Delitos económicos: Una amenaza a los negocios que sigue creciendo

51%
Más de la mitad de los encuestados fueron víctimas de un delito económico.

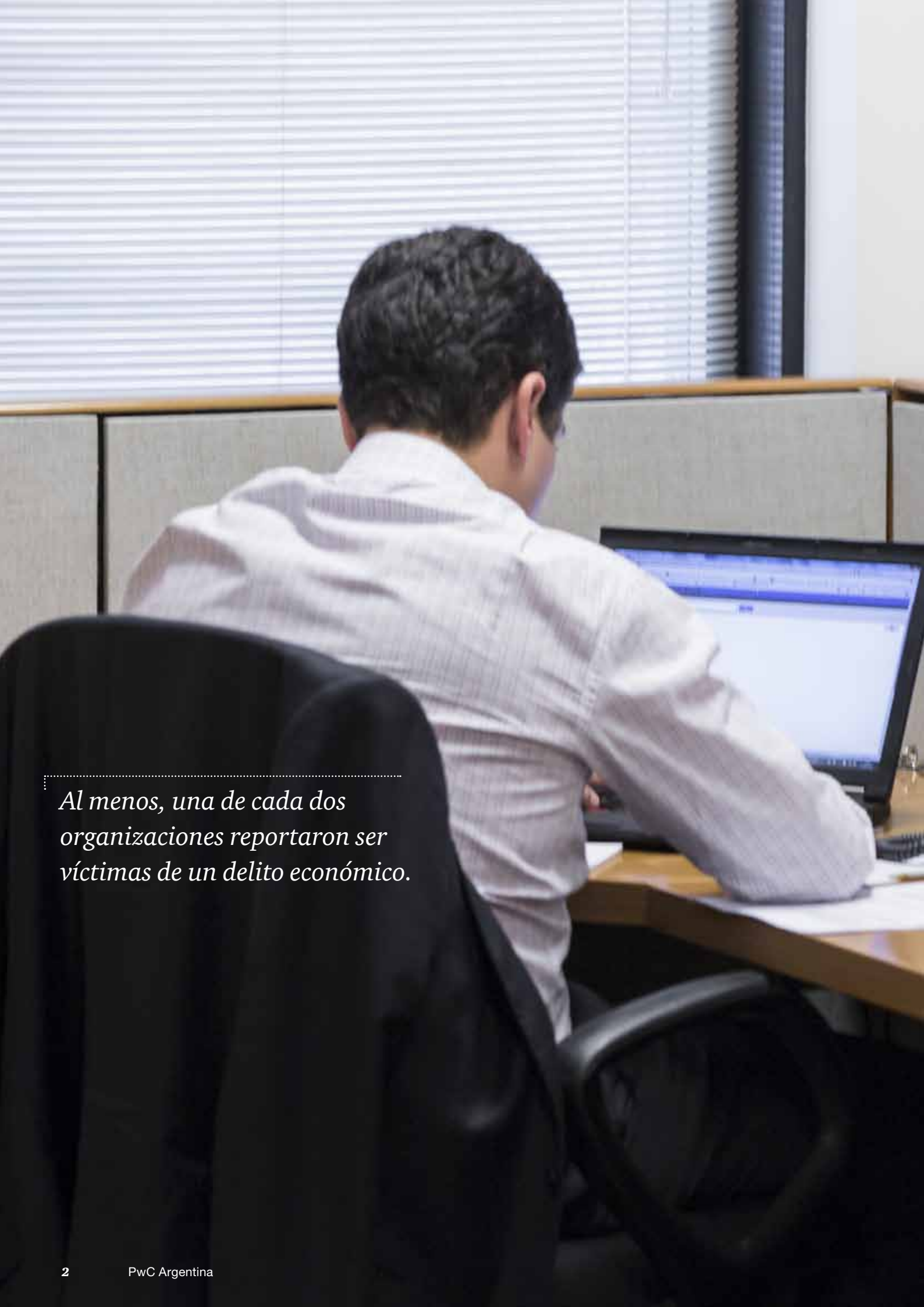
64%
Casi 2 de cada 3 CEOs informaron estar preocupados por el soborno y la corrupción.

33%
1 de cada 3 informó que el riesgo de delito informático ha aumentado casi el 50% con respecto a 2011.

pwc

Los delitos económicos siguen siendo una preocupación importante para las organizaciones de todos los tamaños, en todas las regiones y en prácticamente todos los sectores.

Contenido



Al menos, una de cada dos organizaciones reportaron ser víctimas de un delito económico.

Prólogo

Preocupará a más de uno, pero no sorprenderá, que la Argentina continúe siendo uno de los 10 países que proporcionalmente mayor cantidad de fraudes reportó en los últimos 24 meses.

Este mensaje encabeza el capítulo argentino de la Encuesta Global sobre Delitos Económicos 2014, una de las más amplias y exhaustivas encuestas, con más de 5.000 encuestados en casi 100 países y con récord de participación de empresas argentinas (más de 80).

Es cierto que los fraudes son una amenaza ya conocida por los directivos empresarios, el problema que se suscita en Argentina es que los delitos económicos continúan creciendo año tras año, atacando cada proceso de negocios, erosionando la integridad de los empleados y empañando la reputación de las empresas. El propósito, en esta 7ma. edición, es explicar cómo está siendo afectada la organización y reflexionar sobre cómo afrontar esta amenaza y revertir esta tendencia. Tendencia que, también ubica al país como el más atacado de toda América Latina, ya que 51% de las organizaciones argentinas encuestadas respondieron haber sufrido un fraude en los últimos 24 meses.

Cada uno de los procesos básicos comunes a toda organización –ventas y cobranzas, compras y pagos, altas y bajas de empleados- está bajo amenaza. Es inherente a toda empresa, que tenga que interactuar con diferentes actores económicos para desarrollar su actividad (clientes, distribuidores, agentes, consultores, contratistas, proveedores), exponerse diariamente a diversas formas de fraude en diferentes dimensiones.

Al mismo tiempo, los riesgos continúan evolucionando y –al igual que un virus- los delitos económicos se adaptan a los cambios que experimentan las organizaciones. Así como la tecnología adopta cada vez más un rol protagónico en toda transacción y las compañías se apoyan en la tecnología para desarrollar su actividad, no sorprende que los delitos informáticos escalen posiciones en frecuencia, impacto y sofisticación: es el segundo tipo de fraude más recurrente (en 2011 ocupaba el quinto lugar), después de la malversación de activos.

Asimismo, no resultará novedoso que esta encuesta haya arrojado que los fraudes en compras y contrataciones sean un tema no menor. Sin embargo, esta edición nos permite tomar conciencia de la dimensión de este padecimiento como así también del fraude en los recursos humanos: dos males difíciles de erradicar.

Ante semejante escenario, no es de extrañar que los delitos económicos estén instalados en la agenda de la alta dirección de las empresas. En Argentina, dos de cada tres CEOs –según nuestra reciente **Encuesta Global Anual de CEOs 2014**- respondieron estar preocupados por la corrupción.

Esperamos este informe sea de utilidad a todos sus *stakeholders*, tanto como punto de referencia así como también una herramienta estratégica para la lucha contra el fraude.

Jorge C. Bacher
Socio de PwC Argentina

Resultados destacados

- **Más de la mitad** de los encuestados fueron víctimas de un delito económico en los últimos 24 meses.
- Argentina persiste entre los diez países que proporcionalmente **mayor cantidad de delitos económicos** reportaron en los últimos 24 meses y el más atacado de América Latina.
- El 40% de las organizaciones que reportaron un delito económico sufrieron un **impacto financiero** de más de cincuenta mil dólares.
- La **malversación de activos** fue el delito económico más recurrente durante los últimos 24 meses, con el 67% de fraudes reportados.
- Continúan creciendo los **delitos informáticos**, se convirtieron en el segundo tipo de fraude más reportado (21%). En el 2011, solo 8% de los casos reportados se correspondía con este delito.
- No sorprende, pero preocupa, que el fraude en las **compras y contrataciones** se ubique como el tercer tipo de delito económico más común, habiendo sido esta la primera edición que incluyó esta categoría.
- A casi 20% de los encuestados le pidieron un **soborno** en los últimos 24 meses. Similar porcentaje de encuestados reportó haber perdido una oportunidad de negocio frente a un competidor que ha pagado un soborno.
- La **evaluación del riesgo de fraude** continúa siendo una asignatura pendiente para las organizaciones. Argentina se encuentra entre los 10 países cuyas empresas informaron desconocer o no haber realizado ninguna evaluación del riesgo de fraude en los últimos 24 meses.
- Preocupa que **auditores internos** desconozcan si su organización sufrió un delito económico en los últimos 24 meses.
- El **perpetrador interno** continúa siendo la principal amenaza de la organización (69%).
- La **tolerancia cero** predomina en las organizaciones: 24 de las 29 organizaciones que sufrieron un delito económico perpetrado por un actor interno, informaron que despidieron al empleado involucrado.
- En 2013, la Securities Exchange Commission de los Estados Unidos (SEC) penalizó a 8 compañías por cometer actos de corrupción alrededor del mundo. 2 de esas 8 compañías, fueron **sancionadas por sus delitos cometidos** en Argentina por una suma total de casi 14 millones de dólares.

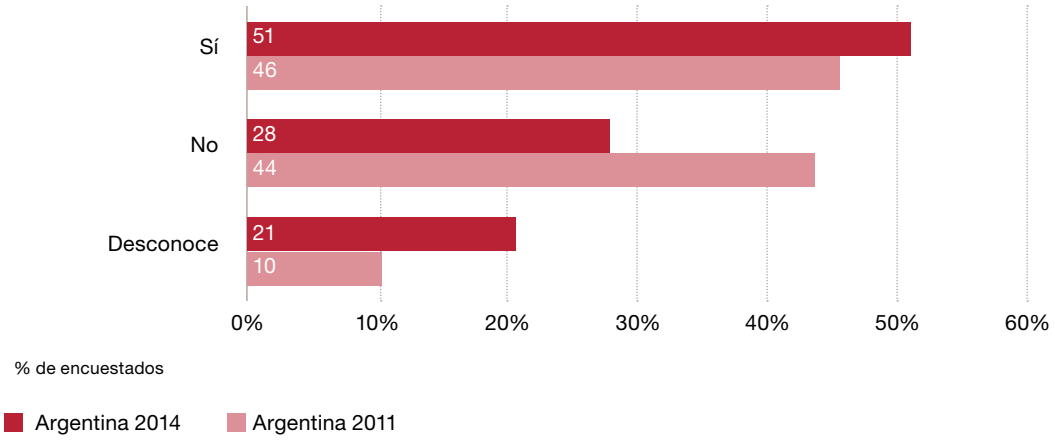
El **futuro** no parece ser prometedor: 33% de los encuestados temen ser víctima de un fraude en los próximos 12 meses. Esta percepción se incrementó 16 puntos porcentuales en comparación con 2011 (17%).

Argentina persiste entre los diez países que proporcionalmente mayor cantidad de delitos económicos reportaron en los últimos 24 meses.

Delitos económicos en el año 2014
Una foto de Argentina

A pesar de los esfuerzos de las organizaciones y de los profesionales que combaten el fraude, la delincuencia económica continúa creciendo en Argentina. Más de la mitad de los encuestados informaron que su organización ha experimentado un delito económico durante los últimos 24 meses, un incremento de 5 puntos porcentuales en comparación con nuestra encuesta del 2011. Además, vale resaltar que más del 48% de las organizaciones que reportaron delitos económicos fueron víctimas de más de un incidente.

Gráfico 1. Organizaciones argentinas que reportaron delitos económicos



Los resultados arrojados posicionan a Argentina entre los 10 países que proporcionalmente mayor cantidad de delitos económicos reportaron en los últimos 24 meses.

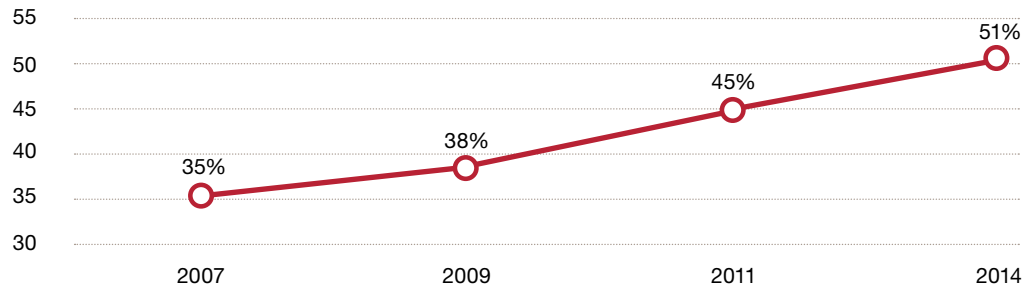
Gráfico 2. Países que proporcionalmente reportaron mayor cantidad de fraudes

País	2014	2011
Sudáfrica	69%	60%
Ucrania	63%	36%
Rusia	60%	37%
Australia	57%	47%
Papúa Nueva Guinea	57%	N/A
Francia	55%	46%
Kenia	52%	66%
Argentina	**51%**	**46%**
España	51%	47%

N/A: no se obtuvo la cantidad de respuestas mínimas requeridas.

Analizando la tendencia de nuestras últimas encuestas, notamos que la cantidad de víctimas crece año tras año. En 2007, 35% de las organizaciones reportaron un fraude. En 2014, esa cifra llegó al 51%. En otras palabras, los delitos económicos han aumentado casi un 50% desde 2007.

Gráfico 3. Evolución del fraude en Argentina 2007 - 2014



% de encuestados

¿A qué responde este incremento de fraudes? ¿Las organizaciones mejoraron sus métodos de detección? ¿Es un problema puntual de una industria? ¿Depende del tamaño? ¿El fraude afecta por igual a toda la región? ¿Cómo frenar esta escalada que Argentina experimenta desde el 2007?

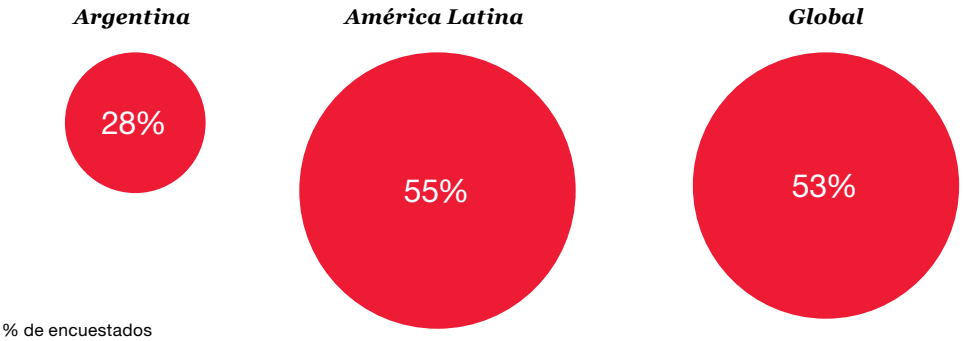
En las páginas siguientes intentaremos ensayar algunas posibles respuestas a esto y otros interrogantes de los delitos de cuello blanco en nuestro país.

Prevenir a partir de la experiencia

Llamó la atención que el 28% de los argentinos encuestados respondió no haber sufrido un delito económico y el 21% reportó desconocerlo. Estas cifras resultan muy lejanas a las de América Latina (55% y 10% respectivamente) y el resto del mundo (53% y 10% respectivamente). Dicho 21%, al compararlo con otras latitudes nos sugiere que la comunicación de los delitos económicos no es frecuente en las organizaciones argentinas.

El primer paso para prevenir y disuadir un hecho delictivo es conocer los incidentes sufridos. No es alentador que de ese 21% que respondió desconocer si su organización fue víctima de un delito económico, poco menos de un tercio de ellos desempeñan funciones dentro del área de **auditoría**.

Gráfico 4. Organizaciones que no reportaron delitos económicos

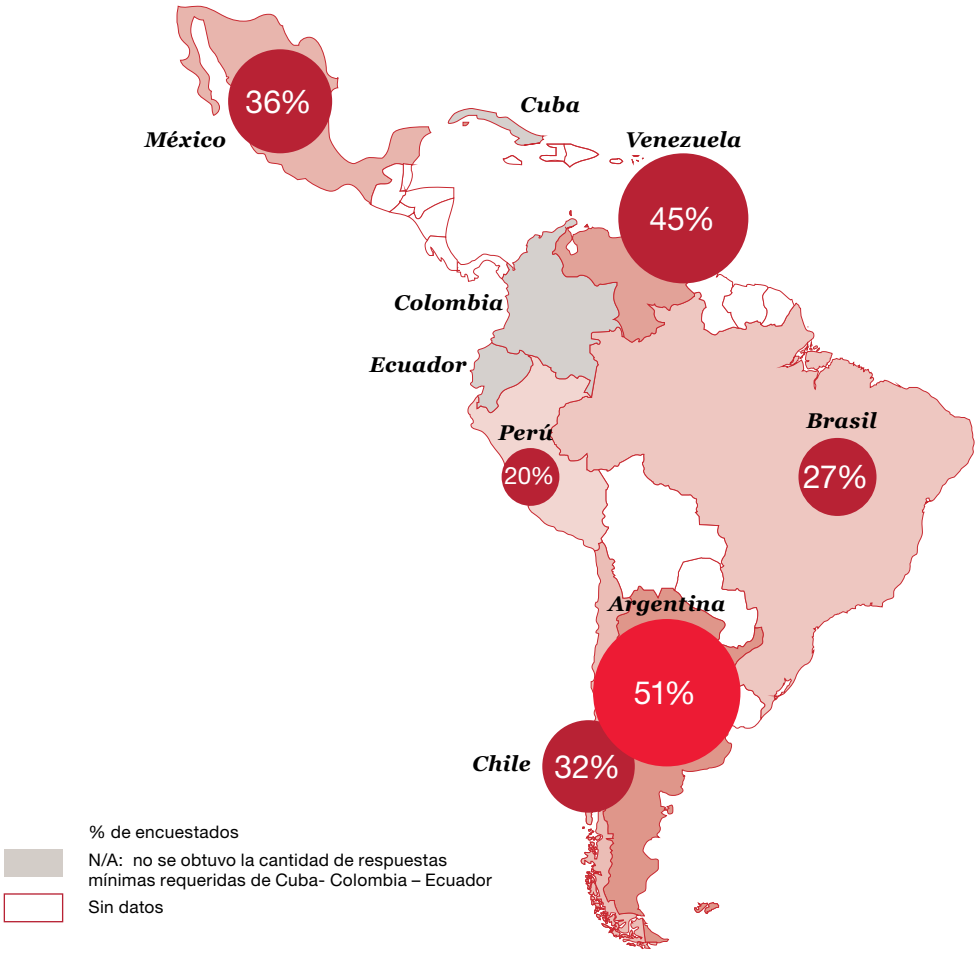


% de encuestados

Argentina y la región

En esta 7ma. edición de la encuesta, 707 organizaciones de 9 países de Latinoamérica respondieron las preguntas. 250 de las empresas en la región sufrieron un delito económico, siendo Argentina el país que proporcionalmente mayor cantidad de delitos económicos reportó. Este lugar que ocupa no es nuevo, también en nuestra encuesta de 2011 las empresas argentinas fueron las que ocuparon la primera posición.

Gráfico 5. Países en América Latina que reportaron delitos económicos en 2014

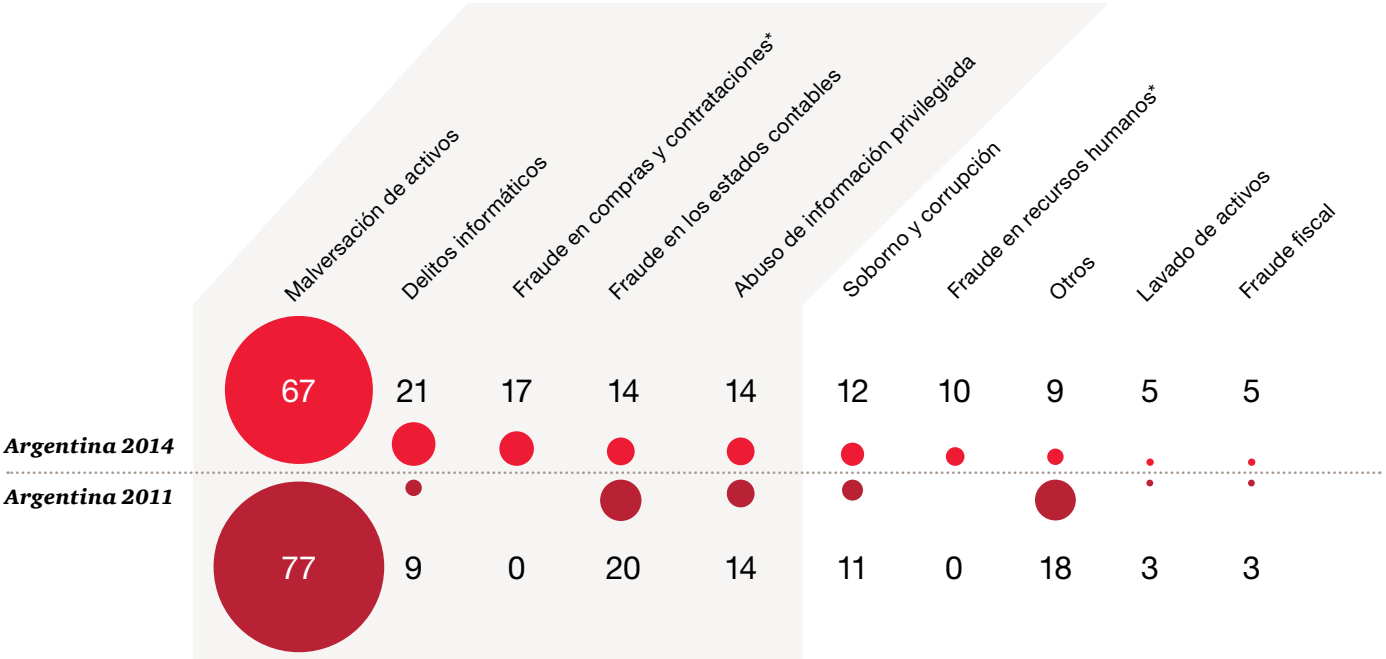


El fraude en compras y contrataciones se posicionó como el tercero más reportado en nuestro país.

¿A qué nos enfrentamos?

Los delitos económicos pueden presentarse en diversas modalidades, cada uno con sus propias características, amenazas y consecuencias.

Gráfico 6. Tipos de delitos económicos reportados por las organizaciones



*No fueron inluidos en la Encuesta de 2011
% sobre los encuestados que sufrieron un delito económico los últimos 24 meses
Nota: Se permitió la selección de respuestas múltiples

Nuestras últimas encuestas (desde el 2007) ubican por un amplio margen a la **malversación de activos** como el fraude más reportado. Sin embargo, este año la tasa disminuyó al 67% (77% en 2011), seguramente dada la incorporación de dos nuevas categorías de delitos económicos en la presente edición: el fraude en compras y contrataciones (17%) y el fraude en recursos humanos (10%).

Al respecto de estas nuevas categorías, los resultados no fueron alentadores; el **fraude en compras y contrataciones** se posicionó como el tercero más reportado en nuestro país (segundo en América Latina y el mundo). Esta ubicación podría estar impulsada por la tendencia global a la subcontratación de servicios y la interconectividad entre las organizaciones.

En los próximos 12 meses, el 32% de las compañías cree que sufrirá fraude en compras y contrataciones y un 21% en torno a recursos humanos.

Es importante mencionar que las industrias que reportaron, al menos un hecho de fraude en compras y contrataciones, fueron aquellas que dependen de una estrecha colaboración con una amplia variedad de proveedores, en toda su cadena de valor:

- Telecomunicaciones.
- Manufactura.
- Energía, Servicios Públicos y Minería.
- Servicios Financieros.
- Venta Mayorista y Minorista.

En lo que se refiere al **fraude en recursos humanos**, si bien no disponemos de datos históricos, surge como una amenaza de la cual no hay que descuidarse. Las organizaciones deberían replantearse qué actividades de control se realizan en procesos tales como la contratación de empleados y la liquidación de novedades (ejemplo: horas extras).

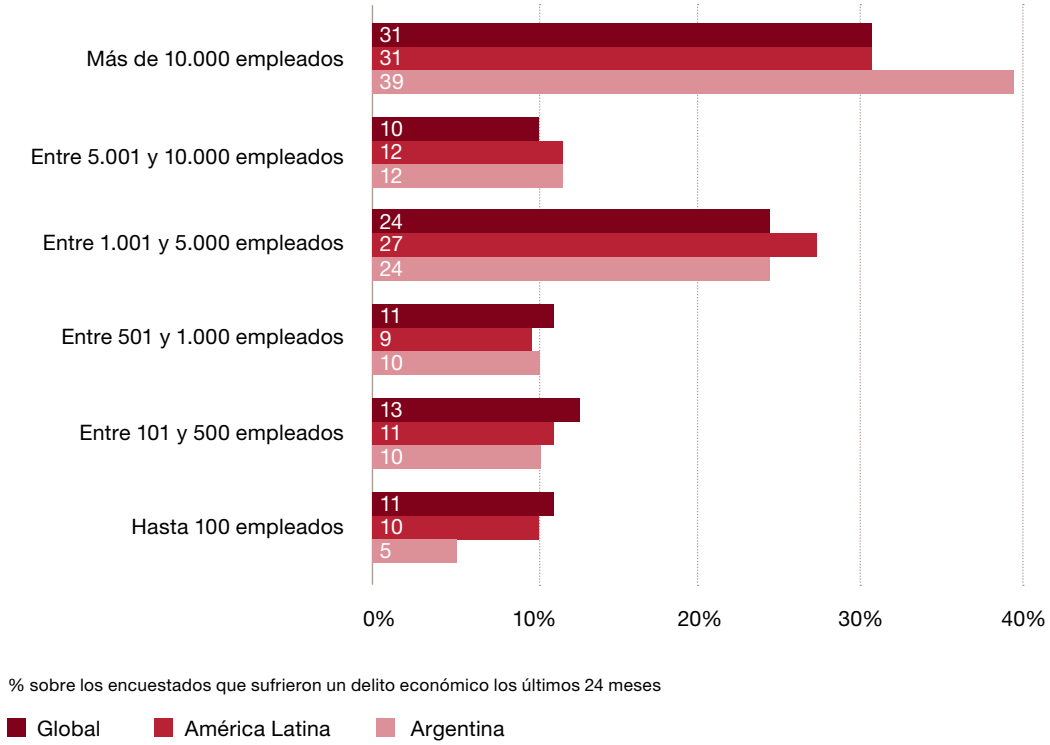
Seguramente, deberán prestar mayor atención aquellas organizaciones que emplean a muchos trabajadores y/o experimentan un significativo y rápido crecimiento de la nómina. La amenaza de sufrir este tipo de fraude crece en relación a la nómina de empleados: en Argentina y en el mundo, las principales víctimas de este tipo de fraude fueron empresas con más de 500 empleados.

Como lo inferíamos al decidir incorporar ambas categorías a la encuesta, son amenazas con entidad propia y requieren una rápida respuesta de las organizaciones. En los próximos 12 meses, el 32% de las compañías espera sufrir un fraude en compras y contrataciones y un 21% un fraude en recursos humanos.

El tamaño y la industria

No es el tamaño o la industria donde opera una compañía razón suficiente para ser víctima de un fraude, sino cómo se prepara para afrontar un ataque. Hoy en día, las organizaciones están expuestas a los delitos económicos de igual manera, sin importar sus características. Sin embargo, podemos afirmar que, en comparación con las pymes, las compañías más grandes disponen de más recursos y, en consecuencia, tienen la posibilidad de invertir en mecanismos más eficaces de prevención, detección y disuasión de fraudes.

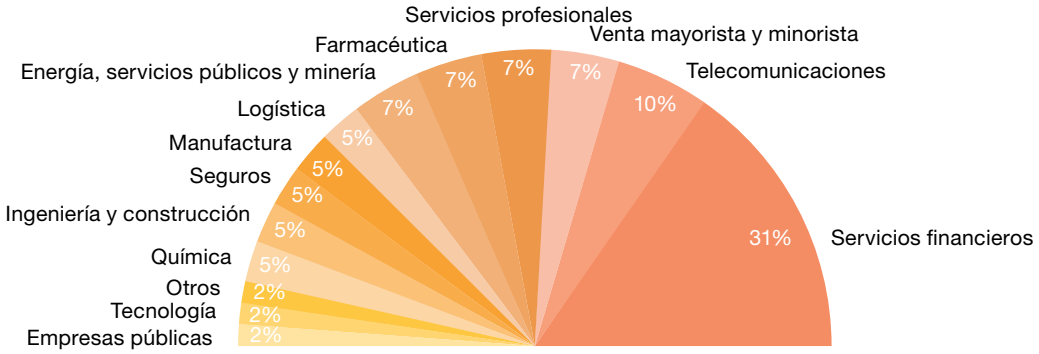
Gráfico 7. Tamaño de la organización



En tal sentido, la encuesta nos dice que las compañías argentinas con más de 500 empleados reportaron mayor cantidad de fraudes (85%) que las compañías con menos de 500 (15%). Estas cifras confirman la tendencia de la región y del resto del mundo.

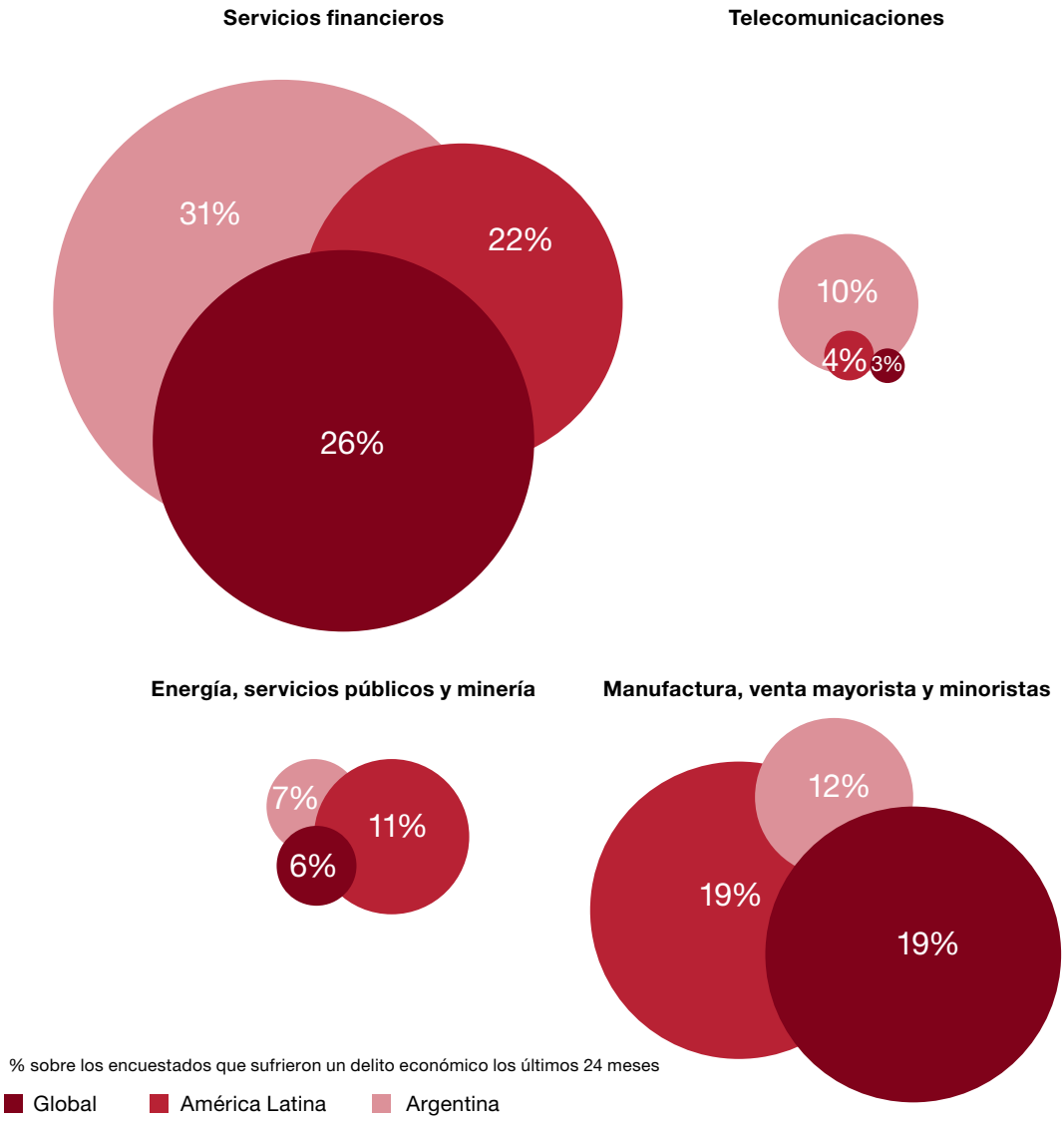
Con respecto a la industria, los **servicios financieros** continúan a la cabeza de las más atacadas a nivel local y global. El perpetrador tiende a preferir cometer el delito que le permita hacerse del efectivo del modo más sencillo posible. Es decir, va a preferir clonar una tarjeta de débito y extraer dinero de un cajero automático, que apropiarse de mercadería la cual después tendrá que venderla en algún mercado informal. Más allá de este factor, observamos que los fraudes se encuentran diseminados en todos los sectores de la economía.

Gráfico 8. Delitos económicos reportados por industria en Argentina



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Gráfico 9. Industrias más atacadas



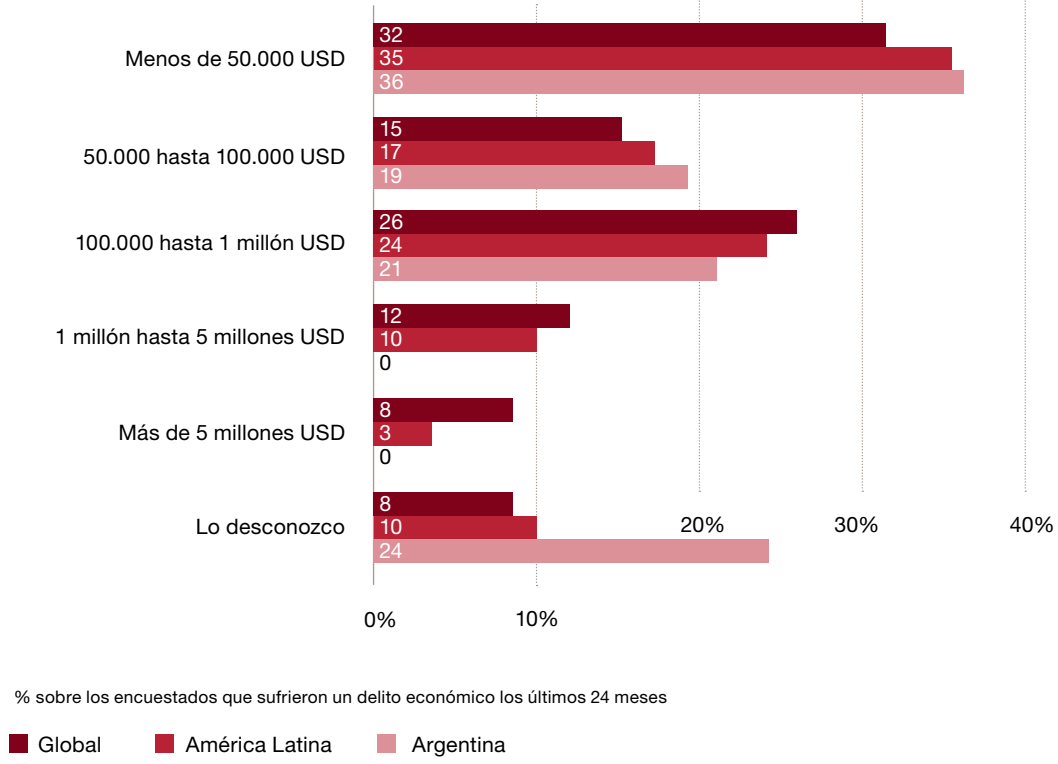
% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Global América Latina Argentina

El daño

Las organizaciones a menudo no logran comprender el verdadero daño de un delito económico. Como en años anteriores, nuestro estudio pone en relieve que el costo del fraude en las organizaciones es un factor que ninguna empresa puede desestimar y que el impacto total de los daños no puede ser medido únicamente de manera monetaria.

Gráfico 10. Cuantificación del perjuicio económico causado directamente por los delitos económicos reportados (en USD)



Como indica el gráfico, un 40% de las organizaciones argentinas víctimas de un incidente tuvieron un impacto financiero que osciló los 50.000 y el millón de dólares. Además, la edición de este año arrojó un dato más que interesante, casi el 24% de los encuestados que sufrió un delito económico en los últimos 24 meses en Argentina no sabe cuál fue el impacto financiero que éste originó a la compañía, más del doble que en Latinoamérica (10%) y el mundo (8%).

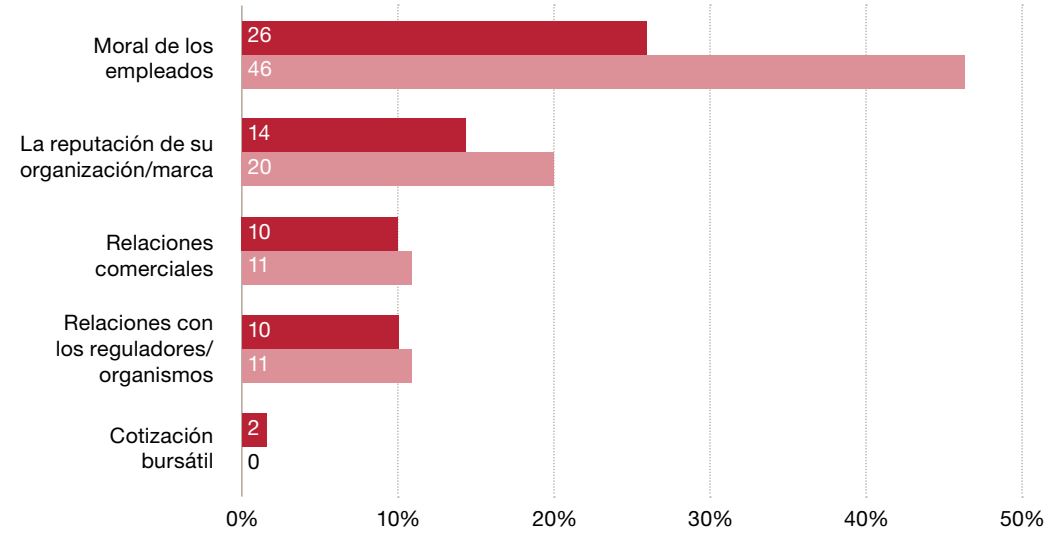
Este último factor, junto a la inexistencia de organizaciones que han reportado algún caso de fraude con un impacto mayor a los 5 millones de dólares en Argentina, nos indicaría que en nuestro país es más difícil poder cuantificar la incidencia de un delito económico cuando éste es de mayor magnitud en términos monetarios.

Daño colateral: difícil de cuantificar, difícil de ignorar

La pérdida económica no es la única preocupación que las empresas enfrentan en la lucha contra el fraude. Al igual que en ediciones anteriores, nuestros encuestados señalaron como algunos de los daños colaterales más graves causados por los delitos económicos:

- la moral de los empleados;
- la reputación de la organización y de la marca; y
- las relaciones comerciales.

Gráfico 11. Daños colaterales causados por los delitos económicos



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Al tomar en cuenta los daños colaterales, el costo real de un delito económico puede provocar un impacto de larga duración. Si bien es difícil cuantificar este tipo de pérdidas en términos estrictamente financieros, hay un hecho que es claro: si el fraude implica perder clientes o proveedores (porque se niegan a continuar la relación comercial), empleados que prefieren cambiar de trabajo o talentosos recursos que deciden no aplicar a un puesto en la organización, definitivamente el impacto se sentirá en el mediano plazo en los resultados de la compañía.

En otras palabras, la larga cadena de efectos adversos que conlleva sufrir un delito económico, tales como la pérdida de ingresos, la pérdida de clientes, la baja en el precio de las acciones, la disminución de la productividad, el aumento del costo de la mano de obra y el daño en la moral de los empleados, no sólo pueden ser difíciles de valorar de forma individual, sino que también son imposibles de ignorar.

Afortunadamente, la alta dirección parece haber comprendido ésto. Nuestra 17° Encuesta Anual Global de CEOs informa que el 55% de los directores ejecutivos locales, ve "la falta de confianza en las empresas" como una problemática, por lo cual atacar esta cuestión se ha transformado en algo clave. Una mayoría significativa reconoce que las empresas tienen un papel más amplio en la sociedad que la mera construcción de valor para los accionistas.

¿Qué nos depara el futuro?

Así como aumentó la cantidad de fraudes reportados, también creció la preocupación de sufrir un fraude en los próximos 12 meses. En particular, 5 tipos de delitos económicos sobresalen como los más temidos por las organizaciones:

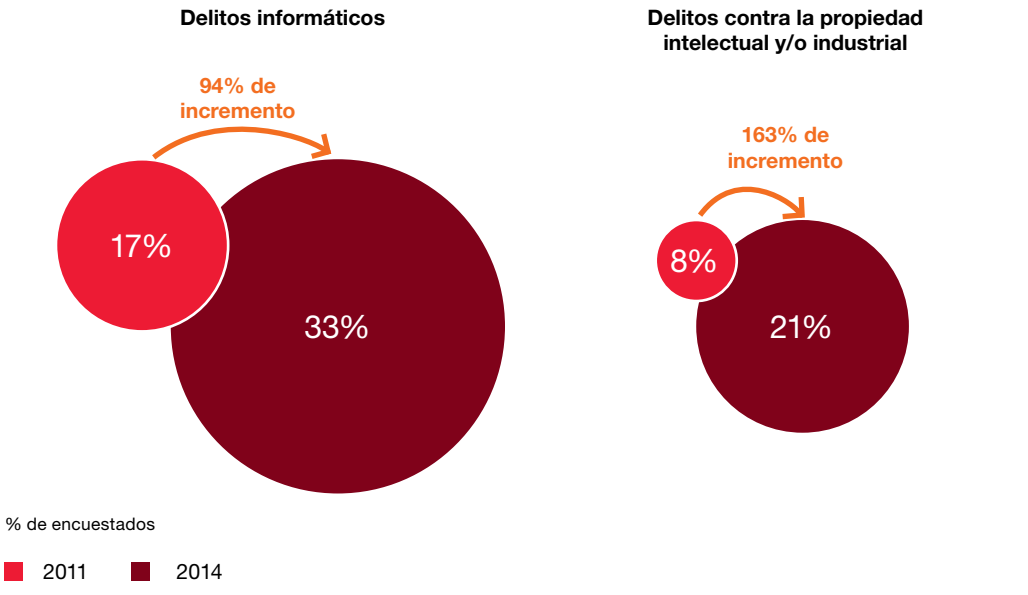
Gráfico 12. Las mayores amenazas

2014		2011
1.	Malversación de Activos	1.
2.	Delitos informáticos	5.
3.	Fraudes en compras y contrataciones	S/D
4.	Abuso de información privilegiada	3.
5.	Fraude en los estados contables	2.
6.	Soborno y corrupción	4.

S/D: nueva categoría agregada en 2014

Más allá de lo expuesto, no queremos que el lector pierda de vista que ha crecido exponencialmente la preocupación de las empresas por dos tipos de delitos económicos: delitos informáticos y delitos contra la propiedad intelectual y/o industrial.

Gráfico 13. Las amenazas que toman protagonismo



¿Cómo podemos defendernos?

Analizando la cantidad de compañías que efectuó una evaluación de riesgo de fraude al menos una vez al año, podemos mencionar las siguientes aseveraciones:

- Así como Argentina se posiciona entre los 10 países que proporcionalmente mayor cantidad de fraudes reportó, también se ubica en la cima de los países que respondieron no haber realizado una evaluación del riesgo de fraude en los últimos 24 meses o desconocerlo (55% de las empresas encuestadas).

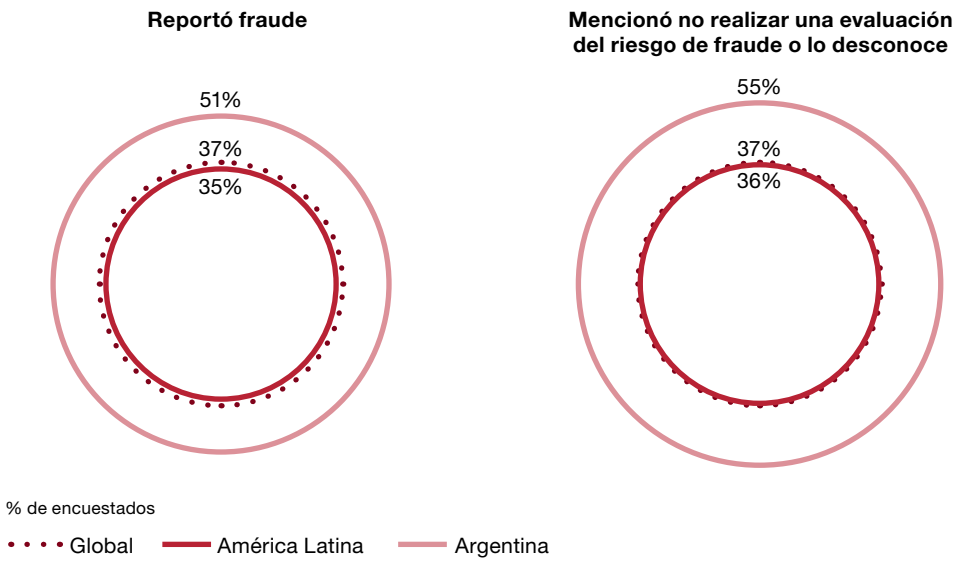
Gráfico 14. Países que proporcionalmente mayor cantidad de encuestados desconocen o no han realizado una evaluación de riesgo de fraude en los últimos 24 meses

Botsuana	80%
Angola	77%
Túnez	65%
Namibia	62%
Turquía	55%
Argentina	**55%**
Suecia	52%
Argelia	50%
Bahréin	50%
Latinoamérica	**36%**
Global	**37%**

% de encuestados

- Desde la perspectiva local y regional, también Argentina se encuentra por encima de la media. En Latinoamérica solo el 36% de las organizaciones mencionó no realizar una evaluación de riesgo de fraude o desconocerlo.

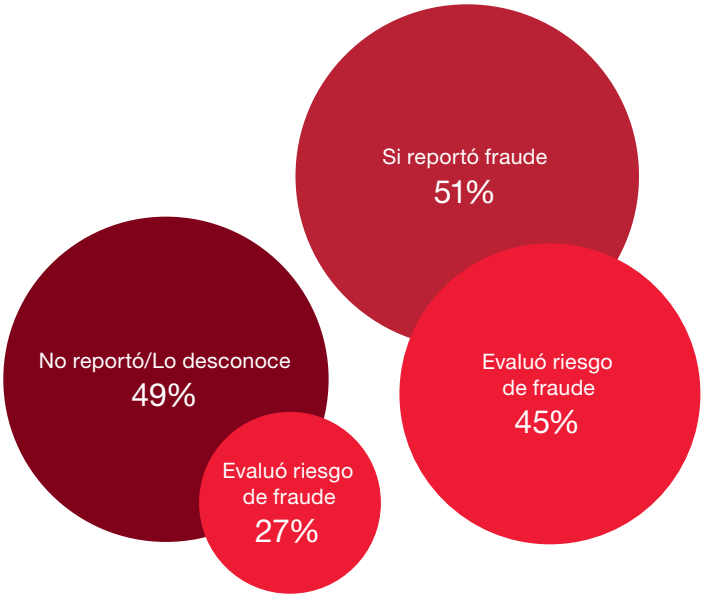
Gráfico 15. Evaluación de riesgo de fraude



¿Por qué una evaluación de riesgo de fraude?

Nuestra experiencia indica que uno de los primeros pasos en la lucha contra el fraude, es conocer a qué riesgos de fraude está expuesta la organización. Haciendo esta evaluación, facilitaremos la detección de un incidente y estaremos mejor preparados para afrontar nuevas amenazas.

Gráfico 16. La evaluación del riesgo de fraude y el porcentaje de casos reportados



% de encuestados

Al igual que en nuestras últimas dos ediciones, observamos que continúa existiendo una correlación entre la cantidad de fraudes reportados y las evaluaciones del riesgo de fraude llevadas a cabo por las organizaciones.

En 2013 la SEC sancionó a 2 compañías por un total de 14 millones de USD por delitos cometidos en Argentina.

Bajo la lupa de los organismos regulatorios

Soborno, corrupción y lavado de activos en primera plana

Problemas como el soborno y la corrupción o el lavado de activos son temas ya conocidos en el ámbito de los negocios. Sin embargo, siguen planteando amenazas importantes a las organizaciones globales, más en un mundo interconectado como el actual. En ese contexto, gobiernos y organismos internacionales incrementaron la regulación y los controles para combatirlas. En nuestro país existen organismos que combaten el fraude y la corrupción tales como la recientemente creada PROCELAC (Procuraduría de Criminalidad Económica y Lavado de Activos) y las ya conocidas UIF (Unidad de Información Financiera) y la Oficina Anticorrupción. Durante 2012, estos organismos iniciaron 352[1] investigaciones (Oficina Anticorrupción) y abrieron 17[2] nuevos sumarios (UIF). Asimismo en la región, se están realizando algunas de las siguientes acciones:

- Brasil aprobó en 2013 una nueva ley anticorrupción que impone nuevas responsabilidades a las personas jurídicas del sector privado. Esta ley prohíbe aquellas prácticas corruptas cometidas por estas compañías ante la administración pública tanto local como extranjera, y plantea sanciones administrativas y judiciales, que no son excluyentes.
- En México, en 2012 entró en vigencia la Ley Federal Anticorrupción en Contrataciones Públicas. El objetivo de la ley, en este caso, es el establecimiento de responsabilidades y sanciones para personas físicas y jurídicas en lo que respecta a las infracciones en las que incurran, en su participación en las contrataciones públicas tanto domésticas como en el exterior.

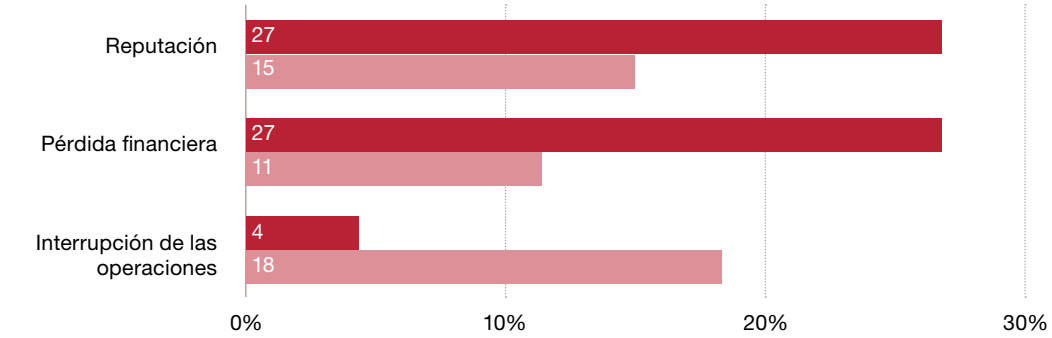
En el resto del mundo, entre las acciones que se están llevando a cabo en países como Estados Unidos en su lucha contra el fraude y la corrupción, vale la pena mencionar las sanciones aplicadas por la Securities Exchange Commission de los Estados Unidos (SEC). En 2013, este organismo penalizó a 8 compañías por cometer actos de corrupción alrededor del mundo. **El dato importante aquí es que 2 de esas 8 compañías fueron sancionadas por sus delitos cometidos en Argentina, por una suma total de casi 14 millones de dólare**s.

Además de las multas y acusaciones criminales, estas violaciones pueden ser vistas como emblemas de problemas para las organizaciones más grandes, y desencadenar daños en la reputación (incluyendo la desaprobación pública, opiniones no deseadas en los medios, litigios y/o reacciones adversas en el precio de las acciones), pérdidas financieras, interrupciones en los planes de negocio y fugas de talento.

Considerando todo lo comentado y conforme se exhibe en el siguiente gráfico, el daño a la reputación, la interrupción de las operaciones y la pérdida financiera son los impactos que más preocupan a las organizaciones argentinas.

1. Informe anual de gestión 2012 – Oficina Anticorrupción, Ministerio de Justicia y Derechos Humanos.
2. Informe de gestión 2012 – Unidad de Información Financiera, Ministerio de Justicia y Derechos Humanos.

Gráfico 17. Impacto más preocupante



% sobre los encuestados que sufrieron un delito económico los últimos 12 meses

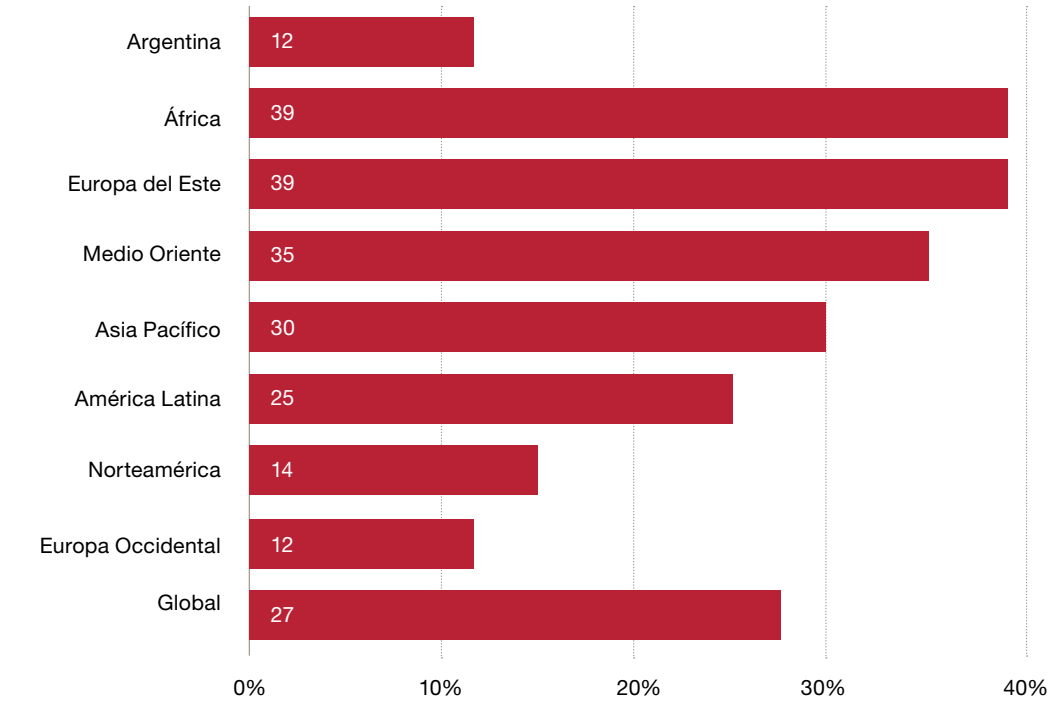
Soborno y corrupción Lavado de activos

El desafío de Argentina

34% de las organizaciones argentinas ubican al soborno y corrupción como una de las amenazas de los próximos 12 meses.

El soborno y la corrupción ocupa el tercer lugar (27%) entre los delitos económicos sufridos por las organizaciones a nivel global en los últimos 24 meses. Sin embargo, en el caso de Argentina, la tasa de casos no supera el 12%, muy por debajo inclusive de la media de la región.

Gráfico 19. Soborno y corrupción por región



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

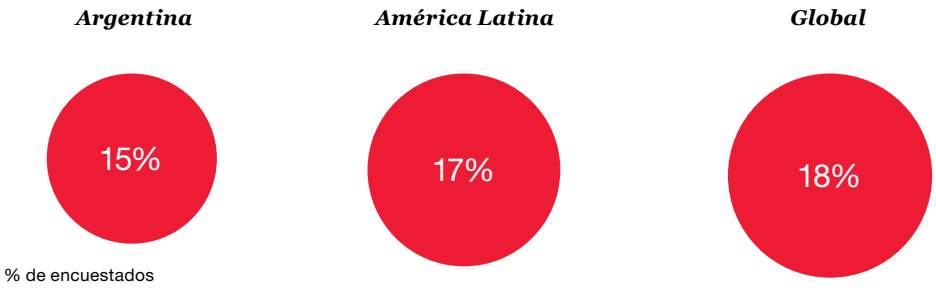
3. Escala del 0 al 100. El número más alto corresponde a un país mas transparente.

En cambio, cuando nos referimos al futuro, 34% de las compañías argentinas ubican al soborno y la corrupción como una de las amenazas de los próximos 12 meses, en línea con América Latina (35%) y el resto del mundo (29%). ¿Será que Argentina percibe que hay mayor cantidad de casos de soborno y corrupción de los que realmente suceden? ¿O será que los casos de soborno y corrupción son más difíciles de detectar, porque generalmente involucran a personas que ocupan altos cargos y tienen las atribuciones suficientes para ocultar el delito más tiempo?

Como mínimo podemos plantear que las organizaciones se encuentran seriamente expuestas a ser víctimas de este tipo de delitos.

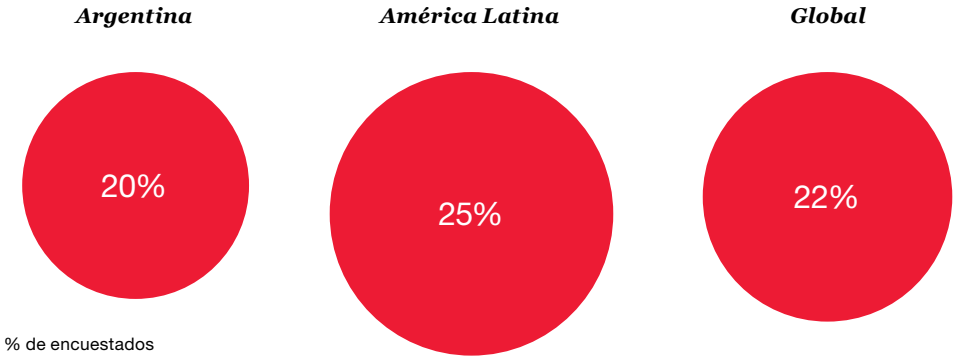
20% de los encuestados locales perdió una oportunidad de negocio con un competidor que ha pagado un soborno, tendencia que Argentina comparte con el resto de los países.

Gráfico 20. Porcentaje de empresas que se les fue solicitado un soborno



% de encuestados

Gráfico 21. Porcentaje de empresas que perdieron una oportunidad de negocios por no pagar un soborno



% de encuestados

El lavado de activos preocupa especialmente a las entidades financieras

En términos de delitos económicos, los servicios financieros son una industria diferente a las demás. El lavado de activos es una de sus principales preocupaciones, ya que presenta un riesgo para la entidad que no lo reporta. De hecho, las entidades financieras encuestadas creen que existe un mayor riesgo de lavado de activos que de corrupción y soborno. Más de un cuarto (27%) de las encuestadas a nivel global manifestaron un evento de lavado de activos en los últimos 24 meses.

Si bien los artilugios para lavar dinero varían en sofisticación y complejidad, el propósito no varía: tener acceso a las prestaciones y servicios de una entidad financiera. Para ello, siempre existe un factor común: la debilidad humana, ya sea por la incompetencia, por la corrupción o el dolo.

El desafío que impone esta amenaza sistémica es que no puede evitarse completamente -al menos sin tomar medidas irracionales como salir del mercado en cuestión- y los procesos de negocio deben afrontarla día a día en distintas etapas:

- ***Conozca a su cliente (KYC).*** Buscar potenciales clientes e integrar nuevos se ve directamente afectado por la amenaza de lavado de activos.
- ***Cumplimiento.*** Con la misma importancia, el lavado de activos amenaza los procesos de la entidad en materia de cumplimiento respecto de las operaciones: en la ventanilla de caja, en la sala de transferencia de dinero y en el procesamiento y cobro de cheques.
- ***Gestión del riesgo.*** El lavado de activos también amenaza los procesos de due diligence, de información de operaciones sospechosas y gestión del riesgo de una entidad, en particular cuando el riesgo se concentra en grupos de cuentas bajo control común o préstamos utilizados por personas que lavan dinero o cuando la capacidad de los sistemas de monitoreo está atrasada respecto de las plataformas de servicio utilizadas.

Considere la dificultad que enfrenta una entidad financiera internacional para administrar sus operaciones en distintos ámbitos culturales y legales -que está sujeta a las normas legales estrictas de una economía occidental desarrollada-. Se debería capacitar a los cajeros, por ejemplo, para que puedan identificar e informar lo que podrían ser ***"operaciones sospechosas"*** ya sea por **la suma, moneda y frecuencia de los depósitos, la identidad del depositante o la naturaleza inexplicable del negocio**.

La entidad podría estar operando en una cultura conocida por la violencia o intimidación a las personas no dispuestas a colaborar, por la deferencia a los pedidos de las personas adineradas, o en una cultura en la que la corrupción es habitual. Podría estar operando en un ámbito donde existen relativamente grandes diferencias entre la situación económica de los clientes y la de los empleados bancarios, lo que genera que existan regalos o amenazas para allanar el camino para el uso inadecuado del sistema financiero por parte de quienes realizan estas operaciones, las aprueban o denuncian.

El lavado de activos tiene amenazas colaterales. Este delito daña a la reputación y otorga publicidad negativa. Las cargas adicionales incluyen el costo operativo de cumplir con nuevas regulaciones de cumplimiento, vigilancia y la actualización que surja de otros procesos de negocio.

Por otro lado hoy en día existe otro desafío que enfrentan los sistemas operativos y de cumplimiento en los bancos: las redes de pago alternativas que utilizan monedas ***"virtuales"***. Si bien las operaciones en estos sitios pueden ser "virtuales", están respaldadas por depósitos reales en entidades financieras de todo el mundo.

Por lo tanto, operar en ámbitos que generan una amenaza sistémica de lavado de activos a los procesos de negocio de las entidades financieras constituye un **desafío crucial**. Los artilugios de lavado de activos no sólo son numerosos y sofisticados sino que además crean una tensión significativa entre metas tan loables como ***conseguir y prestar servicios a un cliente rentable y operar con una entidad que acate totalmente las normas de múltiples jurisdicciones.***

Puede que muchas organizaciones ni siquiera se percaten que están en la mira, o se enteren mucho tiempo después, cuando el daño ya está hecho.

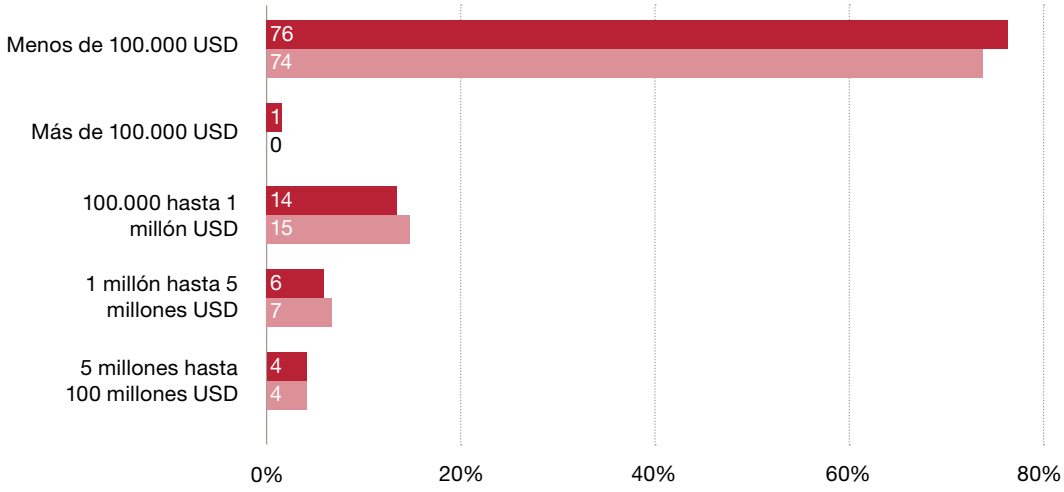
Delitos informáticos
Los riesgos de un planeta interconectado

El avance de la tecnología, combinado con el explosivo crecimiento de las redes sociales y la conectividad de datos alteró definitivamente las relaciones entre las empresas y los consumidores.

Desafortunadamente, esta conectividad tiene un lado oscuro. El delito informático opera en las sombras y puede que muchas organizaciones ni siquiera se percaten que están en la mira, o se enteren mucho tiempo después, cuando el daño ya está hecho.

Este solo factor convierte a los delitos informáticos en uno de los delitos más peligrosos.

Gráfico 22. Pérdida financiera por delitos informáticos



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Global América Latina

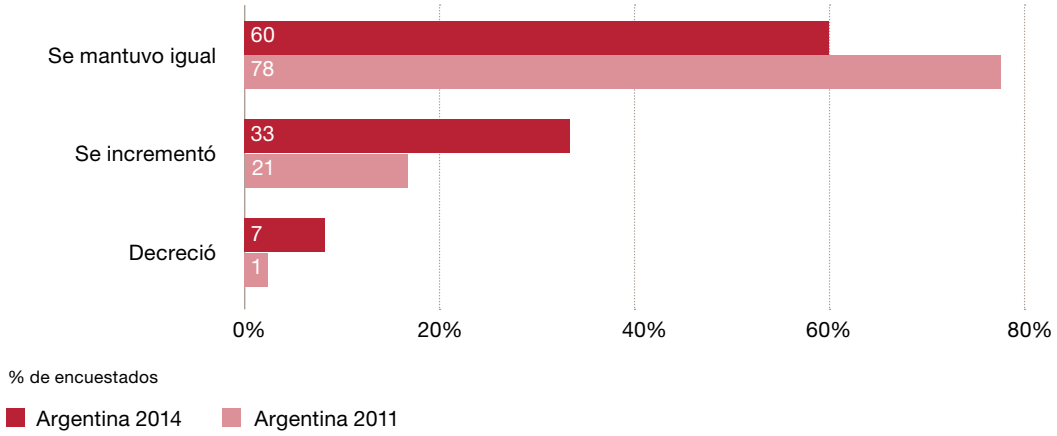
Aumentó 16 puntos porcentuales la percepción de ser víctima de un fraude en los próximos 12 meses.

Una seria amenaza para las compañías argentinas

Nuestro informe de 2011 fue el primero de la serie en destacar los delitos informáticos como una amenaza que exigía la atención de las organizaciones: un 9% de los encuestados en Argentina reportaron ser víctimas de este tipo de delito. Ahora, en el 2014, el porcentaje de casos saltó al 21% (20% en Latinoamérica y 24% a nivel global). Es decir, los delitos informáticos se convirtieron en el segundo tipo de fraude más reportado por las empresas en Argentina.

Esta tendencia también se confirma con la creciente percepción de sufrir un delito informático. Este año, **el 33% de los encuestados sostiene que su empresa se encuentra más expuesta a ser víctima** de un delito informático en los próximos 12 meses, casi un 50% más con respecto al 2011 (21%).

Gráfico 23. Percepción de sufrir un delito informático en los próximos 12 meses



Lo que no sabe y puede causarle daño

Aquellos que informaron no haber sufrido un delito informático pueden ser víctima y ni siquiera saberlo. Esto es un verdadero motivo de preocupación.

Este panorama se complica, en muchas ocasiones cuando es detectado el delito informático, éste no se denuncia. A menudo (como en los casos de robo de propiedad intelectual), puede haber razones de competitividad para que las organizaciones mantengan silencio.

La conclusión es que gran parte de los daños causados por este tipo de ataques no se dan a conocer, ya sea porque desconocen su existencia, porque son difíciles de cuantificar, o bien porque no se desean compartir. Naturalmente, este tipo de comportamientos plantea riesgos para un ecosistema global de negocios, cada vez es más dependiente de la tecnología y de la propiedad intelectual.

Es un entorno peligroso aquél donde puede ser más fácil robar un activo intangible vital, que cuantificar, revelar o al menos darse cuenta de una pérdida de este tipo.

Un objetivo en movimiento

En un contexto tecnológico cambiante, los adversarios sofisticados sacan ventaja atacando nuevas debilidades. Este es el motivo por el cual las compañías tratan al menos de no perderles el ritmo a los delincuentes que las acechan.

Incluso cuando las organizaciones están al tanto de los tipos de ciber-amenazas que enfrentan, muchas no comprenden realmente la capacidad de los ciber-delincuentes, cuáles pueden ser sus objetivos y cuál será el valor de esos objetivos. Las compañías continúan poniendo su información crítica a disposición de la gerencia, los empleados, proveedores y clientes a través de una gran cantidad de plataformas, que pueden ser de alto riesgo, como los dispositivos móviles y la "nube", dado que los beneficios económicos y competitivos parecen ser convincentes.

Si bien nadie espera que los beneficios de la tecnología disminuyan ni que las entidades reduzcan su huella digital, resulta claro que –con más información accesible en más plataformas- la información valiosa estará amenazada, y el costo de las violaciones de seguridad continuará siendo elevado. De hecho, en cada región, entre un cuarto y un tercio de las compañías manifestaron creer que sufrirán delitos informáticos en un futuro cercano.

Los delitos informáticos son un problema estratégico

Creemos que los delitos informáticos no son un problema de la tecnología estrictamente hablando. Sino que son un problema estratégico, humano y de procesos.

Las organizaciones no están siendo atacadas por computadoras, sino por personas que intentan aprovecharse tanto de la fragilidad humana como de la vulnerabilidad técnica. Motivo por el cual, dicha problemática requiere una respuesta en los procesos de negocio, accesos, autoridad, delegación, supervisión y conciencia, y no solamente en herramientas y tecnologías.

Esto se puede ilustrar al menos de cuatro maneras. En primer lugar, las personas son el vínculo más débil en la cadena de seguridad. Los **hackers**, con frecuencia, **se aprovechan de la ingenuidad humana** a través de ataques tales como "spear phishing" (suplantación de identidad) – es un abuso informático realizado a través de un correo electrónico de una fuente confiable, como un banco - para tomar ventaja sobre el usuario distraído. Los hackers pueden tratar de desencriptar códigos de datos, o pueden adivinar, robar o sobornar para conseguir una contraseña. La encriptación se duplica cada 18 meses, pero la habilidad del cerebro humano para recordar una contraseña compleja, sin escribirla, no ha mejorado.

En segundo lugar, **los hackers pueden innovar tanto sus procesos tecnológicos como los no tecnológicos**. Por ejemplo, puede identificar una falla en el sistema de cajeros automáticos y coordinar que varias personas, al mismo tiempo, en diferentes cajeros, extraigan dinero, aprovechándose de la debilidad. Ello refleja cómo la "productividad" del hacker ha multiplicado su eficacia en magnitud; no porque emplee nuevas tecnologías, sino por el mejor uso organizado de las "mulas".

En tercer lugar, **las soluciones de seguridad informática generalmente requieren del uso de herramientas y procesos no tecnológicos:** capacitación y concientización, involucramiento de expertos en asuntos privados o legales, relación con los medios, manejo de crisis y planes de remediación de soluciones para descubrir el delito cibernético.

Finalmente, una seguridad efectiva requiere que la gente **esté concentrada en sus datos más importantes**. Las empresas que realizan un inventario de sus activos de información y priorizan los datos de sus redes, son capaces de concentrarse en sus bienes más preciados, y usarán de manera astuta sus limitados presupuestos para combatir delitos informáticos.

La seguridad informática es una cuestión de negocios para la alta gerencia. El equipo de TI tiene que conocer cuáles son las mejores herramientas y tecnologías para la compañía, pero no podrán ayudar mucho si la **protección de los activos está erróneamente enfocada**.

Los delitos informáticos amenazan los procesos de negocio que utilizan tecnología.

El creciente uso de procesos de negocio que utilizan tecnología hace que los delitos informáticos sean una verdadera amenaza para una amplia gama de operaciones comerciales. En nuestra experiencia reciente, los sistemas más amenazados son aquellos que contienen datos personales, o que se relacionan de manera directa con activos financieros que pueden ser robados. Las amenazas son:

- ***Puntos de venta*** de compras cotidianas por medio de tarjeta de débito o crédito.
- ***Transacciones bancarias*** en cajeros automáticos.
- ***Privacidad de los clientes***. Debe ser preservada y respetada. Esto es particularmente importante en la industria del cuidado de la salud, donde los proveedores por lo general tienen sistemas con información crítica de pacientes, incluyendo identidad, posición financiera, plan de seguro médico y estado de salud.
- ***Comercio electrónico o procesos de venta en línea***. Igual que la penetración de los sistemas de puntos de venta en los comercios minoristas o en bancos, excepto que éstos se producen en línea.
- ***Comunicaciones de negocio electrónicas (correo electrónico)***. Los ciber-delincuentes externos pueden acceder a los sistemas de comunicación corporativos y robar información –crítica- comercial, propiedad intelectual y comunicaciones ejecutivas confidenciales.
- ***Puntos débiles de la infraestructura*** para perpetrar algunos de los delitos expresados anteriormente. Por ejemplo, accediendo a puntos de acceso WIFI o interceptando las comunicaciones de otras personas a través de estos puntos de acceso, o atacando los entornos de servidores que son mantenidos por un prestador de servicios en la "nube".
- ***Incentivos a los consumidores***. La lealtad y otros programas de incentivo que retienen datos de los clientes y sus hábitos/preferencias de gastos, ofrecen un gran volumen de datos que pueden ser utilizados para el robo de identidad y para convertirse en blanco de otros delitos informáticos.
- ***Fusiones y Adquisiciones***. Luego de realizada una fusión o adquisición, la compañía podría demorar la integración completa de las políticas de seguridad de la información, procesos y herramientas. Esto conlleva vulnerabilidades en el ambiente de TI a nivel corporativo, que puede ser aprovechado por hackers, accediendo a bases de datos que contienen propiedad intelectual y demás información confidencial valiosa.
- ***Cadena de abastecimiento***. Los proveedores, contratistas y distribuidores son parte del ecosistema de una compañía - con frecuencia, el personal está autorizado a acceder a datos y sistemas confidenciales. El riesgo de ellos, es su propio riesgo, y una ruptura en la cadena de abastecimiento puede tener efectos en cascada en la seguridad de las redes o, peor aún, permitir el acceso directo a información confidencial.
- ***Investigación, desarrollo e ingeniería***. Las tecnologías propias, los secretos comerciales y la propiedad intelectual son blancos de países, empresas gubernamentales y corporaciones poco éticas. Las empresas han perdido miles de millones de dólares a través del robo, por parte de hackers o personal interno, de propiedad intelectual para beneficiar a los competidores.
- ***Expansión a nuevos mercados***. Cuando una empresa ingresa en un mercado geográficamente nuevo, puede convertirse en el blanco del gobierno o de los competidores locales que quieren robarle su tecnología, listado de clientes o planes de comercialización. Si la empresa está literalmente de "visitante", el problema del personal interno se extiende más allá de los empleados, alcanzando a proveedores de instalaciones, consultoras, servicios de mantenimiento e inclusive organismos gubernamentales.

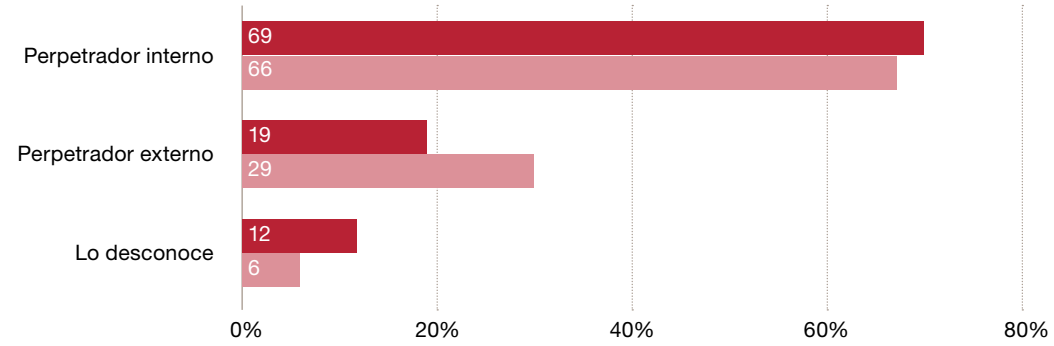
La amenaza de sufrir un fraude continua siendo mayormente interna.

Defraudador: conociendo a su enemigo

Al igual que cualquier batalla, **una regla de oro en la lucha contra los delitos económicos es conocer al enemigo**. En este sentido, es interesante que el 69% de los encuestados señaló como interno al principal perpetrador, continuando la tendencia de nuestra anterior encuesta (66%).

Sin embargo, pareciera ser que no todas las organizaciones están convencidas de esta "regla de oro", o todavía no la lograron aplicar eficazmente. El 12% de los encuestados desconoce si el perpetrador fue interno o externo. Esta cifra no sólo dobla la del 2011, sino que también es superior a la de América Latina (7%) y el resto del mundo (4%).

Gráfico 24. Perpetrador del fraude



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Conocer de dónde proviene la amenaza nos permite distribuir mejor los esfuerzos: si la amenaza es externa, entonces reforzaremos en primer lugar aquellos procesos donde la participación de terceros es relevante.

Gráfico 25. Procesos de negocio bajo amenaza

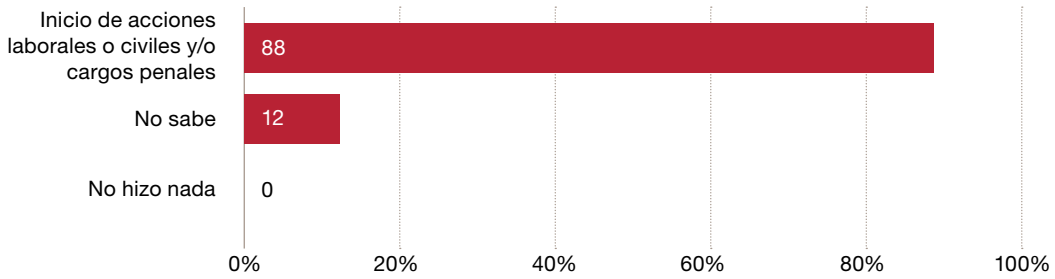
Industria	¿Qué procesos/áreas reforzar?
Servicios financieros	Alta de clientes
	Otorgamiento de préstamos
	Transacciones a través de home-banking
Energía, servicios públicos y minería	Contratación de servicios, contratistas y locaciones
Productos industriales y consumo masivo	Venta canal mayorista
	Transporte de mercadería
Seguros y Salud	Pago a prestadores de servicio
	Reintegro de gastos a beneficiarios
	Pago de siniestros

Al contrario, si el perpetrador es interno, en principio todo proceso es vulnerable, y más que nunca debemos enfocarnos en la cultura de la organización:

- predicando con el ejemplo por parte de la alta dirección,
- transmitiendo los principios y valores de la organización con un código de ética,
- implementando una línea de denuncias independiente, confidencial y anónima donde un empleado pueda denunciar una situación irregular y, sobre todo,
- teniendo tolerancia cero cuando un incidente ocurre.

Analizando los tipos de fraude cometidos, de 28 organizaciones argentinas que reportaron haber sufrido un delito de malversación de activos, 23 identificaron que el delito fue cometido por un perpetrador interno. Sabiendo que el perpetrador más frecuente trabaja en la propia empresa, las **organizaciones disponen de un amplio abanico de herramientas para prevenirlo y disuadirlo**, desde mejorar las actividades de control de cada proceso de negocio expuesto a un siniestro, hasta la aplicación de sanciones ejemplificadoras a los empleados infieles. Justamente, nuestra encuesta nos muestra que el 83% de las organizaciones víctimas de un delito iniciaron acciones laborales, civiles y/o penales contra el perpetrador.

Gráfico 26. Acciones realizadas por las empresas argentinas para con el perpetrador



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

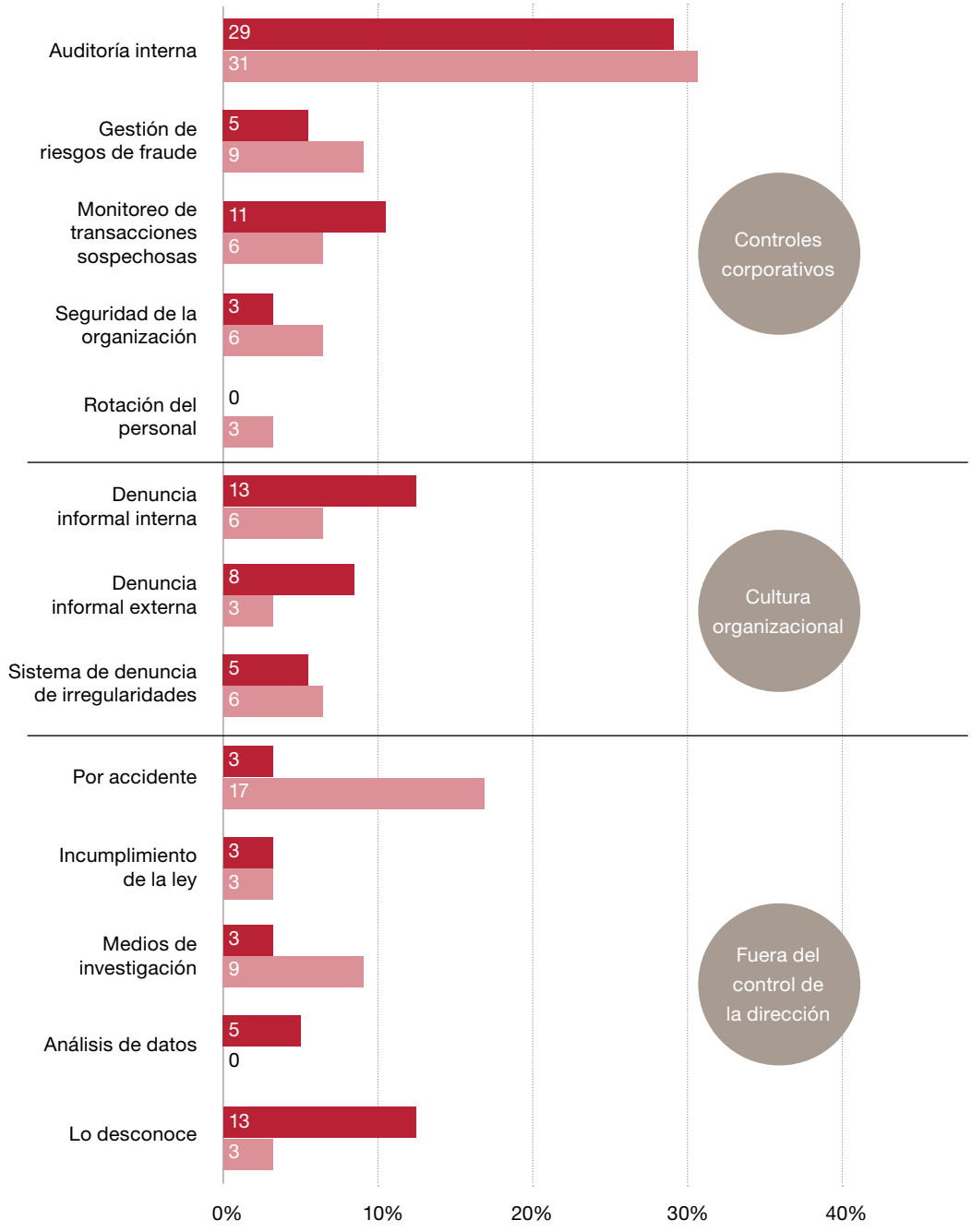
Argentina 2014

Capturar al ladrón

Entonces, ¿cómo prevenir y/o detectar un delito económico antes que suceda o, por lo menos, mientras está ocurriendo?

Los métodos de detección de fraude por lo general se encuadran en una de estas tres categorías: controles corporativos, cultura organizacional o eventos fuera del control de la dirección. El siguiente gráfico muestra los métodos mediante los cuales se detectó al defraudador.

Gráfico 27. Métodos de detección de fraude utilizados



% sobre los encuestados que sufrieron un delito económico los últimos 24 meses

Argentina 2014 Argentina 2011

Al igual que 2011, **auditoría interna** continúa siendo el método que más casos de fraude detectó en nuestro país, mientras que a nivel global el monitoreo de transacciones sospechosas se consolida como el más utilizado. Igualmente, este año podemos observar un leve cambio en ciertas categorías de detección, empezando a **imitar las tendencias globales**. Notamos un crecimiento tanto en el monitoreo de transacciones sospechosas como en el análisis de datos.

Gráfico 28. Métodos de detección más utilizados

	Argentina	América Latina	Global
1°	Auditoría interna	Auditoría interna	Monitoreo de transacciones sospechosas
2°	Denuncia informal interna / Lo desconoce	Análisis de datos	Auditoría Interna
3°	Monitoreo de transacciones sospechosas	Monitoreo de transacciones sospechosas	Evaluación del riesgo de fraudes

Por último y no menos importante, llama la atención el incremento en el número de encuestados que indicaron desconocer cómo fue detectado el fraude con respecto a las cifras de la encuesta de 2011. Ante este dato, hay que recordar que no hay método más eficaz que la **"sensación de control"** o la de **"ser descubierto"**.

Sistema de denuncia de irregularidades

En términos de implementación de una línea de denuncias, 52 % de las compañías argentinas respondieron tenerla implementada. Si bien el porcentaje es considerable, aún se encuentra por debajo de la tendencia regional y global (66% y 62% respectivamente). Un dato relevante es que el 16% de los encuestados en Argentina desconoce si su compañía posee un mecanismo de línea de denuncias, 8% a nivel global y 7% en Latinoamérica. Que los empleados desconozcan si su empresa aplica esta herramienta, revela que **la difusión** de este mecanismo, de haberse implementado, **no fue del todo efectiva**.

Fraude interno: el enemigo escondiéndose de la vista de todos

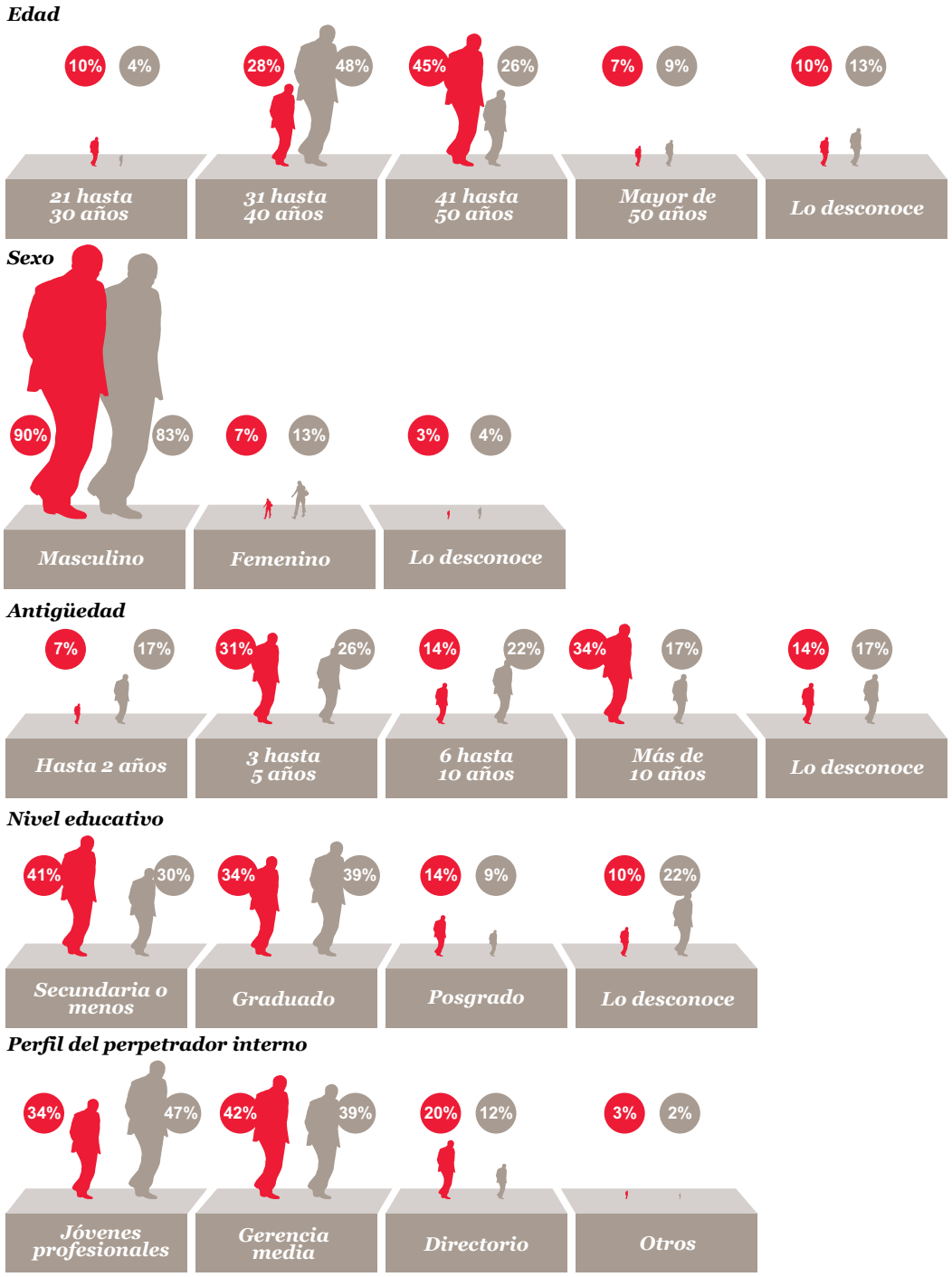
Los profesionales de la práctica contra el fraude se refieren comúnmente al "Triángulo del Fraude", haciendo referencia a tres elementos que a menudo están presentes cuando un perpetrador comete un delito económico: **la presión, la oportunidad y la racionalización**.

En nuestro país, 23 de 29 encuestados indicaron que la **oportunidad** fue el factor desencadenante para que el perpetrador cometa un fraude. Si bien esta noticia puede parecer decepcionante a primera vista, es importante tener en cuenta que, de los tres factores, la oportunidad es el más controlable por la organización. Mientras que las **presiones** y la **racionalización** pueden girar en torno a los empleados, si una organización puede limitar las oportunidades (ejemplo: mitigar el riesgo que un control falle), puede ser capaz de detener el fraude antes que éste comience.

Por otro lado, si bien no podemos especificar cuál fue la presión específica o la racionalización detrás de cada acto de fraude interno, al menos podemos describir el perfil del perpetrador más común: **gerente, de sexo masculino, de entre 41 y 50 años, con estudios secundarios y que ha trabajado en la organización por más de 10 años**.

Comparando con el 2011, este año el perpetrador resultó más grande de edad, con mayor antigüedad en la empresa y menor preparación académica. Ésto, nos confirma que el fraude es una amenaza latente, que atraviesa a la organización en todos sus estamentos, y quien lo comete es aquél que tuvo la capacidad de **identificar la oportunidad para poder cometerlo**.

Gráfico 29. Edad, sexo, antigüedad, nivel educativo y perfil del perpetrador interno



% sobre los encuestados que sufrieron un delito económico por un perpetrador interno

Argentina 2014 Argentina 2011

82 encuestados argentinos completaron la Encuesta Global de Delitos Económicos 2014.

Apéndice
Información regional

Gráfico 30. Países que reportan menos fraude

País	2014	2011
Malasia	24%	44%
Italia	23%	17%
Turquía	21%	20%
Perú	20%	35%
Hong Kong / Macao *	16%	N/A
Japón	15%	5%
Portugal	12%	N/A
Dinamarca	12%	29%
Arabia Saudita**	11%	N/A
Global	**37%**	**34%**

*Parte de China 2011. ** Parte del Medio Oriente 2011

África sigue a la cabeza en cuanto a los delitos económicos reportados, aunque la brecha se ha reducido desde 2011. Medio Oriente presenta una situación única: bajos niveles generales de delitos económicos reportados pero los que informaron haber sufrido un hecho de fraude mostraron un alto número de tipos y casos de fraude.

Gráfico 31. Fraude reportado por regiones

Región	2014	2011
África	50%	59%
Norteamérica	41%	42%
Europa del Este	39%	30%
Latinoamérica	35%	37%
Europa del Oeste	35%	30%
Asia Pacífico	32%	31%
Medio Oriente	21%	28%
Global	**37%**	**34%**

Acerca del perpetrador externo

Los resultados de la encuesta argentina no nos permitieron analizar la situación local de las organizaciones con respecto a los perpetradores externos. En virtud de ello, a continuación se exhiben los resultados más destacables de América Latina y globales.

Gráfico 32. Perfil del defraudador externo

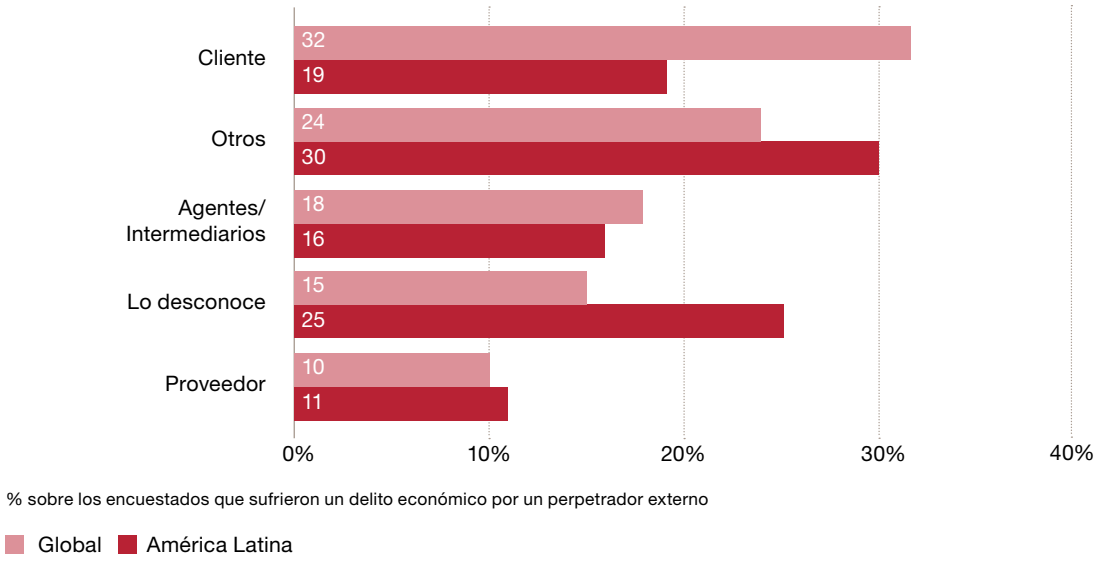
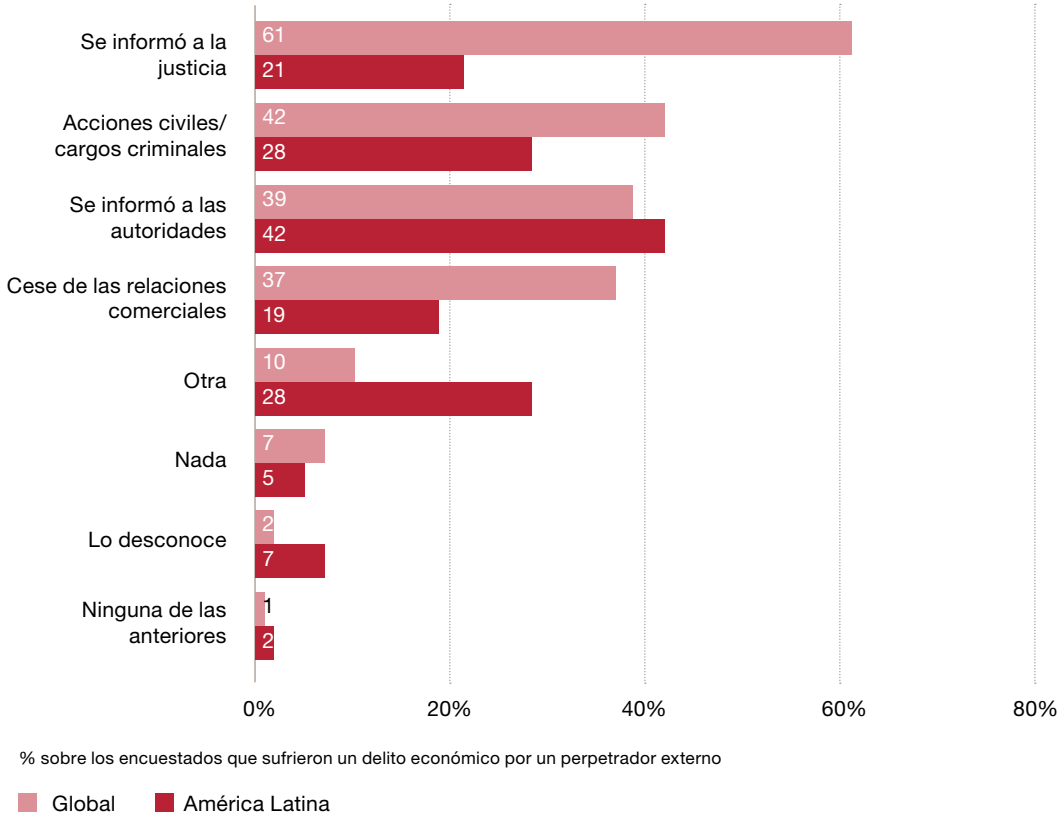


Gráfico 33. Acciones llevadas a cabo contra los defraudadores externos



Metodología

Hemos llevado a cabo nuestra séptima Encuesta Global de Delitos Económicos entre agosto de 2013 y febrero de 2014.

La encuesta constó de cuatro secciones:

- el perfil general de los encuestados;
- las preguntas comparativas teniendo en cuenta qué delito económico habían experimentado las organizaciones;
- las amenazas del delito informático; y
- la corrupción/ soborno y el lavado de activos.

Acerca de la encuesta

La Encuesta Global de Delitos Económicos 2014 se completó con 5.128 encuestados (frente a los 3.877 encuestados en 2011) de 99 países (en comparación con 78 países en 2011). En el caso de Argentina, 82 fueron las empresas encuestadas. Sobre el total de encuestados, 39% eran ejecutivos de la alta gerencia.

Utilizamos las siguientes técnicas de investigación:

1. Encuesta de los ejecutivos en la organización. Los hallazgos de este estudio provienen de las respuestas brindadas por directivos empresarios acerca de los delitos económicos en sus organizaciones. Obtuvimos respuestas sobre los distintos tipos de delincuencia económica sufrida, el impacto en la organización (tanto la pérdida financiera como cualquier otro daño colateral), los perpetradores de estos delitos, qué medidas la organización adoptó y cómo respondieron frente a la delincuencia.

2. Cuestiones relativas al delito informático, la corrupción / soborno y el lavado de dinero. Esta encuesta toma una mirada detallada a estas amenazas que suelen ser de carácter sistémico y por lo tanto son más propensas a ser de largo plazo, dañando con gran impacto a la organización.

3. Análisis de las tendencias en el tiempo. Desde que empezamos a hacer estas encuestas en el año 2001, hemos hecho una serie de preguntas fundamentales, y algunas otras que son relevantes según el momento, lidiando con aspectos que probablemente tengan un impacto en las organizaciones de todo el mundo. Con estos datos históricos disponibles, podemos ver temas actuales, desarrollar gráficos, e identificar tendencias.

Otras fuentes:

- PwC—17ma. Encuesta Anual de CEOs [http://www.pwc.com/gx/en/ceo-survey/]
- PwC—Building Trust in a Time of Change: Global Annual Review 2013 [http://www.pwc.com/gx/en/annual-review/megatrends/index.jhtml]
- PwC—Global State of Information Security Survey [http://www.pwc.com/gx/en/consultingservices/information-security-survey/index.jhtml]
- PwC – 7ma. Encuesta Global sobre Delitos Económicos [http://www.pwc.com/crimesurvey]

Gráfico 34. Posición de los encuestados argentinos

Miembro del consejo de administración	7%
Consejero delegado/ Presidente/ Director General	7%
Director financiero/ Tesorero/ Controller	9%
Director de sistemas de información/ Director Tecnológico	4%
Director de seguridad	2%
Director	9%
Jefe de división	5%
Jefe de departamento	16%
Gerente	38%
Otros	3%

Gráfico 35. Tipo de organizaciones argentinas participantes

Empresa cotizada (en Bolsa de Valores)	34%
Privada	56%
Sector público/ Empresa pública	7%
Otras industrias/ sectores	3%

Gráfico 36. Industrias participantes

Industria	América Latina	Global
Servicios financieros	22%	26%
Telecomunicaciones	4%	3%
Venta mayorista y minorista	11%	10%
Servicios profesionales	4%	4%
Farmacéuticas	6%	4%
Energía, servicios públicos y minería	11%	6%
Logística	6%	5%
Manufactura	8%	9%
Seguros	6%	6%
Ingeniería y construcción	6%	5%
Química	3%	1%
Otros	4%	5%
Tecnología	2%	3%
Empresas públicas	2%	6%
Salud	1%	2%
Medios y entretenimiento	1%	2%
Automotriz	6%	3%
Defensa	0%	1%

Terminología

Fraude en los estados contables

Alteración de los estados contables y/u otros reportes económicos-financieros de modo que no representen la realidad económica de las operaciones que realiza la organización. Ya sea a través de la manipulación de los principios contables, ocultando la verdadera situación patrimonial a la hora de tomar un préstamo, o por ejemplo para poder acceder a financiación en los mercados de capitales.

Malversación de activos incluyendo engaño por parte de los empleados

El robo de activos (incluidos activos monetarios / dinero o suministros y equipamiento) por parte de los directores, aquellos que se encuentren en posiciones fiduciarias o cualquier empleado para su propio beneficio.

Soborno y corrupción

El uso ilegal de una posición privilegiada obteniendo una ventaja en contraposición con el deber. Ésto 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 incentivos. Por ejemplo: sobornos, extorsiones, regalos (con segundas intenciones), propinas, etc.

Delito informático

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.

Delito económico

El uso deliberado del engaño para privar a otro tanto de dinero, propiedad o como de un derecho legal.

Espionaje

Es el acto o la práctica de espiar o contratar espías para obtener información confidencial.

Pérdida financiera

Cuando se estiman las pérdidas financieras debido al fraude, los participantes deberían incluir tanto la pérdida directa como indirecta. La primera refiere al costo del fraude y la segunda puede incluir los gastos relacionados con la investigación y remediación del problema, las sanciones impuestas por las autoridades oficiales y los costos judiciales.

Esto excluiría cualquier monto estimado a “pérdida de oportunidad de negocio”.

Evaluación del riesgo de fraude

Las evaluaciones de riesgo de fraude se utilizan para determinar si una organización ha realizado acciones para establecer:

i. Los riesgos de fraude asociados a cada operación;

ii. Los riesgos críticos (es decir, evaluar los riesgos por impacto y probabilidad de ocurrencia);

iii. La identificación y evaluación de los controles clave (si los hay) vigentes para mitigar los riesgos;

iv. La evaluación del programa anti-fraude en general y los controles establecidos;

v. Las acciones para remediar las debilidades en los controles.

Fraude en recursos humanos (Contratación y payroll)

Es realizado por los miembros del departamento de Recursos Humanos, incluyendo el fraude de payroll, empleados fantasmas, pagar para trabajar, contrataciones (ejemplo, contratar amigos y/o familiares, gente no capacitada, falsificación de documentos, etc.), entre otros.

Incentivos / presión para trabajar

El individuo tiene un problema financiero que es incapaz de resolverlo legítimamente. Entonces considera que cometer un acto ilegal es su única manera de resolver el asunto. El problema financiero puede ser profesional (por ejemplo, el trabajo está en peligro) o personal (por ejemplo, una deuda de juego).

Abuso de información privilegiada

El abuso de información privilegiada se refiere generalmente a la compra o venta de un título de valor, violando la obligación fiduciaria o en detrimento de otro tipo de relación de confianza. Es decir, la obtención de información relevante y no perteneciente al dominio público. Los incumplimientos relacionados con el abuso de información privilegiada también podrán incluir la divulgación de información privilegiada sobre esos títulos, la comercialización de títulos por parte de la persona que recibió esa información privilegiada, y la comercialización de títulos por parte de quienes se apropian indebidamente de esa información.

Delito contra la propiedad intelectual y/o industrial (incluyendo marcas, patentes, falsificación de productos y servicios)

Esto incluye el robo de información de la compañía, la copia y/o distribución ilegal de productos falsificados que se encuentran en infracción ya sea de patente o derecho de autor, o la creación de monedas y billetes con la intención de que sean genuinos.

Mercados con alto nivel de riesgo de corrupción

Basándonos en el Índice de Percepción de Corrupción del organismo "Transparency International", determinamos que para considerar un mercado de alto riesgo debe obtener una puntuación de 50 o menos.

Lavado de activos

Acciones cuya intención es legitimar la procedencia de activos provenientes del crimen organizado, disfrazando su verdadero origen.

Oportunidad o capacidad

El individuo encuentra alguna manera en que pueda abusar de su posición de confianza para resolver su problema financiero con un bajo riesgo de ser atrapado.

Fraude en compras y contrataciones

Conducta ilegal por la cual el delincuente obtiene una ventaja, evita la obligación o daño a su organización. El delincuente puede llegar a ser un empleado, propietario, miembro del directorio, un funcionario, una figura pública o un proveedor que estuvo involucrado en la compra de servicios, bienes o activos de la organización afectada.

Racionalización

El individuo encuentra la manera de justificar el delito cometido de una manera que hace que para él sea un acto aceptable o justificable.

Fraude fiscal

Una práctica ilegal donde una organización o una corporación evitan intencionalmente el pago de su verdadera obligación fiscal

PwC Forensic Services comprende especialistas en investigación de fraudes y en tecnología forense, contadores, economistas, actuarios y ex-funcionarios de la justicia. Ayudamos a las organizaciones a hacer frente a los principales riesgos financieros y reputacionales asociados a los delitos económicos. Identificamos irregularidades, analizamos complejos problemas de negocio, y mitigamos el riesgo de fraude.

Contactos

Jorge C. Bacher
Socio, Buenos Aires, Argentina
(+5411) 4850 6814
jorge.c.bacher@ar.pwc.com

Andrés Sarcuno
Gerente, Buenos Aires, Argentina
(+5411) 4850 6887
andres.sarcuno@ar.pwc.com

Leandro Castro
Financial and Accounting Investigations
Buenos Aires, Argentina
leandro.castro@ar.pwc.com

Ignacio Aquino
Socio, Buenos Aires, Argentina
(+5411) 4850 6816
ignacio.aquino@ar.pwc.com

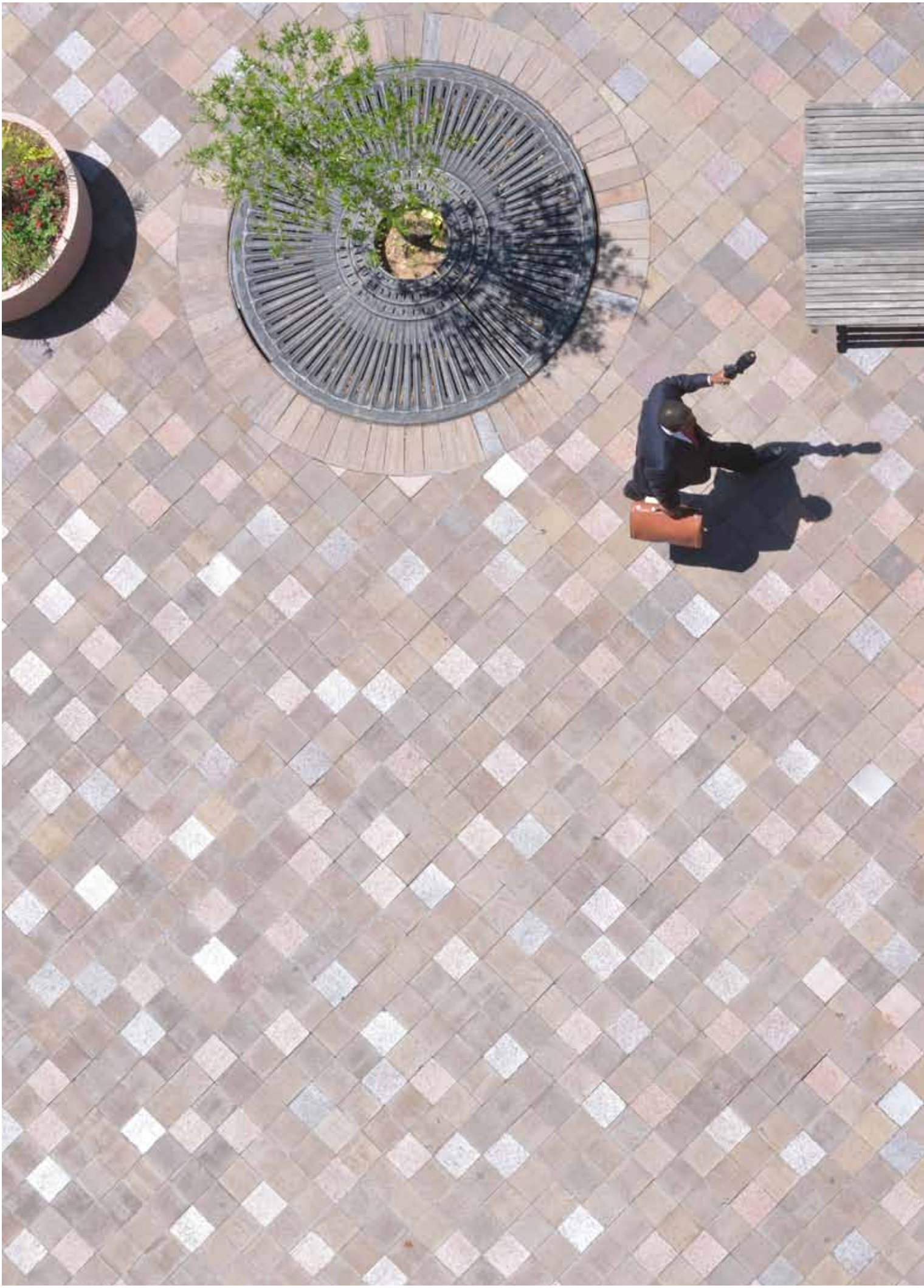
Kurt Kolakauskas
Gerente, Buenos Aires, Argentina
(+5411) 4850 6887
kurt.kolakauskas@ar.pwc.com

Martin Strizic
Corporate Intelligence
Buenos Aires, Argentina
martin.strizic@ar.pwc.com

Forensic Technology Solutions

Diego Taich
Director, Buenos Aires, Argentina
(+5411) 4850 6834
diego.taich@ar.pwc.com

Andrea Navarro
Gerente, Buenos Aires, Argentina
(+5411) 4850 6243
andrea.navarro@ar.pwc.com



www.pwc.com/ar