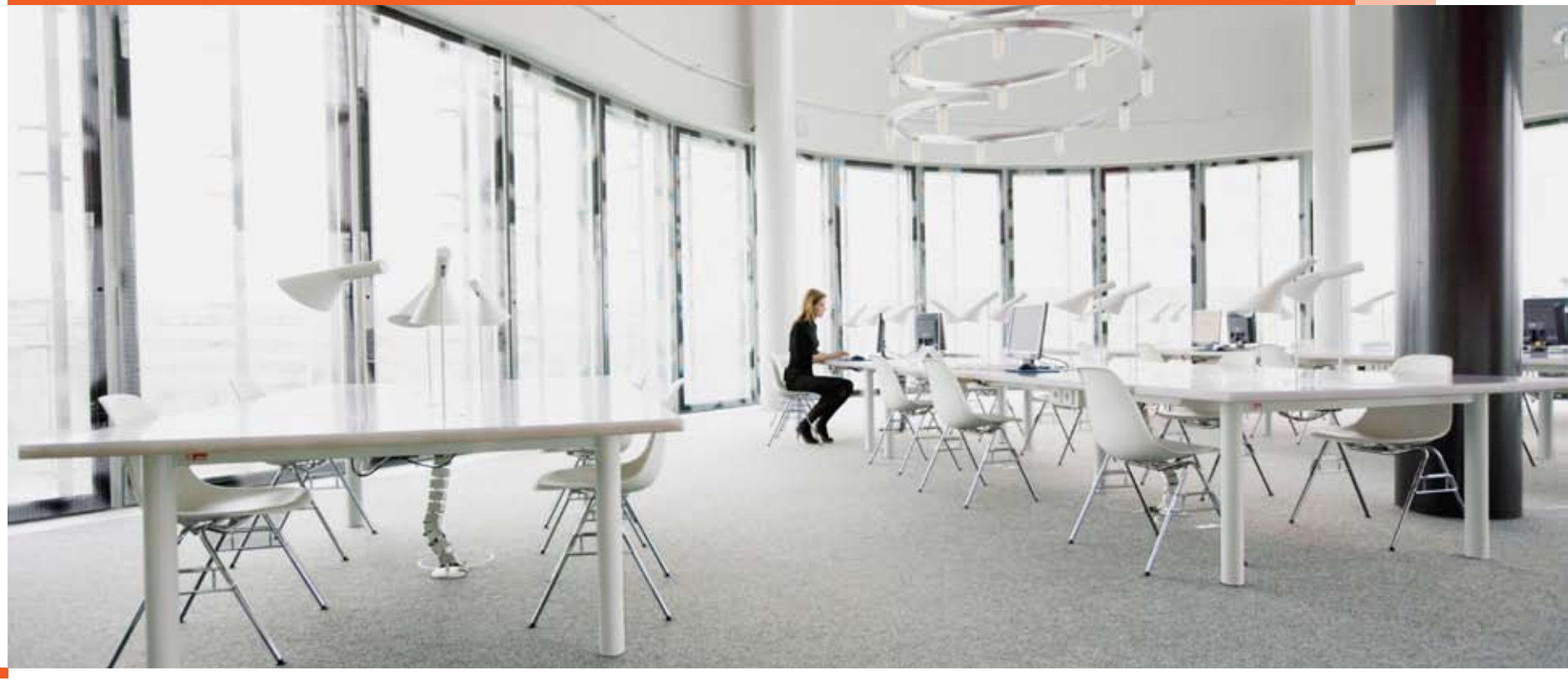
Cibercrimen: ¿Está su organización en riesgo?

Encuesta Global de Delitos Económicos 2011

3.877 entrevistas a organizaciones en 78 países ofrecen una panorámica global del crimen económico

Edición Venezuela
Febrero 2012



pwc

Espiñeira, Sheldon y Asociados

Indice

Haga click en los enlaces para navegar
a través del documento

Para visualizar los gráficos:

- *Haga click sobre el gráfico para ampliarlo.*

- *Para volver a la visualización normal, haga click en retorno*

Prefacio

Cibercrimen: una nueva y seria amenaza

Han pasado diez años desde que hicimos nuestra primera encuesta referente a crimen económico, y ha resultado ser una década bastante acontecida. Hemos visto en los titulares de prensa casos de fraudes multimillonarios, el inicio de la peor crisis económica desde 1930, y cómo la tecnología transforma nuestro estilo de vida y de hacer negocios.

En nuestras encuestas previas hemos reportado crimen económico durante la recesión y fraudes contables. Ahora observamos cómo el incremento de nuestra dependencia a la tecnología ha abierto las puertas a una nueva amenaza: El cibercrimen.

Diez años atrás, nuestra encuesta mostraba que muy pocas personas conocían el concepto de cibercrimen. Pero los reportes de este año indican que es uno de los primeros cuatro crímenes económicos, después de la apropiación indebida de activos, el fraude contable y el soborno/corrupción.

Las empresas enfrentan serias amenazas de 'cibercriminales' tanto internamente como externamente. Queda claro que la alta gerencia necesita tomar en serio estos riesgos: de manera preocupante cuatro de cada diez de los encuestados dicen que en su organización no tienen la capacidad para prevenir ni detectar el cibercrimen.

El fraude sigue creciendo

¿Qué hay del fraude en general? Dos años atrás, casi la mitad de nuestros encuestados pensaron que el fraude estaba en crecimiento. Ellos nos comentaron que existían más oportunidades para cometer fraude y más presiones para realizarlos, y estaban en lo correcto: nuestra encuesta del 2011 muestra que más organizaciones han afirmado haber sido víctimas de fraudes y consideran que esta situación seguirá en aumento.

En conclusión, pasado estos diez años el crimen económico todavía sigue siendo una amenaza.

Esperamos que nuestro reporte los ayude a encontrar instrumentos para combatirlo.

Tony Parton
Socio, Servicios Forenses, PwC UK

Una nota de nuestro asociado académico

He tenido la oportunidad de asesorar a PwC[1] en el desarrollo de su Sexta Encuesta Global de Delitos Económicos. Tanto los negocios como las comunidades académicas dependen de la confianza y de la información imparcial para avanzar en el estudio de este tópico.

El valor de esta encuesta se puede establecer en los siguientes elementos:

- Está basada en la percepción de cerca de cuatro mil individuos conocedores de la materia alrededor del mundo;
- Tuvimos gran cuidado en la elaboración de las preguntas y en cómo cada una se debía presentar en el cuestionario Web, incluyendo el asegurar que el encuestado tuviese presente las definiciones que fueron tomadas en cuenta; y finalmente,
- Realizamos una extensiva revisión de las respuestas.

Existen importantes y numerosos problemas en la evaluación de los riesgos del cibercrimen: generalmente estos no tienen una definición específica; el mismo evento puede ser calificado como “espionaje industrial”, “robo de IP” y a la vez cibercrimen.

Y cuando viene la evaluación de la pérdida, ¿Se limita a demostrar los costos del fraude, o se consideran los costos correctivos y el daño a la reputación?, y si es así ¿cómo lo mides?

Es esencial que la alta gerencia conozca realmente los riesgos y las oportunidades del “cibermundo”.

Esta encuesta global provee invaluable puntos de vistas dentro de los riesgos del cibercrimen en la actualidad

Peter Sommer
Profesor Visitante del Departamento de Gestión (Sistema de Información y el Grupo de la Innovación) en *London School of Economics and Political Science*, y Lector Visitante de la Facultad de Matemáticas, Informática y Tecnología, *Open University,* Reino Unido

1 PwC se refiere a la red de firmas miembro de PricewaterhouseCoopers International Limited (PwCIL) o, según el contexto, las empresas miembros de la red de PwC.

Una nota de nuestro socio local

En un esfuerzo sin precedentes, PwC ha liderado la sexta edición de la Encuesta Global de Delitos Económicos, donde hemos alcanzado una participación muy importante en Latinoamérica, y en el caso particular de Venezuela, hemos superado las metas propuestas para esta edición, lo cual nos permite conocer y contrastar la realidad local con las tendencias de la región y las globales.

Entre los aspectos más resaltantes surgidos de esta edición para el caso Venezuela, es la similitud de los resultados con respecto a la región: Las principales preocupaciones y tendencias del crimen económico en general son áreas de coincidencia para los negocios en Latinoamérica.

Sin embargo destaca de manera importante la incertidumbre que el encuestado venezolano manifiesta en relación a si ha sido víctima del fraude, superando notablemente los valores de la región.

Por otro lado la coincidencia con los resultados globales en cuanto a el cibercrimen es un punto interesante de los resultados, lo cual demuestra que, pese a las particularidades de nuestra economía y el incipiente desarrollo de los negocios electrónicos, la globalización también aplica también al cibercrimen.

Es para nosotros motivo de orgullo compartir con Usted la información que aquí presentamos. Esperamos que estos resultados le ayuden a obtener un mejor entendimiento del crimen económico, y cómo enfrentarlo.

Agradecemos a los más de 3.800 participantes, quienes compartieron sus opiniones sobre el tema, y particularmente a los participantes de empresas que operan en Venezuela, quienes hicieron posible presentar estos resultados.

Roberto Sánchez V.
Socio de Consultoría Gerencial
PwC Espiñeira, Sheldon y Asociados

Sumario

Los crímenes económicos son un problema grave que afecta a las organizaciones en todo el mundo, y ningún sector es inmune a éste. Las consecuencias del fraude no son sólo los costos directos; los daños colaterales y costos de recuperación pueden afectar a una organización en su núcleo. Los efectos pueden dañar seriamente la percepción de una marca, lo que puede ocasionar una pérdida significativa de su cuota de mercado. Así mismo, la sociedad global se está volviendo menos tolerante con la conducta poco ética, por lo cual las empresas deben asegurarse de poner énfasis en fomentar la confianza pública.

Para ayudar a entender y enfrentar estos problemas, nos complace presentar la sexta Encuesta Mundial de Delitos Económicos 2011. Ésta se enfoca en la creciente amenaza de la delincuencia informática en un mundo donde la mayoría de los individuos y las empresas dependen de Internet y tecnologías relacionadas, exponiéndose a los riesgos de ataques de criminales globales.

En el contexto de los incidentes que causan aumento de las pérdidas o robo de datos, virus informáticos y la piratería, nuestro estudio examinó la importancia e impacto de este tipo emergente de delitos económicos y la forma en que afectan a las empresas mundialmente y determinar tendencias a largo plazo.

La Encuesta Global de Delitos Económicos (GECS por sus siglas en inglés) 2011 fue completada por 3.877 encuestados en 72 países. Del total de encuestados, el 53% corresponden a personal de la alta gerencia, 36% representado por compañías que cotizan en el mercado de valores y 38% representa compañías con más de 1.000 empleados.

Tan amplia gama de encuestados nos permitió llevar a cabo un análisis profundo y comparado con estudios previos para establecer tendencias y comportamientos.

A nivel mundial, el 34% de los encuestados informaron haber sufrido uno o más tipos de delitos económicos en los últimos 12 meses.

De este grupo de afectados, uno de cada cuatro declaró haber sido objeto de un cibercrimen en los últimos 12 meses y casi la mitad del total de encuestados señaló una creciente preocupación sobre el cibercrimen.

El informe global de este año se divide en dos secciones:

- Cibercrimen - Cómo está impactando en las organizaciones, su conocimiento de los hechos y las acciones que se están tomando para combatir los riesgos, y
- El entorno actual del crimen económico - se centra en el tipo de fraudes cometidos y la forma en que se detectan; quienes los cometen y cuáles son las repercusiones.

Poniendo la lupa en el cibercrimen

La GECS 2011 se enfocó en la delincuencia financiera, los aspectos del cibercrimen y el fraude. A los efectos de nuestra encuesta, el cibercrimen se ha definido de la siguiente forma:

"El cibercrimen, también conocido como el delito informático, es un delito económico cometido mediante el uso de tecnología. Casos típicos de la delincuencia informática son la distribución de virus, las descargas ilegales de medios, el phishing[2] , el pharming[3] y el robo de información personal, como datos bancarios. Esto excluye el fraude "tradicional" en el que un computador ha sido un medio secundario para el fraude y sólo incluye aquellos delitos económicos en los cuales el computador, Internet o el uso de medios y dispositivos electrónicos es el elemento principal y no uno incidental" [4].

La definición anterior puede considerarse como muy general y obedece a que es un fenómeno amplio que presenta connotaciones diferentes para muchas personas.

Por ejemplo, un ejecutivo de ventas que extrae información sensible de mercadeo y ventas de su actual empleo mediante dispositivos removibles antes de comenzar a trabajar con una empresa competidora, puede haber cometido varios delitos: Se puede calificar como un robo de propiedad intelectual, cibercrimen o ambos.

No existe una definición mundialmente aceptada de cibercrimen, y ello dificulta tomar conciencias sobre sus riesgos, de donde proviene, cómo pueden afectar el negocio, y en consecuencia se hace más difícil detectar y combatir.

En esencia, si el concepto de la amenaza es difuso, los esfuerzos para luchar contra él podrían resultar ineficientes.

Algunas preguntas cuyas respuestas debemos conocer antes de establecer una estrategia contra este delito son: ¿es el cibercrimen más que un medio por el cual un estafador comete el acto ilegal?, ¿es un delito económico en sí mismo?, ¿deberían las organizaciones adoptar medidas concretas, más allá de la prevención del fraude y otros métodos de detección, para controlar este riesgo?

Nuestra encuesta de 2011 provee una visión sobre estos temas, y esperamos poder ayudarle a obtener estas respuestas.

2 Es un término que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

3 El pharming es un timo electrónico más peligroso que el phishing, siendo una variante de éste, y que tiene por objetivo la obtención de las claves bancarias del consumidor a través de Internet.

4 Como fue definido en GECS 2011 por PwC en conjunto con nuestros socio académico, Profesor Peter Sommer.

Poniendo la lupa en el cibercrimen

Principales tipos de cibercrimen

Desde el punto de vista de PwC, existen cinco tipos principales de cibercrimen, cada uno con sus propios métodos y objetivos, aunque a veces se superponen.

Ellos son:

La delincuencia financiera y el fraude

Se trata de criminales (a menudo altamente organizados y financiados) que utilizan la tecnología como una herramienta para el hurto.

Espionaje

Hoy en día, la propiedad intelectual corporativa incluye las comunicaciones electrónicas y datos, infraestructura de tecnología y resultados de las áreas de investigación y desarrollo.

El robo de propiedad intelectual es una amenaza constante, y las víctimas ni siquiera saben lo que ha sucedido hasta que se hace del dominio público una determinada situación, aparecen en el mercado productos en los cuales se estaba trabajando, o una patente sobre la base de sus actividades de investigación y desarrollo es registrada por otra empresa.

Actos de Guerra (Warfare)[5]

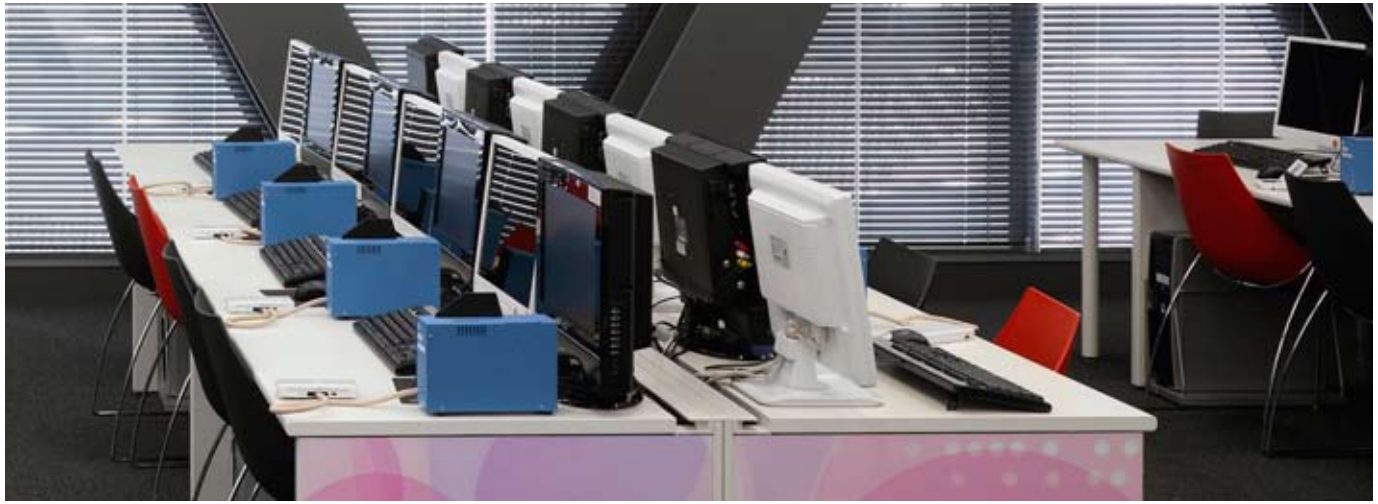
Esta puede tener lugar entre Estados, o puede implicar a Estados atacando organizaciones del sector privado o infraestructura crítica nacional como Energía, Telecomunicaciones y el Sistema Financiero.

Terrorismo[5]

Los ataques son realizados por grupos terroristas (posiblemente respaldados por un Estado), dirigidos ya sea a otro Estado o bienes privados, y a menudo a infraestructuras críticas.

Activismo

Esto puede coincidir con otras categorías, pero los ataques se llevan a cabo por los partidarios de una causa.



5 El terrorismo y el “warfare” son los tipos de ataques cibernéticos que han sido incluidos para efecto de definición, pero no están considerados en el alcance de este estudio, el cual se centra en los delitos económicos.

Poniendo la lupa en el cibercrimen

El cibercrimen entra en escena

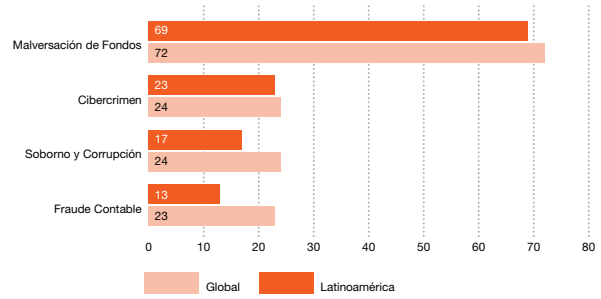
De acuerdo con nuestra encuesta, el cibercrimen está entre los principales cuatro delitos económicos, ligeramente detrás de fraude contable, el soborno y la corrupción.

En nuestros estudios anteriores, cuando realizabamos la pregunta sobre si habían experimentado delitos informáticos, la respuesta de los encuestados arrojaba resultados muy bajos y estadísticamente insignificantes, y por ello quedaban agrupados bajo "otros tipos de fraude".

Este año nos focalizamos en el cibercrimen y se reintrodujo como tipo de delito en la pregunta correspondiente, preguntando a los encuestados si habían sufrido un ataque de este tipo en los últimos 12 meses.

En Latinoamérica, uno de cada cuatro encuestados fue víctima de un delito, y afirmó haber experimentado uno o más incidentes de cibercrimen en los últimos 12 meses. [Figura 1]

Figura 1: Los cuatro tipos de delitos económicos reportados en Latinoamérica



% de encuestados que sufrieron un crimen económico en los pasados 12 meses

¿Cómo y por qué los delitos informáticos se han convertido en uno de los tipos principales de fraude?

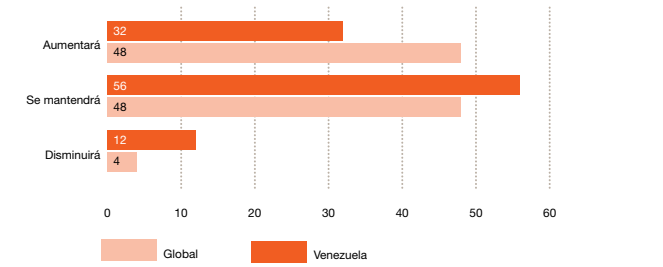
Algunas de las posibles razones podrían ser:

- El aumento de la atención por parte de los medios en torno a casos recientes de cibercrimen, dando lugar a una mayor conciencia sobre este tipo de fraude
- Partiendo de la razón anterior, y dada la ambigüedad en torno a la definición de cibercrimen y lo que constituye, los encuestados pudieron haber clasificado algunas de las formas más tradicionales de delitos económicos como un cibercrimen, bajo la premisa que estos fueron cometidos mediante el uso de un computador, dispositivos electrónicos o Internet
- Una mayor atención de los entes reguladores
- Los avances de la tecnología aumentan su presencia en el entorno del negocio y podrían haber hecho más fácil cometer cibercrímenes.

Para el caso Venezuela, el 32% de los encuestados indicaron que perciben un incremento en el riesgo de cibercrimen, en tanto que sólo el 12% percibe una disminución, y el resto manifiesta permanecer en el mismo nivel.

Estos resultados contrastan sensiblemente con los resultados globales, donde 48% de los encuestados percibieron un aumento en el riesgo, en tanto que sólo un 4% percibió una disminución. Esto indica que 2 de cada 3 encuestados en Venezuela pueden estar subestimando los riesgos del cibercrimen. [Figura 2]

Figura 2: Percepción de los riesgos del cribercrimen en los próximos 12 meses



% de encuestados que perciben riesgos de cibercrimen en los próximos 12 meses

Poniendo la lupa en el cibercrimen

Bajo riesgo y alta rentabilidad para el cibercriminal: una mezcla explosiva

La dinámica del cibercrimen es diferente a otros delitos económicos convencionales. Estos delitos pueden tener una gama diferente de motivos, tales como la ventaja competitiva, una demostración de fuerza y conocimiento, o la curiosidad de penetrar en un sistema y sortear los controles y normas establecidas.

Hemos analizado y evaluado los incentivos y las oportunidades relacionados con el cibercrimen, y contrastamos esto con los riesgos y beneficios de delitos económicos convencionales.

Tomemos por ejemplo un robo a un banco. El autor toma una serie de riesgos significativos con el fin de llevar a cabo el crimen:

- Presencia física en el lugar, la cual lo expone a su captura. Otros medios disuasorios como cámaras de circuito cerrado de televisión ("CCTV") y los sistemas de alarma de seguridad, aumentan los riesgos

- Agresor armado con un arma letal, la cual puede causar lesiones o muerte a aquellos que se interponen en el camino. Esta situación expone al autor a cargos criminales adicionales, tales como asesinato u homicidio.

En contraposición, cuando un atacante se infiltra en un sistema bancario de forma remota para robar fondos, datos de clientes u otra información personal, toma menos riesgos:

- El delito puede ser cometido desde cualquier lugar y momento, es decir, el perpetrador no necesita estar físicamente presente, lo que reduce el riesgo de quedar atrapados en el acto o ser identificado;

- El autor no tiene que estar armado para llevar a cabo el acto y es improbable que cause daño físico a otros;

- Hay menos posibilidades de aplicación de la ley, dada la imposibilidad de identificar al autor o determinar donde se encontraba al momento de cometer el crimen.

- En la mayoría de los casos, el autor se encuentra en una jurisdicción diferente y, en muchos casos, fuera del país en el que ocurre el delito, lo cual dificulta las actividades de identificación y aprehensión del perpetrador. Además, en muchos países las leyes vigentes no son lo suficientemente maduras como para procesar a cibercriminales. A esto se suma los avances constantes y crecientes en tecnología, que rezagan aún más el marco jurídico.

Mientras robustecer las medidas preventivas es una necesidad para mitigar el riesgo de los delitos económicos tradicionales (p. ej. apropiación indebida de activos, fraude contable o el soborno y la corrupción), el rápido cambio de la tecnología hace difícil a las organizaciones utilizar estrategias similares y contar con lapsos holgados para prepararse preventivamente ante el cibercrimen, lo que amerita un enfoque pragmático para las estrategias.

Poniendo la lupa en el cibercrimen

¿Es realmente el cibercrimen una amenaza externa para las organizaciones venezolanas?

Desde el surgimiento de Internet, el cibercrimen en general ha sido percibido como una amenaza externa a nivel mundial. En Venezuela el 46% de los encuestados cree que el cibercrimen es más una amenaza externa que interna, en concordancia con los resultados globales.

Sin embargo, otro 23% (Global: 13%) de los encuestados venezolanos ve esto como una amenaza interna. Comparado con resultados anteriores, esto sugiere que la percepción del cibercrimen como un elemento exógeno está cambiando, y con ello se empieza a reconocer los riesgos internos.

Para los encuestados en Venezuela que indicaron que la amenaza del cibercrimen está dentro de su organización, el 69% indicó que el departamento de Finanzas es la fuente más probable, debido a la gran cantidad de información sensitiva que estos manejan, seguido por el departamento de tecnología de la información ("TI") con un 63%, esta situación no es de extrañar ya que el personal que pertenece a este departamento cuenta con los conocimientos, habilidades y oportunidades para llevar a cabo tales crímenes.

Además, el personal de TI puede tener acceso a "super usuarios" que poseen derechos administrativos para acceder a los sistemas y la capacidad de eliminar pistas de auditoría, reduciendo la posibilidad de ser imputado.

También nuestros encuestados locales reconocen el hecho que los riesgos del cibercrimen no se limitan únicamente a estos dos departamentos, sino que otras áreas como las de operaciones (37%), Ventas y Marketing (31%) y seguridad física/lógica (25%) representan un riesgo. Los departamentos de Recursos Humanos (14%) y Legal (11%) se consideran como los responsables internos menos probables de cometer este tipo de delitos.

Sin embargo, es importante que esos departamentos no sean ignorados, dado que el delito puede provenir desde cualquier lugar, por ejemplo, un empleado malicioso o un equipo comprometido.

Para ilustrar esto, hemos expuesto algunos ejemplos de potenciales cibercrímenes. Algunos de estos ejemplos contienen elementos de otras formas de delincuencia económica:

1. Empleado descontento accede a los datos de recursos humanos para extraer información personal con respecto a determinados empleados, tales como salarios, bonos y otros beneficios y utiliza esta para su beneficio;
2. Un empleado accede a mensajes de correo electrónico de un colega y envía correos electrónicos maliciosos de esta cuenta, intimidando a otros miembros del personal ("cyber-bullying");

3 Extraer información clave en el departamento de cuentas por pagar a través de correo electrónico, creación de proveedores "fantasmas" y la extracción de fondos de la compañía por esta vía.

4. Uso inapropiado de las redes sociales – Información sensible hecha pública. Intercambio de información entre "amigos" o conexiones -, mientras se está trabajando.

¿Son estos estrictamente cibercrímenes, o son formas de delincuencia económica donde la computadora y el Internet son sólo un medio para un fin?

Independientemente de la ambigüedad en torno a la definición de cibercrimen, lo que se desprende de nuestros resultados es que esta amenaza no es exclusiva del departamento de TI, sino que puede provenir de cualquier departamento de la organización.

Poniendo la lupa en el cibercrimen

¿De dónde proviene la amenaza externa?

Como se destacó anteriormente, muchos de los encuestados perciben que el cibercrimen es una amenaza externa. En este sentido, preguntamos a los encuestados si consideraban el riesgo del cibercrimen como algo generalizado dentro de su país y cuáles creían eran los países que mayor amenaza representaban. Para el caso Venezuela, los siguientes cinco países destacaron en la percepción de origen de ciberataques hacia Venezuela. [Figura 3]

Figura 3: Top de los cinco países que fueron percibidos como orígenes para perpetrar un cibercrimen en Venezuela

1	USA	67%
2	Hong Kong y China	26%
3	Rusia	22%
4	Colombia	15%
5	Brasil	22%

Este resultado corrobora claramente que el cibercrimen es una amenaza global inmune a las distancias y las barreras lingüísticas, sólo requiriendo tener visibilidad sobre los objetivos de ataque en Internet.

Los autores del cibercrimen externo podrían además ser criminales organizados que operan desde varios lugares en el mundo.

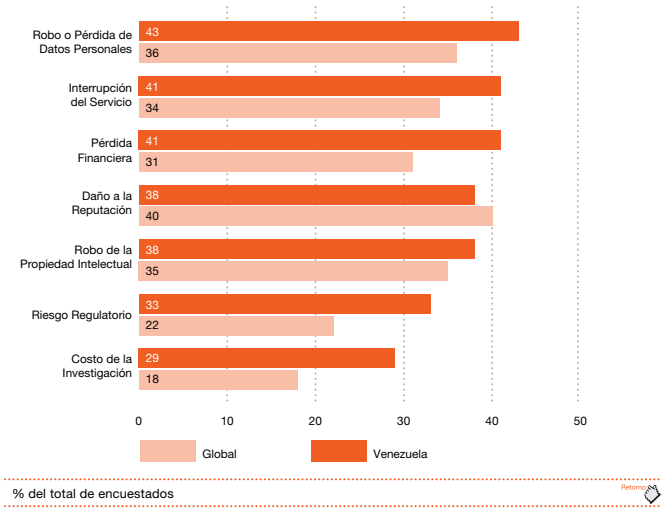
¿La reputación de su organización está en juego?

Nuestra encuesta indagó las preocupaciones sobre los efectos de la actividad del cibercrimen en las organizaciones venezolanas, específicamente sobre el daño a la reputación, pérdidas financieras, los costos de la investigación, el robo de propiedad intelectual, la interrupción del servicio y el robo o pérdida de datos personales.

En este sentido, 43% de los encuestados venezolanos (Global: 36%) indicó que el robo o pérdida de datos personales tiene un impacto significativo, contrastando con el resultado global, el cual indica el daño a la reputación como su principal preocupación (Global: 40%, Local: 38%).

Otros riesgos como las pérdidas financieras, interrupción de servicio y robo de propiedad intelectual también se consideran relevantes para los encuestados en general. [Figura 4]

Figura 4: Las preocupaciones en torno al cibercrimen en Venezuela y a nivel Global



Poniendo la lupa en el cibercrimen

Su organización puede estar paralizada ante este riesgo

Los datos demuestran que las organizaciones están haciendo muy poco al respecto y parecen ser más reactivas que proactivas a las amenazas del cibercrimen. A nivel global, los resultados indican que:

- Uno de cada cuatro encuestados no cuenta con las capacidades internas para hacer frente al cibercrimen.
- Uno de cada cuatro no tiene procedimientos de contención ante incidentes
- Dos de cada cinco no tienen capacidad para investigar internamente el cibercrimen
- Uno de cada dos no tiene en su organización acceso a investigadores forenses especialistas en tecnología

El monitoreo de las redes sociales por las empresas en Venezuela

El 57% de los encuestados afirmó que su organización no supervisa el uso de sitios de redes sociales o son conscientes de si su organización tiene que vigilarlos.

Este es un hallazgo relevante, ya que indica una baja percepción de los riesgos que estos sitios pueden representar para la organización.

Mientras que las redes sociales como Facebook, Twitter o LinkedIn pueden no ser la verdadera fuente de delitos económicos, estos son un medio eficaz para la ingeniería social. Por ejemplo, las redes sociales se pueden utilizar para recopilar información sobre un individuo, la investigación de ciertos miembros del personal o para operar software malicioso que procure información que permita suplantar la identidad de su víctima.

De los encuestados venezolanos que dijo que su organización está tomando medidas para prevenir los riesgos asociados al cibercrimen, 92% indicó realizarlo mediante el análisis del tráfico y seguimiento a páginas web (interna y externa) (Global: 85%), el 58% de los venezolanos encuestados indica haber establecido políticas sobre el uso adecuado de la información y documentación (Global: 62%), y el 31% mediante la puesta en marcha programas de concientización para los empleados sobre el uso apropiado de Internet (Global: 37%).

Como puede apreciarse en la comparación con los resultados globales, las organizaciones venezolanas no están muy lejanas con respecto a las medidas que actualmente están siendo tomadas por las organizaciones mundialmente.

En el perfil del cibercriminal interno, a menudo se asocia con la generación más joven de la organización, por su pericia con la tecnología y poco tiempo en la organización. Los resultados de la encuesta, se encuentran alineados con esta percepción:

- Empleados junior o gerencia media (67%)
- Menos de 40 años de edad (100%)
- Empleados que han estado en la organización por menos de 5 años (33%)

La generación más joven por lo general hace un uso amplio de las redes sociales y hay compañeros y presiones sociales para compartir información con otros. Por lo tanto, no se puede subestimar el riesgo y es necesario monitorear estos sitios antes que pueden crear problemas potenciales para las organizaciones desde una perspectiva del cibercrimen y el riesgo reputacional.

Es necesario agregar que las nuevas generaciones han crecido con las redes sociales y compartir información personal se ha convertido en la norma para ellos, por lo cual pueden tener una comprensión muy diferente de los riesgos que plantean estos sitios. Las organizaciones tienen que ser conscientes de esta realidad, y establecer esquemas novedosos de prevención y respuesta más allá de un simple bloqueo en el acceso a los sitios o la simple definición de políticas.

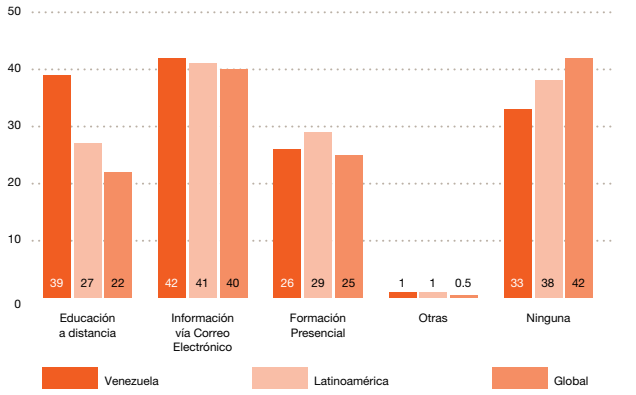
Poniendo la lupa en el cibercrimen

Manejando los riesgos del cibercrimen

Si bien los resultados de la encuesta indican que la percepción del cibercrimen va en aumento, 33% de los encuestados en Venezuela manifiesta no haber recibido formación en seguridad de información en los últimos 12 meses, lo que implica que, potencialmente, no poseen conocimiento o actualización sobre los riesgos que el cibercrimen representa para su organización.

Para capacitar a su personal, las organizaciones tienen gran variedad de medios a su disposición: En el caso Venezuela, 39% de los encuestados dijo haber recibido educación a distancia (e-learning), el 42% recibió información vía correo electrónico e invitaciones a eventos y el 26% recibió formación presencial[6]. [Ver figura 5].

Figura 5: Formación recibida en los últimos 12 meses acerca del Cibercrimen

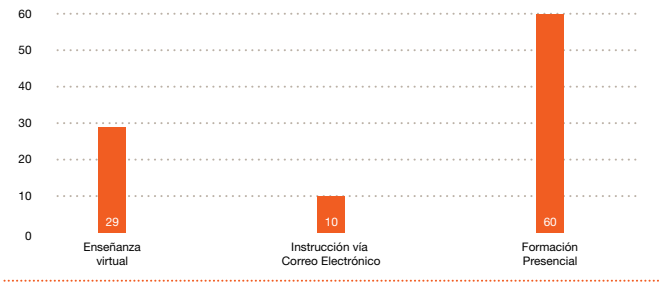


No es sorprendente ver que sólo algunos encuestados han recibido capacitación presencial, ya que se considera generalmente la más costosa y difícil de gestionar.

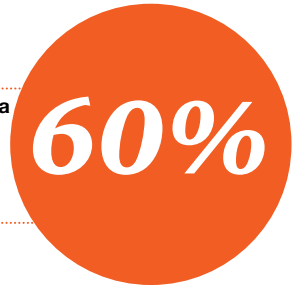
A la luz de los recortes presupuestarios en la mayoría de las organizaciones en los últimos 12 meses, los planes de formación probablemente se han visto afectados.

Sin embargo, el 60% de los encuestados venezolanos, al igual que a nivel global, clasificaron los cursos de formación presencial como la forma más eficaz para la formación y sensibilización sobre el cibercrimen [Ver figura 6].

Figura 6: Tipo de formación que se percibe como la más efectiva para capacitar sobre el cibercrimen en Venezuela



El 60% de los encuestados en Venezuela señaló los cursos de formación presencial como la herramienta más eficaz para formar y sensibilizar acerca del cibercrimen



6 Las actividades de formación presencial se aquellas que se llevan a cabo *in situ,* como presentaciones, reuniones en equipo, talleres, seminarios, etc.

El fraude, el defraudador y la víctima

¿Quién tiene la responsabilidad de lidiar con el cibercrimen en su organización?

La seguridad de información sigue asumiéndose como un problema de TI, creando una brecha de comunicación entre los gerentes de empresas y profesionales de la seguridad. Hoy en día la seguridad de información no es sólo una cuestión técnica, sino un imperativo del negocio, y los resultados de nuestra Encuesta de Seguridad de la Información 2011[7] confirman el creciente reconocimiento sobre el valor estratégico de una seguridad de información alineada más con el negocio que con TI, para lo cual se requiere al CISO[8] reportando al CEO[9] en lugar de al CIO[10] .

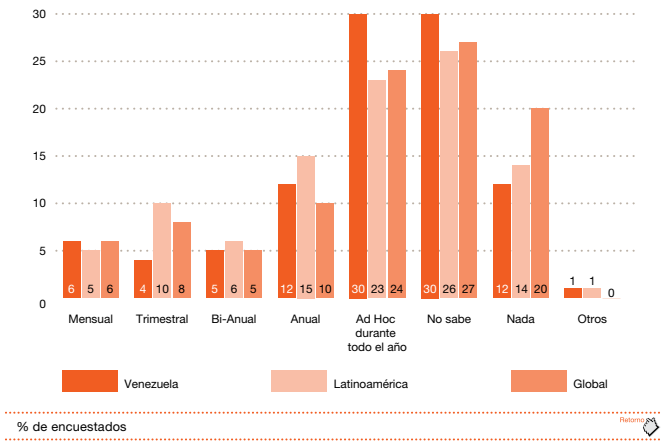
En esta encuesta, hemos estado evaluando el cibercrimen desde la perspectiva de delito económico en lugar de desde la perspectiva de la seguridad de la información y la comprensión de los sub-tipos de delitos económicos en lugar de una agrupación meramente técnica. Es por ello que llama la atención que los resultados indican que el 60% (Global: 54%) de los encuestados en Venezuela cree que la responsabilidad de gestionar el cibercrimen dentro de la organización recae en el CIO, y sólo el 14% (Global: 21%) afirma que la responsabilidad máxima recae en el CEO o la Junta.

Si bien los riesgos relacionados con TI son inherentes a la función de TI, el cibercrimen es un delito económico, y como tal es necesario que la alta gerencia se involucre y evalúe su gestión de manera regular.

Los resultados anteriores son consistentes con el hecho que el CEO y la Junta no realizan evaluaciones regulares sobre los riesgos del cibercrimen en las organizaciones venezolanas: 27% de los encuestados informó que revisan estos riesgos por lo menos una vez al año (Global: 36% Latinoamérica: 28%), 30% realizan evaluaciones “ad hoc” (Global: 23% , Latinoamérica: 24%) y un elevado 43% afirmó no contar o saber sobre evaluaciones de esta índole (Global: 41%, Latinoamérica: 48%).
[Ver figura 7].

Se plantea entonces la necesidad de un mayor involucramiento de la alta gerencia en la gestión de las amenazas reales que los fraudes generados por el cibercrimen presentan a sus organizaciones. El CEO requiere afrontar las amenazas de Internet, y su liderazgo en esta materia le permitirá gestionar mejor los riesgos y oportunidades en el cibermundo, que en el futuro inmediato será una característica definitoria de las organizaciones líderes.

Figura 7: Frecuencia de la revisión de los riesgos del cibercrimen por el CEO y la Junta



7 http://www.pwc.com/crimesurvey
8 Chief Security Officer
9 Chief Executive Officer
10 Chief Information Officer

El fraude, el defraudador y la víctima

Un problema global

De los 3.877 encuestados a nivel mundial, el 34% reportó haber sido víctima de uno o más delitos económicos en los últimos 12 meses, lo que representa un incremento del 4% sobre los resultados del 2009.

Si analizamos la figura 8 se observa además que Latinoamérica supera el promedio mundial, y sin embargo Venezuela se encuentra por debajo de este promedio. Si bien esto pareciera un resultado favorable, un 25% de los encuestados en Venezuela, no tenían certeza si su organización estuvo expuesta al fraude, lo cual indica el nivel de incertidumbre, probablemente asociado al desconocimiento o carencia de recursos para identificarlo.

¿Cuál es el panorama mundial?

La figura 9 muestra que tanto los países desarrollados como las economías en crecimiento reportaron fraudes. Llama la atención algunas economías emergentes que reportaron bajos niveles de fraude: Indonesia, India, Rumania y Grecia.

En estos casos, podría asumirse que lo resultados obedecen a métodos de detección de fraudes ineficaces o la reticencia del encuestado en admitir su ocurrencia

Figura 8: La experiencia de los delitos económicos a nivel global

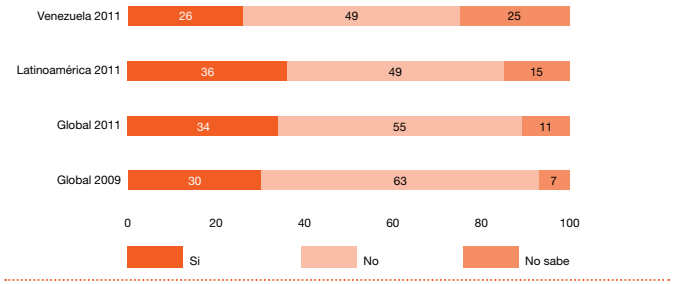


Figura 9: Fraude reportado por territorio

Territories que reportaron altos niveles de fraude (<40%)	% Encuestados 2011	% Encuestados 2009
Kenya	66%	57%
Sur Africa	60%	62%
Reino Unido	51%	43%
Nueva Zelanda	50%	42%
España	47%	35%
Australia	47%	40%
Argentina	46%	39%
Francia	46%	29%
Estados Unidos	45%	35%
Malasia	44%	28%
México	40%	51%
Territories que reportaron bajos niveles de fraude (>25%)	**% Encuestados 2011**	**% Encuestados 2009**
Rumania	24%	16%
India	24%	18%
Suecia	22%	19%
Eslovaquia	21%	29%
Turquía	20%	15%
Suiza	18%	17%
Holanda	17%	15%
Italia	17%	19%
Grecia	17%	23%
Eslovenia	17%	(no participó)
Indonesia	16%	18%
Japón	6%	10%

El fraude, el defraudador y la víctima

¿Existen sectores más proclives al Fraude?

La delincuencia económica afecta a todos los sectores de la industria. Sin embargo algunos se ven más afectados que otros. A continuación se muestran las cifras obtenidas en los resultados globales. [Figura 10]

A nivel mundial, vemos que los sectores más afectados son Comunicaciones y el sector de Seguros (48%), seguidas por las empresas estatales (46%).

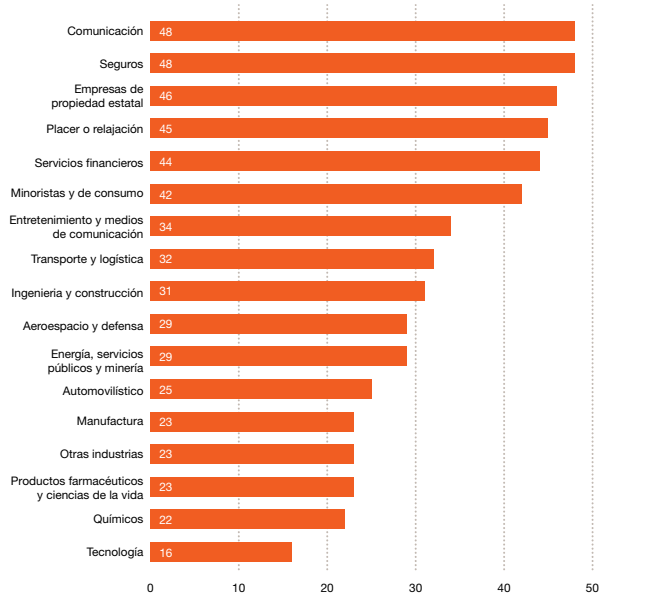
Históricamente, los sectores altamente regulados han reportado un mayor número de incidentes.

Esto es consecuencia de las obligaciones de transparencia y control impuestas por los organismos reguladores. Otros sectores son menos proclives a informar, y en muchos casos se encuentran menos preparados para identificar este tipo de incidentes, e incluso asumen las pérdidas por delitos económicos como algo inherente al sector incorporándolas a sus costos operativos.

¿Qué organizaciones están experimentando los fraudes?

Existe una importante correlación entre el tamaño de la organización (medida por el número de empleados) y la cantidad de incidentes de fraude reportados [Figura 11]. Así lo indican los resultados globales. Los resultados locales sin embargo muestran un comportamiento inusual, pero constante en el tiempo, donde se presenta una reducción importante en las empresas de más de cinco mil empleados.

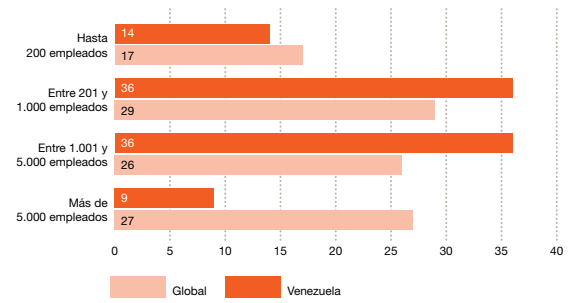
Figura 10: Fraude por sector industrial



% de encuestados representantes de sectores industriales

Nuestra interpretación apunta a que las grandes empresas tienen más éxito en la identificación y prevención de fallas, ya que tienden a dedicar más recursos y personal para la detección y su prevención.

Figura 11: Fraudes reportados basados en el tamaño de la organización en Venezuela



% de encuestados

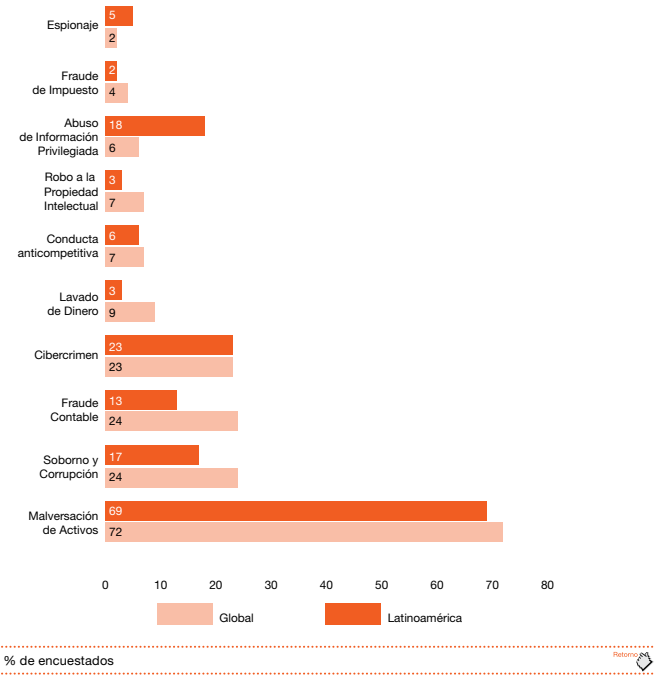
Los resultados que se muestran en la figura 11 confirman que las organizaciones entre 200 y 5.000 empleados son más propensas a sufrir el fraude. Una de las posibles razones de los altos niveles de fraude reportados en estas organizaciones podría ser su mejor capacidad para detectarlos o el cúmulo de tener un gran volumen en activos y un bajo esquema de control, hipótesis que también apalancaría la reducción identificada en empresas con más de 5.000 empleados. En general, las grandes organizaciones tienden a dedicar más recursos y personal para la detección y prevención de fraudes cometidos contra la organización, y esto también puede explicar este comportamiento.

El fraude, el defraudador y la víctima

Tipos de delitos económicos

El crimen económico puede adoptar muchas formas diferentes, siendo algunos más comunes y persistentes que otras. La figura 12 muestra los diferentes tipos de delitos económicos experimentados por los encuestados en Latinoamérica durante los últimos 12 meses.

Figura 12: Tipos de crímenes económicos



La figura 12 muestra que los tres tipos más comunes de los delitos económicos experimentados en los últimos 12 meses fueron la malversación de activos, soborno y corrupción, fraude contable y el cibercrimen

Un dato que llama la atención, es que a nivel global el fraude contable ha tenido un retroceso del 39% con respecto a los resultados del 2009, retornando a los valores reportados en el año 2005. Algunos de los argumentos en relación con esta disminución pueden ser:

- El fortalecimiento del control interno
- Mayor intervención de los organismos reguladores y sanciones más punitivas para el involucrado
- En nuestra encuesta de 2009, se observó un incremento inusual en este rubro. Algunas estadísticas asocian este fenómeno con la necesidad de las organizaciones, en aquel entonces, a sobrevivir en un escenario de crisis y la presión de la alta gerencia para alcanzar unas metas afectadas por la crisis.
- Organizaciones menos capacitadas para detectar el fraude: La reducción de personal genera un cúmulo de trabajos y funciones en el capital humano, generando en éste la presión/oportunidad de incurrir en este tipo de delitos

A nivel mundial, uno de cada cuatro afectados por un crimen económico fueron víctimas de fraudes y corrupción.

Los sectores con mayores índices son Energía, Utilities y Minería (40%), Construcción (35%) y Comunicaciones (34%).

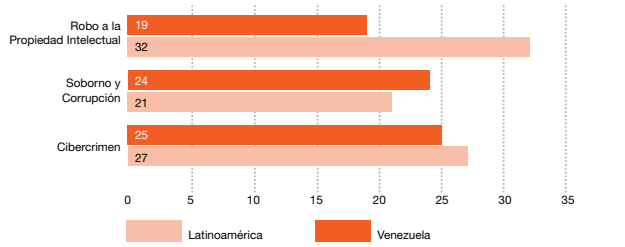
El fraude, el defraudador y la víctima

Más fraude se avecina en Venezuela

El 25% de los encuestados cree que su organización es susceptible al fraude dentro de los próximos 12 meses.

Del mismo modo, el 25% y 24% de los encuestados creen que sus organizaciones pueden verse envueltas en casos de cibercrimen o soborno/corrupción, respectivamente (ver figura 13).

Figura 13: Percepción de fraude en Venezuela vs. Latinoamérica



% de encuestados

Costo de los daños colaterales y el fraude en Latinoamérica

Es muy difícil medir el impacto financiero de la delincuencia económica. Sin embargo, preguntamos a nuestros encuestados para estimar, en la mayor medida posible, el costo del fraude.

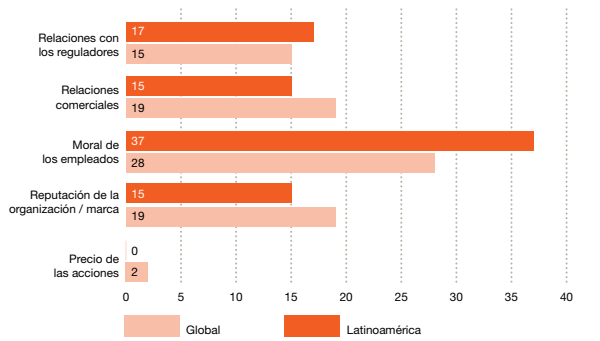
Del total de los encuestados que informaron haber sido objeto de los delitos económicos en los últimos 12 meses en Latinoamérica, uno de cada tres reportó pérdidas de hasta 5 millones de dólares.

Sin embargo, los costos pueden ser muy superiores en algunos casos: 10% de los encuestados que afirmaron ser víctimas del fraude han perdido hasta un millardo de dólares.

A nivel global, uno de cada cinco de los que fueron víctimas del soborno y la corrupción perdieron más de cinco millones de dólares.

Además de las pérdidas directas, nuestro estudio investigó el daño colateral que sufren las organizaciones y se les preguntó sobre el impacto del crimen económico en su reputación / marca, precio de la acción, la moral del empleado, las relaciones comerciales, y las relaciones con los reguladores (ver figura 14).

Figura 14: Daños colaterales en Latinoamérica



% de encuestados que reportaron fraudes

Si bien es difícil de medir, de los que reportaron delitos económicos en Latinoamérica, como resultado de un fraude, un 37% ve un impacto significativo en la moral de los empleados (Global: 28%), el 17% considera que las relaciones con los reguladores pueden ser perjudicadas de manera significativa (Global: 15%) y un 15% menciona la reputación de la organización/ marca como afectada (Global: 19%).

El fraude, el defraudador y la víctima

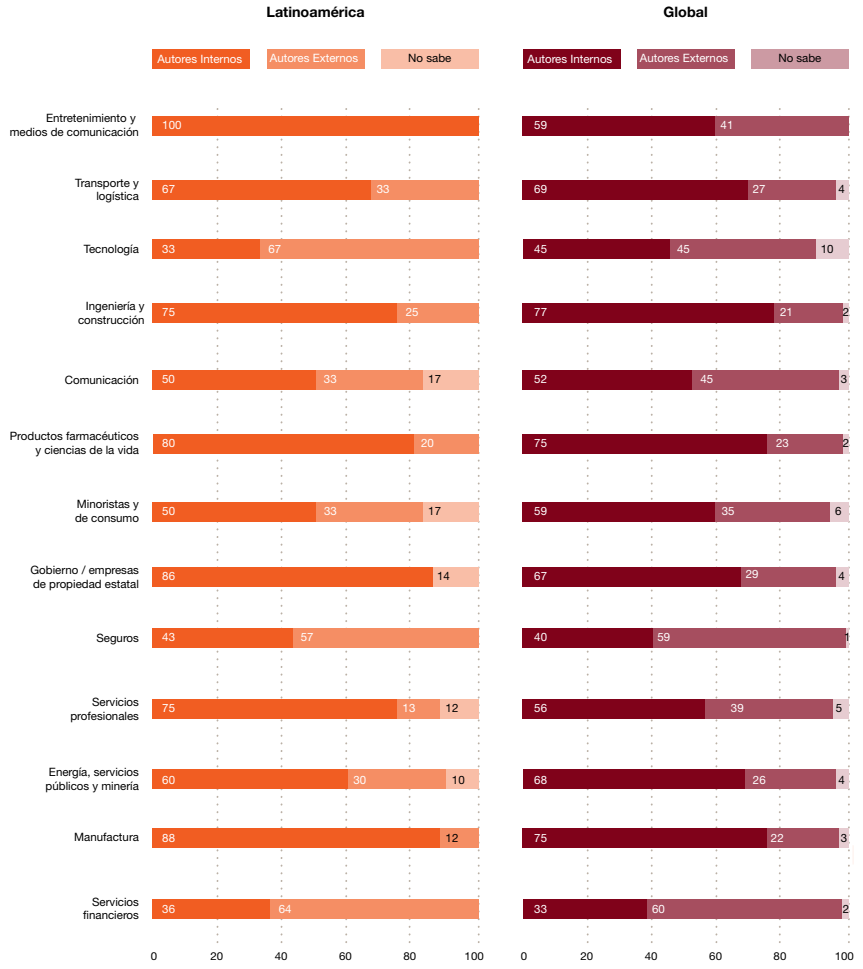
¿Quién está cometiendo el fraude?

Un aspecto importante en la lucha contra la delincuencia económica es la recopilación de información, tanta como sea posible, sobre los autores del fraude. A medida que aumenta el nivel de fraude, la estrategia reactiva se hace ineficiente.

En consecuencia las organizaciones necesitan ser proactivas en sus esfuerzos por fortalecerse ante estos ataques. En Latinoamérica, de los encuestados que han sufrido delitos económicos, 64% dijo que el origen del mismo fue interno (Global: 56%), y 32% indicó un fraude externo (Global: 40%).

En todos los sectores de la industria latinoamericana, la mayoría de los principales autores eran internos, sin embargo, cuando analizamos las respuestas por sector de actividad, observamos que hay cuatro sectores que indicaron que sus fraudes más significativos fueron cometidos por autores externos: servicios financieros, seguros, tecnología y comunicaciones, situación que es consistente con los resultados globales (ver figura 15)

Figura 15: Autores de Fraude– por industria



% de encuestados que sufrieron un crimen económico en los pasados 12 meses

El fraude, el defraudador y la víctima

El perfil de los autores del fraude interno

Conocer el perfil del estafador y su origen puede ser instructivo a la hora de identificar debilidades en los mecanismos de respuesta y controles internos de una organización.

Consultamos a nuestros encuestados que reportaron haber sufrido al menos un delito económico, sobre el perfil del responsable del fraude sufrido en su organización en los últimos 12 meses.

La figura 16 muestra las características típicas de los autores del fraude interno de acuerdo a nuestra encuesta.

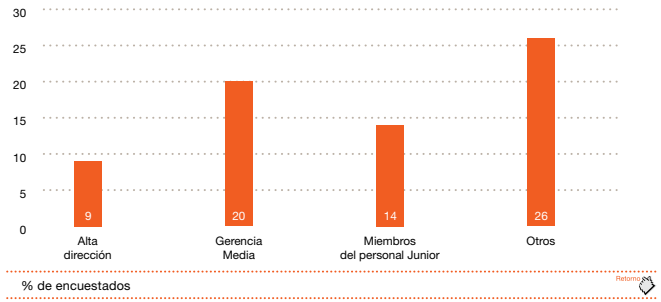
Figura 16: Perfil típico de un estafador interno en Latinoamérica

• Masculino	83%
• Entre 31 y 40 años de edad	55%
• Con título universitario	42%
• Entre 3 y 5 años en la organización	34%

Un detalle importante encontrado en nuestra encuesta fue que 8% de los encuestados latinoamericanos y 10% a nivel mundial que habían sido objeto de delitos económicos por un fraude interno, no sabían por cuánto tiempo el autor había estado trabajando en la organización.

Proporcionalmente, las probabilidades apuntan al ataque interno como el mayor riesgo, y es allí donde debe enfocarse el control. Para ahondar sobre el perfil del defraudador que labora en nuestra organización, consultamos más datos sobre su rol dentro de la organización. La Figura 17 muestra el perfil de cargo resultante de nuestra encuesta.

Figura 17: Defraudador interno

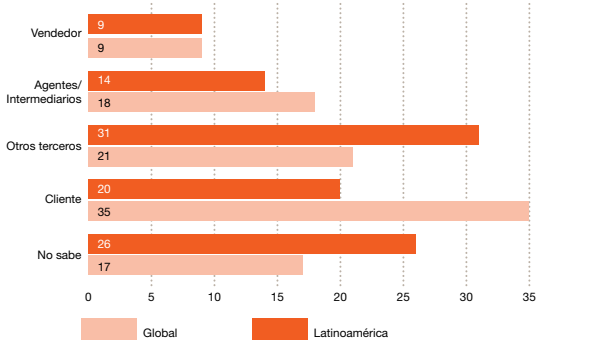


El fraude, el defraudador y la víctima

El perfil de los autores del fraude externo

De los participantes que comunicaron que fueron atacados por autores externos en Latinoamérica, el 20% (Global: 35%) fue objeto de fraude por parte de clientes y el 16% (Global: 18%)por parte de agentes o intermediarios. Se pudo observar que un 26% (Global: 17%) manifestó no saber. Aunque puede ser difícil recoger información sobre un fraude externo, aquellas organizaciones que llevan a cabo una investigación a fondo tienen una mayor posibilidad de identificar al autor. (Ver figura 18)

Figura 18: Defraudador externo



% de encuestados que perciben riesgos de cibercrimen en los próximos 12 meses

El fraude, el defraudador y la víctima

El perfil de los autores del fraude externo *(cont.)*

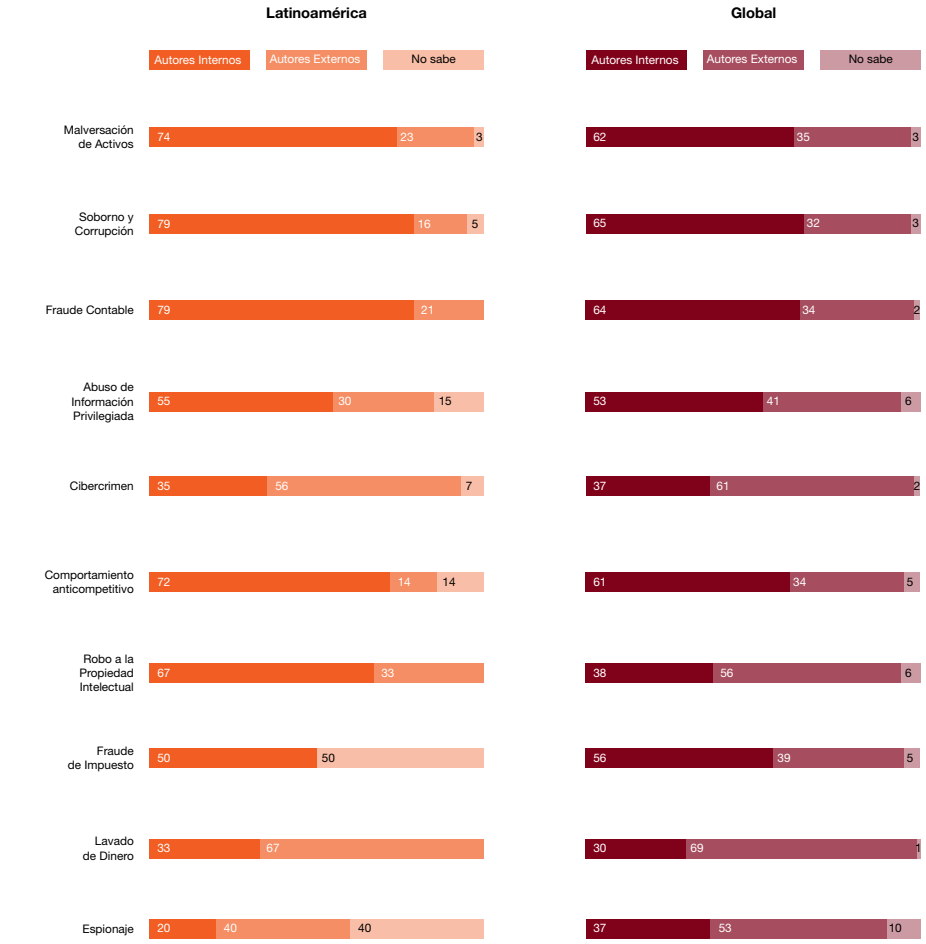
Los delitos económicos más comúnmente perpetrados por un desconocido fueron los delitos informáticos y la apropiación indebida de activos. El cibercrimen es a menudo perpetrado por el crimen organizado, quienes protegen su identidad amparados en el anonimato de la red, y en consecuencia no es de extrañar que las organizaciones víctimas desconozcan el perfil del autor. Por otro lado, los delitos como la malversación de activos, fraude contable y el soborno y la corrupción son más frecuentes cometidos por los responsables internos.

Sin embargo, la apropiación indebida de activos y el espionaje también fueron cometidos por un número significativo de los defraudadores externos desconocidos para la organización, lo que demuestra que los controles de detección no están funcionando correctamente (ver figura 19).

Una de las mejores maneras de prevenir el fraude, es saber con quién usted está haciendo negocios (clientes, proveedores y agentes).

Desde hace mucho tiempo se ha reconocido que “El fraude se esconde tras las sombra”, por lo que programas de transparencia, tales como “Conoce a las personas con las que haces negocio” siguen siendo una de las herramientas preventivas más eficaces en las organizaciones.

Figure 19: Autores de delito económico- por tipo de fraude



% de encuestados que sufrieron un crimen económico en los pasados 12 meses

El fraude, el defraudador y la víctima

¿Qué acciones toman las organizaciones en contra de los autores del fraude?

Una vez que un caso de delincuencia económica y su autor han sido identificados, las organizaciones tienen varias opciones a su disposición en la forma de tratar con el defraudador.

En cuanto a los autores del fraude interno, la acción más frecuente en Latinoamérica fue el despido con 82% (Global: 77%), seguido de la adopción de medidas civiles con el 34% (Global: 62%) e informando a la policía con un 18% (Global: 17%) en Latinoamérica.

Mientras que algunas organizaciones han tenido una "línea dura" de enfoques como la aplicación de las acciones comentadas anteriormente contra el estafador interno, es preocupante ver que para los delitos económicos cometidos por un agresor interno en Latinoamérica, el 7% de los que sufrieron el fraude "no hizo nada" (Global: 4%), el 6% amonestó al involucrado (Global: 18%) y 2% movilizó internamente a los autores del fraude (Global:4%).

Estos datos sugieren que algunas organizaciones mantienen una postura laxa sobre estos delitos, facilitando su ocurrencia.

Es importante establecer estrategias de "tolerancia cero" ante el fraude con el fin de establecer el tono adecuado y transmitir un mensaje fuerte dentro de la organización, las organizaciones deben hacer frente a los autores del fraude de manera oficial y externa, en lugar de tomar un "enfoque" suave y tratar con él en voz baja e internamente

En América Latina, el 82% de los autores de fraudes internos son despedidos y sólo se informa a la policía en el 18% de los casos.

82%

El fraude, el defraudador y la víctima

La detección de fraudes

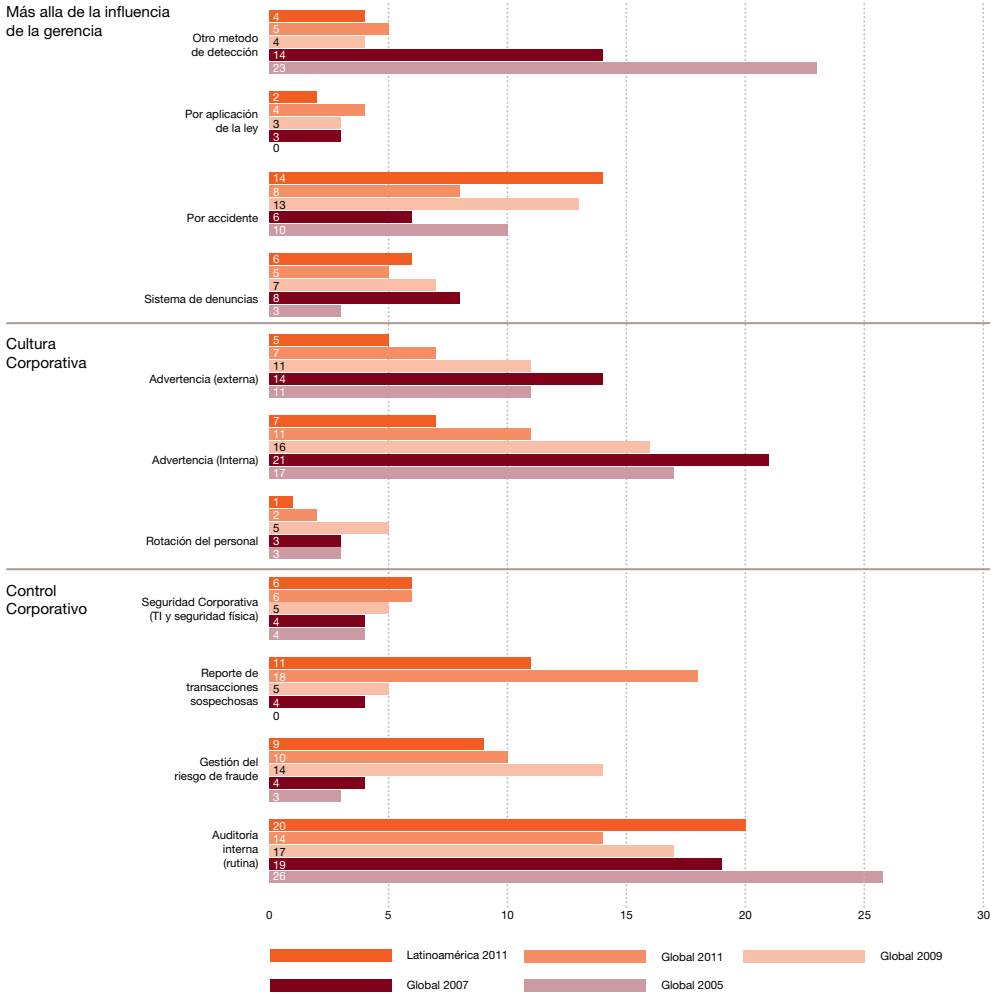
La figura 20 muestra que la eficacia de las auditorías internas para detectar el fraude ha bajado constantemente desde 2005. Sólo 14% de los encuestados dijo que los fraudes se han detectado por la auditoría interna a nivel mundial, mientras que en Latinoamérica este método pasa a ser el más efectivo (20%).

Del mismo modo, la gestión del riesgo de fraude no resultó tan eficaz como en 2009, pasando de 14% a 10%.
Destaca el declive de los métodos de "cultura corporativa" con respecto a 2007.
En esta misma situación se encuentran las advertencias internas y externas, lo que sugiere que la gente está menos dispuesta a informar sobre sus colegas y clientes, o que las diferentes unidades de negocio no están hablando entre si o actúan sobre la información que reciben.

El método de detección que ha aumentado en los resultados de esta nueva edición de nuestra encuesta es el "Control de transacciones sospechosas", de un 5% en 2009 a 18% en 2011. Este método se utiliza comúnmente en el sector de servicios financieros. Dado que el número de los delitos económicos detectados por las computadoras va en incremento en contraste con el número detectado por las personas, tememos que el fraude en general no está siendo detectado, en la medida que ocurran recortes de personal en las áreas de control.

Otro resultado que destaca este año es que 10% de los encuestados a nivel mundial y 11% en Latinoamérica manifestó no tener conocimiento sobre cómo fue detectado el fraude de mayor en su organización. Esto destaca la necesidad que los altos ejecutivos estén conscientes de los riesgos del fraude y la necesidad de tener métodos de detección y prevención efectivos.

Figura 20: Métodos de detección utilizados a nivel mundial



% de encuestados que experimentaron crimen económico en los últimos 12 meses (para 2011 y 2009) y en los dos últimos años (2007 y 2005)

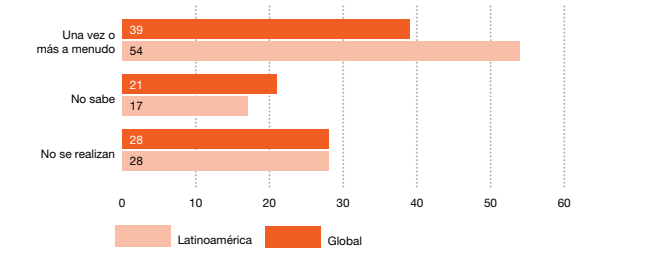
El fraude, el defraudador y la víctima

Evaluaciones de riesgo de fraude, una herramienta útil para la detección del fraude

La mejor manera de combatir el fraude es conociendo cómo identificar el riesgo y valorarlo. Para ello es necesario que las organizaciones realicen evaluaciones periódicas de sus riesgos y analizar su exposición al fraude. La figura 21 muestra la correlación entre la frecuencia de las organizaciones que realizan evaluaciones de riesgo de fraude y los incidentes de fraude reportados.

La figura demuestra que mientras más evaluaciones de riesgo de fraude se realicen, es más probable para las organizaciones detectarlos.

Figura 21: Porcentaje de fraudes reportados en los últimos 12 meses en relación con la frecuencia de las evaluaciones de riesgo de fraude a nivel global

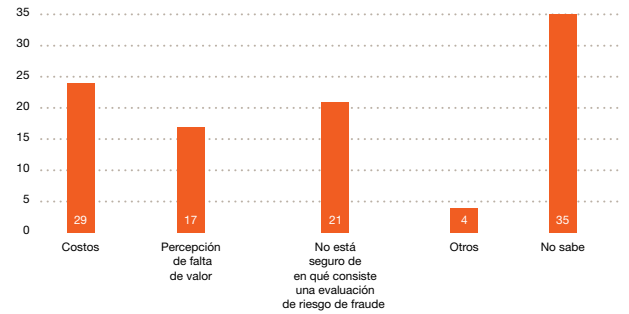


Aquellas organizaciones que reportan no saber o no llevar a cabo ninguna evaluación del riesgo de fraude registran en su totalidad menos casos de fraude, mientras que las organizaciones que declararon llevar a cabo evaluaciones trimestrales o a menudo reportan un mayor número de incidentes de fraudes. Estas cifras, por tanto, confirman el dicho: “busca y encontrarás”.

Esto parece ser un problema de educación y sensibilización y a su vez de las necesidades de trabajo por hacer en cuanto al valor, eficacia, calidad y la necesidad de la realización periódica de evaluaciones de riesgo de fraude en las organizaciones.

Además, la concientización necesita ser promovida como una valiosa herramienta en la detección y lucha contra el fraude.

Figura 22: razones para no realizar las evaluaciones de riesgo de fraude (cifras para Latinoamérica)



Conclusión

Es hora de que todos asumamos el reto

Los resultados de la encuesta muestran que el fraude es persistente, y las organizaciones están en la necesidad de ser vigilantes y proactivas en la lucha contra la delincuencia económica

Los fraudes “tradicionales” como la apropiación indebida de activos, fraude contable, el soborno y la corrupción siguen siendo los tres principales tipos de delito en los últimos 12 meses. Pero “nuevos” tipos de fraude emergen, en particular el cibercrimen. Con la nueva forma de hacer negocios, las nuevas tecnologías y el cambio de ambiente de trabajo, vienen nuevos riesgos y nuevas técnicas para que los estafadores puedan llevar a cabo sus crímenes.

Las organizaciones tienen que estar consciente de estos cambios y en consecuencia adaptar sus mecanismos de respuesta y métodos de detección.

Esto es aún más cierto cuando se trata de las nuevas tecnologías como los teléfonos inteligentes, “Tablets”, los canales de “Social Media” y el “Cloud Computing”, que ofrecen una gran cantidad de soluciones de negocio y oportunidades, pero también pueden ser una caja de Pandora en cuanto a riesgos y amenazas.

Tener un teléfono inteligente o una ‘tablet’ significa llevar información sensible y datos confidenciales de la organización en su bolsillo, y hacer esto sin tomar las precauciones necesarias expone dicha información a su acceso por parte de terceros, potenciando la ocurrencia de eventos cuyo impacto financiero, operativo o reputacional puede ser considerable.

Una década más tarde, el riesgo de fraude sigue en aumento. Pese al desarrollo y adopción creciente de sistemas de gestión de riesgos, hay siempre individuos u organizaciones criminales capaces de detectar una oportunidad y sortear los controles establecidos.

Esto es especialmente cierto cuando se trata de la seguridad de la información, y es nuestro temor que, con las reducciones de personal producto de la crisis, este tipo de fraudes no será detectado oportunamente.

Los avances en la tecnología son vertiginosos, así como las oportunidades que se les presentan a los defraudadores, y usualmente las organizaciones están rezagadas en esta lucha. Es esencial tener las consideraciones de ciberseguridad y seguridad de la información dentro de los riesgos de fraude que maneja la organización.

Las organizaciones que estén dispuestas a comprender y aceptar los riesgos y las oportunidades del mundo cibernético, serán las que ganen ventaja competitiva en las áreas de Tecnología e Innovación.

Establecer conciencia y compromiso a nivel ejecutivo es la clave en la lucha contra la delincuencia económica.

Metodología y agradecimientos

Nuestra sexta Encuesta Global de Delitos Económicos se llevó a cabo entre julio y noviembre de 2011.

La encuesta constó de tres secciones:

- *Preguntas generales de perfiles*
- *Preguntas comparativas centradas en la experiencia de los delitos económicos, y*
- *El cibercrimen como tema central de esta encuesta.*

En total, 3.877 encuestados de 72 países participaron en la encuesta mediante un cuestionario en línea.

Los participantes fueron invitados a responder a las preguntas con respecto a (a) su organización y (b) el país en el que conducen su principal operación.

La encuesta de 2011 se basó en las siguientes estrategias de investigación:

1. Encuesta a ejecutivos de las organizaciones. Los resultados de esta encuesta se basan en las respuestas de los ejecutivos sobre sus experiencias y percepciones de los delitos económicos en sus organizaciones.

   A los participantes se les consultó sobre los diferentes tipos de delitos económicos, su impacto en la organización, tanto en lo que respecta a daños financieros y colaterales, al autor de estos delitos, así como sobre las medidas correctivas adoptadas y los mecanismos de respuesta.

2. Preguntas relativas a los delitos cibernéticos. Nuestra encuesta indagó ampliamente en el crecimiento de la delincuencia informática y la vulnerabilidad de las empresas a este tipo de ataques.

   Nuestro enfoque en este tipo de delincuencia económica nos ha permitido comprender su impacto a nivel corporativo.

3. Análisis de las tendencias en el tiempo. Desde el comienzo de nuestro estudio en el año 2001, hemos realizado una serie de preguntas básicas y preguntas adicionales ajustadas a los temas de interés del momento para las empresas de todo el mundo.

   En consecuencia, nuestros resultados están avalados por una década de información, lo cual nos permite establecer tendencias e identificar situaciones comunes.

Terminología

Abuso de información privilegiada

El uso de información privilegiada se refiere generalmente a comprar o vender un título valor, en violación de un deber fiduciario u otra relación de confianza, estando en posesión de información material no pública.

Las violaciones de información privilegiada incluyen dar consejos o asesorías a otros con esta información y la compra de valores por la persona asesorada o por los que apropiaron indebidamente de la información.

Alto ejecutivo

El alto ejecutivo (por ejemplo, el CEO, Director General o Director Ejecutivo) es el que toma las principales decisiones en la organización

Apropiación indebida de activos (incluida la malversación de fondos / engaño por parte de los empleados)

El robo de los activos (incluidos activos monetarios / efectivo o materiales y equipos) por parte de altos directivos, personas en posiciones de fiduciarios o de un empleado, para su propio beneficio.

Cibercrimen

También conocido como el delito informático, es un delito económico comprometido con la computadora e Internet. Casos típicos de la delincuencia informática son la distribución de virus, las descargas ilegales de los medios de comunicación, el phishing y el pharming y el robo de información personal, como datos bancarios.

Esto excluye fraudes rutinarios en los que un computador es utilizado como un producto con el fin de crear el fraude y sólo incluye delitos económicos en los cuales la computadora, Internet o el uso de medios y dispositivos electrónicos son el elemento principal y no uno incidental.

Comportamiento anticompetitivo

Incluye prácticas que previenen o reducen la competencia en un mercado como el funcionamiento de un cártel que implica colusión con los competidores (por ejemplo, la fijación de precios, manipulación de licitaciones o de reparto de mercados) y abuso de posición de dominio.

Delitos económicos o fraude

El uso deliberado de engaño para privar a otro de dinero, propiedades o derechos legales.

Desempeño financiero

Esto se puede definir como la medición de los resultados de las políticas de la organización y las operaciones en términos monetarios.

Estos resultados se reflejan en el retorno de la inversión, el rendimiento de los activos y el valor añadido, por lo general, en el sector privado, los rendimientos se miden en términos de ingresos, de las empresas / de propiedad estatal o gobiernos, las devoluciones se miden en términos de prestación de servicios.

Espionaje

El espionaje es el acto o práctica de utilización de espías para obtener información secreta o el uso de la tecnología para actuar en su nombre como espías.

Evaluación de los riesgos de fraude

Las evaluaciones de riesgo de fraude se utilizan para determinar si una organización ha realizado un ejercicio para abordar de forma específica:

(i) Los riesgos de fraude a que las operaciones están expuestos;

(ii) Una evaluación de los riesgos más peligrosos (es decir, evaluar los riesgos de importancia y probabilidad de ocurrencia);

(iii) La identificación y evaluación de los controles (de haberlos) que se aplican para mitigar los riesgos clave;

(iv) Evaluación de los programas generales de lucha contra el fraude y los controles en una organización, y

(v) Las acciones para remediar las deficiencias en los controles.

Terminología

Fraude contable

Estados financieros y / o otros documentos alterados o presentados de tal manera que no refleja el verdadero valor o las actividades financieras de la organización. Esto puede implicar la manipulación contable, los préstamos fraudulentos / obtención de financiación, la aplicación fraudulenta de crédito y transacciones no autorizadas / comerciales sin escrúpulos.

Infracción de propiedad intelectual (marcas, patentes, productos y servicios falsificados)

Esto incluye la copia ilegal y / o distribución de productos falsificados en violación de patente o derechos de autor, y la creación de billetes y monedas falsas con la intención de usarlos como genuinos

La corrupción y el soborno (incluyendo chantaje y extorsión)

El uso indebido de una posición oficial para obtener una ventaja en contravención del deber. Esto puede implicar la promesa de un beneficio económico u otro favor, el uso de la intimidación o el chantaje. También puede referirse a la aceptación de tales incentivos.

Las pérdidas financieras

Al estimar las pérdidas financieras debido al fraude, los participantes deben incluir tanto la pérdida directa e indirecta. Las pérdidas directas son la cantidad real producto de fraude y las pérdidas indirectas por lo general incluyen los gastos relacionados con la investigación y solución del problema, las sanciones impuestas por las autoridades reguladoras, costas procesales y daños a la reputación.

Esto debería excluir cualquier monto estimado debido a la “pérdida de oportunidad de negocio”.

Lavado de dinero

Acciones destinadas a legitimar el producto del delito para ocultar su verdadero origen.

Respuesta a incidentes cibercriminales

Típicamente incluye a la capacidad técnica interna para prevenir, detectar e investigar los delitos informáticos, el acceso a investigadores forenses de tecnología, la disponibilidad de acceso a los medios con un plan de relaciones públicas coordinado, los procedimientos de emergencia para el corte de la red involucrada, etc.

Triángulo del Fraude

En el Triángulo del Fraude se describen las condiciones interconectadas que actúan como precursores para el fraude: oportunidad para cometer el fraude, el incentivo (o presión) para cometer un fraude, y la capacidad del autor para racionalizar el acto.

Acerca de PwC Servicios Forenses

El grupo de Servicios Periciales de la red global de PwC juega un papel principal en el tratamiento del ciclo de vida de fraude, para evitar otras pérdidas, proporcionando servicios de investigación reactivos, correctivos y proactivos

Agradecimientos

El equipo de la Encuesta Global de Delitos Económicos estuvo integrado por las siguientes personas:

Equipo líder de la encuesta

Tony Parton, Socio, Reino Unido

Vidya Rajarao, Socio, India

Steven Skalak, Socio, USA

Wayne Anthony, Director, Reino Unido

Equipo gerencial de la encuesta

Faisal Ahmed, Global Project Manager, Reino Unido

Zina Hunt, Global Marketing Manager, Reino Unido

Rhona Foy, Manager, Reino Unido

Socio académico

Peter Sommer
Profesor Visitante del Departamento de Gestión (Sistema de Información y el Grupo de la Innovación) en *London School of Economics and Political Science*, y Lector Visitante de la Facultad de Matemáticas, Informática y Tecnología, *Open University,* Reino Unido

www.pmsommer.net

Miembros del equipo editorial

William Beer, Director, Reino Unido

Mona Clayton, Socio, Brasil

Dyan Decker, Socio, USA

John Donker, Socio, Hong Kong

Peter Forwood, Senior Manager, Australia

Ed Gibson, Director, USA

Jon Hayton, Director, Reino Unido

Tom Lewis, Socio, Reino Unido

Malcolm Shackell, Socio, Australia

Louis Strydom, Socio, Suráfrica

Peter Vakof, Socio, Canada

John Wilkinson, Socio, Rusia

Information Security Forum

Michael de Crespigny
Chief Executive Officer, Information Security Forum

www.securityforum.org

Un agradecimiento especial a quienes colaboraron en PwC en la compilación de este informe: Mike Ascolese, Jonti Campbell, Arjit Chakraborti, Sarah Craig,Matthew Curry, Bonnie Fagan, Gary Fairman, Anjali Fehon, Freddy Fobian, Ayse Francis, Jack Gray, Kunal Gupta, Harry Holdstock, Jonathan Holmes,Fran Marwood, Noel McCarthy, Kim McCourt, Derek Nash, Richard Nugent, Kathrin Prietzel, Mayukh Ray, Aida Roslan, Keith Smith, Rick Stevenson, Josh Williams y Neal Ysart.

Contactos

Equipo líder de la encuesta

Tony Parton
Partner, United Kingdom
+44 (0) 20 721 34068
tony.d.parton@uk.pwc.com

Vidya Rajarao
Partner, India
+91 (0) 80 4079 7002
vidya.rajarao@in.pwc.com

Steven Skalak
Partner, Peoples Republic of China
+86 (10) 6533 2630
steve.l.skalak@cn.pwc.com

Wayne Anthony
Director, United Kingdom
+44 (0) 20 721 26582
wayne.g.anthony@uk.pwc.com

Equipo gerencial de la encuesta

Faisal Ahmed
Global Project Manager, United Kingdom
+44 (0) 20 780 46128
faisal.a.ahmed@uk.pwc.com

Zina Hunt
Global Marketing Manager, United Kingdom
+44 (0) 20 780 44031
zina.hunt@uk.pwc.com

Líderes de Servicios Forenses

Chris Barbee
Partner, USA, Global Leader
+1 (267) 330 3020
chris.barbee@us.pwc.com

John Donker
Partner, Hong Kong, East Cluster Leader
+852 2289 2411
john.donker@hk.pwc.com

Andrew Palmer
Partner, United Kingdom, Central Cluster Leader
+44 (0) 20 7212 8656
andrew.palmer@uk.pwc.com

Erik Skramstad
Partner, USA, West Cluster Leader
+1 (617) 530 6156
erik.skramstad@us.pwc.com

Venezuela

Roberto Sánchez V.
Socio, Venezuela
+ (58212) 700 6666
roberto.sanchez@ve.pwc.com

David Kivilevic
Gerente Senior, Venezuela
+ (58212) 700 6666
david.kivilevic@ve.pwc.com

Servicios Forenses

La red de servicios forenses de PwC está compuesta por contadores forenses, economistas, estadísticos, ex reguladores, examinadores de fraude, y técnicos forenses. Ayudamos a las organizaciones a hacer frente a los principales riesgos financieros y de reputación relacionados con los delitos económicos. Podemos identificar las irregularidades financieras, analizar problemas complejos de negocios, y mitigar el riesgo futuro de fraude.

Oficinas

Caracas
Oficina Principal

Avenida Principal de Chuao
Edificio del Río
Apartado Postal 1789
Caracas 1010-A
Teléfonos: 58 212 700-6666
Fax: 58 212 991-5210

Barquisimeto

Urbanización El Parque
Calle Los Comuneros
Centro Ejecutivo Los Leones
Piso 5, PH 5-2
Apartado Postal 3001
Teléfonos: 58 251 255-4983
58 251 255-0061
58 251 255-0404
Fax: 58 251 254-6284

Maracaibo

Avenida 9B entre Boulevard 5 de
Julio y Avenida Dr. Portillo
Edif. Banco Industrial, Piso 6
Apartado Postal 490
Teléfonos: 58 261 797-9805
58 261 797-9806
58 261 798-3869
Fax: 58 261 798-8194

Maracay

Avenida Las Delicias,
Urbanización El Bosque
Edificio Banvenez, Centro
Financiero, Piso 2
Apartado Postal 4700
Teléfonos: 58 243 232-2742
58 243 232-2745
Fax: 58 243 232-2742

Puerto La Cruz

Av. Intercomunal Andrés Bello
Sector Las Garzas
Centro Comercial MT (CCMT)
Piso1, local 39
Lecherías
Teléfonos: 58 281 267-0845
58 281 418-7935 al 38
Fax: 58 281 286-9616

Puerto Ordaz

Avenida Guayana
Sector Alta Vista
Torre Colón
Piso 6, oficinas 2, 3 y 4
Teléfonos: 58 286 962-6451
58 286 962-4995
58 286 962-5926
Fax: 58 286 962-6875

Valencia

Avenida Bolívar Norte
Centro Comercial y Profesional
El Camoruco
Piso 21
Apartado Postal 541
Teléfonos: 58 241 823-2321
58 241 824-1383
Fax: 58 241 824-4905

Contactos

Si está conectado a internet, haga click sobre el nombre o el icono

Página web:
www.pwc.com/ve

Consultoría Gerencial
consultoria.gerencial@ve.pwc.com

Facebook
(http://facebook.com/pwcVenezuela)

Twitter
(http://twitter.com/pwc_venezuela)

LinkedIn
(www.linkedin.com/companies/pwc-venezuela)