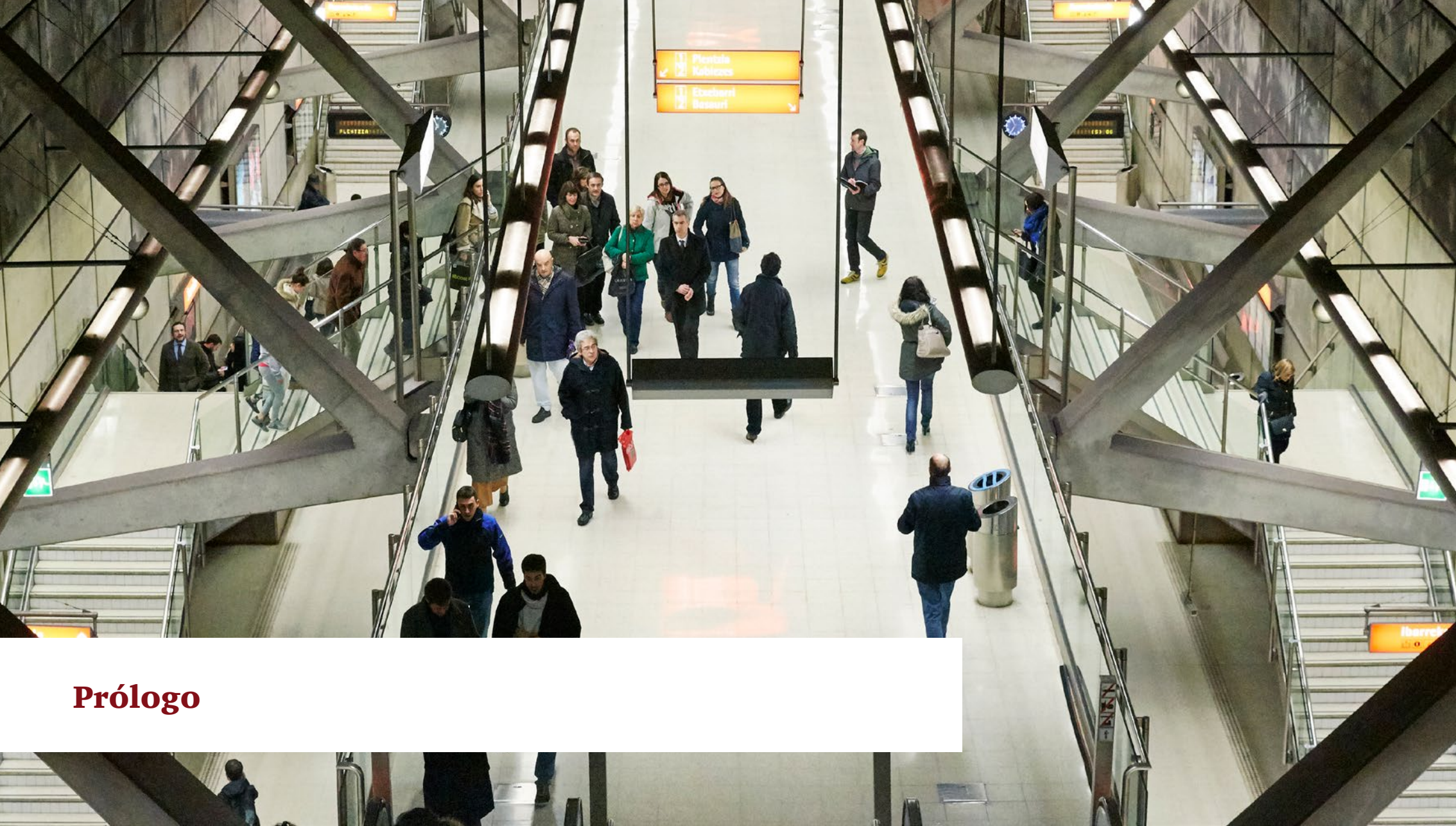
Fraude al descubierto

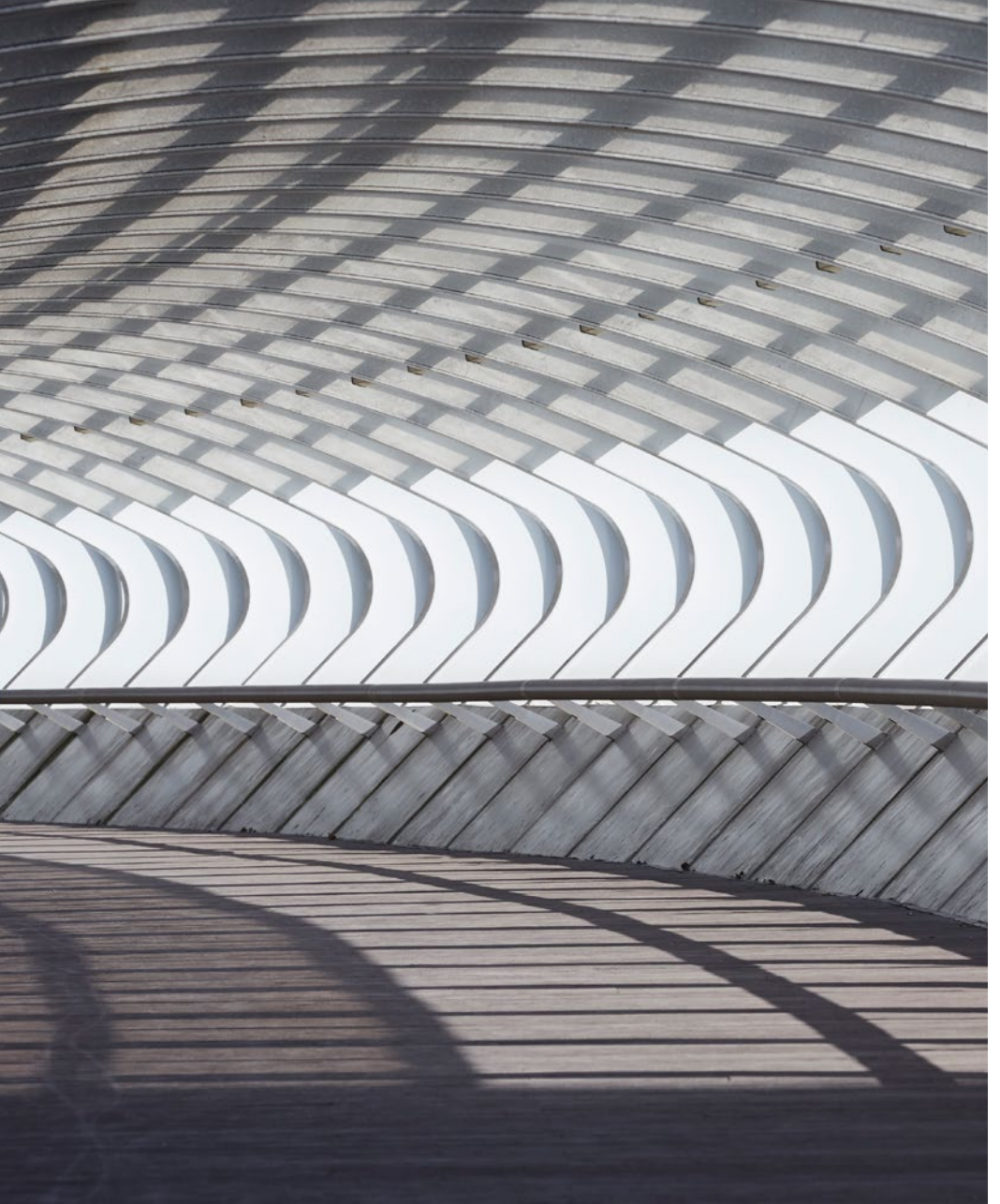
Encuesta Global Crimen Económico 2018

Colombia

pwc



Prólogo



Mónica Jiménez
Socia Líder Advisory

Uno de los primeros pasos en un proceso de cambio o transformación, es el reconocer que algo debe ser cambiado porque está fallando, o porque se puede mejorar. Tener consciencia, es la capacidad de reconocerse y verse, ¿entonces será que estamos teniendo más consciencia del fraude y por lo tanto estamos reconociendo en una mejor medida su existencia? Las estadísticas de este año en las compañías colombianas muestran un crecimiento del fraude; hoy el 39% de los encuestados reconoce haberlo sufrido, comparado con el 32% de hace un par de años. ¿Ha crecido más de un 20% el fraude en los últimos dos años? o ¿Somos más conscientes de su existencia?

Otro de los aspectos importantes que aparecen alrededor del tema de fraude, y del que hoy somos más conscientes, es el riesgo reputacional y la exposición que tenemos al mismo con la materialización de un fraude. Las noticias malas viajan rápido, y con las comunicaciones digitales que existen hoy en día, viajan literalmente a la velocidad de la luz. Este fenómeno ocurre en todos los continentes y en todos los países, no importa su nivel de desarrollo; las comunicaciones están llegando a todos los lugares del mundo y con ellas el riesgo reputacional se irradia como una ráfaga de luz. Hoy se observa una gran preocupación por este tema y con ello hay una gran cantidad de signos de convergencia sobre los estándares de transparencia y el comportamiento ético del individuo.

¿Entonces qué actividades están emergiendo para pensar que estamos combatiéndolo en la dirección correcta?

Una de ellas es la tecnología, que si bien nos vuelve vulnerables, también nos puede dar herramientas que nos permitan dar un paso adelante en la lucha contra el fraude. Si utilizamos la tecnología en toda su capacidad predictiva, podemos incrementar nuestra capacidad de protegernos también.

Hoy tenemos la robotización como una de las herramientas que transformarán el entorno de los negocios. Hemos pasado de la automatización de procesos de negocios (BPM), a la automatización de

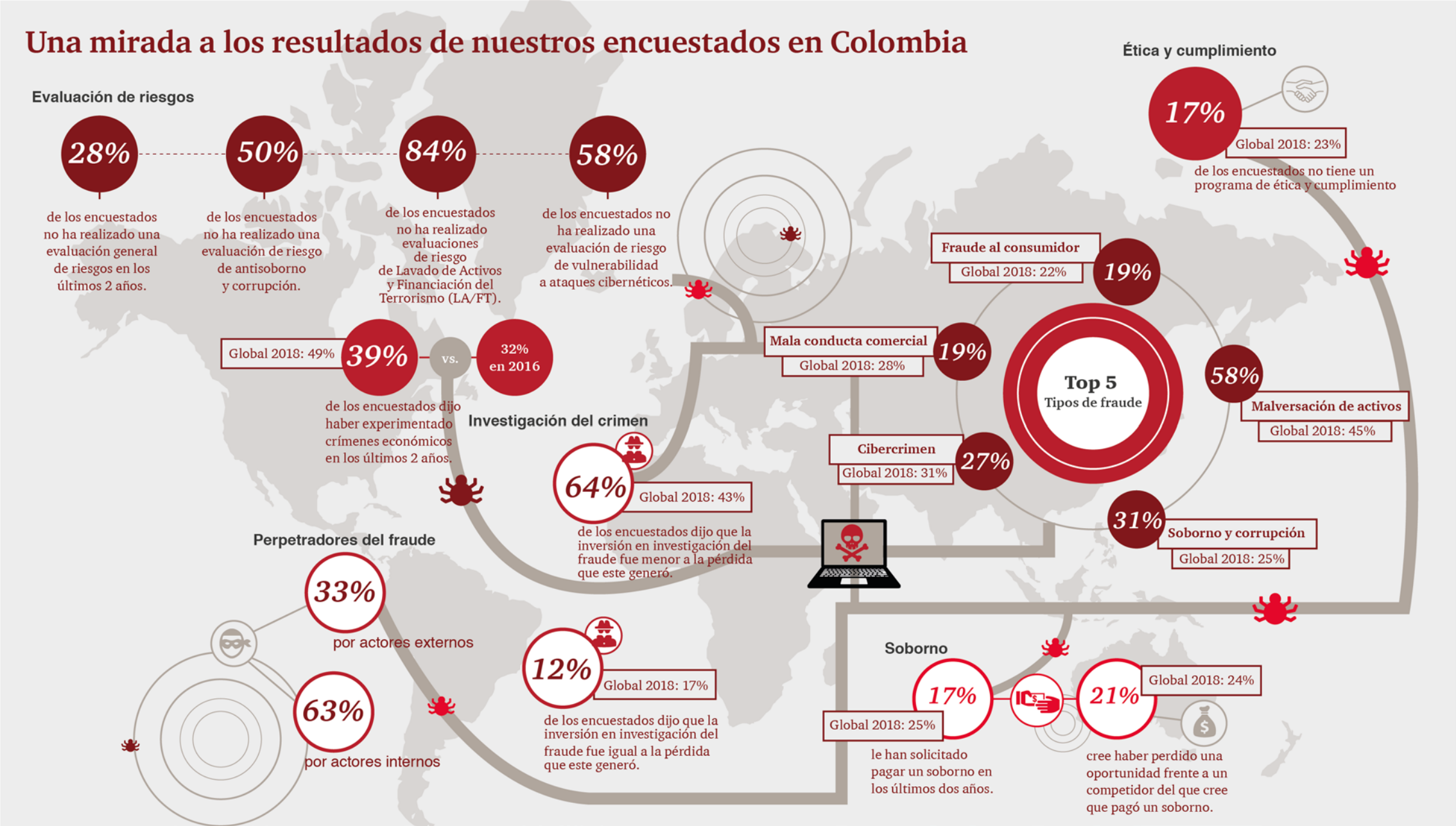
procesos con robots (RPA), para seguir a la automatización inteligente de procesos (IPA). Todo esto lo podemos utilizar para una detección preventiva del fraude, sobre un establecimiento de patrones, banderas rojas y generación de lenguaje natural, sobre máquinas que aprenden. La otra herramienta muy útil será el análisis predictivo de datos, a través de herramientas de analítica, que permitan precisamente alimentar los patrones, alarmas y cada vez predecir con mayor exactitud un comportamiento diferente.

Pero existe un factor fundamental que no podemos dejar a un lado, porque es definitivamente el principal actor en este proceso, y es el ser humano. Detrás de cada máquina, detrás de cada fraude, hay un ser humano protagonista en este escenario. ¿Cuántas y cuáles son las razones para que un individuo o un tercero de una compañía decida involucrarse en cometer un fraude? Son muchas las razones que podemos enumerar, pero indudablemente hay una común a todos, los principios y valores que rigen una sociedad de bien pasan a un segundo plano, y el individuo está dispuesto a sobrepasarlos y asumir el riesgo y las consecuencias que de él se deriven, a costa de conseguir sus objetivos. Y entonces, ¿por qué no invertir en nuestra gente? ¿No podríamos tener una excelente retribución de inversión si sensibilizamos a nuestra gente sobre principios, valores y ética? ¿Y la convertimos en la mejor estrategia para combatir el fraude?

Debemos reconocer cuáles son nuestras fortalezas y debilidades, y trabajar en forma consistente y permanente en esas debilidades de nuestra cultura organizacional, para que la gente comprenda claramente las cosas que la organización está dispuesta a aceptar y aquellas que son inaceptables. Aunque parezca obvio tener claros los comportamientos éticos, los valores y los principios aceptados, esto no es siempre una realidad; es como decir que “una vaca” tiene el mismo significado en India y en Colombia, son significativamente diferentes y así ocurre con los sistemas de valores de los individuos, que pueden ser significativamente diferentes dependiendo de las características del entorno en los que se desarrollen. Nuestro deber es indicarles a nuestros colaboradores que es lo aceptable e inaceptable en el esquema de valores de nuestra compañía, y recordarlo una y otra vez, en forma permanente.

La mitigación del riesgo de fraude debe estar en la agenda de la alta dirección, pues cada vez más se reclama su participación, conocimiento, respuesta e inclusive responsabilidad, en cada evento de este tipo. El riesgo de fraude es un desafío para todos y debemos estar involucradas todos y cada uno de los funcionarios de una organización.

Una mirada a los resultados de nuestros encuestados en Colombia



Evaluación de riesgos

28% de los encuestados no ha realizado una evaluación general de riesgos en los últimos 2 años.

50% de los encuestados no ha realizado una evaluación de riesgo de antisoborno y corrupción.

84% de los encuestados no ha realizado evaluaciones de riesgo de Lavado de Activos y Financiación del Terrorismo (LA/FT).

58% de los encuestados no ha realizado una evaluación de riesgo de vulnerabilidad a ataques cibernéticos.

Ética y cumplimiento

17% de los encuestados no tiene un programa de ética y cumplimiento

Global 2018: 23%

Investigación del crimen

Global 2018: 49% **39%** vs. **32% en 2016**

de los encuestados dijo haber experimentado crímenes económicos en los últimos 2 años.

64% de los encuestados dijo que la inversión en investigación del fraude fue menor a la pérdida que este generó.

Global 2018: 43%

12% de los encuestados dijo que la inversión en investigación del fraude fue igual a la pérdida que este generó.

Global 2018: 17%

Perpetradores del fraude

33% por actores externos

63% por actores internos

Top 5 Tipos de fraude

- **Fraude al consumidor** — **19%** — Global 2018: 22%
- **Mala conducta comercial** — **19%** — Global 2018: 28%
- **Cibercrimen** — **27%** — Global 2018: 31%
- **58%** **Malversación de activos** — Global 2018: 45%
- **31%** **Soborno y corrupción** — Global 2018: 25%

Soborno

17% le han solicitado pagar un soborno en los últimos dos años.

Global 2018: 25%

21% cree haber perdido una oportunidad frente a un competidor del que cree que pagó un soborno.

Global 2018: 24%

Cuatro pasos en la lucha contra el fraude

01

Reconozca el fraude cuando lo vea

02

Tenga un enfoque dinámico

03

Aproveche la capacidad de protección de la tecnología

04

Invierta en la gente, no solo en las máquinas

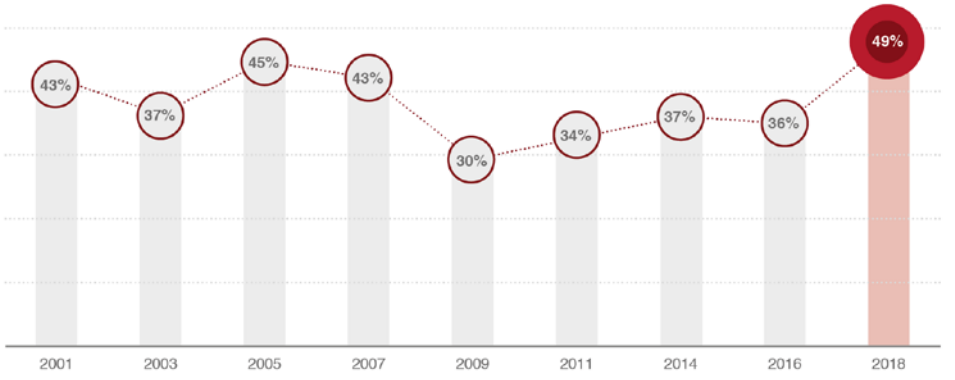
01 Reconozca el fraude cuando lo vea

¿Está **creciendo** realmente el fraude o simplemente ahora somos más **conscientes** de su existencia?

Este año, el 39% de los entrevistados colombianos indicó que su empresa ha sido víctima de algún delito económico; lo cual, se encuentra siete puntos por encima de los reportados en la Encuesta de 2016 (32%). Las cifras de los encuestados globales muestran un incremento de 13 puntos, pasando de 36% en 2016 a 49% en 2018.

Este aumento se puede explicar debido a la combinación de la creciente conciencia global sobre el fraude, un mayor número de respuestas a las encuestas, así como una mayor claridad sobre el significado real de "fraude". Pero cada organización, sin importar cuántos controles y medidas haya implementado, es vulnerable a los puntos ciegos. Y debido a que estos puntos por lo general solo son evidentes cuando algún riesgo se materializa, el identificarlos lo antes posible, puede optimizar sustancialmente los esfuerzos para combatir cualquier delito económico, como el fraude.

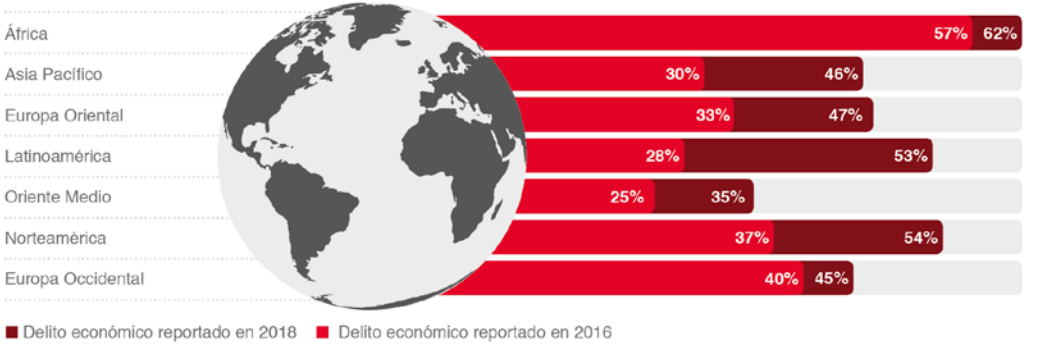
Figura No. 1: La tasa global reportada de delito económico está en ascenso



P. ¿Ha sufrido su organización algún fraude y/o delito económico en los últimos 24 meses?

Fuente: Encuesta Global Crimen Económico PwC 2018

Figura No. 2: La tasa global reportada de delito económico ha aumentado en todos los territorios



P. ¿Ha sufrido su organización algún fraude y/o delito económico en los últimos 24 meses?

Fuente: Encuesta Global Crimen Económico PwC 2018

Así como la tasa reportada de delito económico ha aumentado a nivel global y en Colombia, igualmente ha crecido el número de empresas que invierte en la lucha para combatirlo:

- En ***Colombia***, el 38% de los encuestados dijo que las empresas habían aumentando la inversión para combatir delitos económicos en los últimos dos años.

- Y el 47% de los encuestados expresó que planea aumentar el gasto en los próximos dos años.

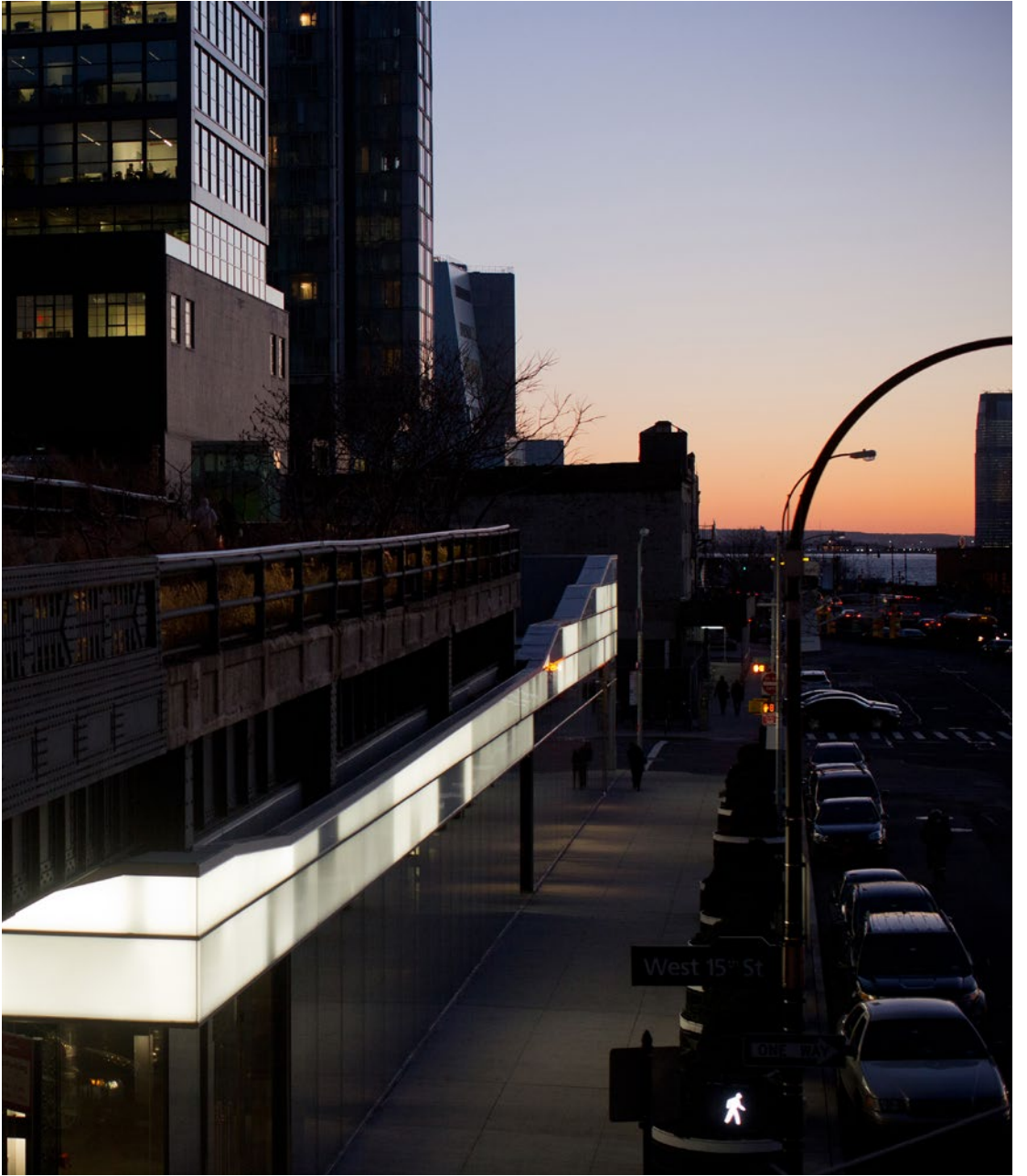
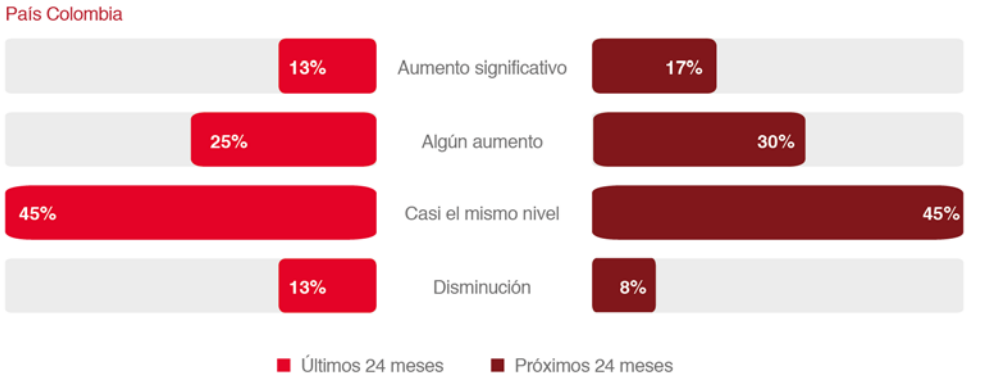


Figura No. 3: En Colombia las organizaciones continúan aumentando la inversión para combatir el fraude



P. ¿Cómo ha ajustado/está ajustando su organización los fondos utilizados para combatir el fraude y/o delito económico?

Fuente: Encuesta Global Crimen Económico PwC 2018

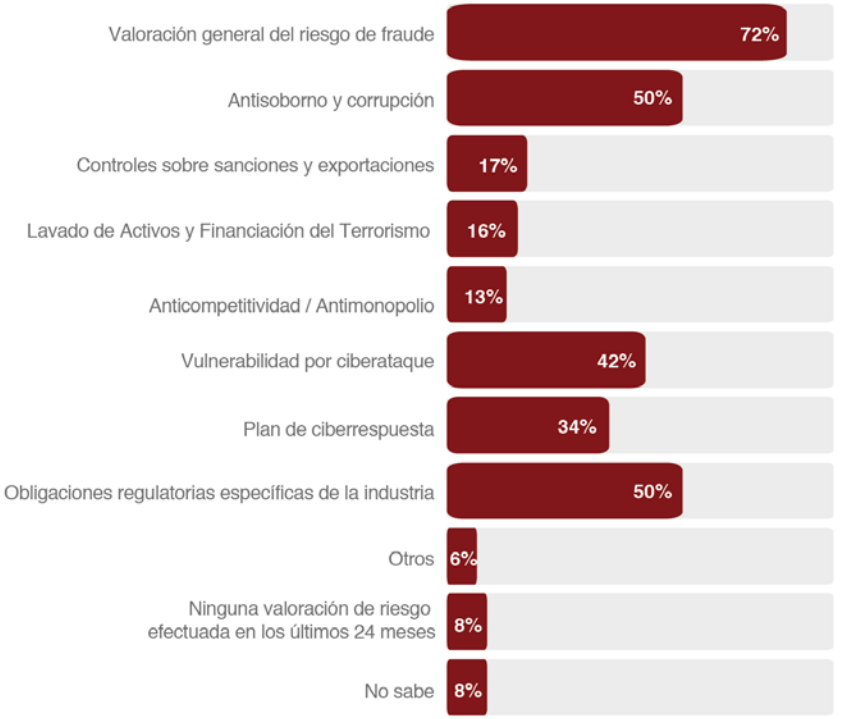
Más que nunca las organizaciones están utilizando tecnología poderosa y herramientas para el análisis de datos con el fin de combatir el fraude. Varios están ampliando también sus sistemas internos de denuncias y tomando las medidas necesarias para mantenerse a la vanguardia. Sin embargo, ¿son estas medidas un cambio genuino hacia enfoques más proactivos con respecto al fraude y la corrupción? ¿O son simplemente una acción defensiva, motivada principalmente por el endurecimiento de la legislación antisoborno y/o anticorrupción, y por formas cada vez más globalizadas del cumplimiento? En otras palabras ¿nos estamos perdiendo todavía de algo vital en la lucha contra el fraude? Los resultados de nuestra encuesta fuertemente sugieren que así es.

"Empezar por el principio": Las evaluaciones de riesgo de fraude, el primer paso para prevenirlo

A pesar del incremento del gasto, muchas organizaciones todavía abordan la prevención del fraude desde una perspectiva reactiva y defensiva, lo cual se refleja en algunos resultados de nuestra encuesta:

- Solo la mitad de las compañías encuestadas llevó a cabo evaluaciones de riesgo en las áreas críticas para prevenir el soborno y la corrupción.
- Menos de la mitad (42%) dijo haber llevado a cabo una evaluación de riesgo de cibercrimen.
- Menos de un tercio indicó haber realizado valoraciones de riesgo relacionadas con lavado de activos, sanciones y control de exportaciones.
- El 28% de las organizaciones colombianas dijo haber llevado a cabo solo una evaluación general de fraude o riesgo de delito económico.
- Y el 8% de los encuestados colombianos dijo no haber realizado ninguna evaluación de riesgo en los últimos 2 años.

Figura No. 4: Solo la mitad o menos de la mitad de los encuestados colombianos realizaron evaluaciones de riesgo específicas en los últimos 2 años



P. ¿En los últimos 24 meses, ha llevado a cabo su organización una valoración de riesgo sobre cualquiera de las siguientes áreas?

Fuente: Encuesta Global Crimen Económico PwC 2018

P. ¿Qué es lo que ha provocado que su organización realice la valoración de riesgo?

Fuente: Encuesta Global Crimen Económico PwC 201

63%

de los CEOs está de acuerdo o totalmente de acuerdo en que actualmente las organizaciones están experimentando una mayor presión para exigir que los líderes sean responsables individualmente por cualquier mala conducta organizacional.

Fuente: CEO Survey Colombia 8va Edición

65%

de los CEOs mide la confianza que existe entre su fuerza laboral y el liderazgo *senior* de su organización.

Fuente: CEO Survey Colombia 8va Edición

Sin embargo, las reglas del juego están cambiando de manera profunda e irreversible. La tolerancia pública frente a la mala conducta corporativa y/o personal se está desvaneciendo.

No solo la sensibilidad sobre la mala conducta corporativa se encuentra en un punto sin precedentes, sino que algunas corporaciones y sus líderes también están siendo llamados a rendir cuentas sobre sus conductas pasadas, cuando las "reglas tácitas" de hacer los negocios se pensaban de otra manera. La XXI Encuesta de CEOs de PwC destaca este tema: en esta, los ejecutivos citan la responsabilidad sobre la confianza y el liderazgo, como las dos amenazas más significativas para el crecimiento empresarial.

Esto conlleva a un mayor riesgo cuando el fraude o el delito económico se filtra a la opinión pública y a una mayor necesidad para que las organizaciones tomen el liderazgo en la prevención del fraude antes de que este se arraigue. Las evaluaciones de riesgo de fraude pueden ayudar a las organizaciones en esta tarea, identificando los fraudes específicos que deben buscar, de acuerdo al perfil de su organización. Esto es relevante además, si se tiene en cuenta que en casos de acciones legales, los reguladores toman este tipo de evaluaciones como un punto a favor de las compañías.

¿En qué debería pensar la dirección al considerar el delito económico?

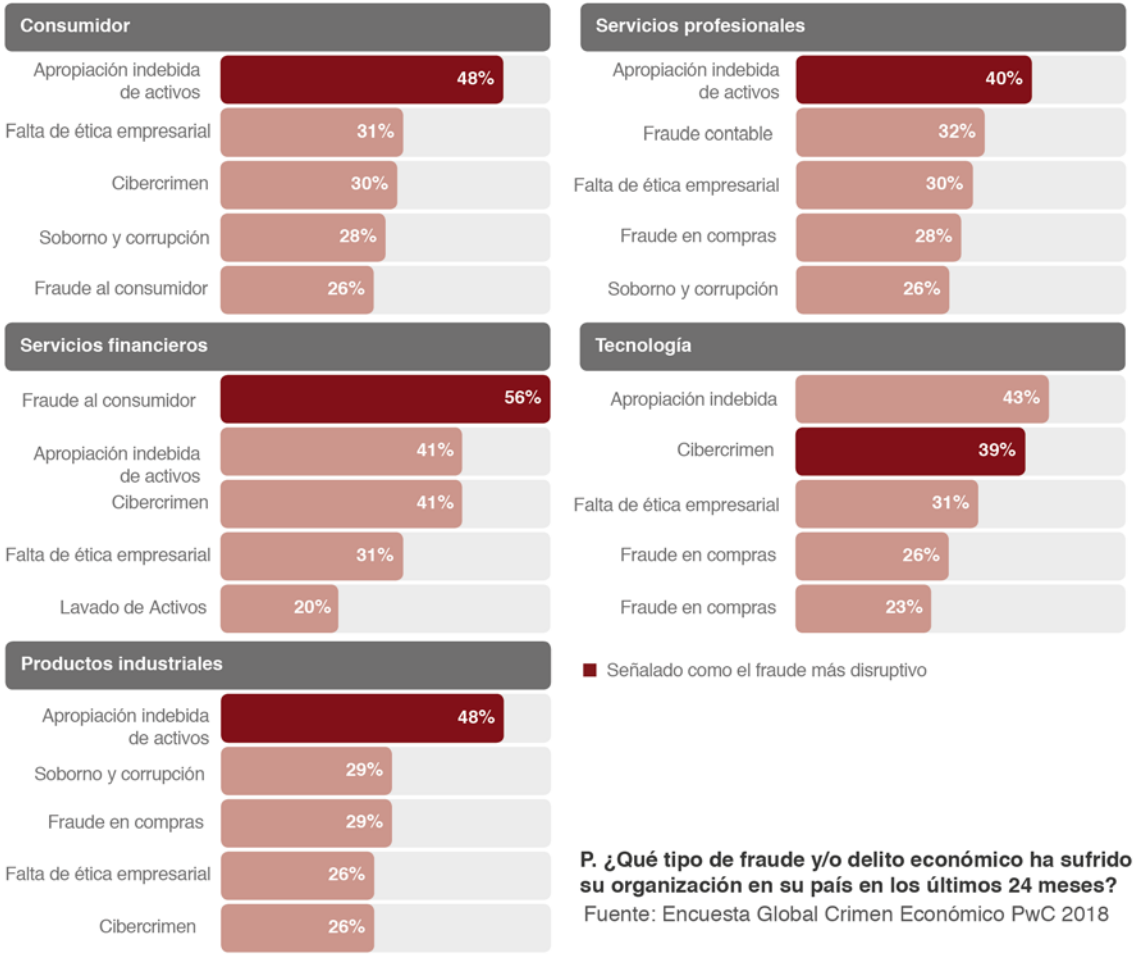
- ¿Cuándo fue la última vez que efectuó una evaluación de riesgo de fraude completa?
- ¿Cómo está estructurada y qué tiene en cuenta una evaluación de riesgo de fraude en su Organización?
- ¿En qué medida las actuales tendencias de fraude, sean de un sector específico u otro, se han identificado y considerado en la evaluación de riesgo de su organización?
- ¿La evaluación de la exposición al riesgo de la organización se ha documentado y es integral?
- ¿Cómo se ha medido el riesgo de fraude y con base en qué criterios se ha determinado que los riesgos inherentes y/o residuales son aceptables con respecto al apetito de riesgo de su organización?

Riesgo conductual: el "Riesgo Escondido" detrás de muchos fraudes internos

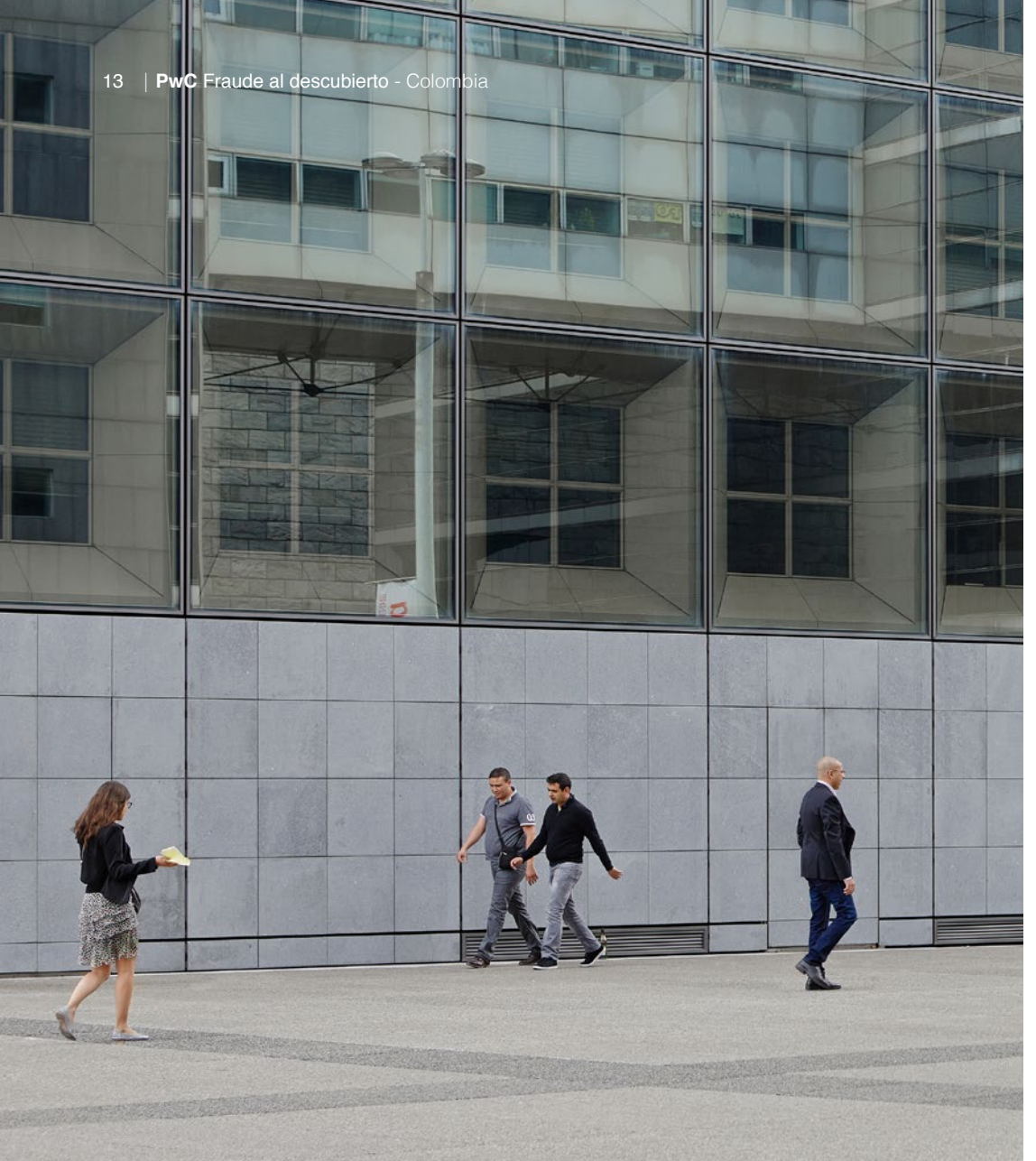
Dado que el fraude es un adversario en permanente cambio, este año en nuestra encuesta modificamos nuestras definiciones para reflejar con la mayor precisión posible las más recientes formas de fraude.

Hemos introducido dos nuevas categoría, el fraude al consumidor y la falta de ética empresarial, las cuales se clasificaron en el ranking global de fraudes más denunciados respectivamente, en el 3° (29%) y 4° puesto (28%), por detrás de la apropiación indebida de activos o también conocida como malversación de activos, que tuvo el 45% y el cibercrimen que contó con el 31%.

Figura No. 5: Globalmente la apropiación indebida de activos, el fraude al consumidor y el cibercrimen fueron los fraudes más denunciados en todas las industrias



P. ¿Qué tipo de fraude y/o delito económico ha sufrido su organización en su país en los últimos 24 meses?
Fuente: Encuesta Global Crimen Económico PwC 2018



Estas nuevas definiciones reflejan el creciente reconocimiento de una categoría amplia del riesgo de fraude interno, definido como “riesgo de conducta o riesgo conductual”. Este tipo de riesgo incluye aquellas actuaciones de los empleados que ponen en riesgo o perjudican las actividades de las compañías, en términos de proveer los mejores resultados a sus clientes, así como la libre competencia e integridad de los mercados. Más aún, a diferencia de las fallas operativas o las amenazas externas (que a menudo pueden ser verificadas por controles internos), el riesgo conductual requiere una respuesta más holística y por tanto, un cambio en la forma en la que se le aproxima.

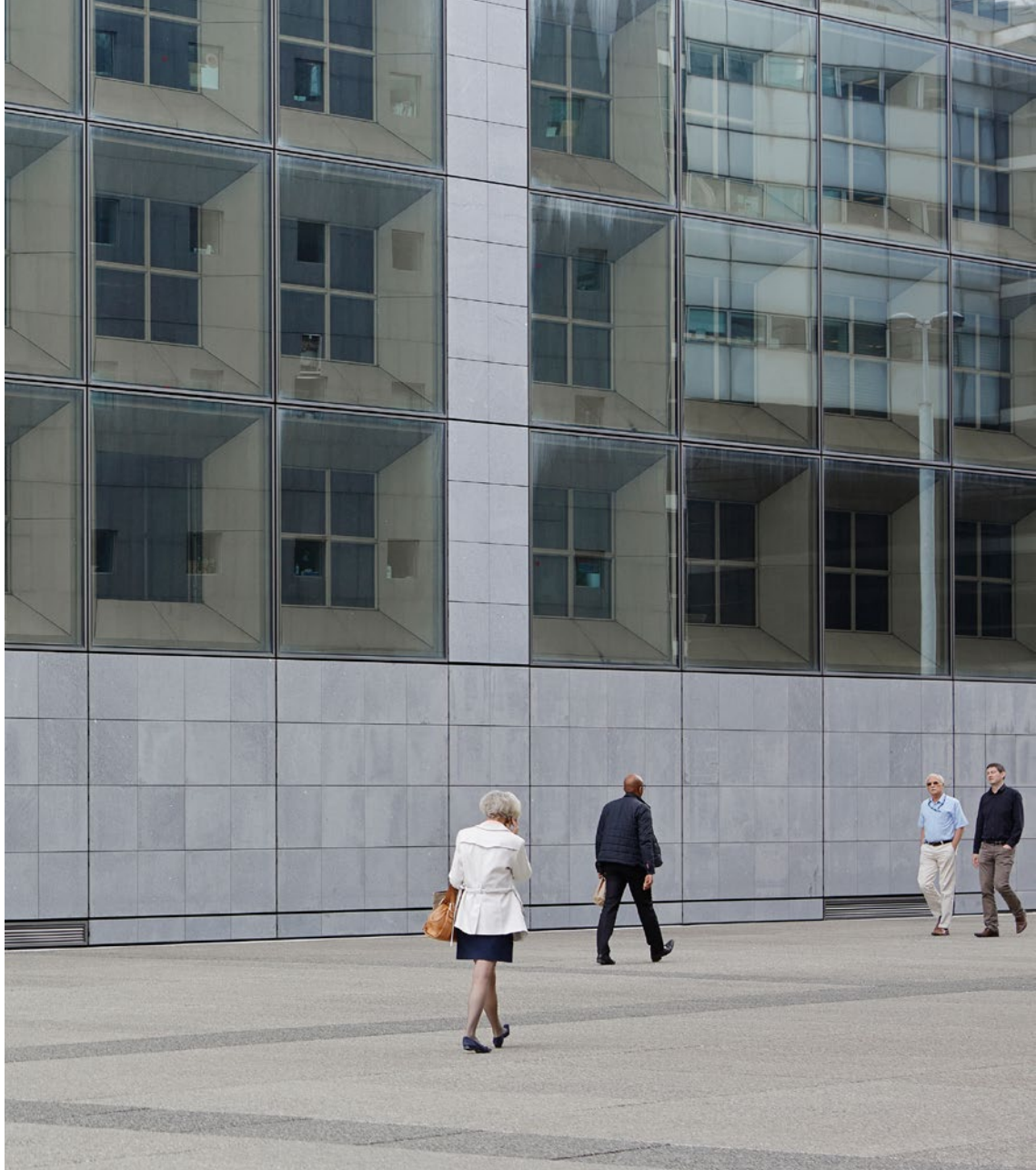
Actualmente muchas compañías tratan el cumplimiento, la ética y la gestión de riesgo corporativo como funciones separadas, incluso existen en silos separados dentro de una misma organización, lo que no contribuye con una visión integrada de la estrategia de la compañía. Las partes de una organización que investigan el fraude, las que gestionan el riesgo de fraude y las que reportan el fraude a la junta o los reguladores están desconectados.

Cuando esto ocurre pueden aparecer vacíos operacionales y en ocasiones, el fraude “se puede barrer bajo el tapete” fácilmente o verse como el problema de alguien más, lo cual, sin duda alguna, actúa en detrimento de la efectividad general de la prevención del fraude, el desempeño financiero, así como las responsabilidades ante los reguladores.

Un enfoque más innovador incluye reestructurar estas funciones como componentes del riesgo conductual. Esto le permite a la compañía medir de una mejor forma y gestionar el cumplimiento, la ética y la gestión de riesgo horizontalmente e integrarlas en un proceso estratégico para la toma de decisiones.

También significa que las faltas éticas y las irregularidades asociadas a eventos de fraude, se pueden manejar con menos pasión y emoción, y ser tratadas como elementos con los que la organización debe lidiar en el curso de sus actividades.

Más aún, al adoptar esta postura más sistémica y realista frente al riesgo, puede significar una medida más costo-eficiente entre los programas de cumplimiento de ética, fraude y anticorrupción. Este es un paso importante para derribar los silos entre las funciones clave para prevenir el fraude y para finalmente, procurar su plena identificación.



Buscar el fraude en los lugares correctos

Nuestra encuesta global reveló un aumento significativo en la participación del delito económico cometido por actores internos –pasando del 46% en 2016 al 52% en 2018-; y un aumento dramático en la proporción de tales delitos atribuidos a la dirección senior –pasando del 16% en 2016 al 24% en 2018-. De hecho, nuestra encuesta indica que la probabilidad de que los perpetradores de un fraude de gran impacto sean actores internos es un tercio mayor a los actores externos.

Sin embargo, uno de los mayores puntos ciegos del fraude en una compañía, y la mayor amenaza, a menudo no tiene nada que ver con sus empleados, sino con la gente con quien se hace negocios. Estos son los terceros con quienes las compañías tienen relaciones regulares y rentables, tales como los representantes, intermediarios, vendedores, proveedores, clientes, entre otros. Es decir, palabras, son estos terceros las personas y las organizaciones con quienes se espera un cierto grado de confianza mutua, pero quienes de hecho, pueden estar robando a la compañía.

Figura No. 6: A nivel global, los actores internos son los principales perpetradores del fraude

24% de los fraudes internos denunciados fueron cometidos por la alta dirección.

68% de los actores externos que cometieron fraude son "amienemigos" de la organización - agentes, vendedores, proveedores de servicios compartidos y clientes.

P. ¿Quién fue el principal perpetrador del fraude más disruptivo?

Fuente: Encuesta Global Crimen Económico PwC 2018

¿Cómo podemos ayudar?

Identify es una herramienta interactiva de análisis de datos para investigaciones de fraude. Combina cuadros de mando intuitivos, con técnicas avanzadas para el análisis de información tales como el establecimiento de perfiles de los empleados y minería de textos, permitiendo la revisión e investigación de pagos sospechosos, actividades anómalas y comportamientos irregulares.

PwC cuenta con una amplia experiencia para ayudar a las organizaciones en el diagnóstico e implementación de evaluaciones de riesgo de fraude, corrupción y AML, entre otros riesgos estratégicos.

También establecemos y administramos sistemas locales integrados para la denuncia de irregularidades en diversas compañías de diferentes sectores, ayudando así a que nuestros clientes no solo reciban las reclamaciones, sino que puedan manejarlas e investigarlas.

02 Tenga un enfoque dinámico

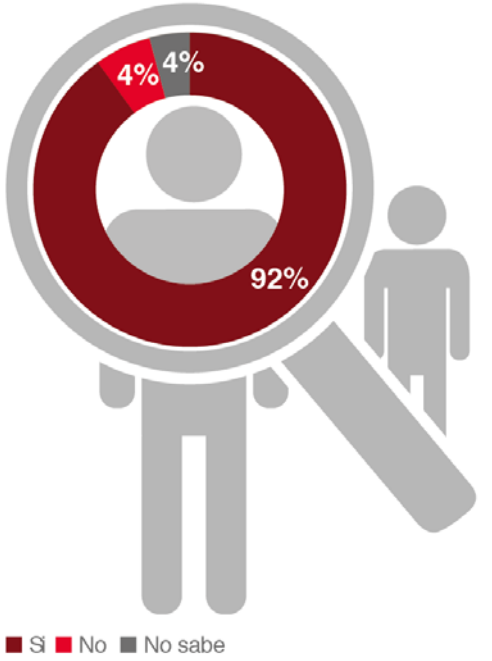
Los directivos son responsables

Con más frecuencia, el gerente general o presidente es visto como la personificación de una organización, estando en todo momento, al tanto de cada detalle del desarrollo de la cultura organizacional y sus operaciones. Por lo que, cuando ocurren fallas éticas o de cumplimiento, estas personas deben responder ante la opinión pública como ante los reguladores. Independientemente de que lo merezcan o no, una cosa es clara: la *C-suite*[1] o alta gerencia, ya no puede alegar el desconocimiento o la ignorancia como una excusa.

Nuestra encuesta muestra que en Colombia los incidentes de fraude más graves han sido presentados ante los ejecutivos de la Junta o de la dirección senior de las compañías en el 92% de los casos. Adicionalmente, con mayor frecuencia se reconoce la responsabilidad de la C-suite, ya que el 45% de los encuestados indicaron que sobre ellos recae la principal responsabilidad del programa de ética y cumplimiento de la organización. Esto llama la atención sobre cómo la oficina principal está manejando las crisis y en qué medida está ajustando (o no) sus perfiles de riesgo como corresponde.

[1]Término usado para denominar a los altos ejecutivos y directivos de una compañía, cuyos titulos en inglés tienden a iniciar con la letra C, de "Chief", como por ejemplo el Chief Executive Officer (CEO), el Chief Financial Officer (CFO), el Chief Operating Officer (COO), y el Chief Information Officer (CIO).

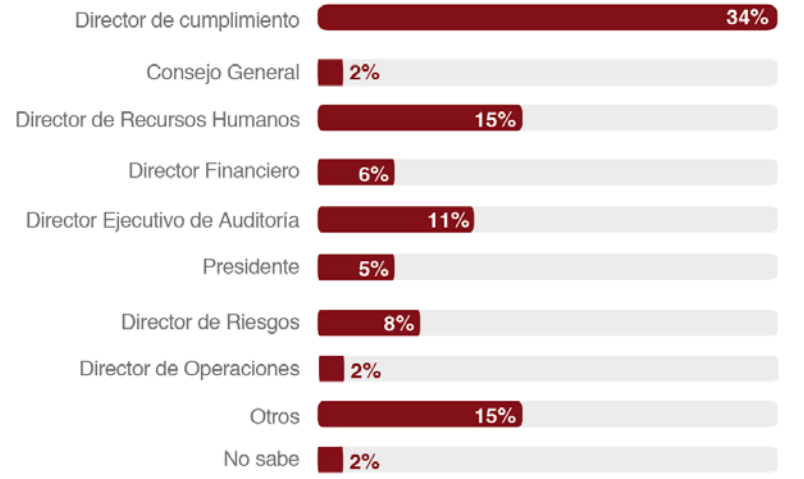
Figura No. 7: En Colombia se involucra con mayor frecuencia a la Alta Gerencia en la gestión de fraude



P. ¿El incidente de mayor impacto que indicó, fue dado a conocer a la alta gerencia o lideres senior del gobierno corporativo?

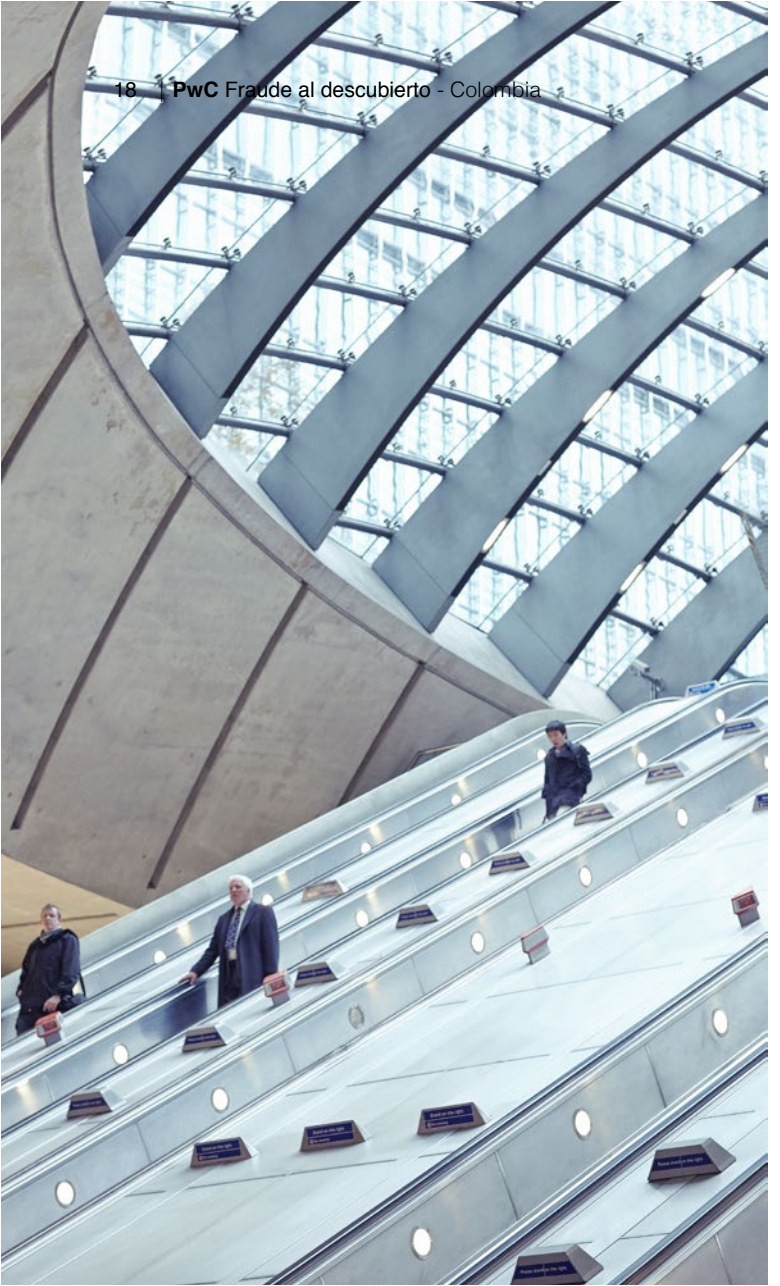
Fuente: Encuesta Global Crimen Económico PwC 2018

Figura No. 8: En Colombia la responsabilidad principal por los programas de ética y cumplimiento recae en la *C-suite*



P. ¿Quién es el responsable principal del Programa de Ética y Cumplimiento de su organización?

Fuente: Encuesta Global Crimen Económico PwC 2018



Aunque tradicionalmente la prevención y detección del fraude habían sido del dominio de la segunda línea de defensa de las organizaciones (gestión de riesgo, legal, cumplimiento, etc.), las compañías de hoy en día están incorporando cada vez más medidas reforzadas de prevención de fraude en el tejido de su primera línea de defensa.

Esto parece ser solo el comienzo de un cambio significativo, donde las capacidades para la prevención y detección de fraude de primera línea continúan madurando y fortaleciéndose. En la medida que lo hacen, facilitarán que la segunda línea de defensa cambie a un enfoque de segunda línea más tradicional, relacionada con temas de gobierno, supervisión, definición del apetito al riesgo, así como el desarrollo de la estructura organizacional, políticas y lineamientos.

Lo anterior es importante si se tiene en cuenta el entorno en el que nos desarrollamos, en donde los límites entre las industrias, tecnologías y organismos regulatorios se siguen diluyendo, y donde los defraudadores están buscando nuevos puntos débiles para atacar, más allá de los tradicionales y altamente protegidos servicios financieros.

Figura No. 9: La detección del fraude asciende a la primera línea de defensa

Las malas noticias vuelan: el riesgo reputacional sobrepasa ahora el riesgo regulatorio

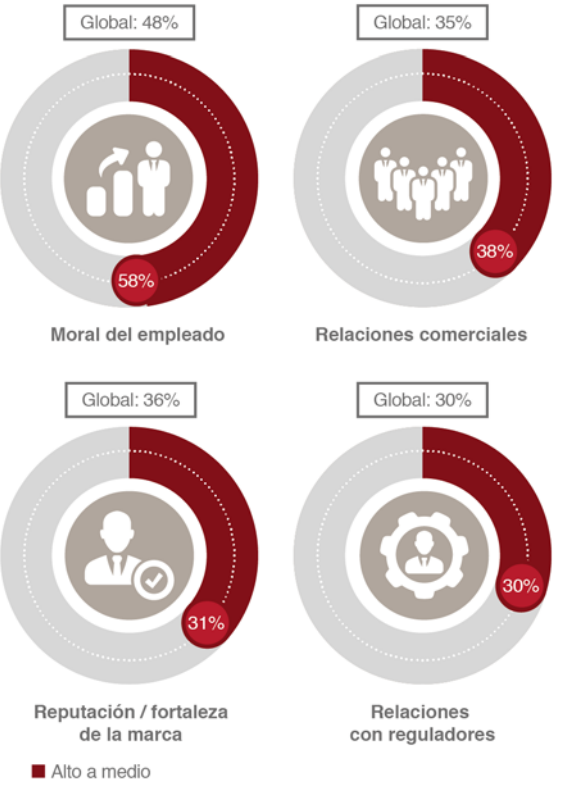
Durante los últimos años se ha producido un cambio significativo en la forma en la que el mundo ve el fraude y la corrupción; los datos de nuestra encuesta reflejan una arraigada exigencia por parte de la opinión pública, los reguladores, los empresarios, etc.

En cada región del mundo y en las diferentes culturas, existen signos de convergencia sobre los estándares de transparencia y las expectativas sobre la conducta. Colombia, así como otros países en Latinoamérica, se ha unido a estos esfuerzos y en los últimos años ha tomado medidas importantes en la lucha contra la corrupción, para entre otros, demostrar su compromiso serio de cumplir con todos los requisitos para su ingreso a la Organización para la Cooperación y el Desarrollo Económico -OCDE[2]- , el cual se hizo efectivo en mayo de 2018.

Como parte de este esfuerzo, Colombia ha adoptado otras leyes en la lucha contra el soborno trasnacional, materializado en la Ley 1778 de 2016, por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción, relacionada con servidores públicos extranjeros y se dictan otras disposiciones en materia de lucha contra la corrupción.

[2]Cartilla "Convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales". Superintendencia de Sociedades.

Figura No. 10: Impacto del delito económico en los elementos del negocio



Fuente: Encuesta Global Crimen Económico PwC 2018

Su reputación no se encuentra sujeta a ninguna jurisdicción, ley o debido proceso.

Si bien, las compañías están más preocupadas por el cumplimiento de las regulaciones locales e internacionales y la implementación de controles, las crisis no pueden evitarse por completo y la reputación de las compañías puede verse afectada en cualquier momento. Además, la percepción de la ética y el cumplimiento en la sociedad parece haberse endurecido, por lo que parece haber poca tolerancia pública para aquellos que infrinjan las reglas. Por definición, los reguladores operan dentro de una jurisdicción limitada y de acuerdo con reglas bien definidas. Por otra parte, la reputación de la marca de una compañía no se somete a ninguna jurisdicción fija, ley o proceso debido.

Los ejecutivos colombianos que encuestamos ubicaron consistentemente el daño reputacional dentro de los principales impactos negativos de diferentes formas de delito económico, siendo la percepción pública (reputación/fortaleza de la marca, relaciones comerciales y la cotización bursátil) la más afectada y en crecimiento continuo desde 2016.

El cumplimiento regulatorio continúa siendo tan crítico como siempre, o incluso más. En la Junta los requerimientos de reportes y de los reguladores, abordando tanto aspectos legales como éticos, siguen expandiéndose. El escrutinio y las acciones legales también están en alza globalmente y la cooperación regulatoria internacional es cada vez más habitual.

¿Existe alguna correlación entre el desarrollo económico y el fraude?*

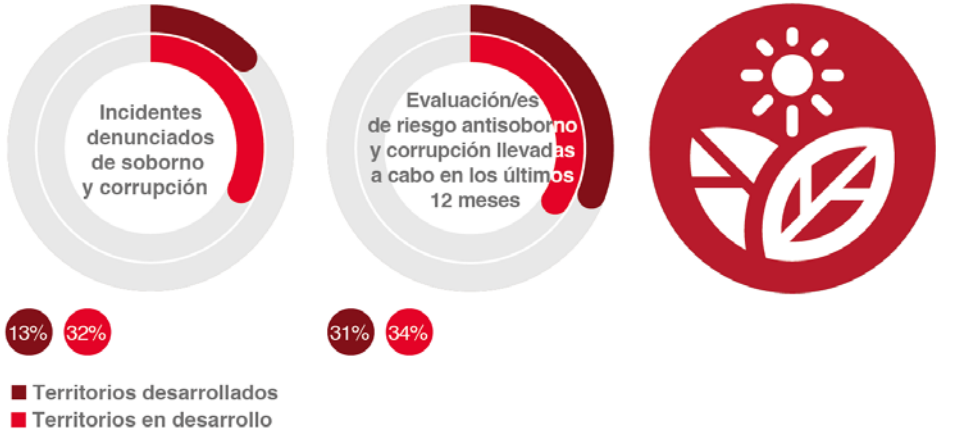
La encuesta global revela algunos matices interesantes acerca de las diferentes aproximaciones en el mundo al riesgo de fraude; los cuales, podrían ofrecer importantes pautas para aquellos países que continúan su camino hacia el desarrollo económico.

En los territorios en desarrollo, los encuestados dijeron que el delito económico se comete más a menudo por los actores internos (59%). La cifra equivalente en los territorios desarrollados fue de solo el 39%.

En los territorios en vías de desarrollo, el 58% de las compañías involucradas en movimientos de dinero (y/o cualquiera de las siguientes líneas de negocio: instituciones financieras, fondos mutuos, negocios de servicios monetarios, comisionistas, aseguradoras o comerciantes de metales preciosos, piedras o joyas), indicaron haber sido objeto de alguna actuación legal por parte de los reguladores en temas de lavado de activos durante los últimos dos años. La cifra equivalente en los territorios desarrollados fue de solo el 48%.

El 15% de los encuestados provenientes de países en desarrollo indicaron que esperaban un incremento significativo de los recursos para la financiación de programas antifraude en los siguientes 24 meses. La cifra equivalente en los territorios desarrollados fue

Figura No. 11: La lucha contra la corrupción continúa siendo un desafío para los países en desarrollo



Fuente: Encuesta Global Crimen Económico PwC 2018

Organizaciones en territorios en desarrollo son casi tres veces más propensas a sufrir la corrupción que las que están en territorios desarrollados. Sin embargo, solo un tercio llevan a cabo valoraciones de riesgo sobre las medidas para prevenir soborno y corrupción, casi igual a aquellas realizadas en los territorios desarrollados.

* La agrupación que hicimos de los territorios desarrollados y en desarrollo se basó en la clasificación de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Para fines de la presente encuesta, los territorios en transición fueron tratados como territorios en desarrollo.

En Colombia, como país en desarrollo, el desafío relacionado con el soborno y la corrupción se encuentra todavía en el principal punto de foco. A diferencia de algunos de los países desarrollados encuestados, en los cuales, los delitos económicos de mayor impacto fueron la mala conducta comercial o corporativa y/o el fraude cometido por los clientes; en Colombia la tipología de fraude número uno fue la corrupción, junto a uno de sus exponentes principales: el soborno, con un 17%.

En este contexto no es de sorprenderse que desde 2016 se haya más que triplicado los encuestados que dijeron que se les había pedido pagar un soborno, pasando del 5% en 2016 al 17% en 2018. Además, el porcentaje de los encuestados colombianos que creían haber perdido una oportunidad frente a un competidor del que creen que pagó un soborno es casi equivalente al resultado global, con el 21% contra el 24%.

Como lo indicamos, el crecimiento de la corrupción sigue en aumento, pero los números de nuestra encuesta sugieren que las medidas para combatirlo no se están incrementando al mismo ritmo, pues solo el 50% de los encuestados colombianos dijo haber realizado, en los últimos dos años, evaluaciones de riesgo específico incluyendo tipologías como soborno y corrupción y solo el 54% tenía políticas específicas para gestionarlos.

Figura No. 12: Corrupción en crecimiento

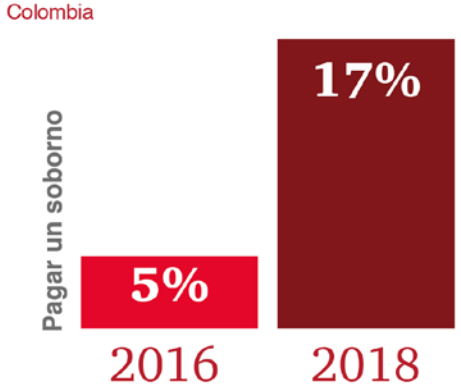
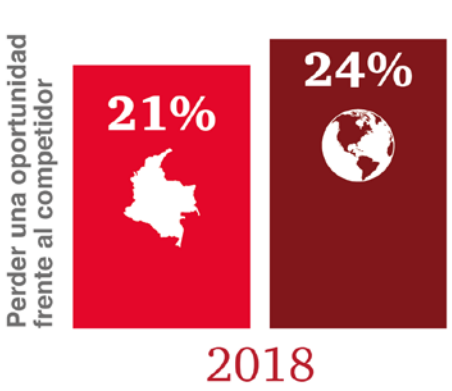


Figura No. 13: Desventaja frente al competidor



P. ¿En los últimos 24 meses se le pidió a su organización pagar un soborno, o ha perdido una oportunidad frente a un competidor que usted cree que lo pagó?

Fuente: Encuesta Global Crimen Económico PwC 2018

¿Cómo podemos ayudar?

Le ayudamos a entender sus riesgos y gestionarlos adecuadamente, a través de nuestros proyectos de diagnóstico e implementación de regulación local e internacional en material de fraude, corrupción, lavado de activos y financiación del terrorismo.

Igualmente le ayudamos a identificar las contrapartes de su negocio, transacción o socio, mediante el análisis de:

- Una amplia red de información pública y bases de datos, incluyendo información corporativa, judicial, sanciones, entre otros.
- La identificación de potenciales intereses comerciales de su contraparte que pueda afectarlo.
- Búsquedas inteligentes en diversos idiomas a través de internet en redes sociales, blogs, sitios especializados y medios de prensa.
- Indagaciones especializadas a través de nuestra amplia red de fuentes humanas tanto a nivel local como internacional, provenientes de diversas industrias, países y especialidades.

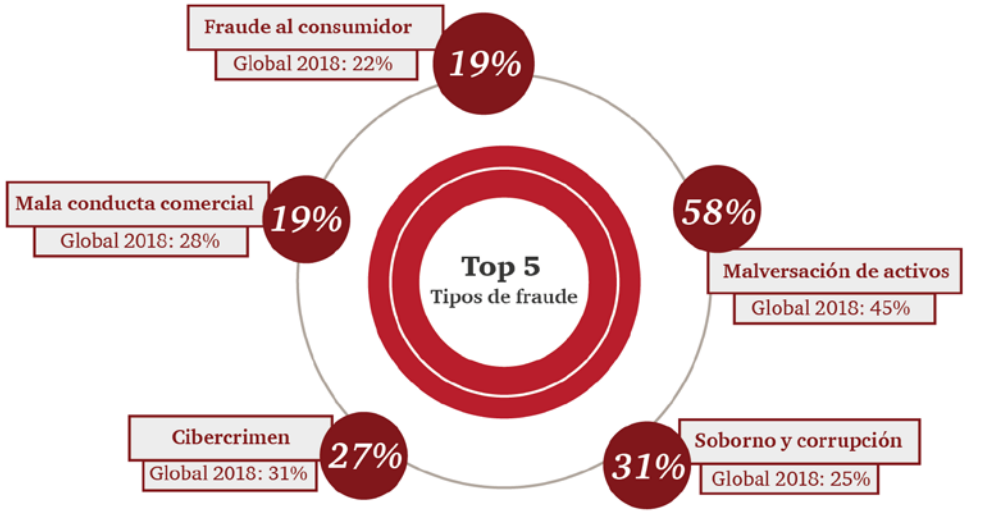
03 Aproveche la capacidad de protección de la tecnología

Encontrar el punto exacto...

En la actualidad las organizaciones tienen acceso a una diversidad de tecnologías innovadoras y sofisticadas, con las cuales se pueden defender contra el fraude, orientadas hacia el monitoreo, análisis, aprendizaje y predicción del comportamiento humano. Estas incluyen el aprendizaje automático, análisis predictivo y otras técnicas de inteligencia artificial. Nuestra encuesta muestra que las compañías están utilizando en diferentes grados tales tecnologías, dependiendo del sector de la industria. Adquirir e implementar tecnología requiere de importantes inversiones de capital y la decisión sobre qué comprar y cuándo es un tema sensible. Por ejemplo, algunos invierten en tecnologías emergentes o disruptivas que no utilizan de la manera más óptima; otros las adoptan demasiado tarde y se quedan rezagados.

De acuerdo con los encuestados en Colombia, el cibercrimen es el tercer tipo de crimen económico con mayor probabilidad de ocurrencia, detrás del soborno y la corrupción y la malversación de activos, identificado como uno de los riesgos de mayor impacto y gravedad en las organizaciones. De tal manera, nuestra encuesta indica que las compañías colombianas están comenzando a implementar técnicas avanzadas, migrando de un enfoque reactivo de análisis de datos, a una postura más preventiva por medio del análisis predictivo.

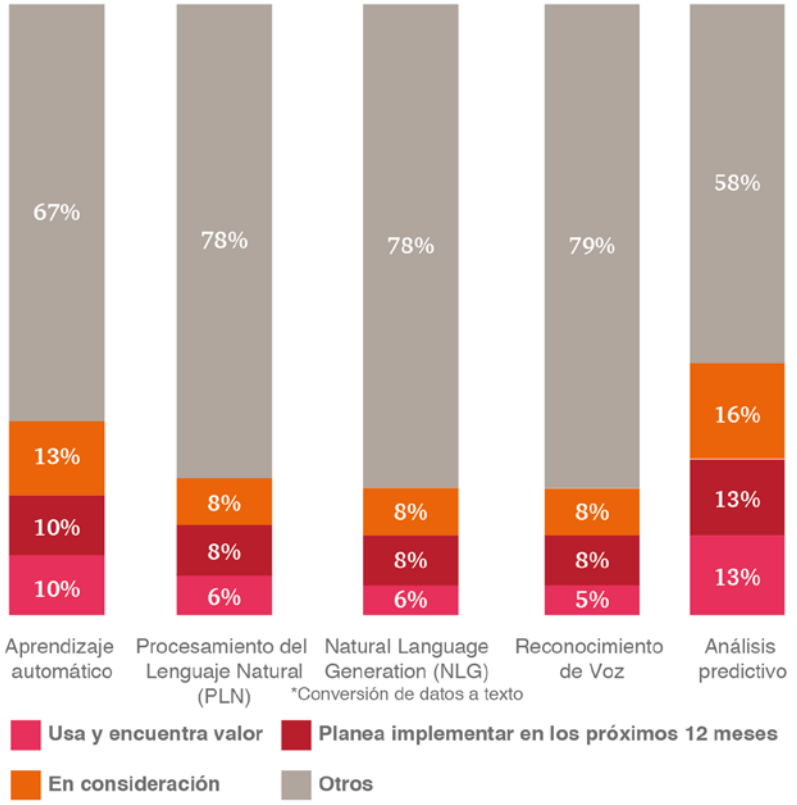
Figura No. 14: Cibercrimen, uno de los crímenes económicos de mayor impacto en Colombia



P. ¿Qué tipo de crimen económico ha sufrido su organización en los últimos 24 meses?

Fuente: Encuesta Global Crimen Económico PwC 2018

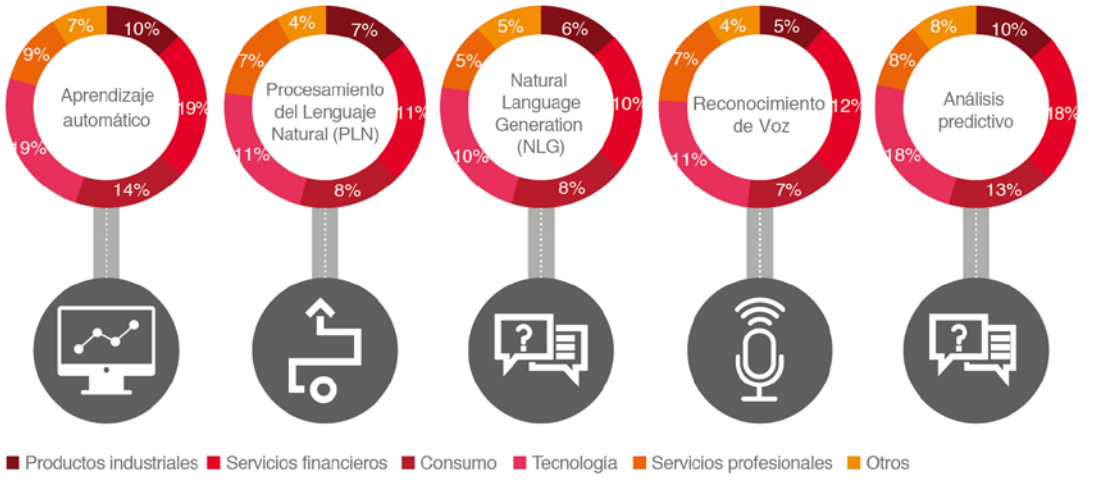
Figura No. 15: Análisis predictivo como medio de detección y monitoreo en Colombia



P. En qué medida su organización está utilizando Inteligencia Artificial o Analítica Avanzada para combatir/monitorear potenciales fraudes u otras actividades potencialmente relacionadas con crimen económico?
Fuente: Encuesta Global Crimen Económico PwC 2018

La tendencia global sobre la implementación de tecnología avanzada va más allá de la situación actual en Colombia, y los sectores tales como los servicios financieros y las industrias tecnológicas están encontrando más valor en la inteligencia artificial y en el análisis avanzado.

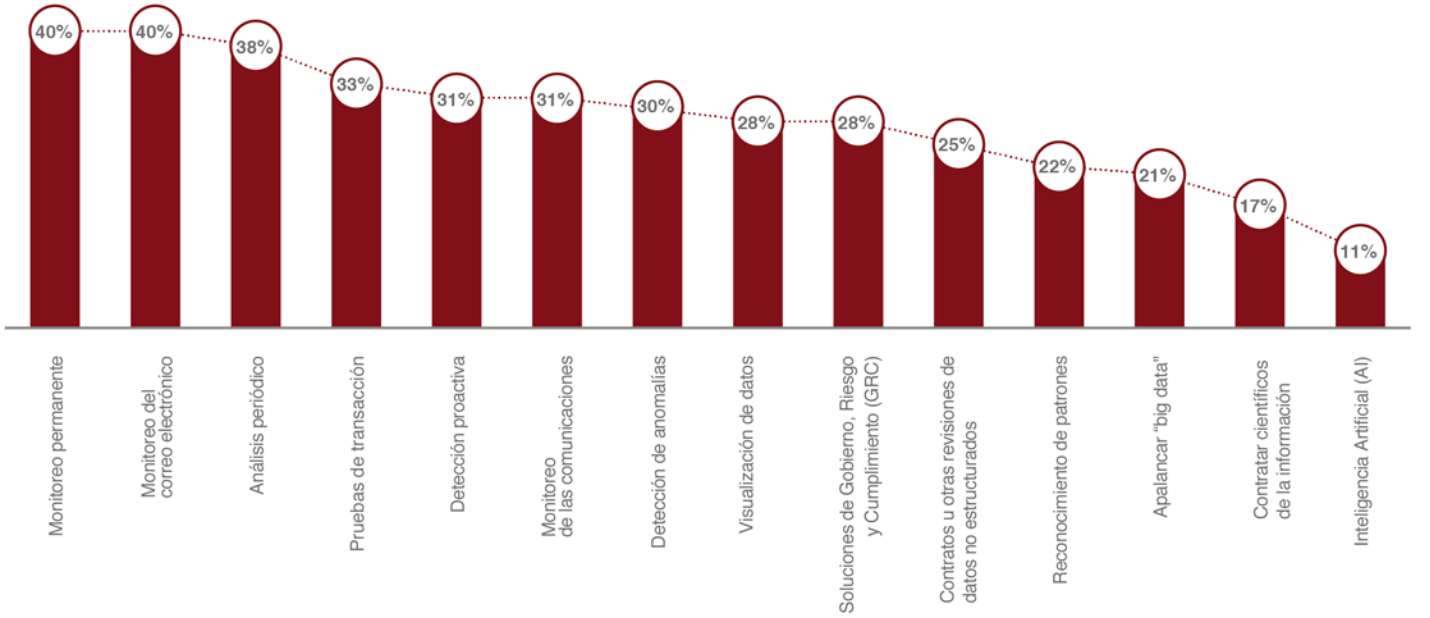
Figura No. 16: Uso de Inteligencia Artificial y Análisis Avanzado



P. ¿Hasta qué nivel está utilizando y encontrando valor su organización en la Inteligencia Artificial o en el Análisis Avanzado para combatir / monitorear el fraude y otros delitos económicos? (% de los encuestados que respondieron que sus organizaciones utilizan y derivan valor).

Fuente: Encuesta Global Crimen Económico PwC 2018

Figura No. 17: Las organizaciones están comenzando a identificar el valor de las tecnologías alternativas y disruptivas en la lucha contra el fraude.

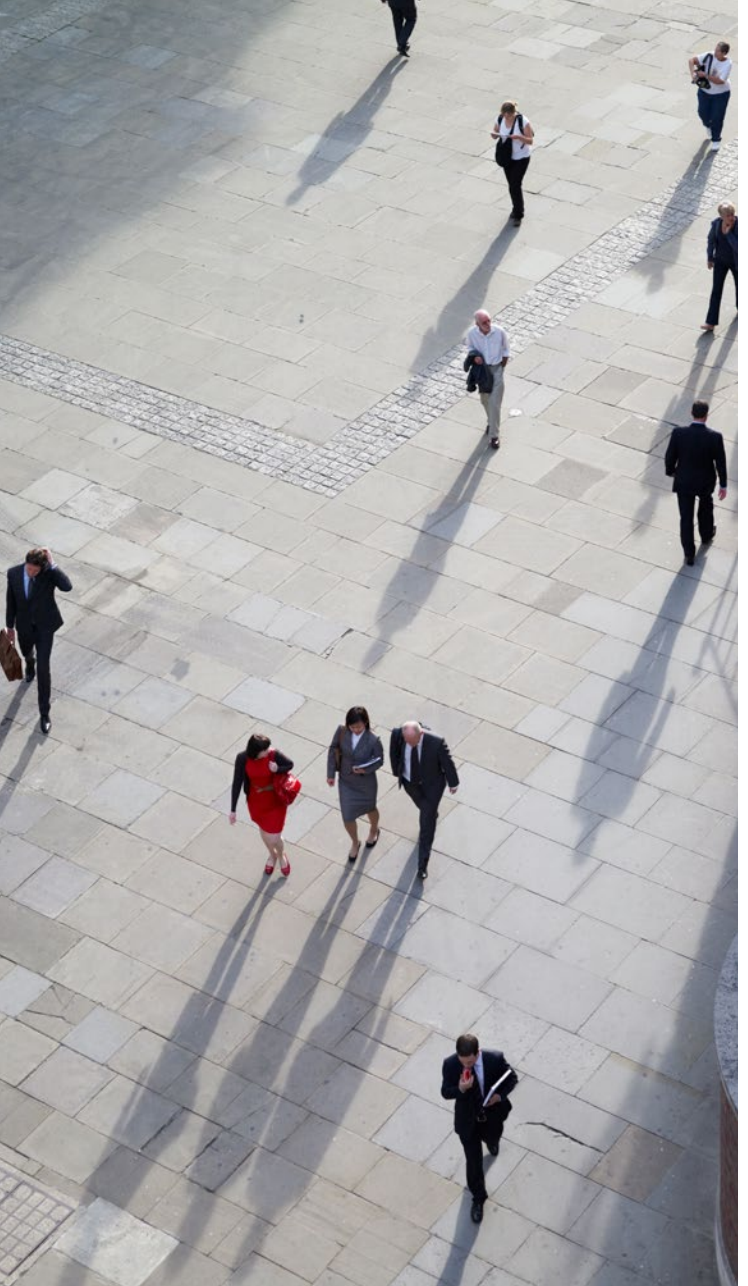


P. ¿Hasta qué nivel está utilizando y encontrando valor su organización en las siguientes tecnologías y técnicas alternativas / disruptivas en su ámbito de control para combatir el fraude y/u otros delitos económicos? (%de los encuestados que respondieron que sus organizaciones utilizan y derivan valor).

Fuente: Encuesta Global Crimen Económico PwC 2018

El uso de tecnologías innovadoras para combatir el fraude es ahora un fenómeno mundial. De hecho, nuestra encuesta muestra que las compañías en territorios en desarrollo están invirtiendo actualmente en tecnologías avanzadas a una velocidad mayor que los territorios desarrollados. Encontramos que el 27% de las compañías en territorios en desarrollo indicaron que en la actualidad utilizan o planean implementar la inteligencia artificial para combatir el fraude, frente a un 22% de los encuestados en territorios desarrollados.

Para aquellos territorios en desarrollo, este enfoque podría representar un medio efectivo de recuperar terreno en un área en la cual otras naciones ya han invertido en costos de infraestructura considerables. Al final, la ubicuidad de la tecnología crea un desafío doble para todas las organizaciones: ¿Cómo encontrar el punto ideal entre la efectividad de la tecnología y su costo?, y al mismo tiempo llevar la delantera a los defraudadores?



¿En qué consiste la “fricción del cliente”*?

Como cliente puede ser reconfortante, en primera instancia, saber que una compañía está monitoreando de forma permanente el fraude en los servicios que suministra. Pero si dicho monitoreo genera alertas frecuentes o repetitivas, ese confort puede convertirse rápidamente en molestia.

Esto se conoce como “fricción del cliente” y es un desafío creciente para las organizaciones en la medida en que buscan encontrar el equilibrio perfecto entre actuar adecuadamente ante las banderas rojas del fraude, y el generar de manera excesiva alertas a sus clientes.

Este no es un equilibrio fácil de conseguir y el margen de error es pequeño. Si se es demasiado pasivo, la organización se arriesga a pasar por alto una transacción fraudulenta con todas las consecuencias financieras y reputacionales que eso implica; pero si se es demasiado proactivo, se arriesga a desequilibrar o incluso perder la base de clientes.

> **26% de los encuestados colombianos (34% globalmente)** cree que el uso de tecnología por parte de su organización para combatir el fraude y/o el delito económico produce demasiados falsos positivos.

* De la expresión en inglés "customer friction".

Crimen cibernético: desconexión entre sus efectos y los mecanismos para combatirlo

Hoy en día quienes cometen crímenes cibernéticos tienden a ser tan perceptivos y profesionales como el negocio que atacan. Esta madurez requiere una nueva perspectiva sobre la naturaleza multifacética de las amenazas cibernéticas y los fraudes que las acompañan.

A menudo la primera señal que recibe una organización indicando que algo sistémico no está bien es la detección de un ataque cibernético, tal como phishing, malware o cualquier otro ataque sistemático tradicional. El aumento de la frecuencia, sofisticación y letalidad de tales ataques está instando a las compañías a que vean formas para prevenirlos. Este enfoque tiene el beneficio adicional de facilitar un enfoque más profundo sobre la prevención del fraude.

Aunque para las compañías puede ser difícil medir con exactitud el impacto financiero de los ataques cibernéticos, el 14% de los encuestados a nivel global que indicaron que el cibercrimen había sido la tipología de fraude de mayor impacto en sus organizaciones, dijo haber tenido pérdidas cercanas a US$1 millón como resultados de dichos ataques. El 26% de los encuestados indicó esperar recibir un ataque cibernético en los próximos dos años, con lo que la probabilidad de ocurrencia de este crimen se dobló al compararse con las cifras de 2016.

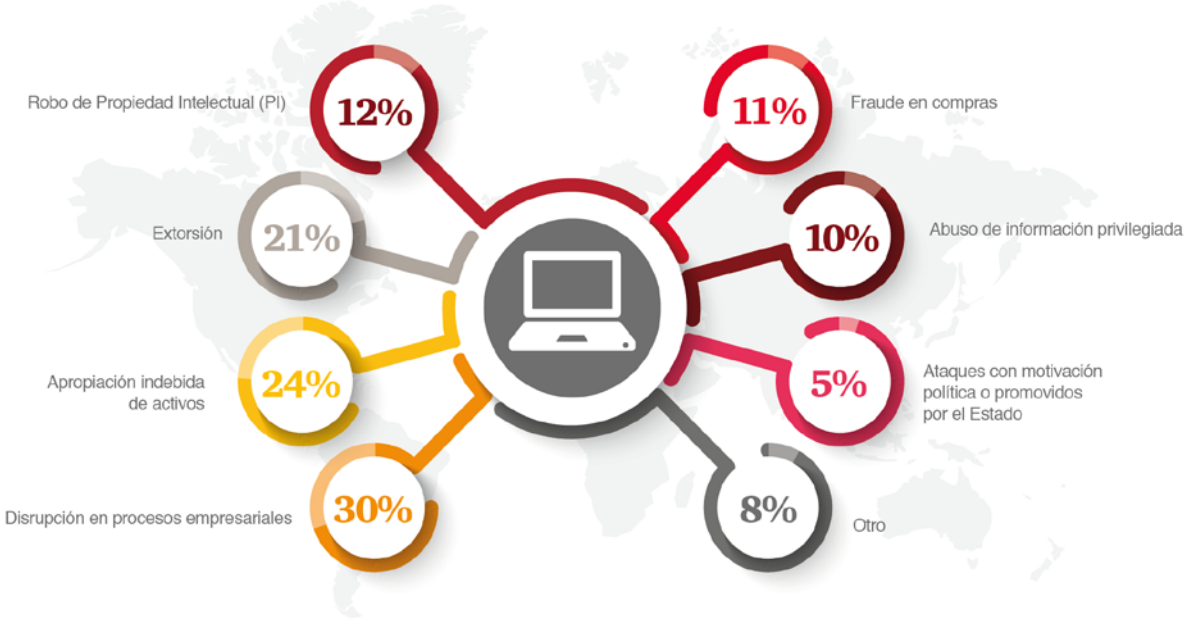
De hecho, los ataques cibernéticos se han intensificado de tal forma, que medir su ocurrencia e impacto parece ser menos estratégico y útil que enfocarse en los mecanismos que los atacantes usaron en cada caso. Pero los esfuerzos de las organizaciones en esta materia parecen no estar enfocados hacia ese fin.

Según la Encuesta de PwC sobre Ciberseguridad y Privacidad de la Información de 2018[1] , solo un pequeño porcentaje de encuestados dijo que sus organizaciones planean llevar a cabo una evaluación de riesgos de su área de tecnología de la información. De hecho, no hay un consenso frente a la responsabilidad de adelantar este tipo de evaluaciones de riesgos, lo cual se evidencia en la gráfica a continuación.

Figura No. 18: Opiniones divididas frente a la responsabilidad de las evaluaciones de riesgo de las áreas de tecnología de la información

[1]The Global Sate of Information Security 2018. https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf.

Figura No. 19: Tipos de fraude de los cuales son víctimas las organizaciones por medio de ciberataques



P. ¿De cuáles de los siguientes tipos de fraude y/o delito económico fue victima su empresa a través de un ciberataque?
Fuente: Encuesta Global Crimen Económico PwC 2018

A esto se suma el hecho que, solo la mitad de los encuestados dijo que en sus organizaciones se adelantan revisiones periódicas que incluyen pruebas de penetración, evaluaciones de amenazas, monitoreo activo de seguridad de la información; así como evaluaciones de inteligencia y vulnerabilidad que han sido adoptadas por menos de la mitad de los encuestados.

A nivel global los encuestados señalaron como los dos tipos de ciberataques más comunes la disrupción de los procesos del negocio (30%) y la apropiación indebida de activos (24%).

Figura No. 20: Técnicas de ciberataque utilizadas contra las organizaciones colombianas

P. ¿En los últimos 24 meses, de cuáles de las siguientes técnicas fue víctima su empresa a través de un ciberataque?

Fuente: Encuesta Global Crimen Económico PwC 2018

Aunque todo fraude digital es fraude, no todo fraude es digital.
Por lo tanto, puede ser de utilidad el diferenciar dos formas de cibercrimen:

- Robo digital: Este tipo de ataque podría incluir el robo de efectivo, información personal, propiedad intelectual, y podría involucrar extorsión, ransomware (pago de rescates por información personal), o host de otros crímenes.

- Fraude digital: Este tipo de ataque es, en muchas formas, el de mayor duración y de mayor impacto, debido a que el defraudador penetra por una puerta abierta (por lo general pero no siempre, un cliente o un empleado) y utiliza los propios procesos empresariales de la compañía para atacarla.

¿Vamos de *phishing*?

De acuerdo con nuestra encuesta, el *phishing* es la segunda técnica de ciberataque más usada contra las organizaciones colombianas con un 17% de los encuestados, siguiendo al malware, técnica que ocupó el primer puesto con el 33% de las opiniones.

Phishing (un término amplio que se refiere a ataques masivos a los sistemas internos de los usuarios para obtener información privilegiada) o el *spear-phishing* (ataques más específicos sobre un individuo como objetivo) son a menudo solo el punto de inicio de un ataque mayor. El *phishing* le permite a los defraudadores obtener acceso a los sistemas de una compañía, bien sea con el fin de robar información, chantajear o simplemente ocasionar una disrupción.

El filtro de correos electrónicos capta algunos ataques de *phishing*, pero dado que los negocios casi siempre requieren permitir el ingreso de correos externos, es difícil tener un control total sobre posibles ataques de *phishing*.

Además, las tácticas de *phishing* de los delincuentes están cambiando siempre. Las consecuencias de un ataque pueden ser devastadoras, de tal manera que el conocimiento y el comportamiento diligente por parte de los usuarios de la tecnología son una defensa vital.

El *phishing* capitaliza nuestras vulnerabilidades como humanos, jugando con nuestra curiosidad o miedo y actuando como un disparador que ocasiona que hagamos algo que no haríamos normalmente. Los archivos usados en actos de *phishing* son nombrados de manera deliberada para tomar ventaja de la curiosidad y el comportamiento humano; nombres como “Detalles_de_pago_del_personal.xls” y “Redundancias_proyectadas.ppt” han sido utilizados en el pasado.

Al final del día, la defensa contra los ataques de *phishing* recae sobre los humanos, al igual que la tecnología, de tal manera que la capacitación, el conocimiento y los procedimientos de escalamiento son herramientas clave que deben utilizarse.

Más allá de la compensación a los clientes … ¿A dónde va el dinero?

Aunque mantener felices a los clientes es la primera premisa de un negocio, existen dimensiones más profundas para prevenir el fraude. Éstas comprenden el submundo del fraude y la regulación e implementación de regímenes cuya misión es controlarlo.

En el caso de robo de identidad, por ejemplo, un banco o comerciante cubrirá la pérdida para el cliente y lo absolverá de una mayor responsabilidad si, digamos, el defraudador toma una tarjeta de crédito a su nombre y gasta un valor importante. Hasta ahora, el sistema de remediar dichos fraudes externos ha funcionado de esta manera y en todas partes, los bancos, comerciantes, consumidores y reguladores, lo han aceptado como parte del costo de hacer negocios juntos.

Aunque varias actividades fraudulentas se pueden detectar por los sistemas de monitoreo de transacciones construidos en respuesta a determinadas regulaciones locales e internacionales, es probable que tanto los bancos como los negocios de servicios monetarios no estén dándose cuenta de la forma en que dichas transacciones se manifiestan en el sistema.

Puede que las compañías fuera del sector financiero no tengan las mismas obligaciones regulatorias que las de ese sector, pero podrían encontrarse incumpliendo la ley. Los reguladores y las autoridades están buscando ahora más allá del impacto primario de un delito, por ejemplo, el tráfico de bienes falsificados, para examinar las posibles actividades ilegales que han financiado los activos robados.

Para eso, las compañías pueden promover métodos de detección beneficiosos, incluyendo las líneas de denuncias de irregularidades o actos de fraude, corrupción y/o lavado de activos; las evaluaciones de riesgo de fraude; y las revisiones internas periódicas. Sin embargo, de acuerdo con nuestra encuesta, identificamos que las compañías colombianas reportaron gastar menos tiempo y recursos en aquellos métodos comprobados de prevención y detección:

- El 84% de los encuestados no ha efectuado una evaluación de riesgo de AML.
- El 58% no ha llevado a cabo un diagnóstico sobre la vulnerabilidad a un ciberataque.
- El 50% de los encuestados no ha llevado a cabo una evaluación de riesgo específica en la que incluya tipología de fraude como el soborno y la corrupción.
- El 28% de los encuestados no ha llevado a cabo una evaluación de riesgo general en los últimos dos años.

¿Cómo podemos ayudar?

PwC proporciona un completo espectro de servicios para que las organizaciones puedan entender el panorama de la ciberseguridad y privacidad; permitiéndoles proteger los activos críticos y la información sensible, entre otros. A continuación mencionamos los principales componentes de nuestra oferta de servicios de ciber-seguridad:

- **Estrategia y Transformación:** Proporcionamos los fundamentos para diseñar, administrar y operar un programa de ciberseguridad alineado con la estrategia del negocio e incrementando la resiliencia organizacional frente al escenario de amenazas siempre cambiante.

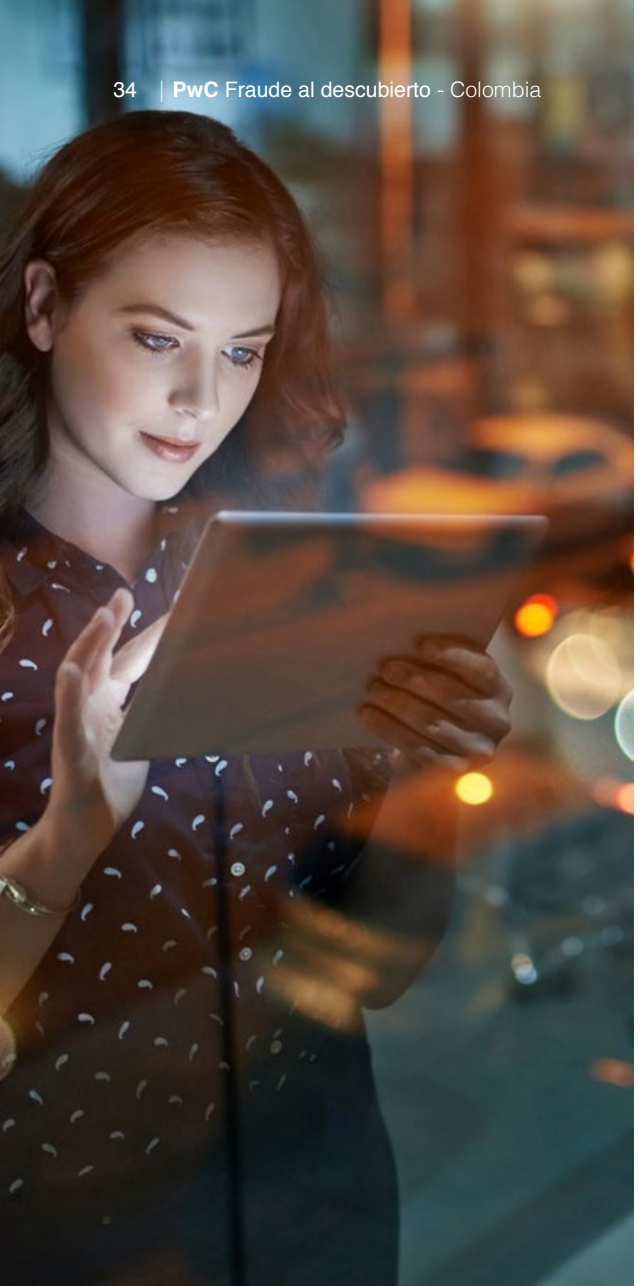
- **Privacidad y Protección del Consumidor:** Capacitamos a los clientes para que descubran y mapeen los ciclos de vida de la información para crear valor del negocio, al igual que diseñamos un programa que pueda impulsar el éxito y construir confianza entre los consumidores. Nos enfocamos en ayudar a los clientes para que mantengan el cumplimiento de las transferencias de información internacional bajo las leyes globales de privacidad y ganar así la confianza de las partes interesadas para utilizar los datos personales.

- **Manejo de Incidentes y Amenazas e Intercambio de Información**: Los clientes reciben asistencia para llevar a cabo las evaluaciones y preparaciones para responder a los impactos tácticos y estratégicos de los incidentes de ciberseguridad. Asistimos en el entendimiento de las amenazas únicas a las organizaciones de los clientes por medio del análisis del escenario de la amenaza. Igualmente, apalancamos la implementación de leyes, de gobierno y de recursos de colegas para combatir las amenazas de una manera más efectiva, compartiendo información tal como ISAOs y modelos de intercambio de datos.

- **Implementación y Operaciones:** De una manera fluida y eficiente, los clientes reciben ayuda para integrar los nuevos sistemas tecnológicos en el negocio, garantizando que la tecnología está sintetizada y gestionada adecuadamente y que los temas desconocidos se encuentran y resuelven. Ayudamos a que los clientes diseñen la arquitectura, implementen y optimicen las tecnologías de seguridad para manejar la visibilidad, el acceso, identificación y el control sobre áreas de información y sistemas sensibles. También proporcionamos servicios diferenciados de alto valor, dando soporte a las tecnologías clave de seguridad por medio de actividades operativas tradicionales.

- **Investigaciones Digitales:** Nuestro equipo de tecnología forense asiste a los clientes para gestionar amplias cantidades de información electrónica y navegar los procesos legales y comerciales exigidos en caso de eventos críticos. Ofrecemos un completo rango de servicios de investigación electrónica que incluyen gobierno de la información, recolección de datos, evaluación de la evidencia y revisión documental. Esta solución integral le permite al cliente responder con efectividad a los incidentes legales o regulatorios y a las crisis.

04 Invierta en la gente, no solo en las máquinas



Invertir en la gente puede generar importantes dividendos

Confrontadas con lo que parece irresoluble para manejar el fraude, muchas organizaciones han decidido invertir más recursos en tecnología. Sin embargo, tales inversiones no siempre se reflejan en acciones efectivas, en especial cuando se trata de la lucha contra el fraude interno.

De tal manera que, aunque la tecnología es claramente una herramienta vital en la lucha contra el fraude, solo puede ser parte de la solución. Esto se debe a que el fraude es el resultado de una mezcla compleja de condiciones y motivaciones humanas. El factor más crítico en una decisión para cometer un fraude es finalmente la conducta humana y esto ofrece la mejor oportunidad para combatirlo. Existe un poderoso método para entender y prevenir los tres principales motivadores del fraude interno, el triángulo del fraude.

Figura No. 21: El triángulo del fraude: ¿Qué hace que un empleado cometa fraude?

P: ¿En qué medida contribuyó cada uno de los siguientes factores en la incidencia del fraude y/o delito económico cometido por actores internos? (% de los encuestados que clasificaron los principales factores que contribuyeron al fraude interno).

Fuente: Encuesta Global Crimen Económico PwC 2018

Figura No. 22: Nivel de esfuerzo organizacional requerido para combatir el fraude interno *

P ¿Qué nivel de esfuerzo aplica su organización a las siguientes categorías para combatir el fraude y/o el delito económico internamente? * % incluye encuestados que clasificaron el nivel alto

Fuente: Encuesta Global Crimen Económico PwC 2018

El triángulo del fraude comienza con un incentivo (normalmente una presión para actuar desde dentro de la organización) seguido por una oportunidad y finalmente, por un proceso de racionalización interna. Debido a que todos los tres motivadores deben estar presentes para que ocurra un acto de fraude, cada uno de ellos deberá abordarse de manera individual.

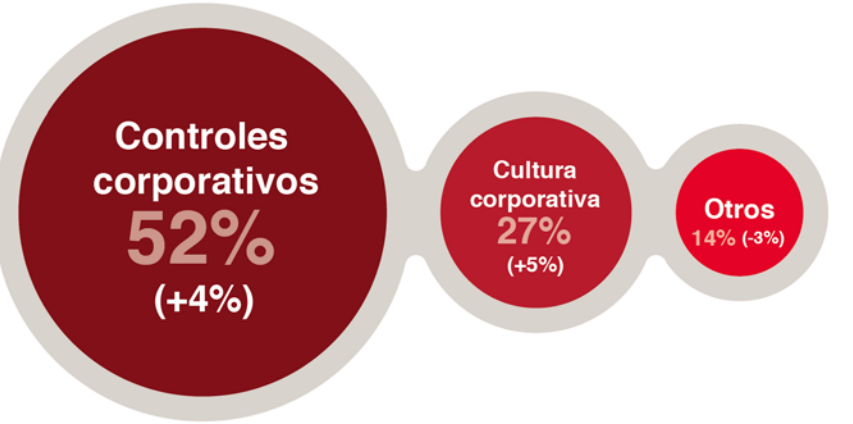
Evitando la oportunidad: controles

La mayoría de esfuerzos de las organizaciones para prevenir el fraude en los últimos años se ha enfocado en la reducción de las oportunidades que permitan la materialización de actos fraudulentos: el 49% de los encuestados en Colombia dijo haber gastado un alto nivel de esfuerzo en construir los procesos de la organización, enmarcados en un esquema de control interno que reduzca la ventana de oportunidad para la ocurrencia de algún fraude.

Por otro lado, de acuerdo a nuestra encuesta, las compañías están poniendo menos esfuerzo en medidas para contrarrestar los otros dos factores, los incentivos y la racionalización; con lo que, solo el 40% de los encuestados indicó haber gastado un alto nivel de esfuerzo en lineamientos o medidas relacionadas con tales factores. Esto se refleja en los resultados de la encuesta, donde solo el 21% y 11% de los encuestados clasificaron los incentivos y la racionalización como los factores de mayor impacto que contribuyen al fraude interno.

Esta falta de foco en las medidas culturales/éticas señala un potencial punto ciego y de hecho, puede ser un motivo por el cual el fraude interno perdura. Debido a que el fraude es el resultado de la intersección entre las decisiones humanas y las fallas del sistema, es importante ser consciente del posible falso sentido de seguridad al que los controles internos, incluso los bien diseñados, pueden conllevar.

Figura 23: Solo la mitad de los fraudes más disruptivos fueron detectados por controles corporativos



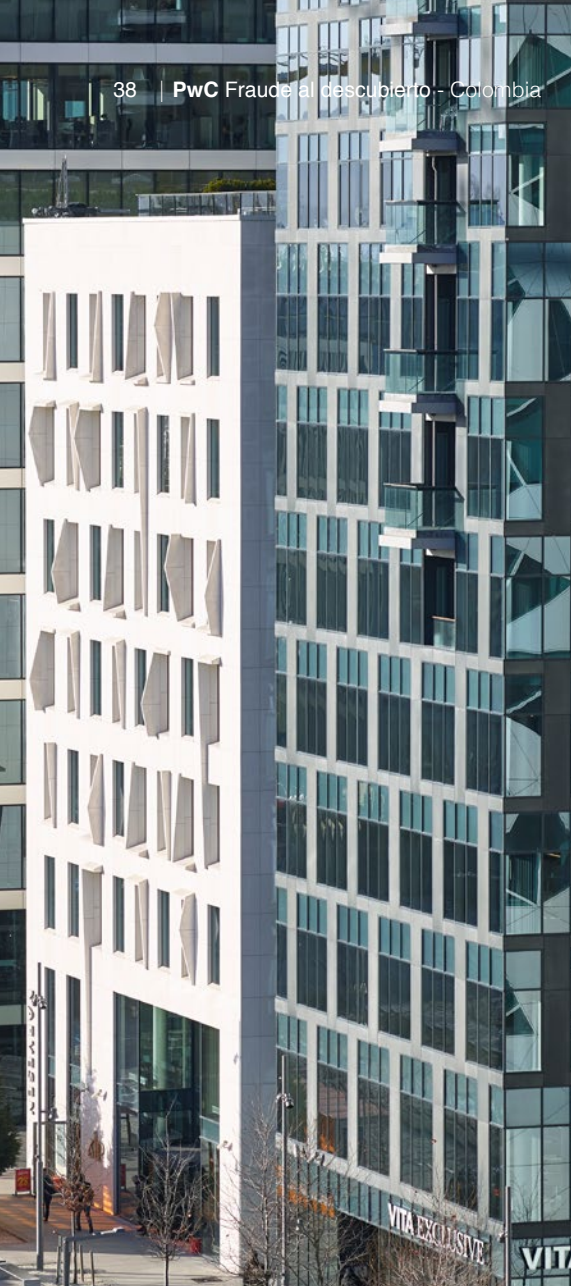
P: ¿Cómo se detectó inicialmente el fraude y/o delito económico más disruptivo?
Fuente: Encuesta Global Crimen Económico PwC 2018

Figura No. 24: Nivel del defraudador en la organización a nivel global

P: ¿En qué nivel se encontraba el perpetrador principal del fraude interno dentro de su organización?
Fuente: Encuesta Global Crimen Económico PwC 2018

De hecho, existe un error fundamental relacionado con la creencia de que solo los controles internos dirigidos hacia la implementación de tecnología pueden captar el fraude de manera indirecta y se asume que la gerencia siempre se comportará de forma ética. En realidad, la experiencia muestra que virtualmente, cada fraude interno importante es el resultado de la omisión o evasión de los controles por parte de la Dirección.

Nuestros resultados globales soportan esta posición: indicando que los fraudes internos de mayor impacto, cometidos por la gerencia *senior*, se ha elevado dramáticamente en los últimos dos años, pasando del 16% en 2016 al 24% en 2018. Para solucionar este problema estructural, las organizaciones necesitan crear controles que realmente hagan que los directivos respondan por ignorar o ser cómplices de cualquier acto irregular o ilegal.



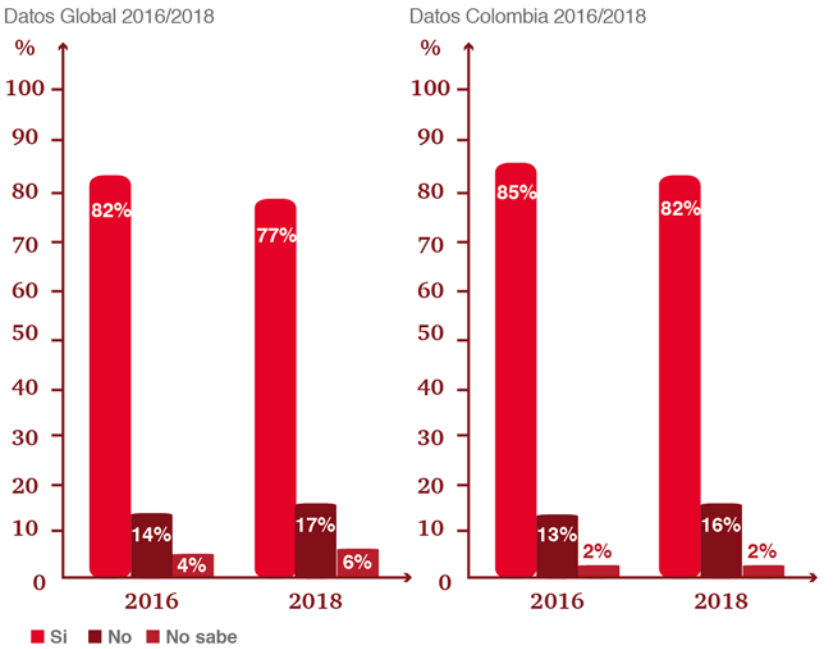
Evitando el incentivo: apertura

Es importante no sobrevalorar los incentivos financieros al considerar lo que motiva a una persona a cometer fraude. El miedo y la vergüenza al haber cometido un error pueden ser de igual importancia. De tal manera, los incentivos que motivan a la alta gerencia de la organización deben examinarse, revisando ¿en qué medida estos están alineados con las regulaciones y con el principio de "hacer lo correcto"?

Adicionalmente, los controles a medida, de corto plazo, pueden servir como controles útiles para identificar si los programas de ventas demasiado agresivos están conduciendo a un comportamiento fraudulento. Una puerta abierta o un sistema robusto de mecanismos de denuncias puede suministrar también un sistema de alerta temprana de problemas potenciales en la organización.

Estos asuntos son manejados por lo general dentro de los programas de ética y cumplimiento de las organizaciones, los que contra todo pronóstico y a pesar de la fuerte "corriente de cumplimiento" actual, según nuestra encuesta, parecen estar implementados por menos compañías este año, en comparación con 2016.

Figura No. 25: Menos compañías reportaron tener programas de ética y cumplimiento



P: ¿Cuenta con un programa formal de ética y cumplimiento empresarial en su organización?

Fuente: Encuesta Global Crimen Económico PwC 2018

Evitando la racionalización: cultura

Los diferentes escándalos corporativos que han salido a la luz en el último año han comprobado, por si no lo sabíamos, que el delito económico es también un tema cultural, no solo un asunto de cumplimiento. Incluso los programas de cumplimiento más rigurosos fallarán si la cultura de una compañía permite o acepta los actos indebidos como una forma de hacer negocios.

El primer paso para evitar la racionalización es enfocarse en el entorno que rige el comportamiento del empleado, la cultura organizacional. Las encuestas, los grupos de enfoque y las entrevistas profundas deberán, por lo tanto, ser usadas para evaluar las fortalezas y debilidades de dicha cultura. La capacitación consistente también es clave. Si la gente entiende claramente lo que constituye una acción inaceptable y el por qué de la misma, será más difícil el racionalizar la actividad fraudulenta.

Implementar programas específicos que dejen el fraude al descubierto con estrategias claras, que promuevan la cultura de lo correcto, del compromiso con lo que se dice, de proteger el buen nombre personal y la reputación de la organización son aspectos fundamentales que diferencian a una organización de otra y a los talentos que coherentemente la proyectan. De elevada relevancia es, por tanto, construir la cultura con personas que en sí mismas tienen mecanismos de autocontrol, viven la ética en su día a día y movilizan a otros con su ejemplo; es un asunto personal y no un lejano lema de la gerencia.

Solo un bajo porcentaje de compañías en Colombia tienen en sus programas de ética y cumplimiento políticas específicas en materia de:

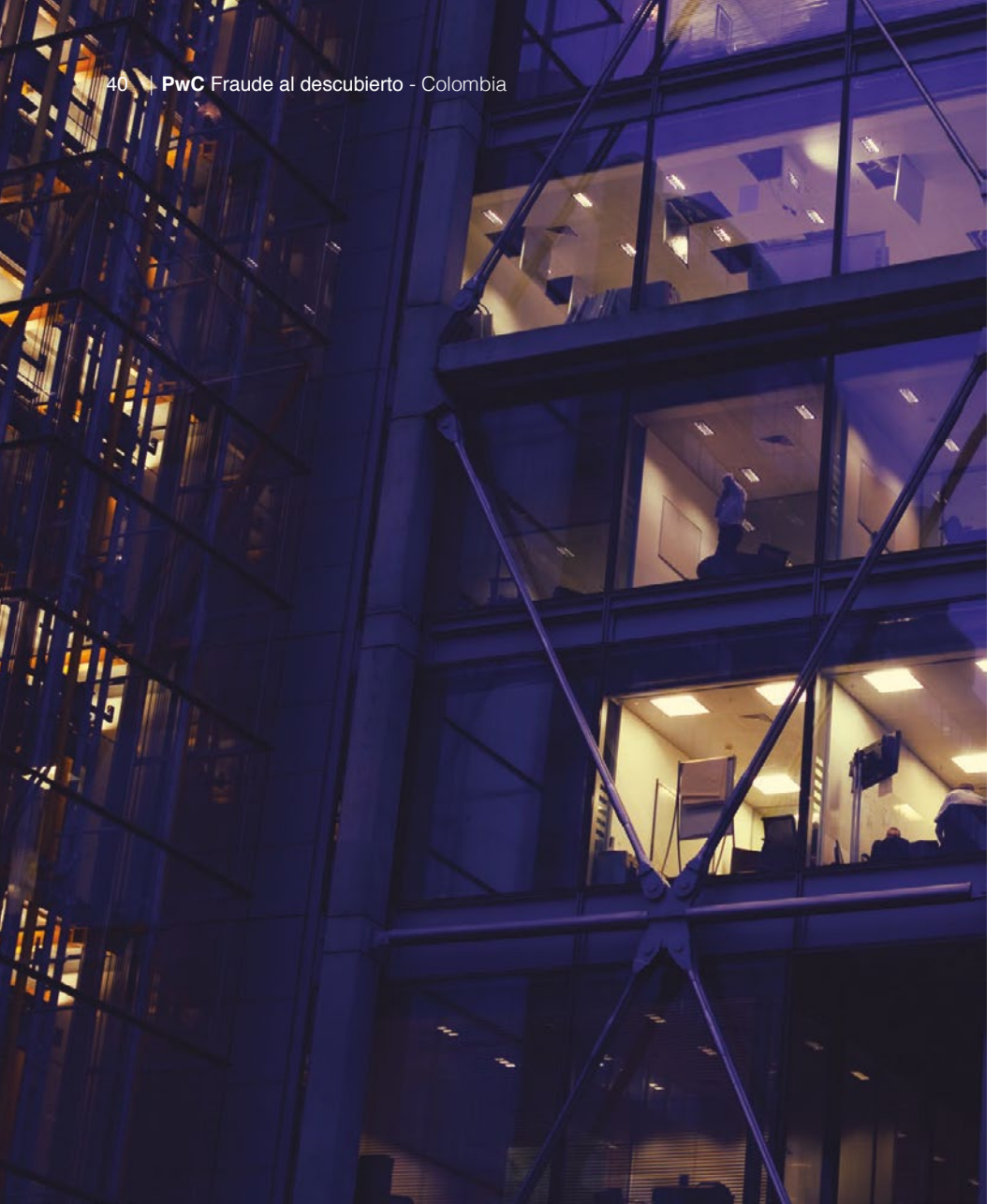
- **54%** Fraude
- **21%** Sanciones y controles de exportación
- **25%** Lavado de Activos
- **21%** Competitividad y antimonopolio
- **37%** Seguridad de la Información y ciberseguridad

La confianza dada a los empleados para que trabajen en diversos cargos bajo un ambiente de autonomía y con directrices claras sobre su comportamiento, deberá ser combinada con los programas de cumplimiento para construir una cultura potente, una cultura basada en valores, donde los empleados y la gerencia son el mejor blindaje para prevenir fraudes. Los líderes, con sus actos y mensajes, construyen la cultura e inspiran a los empleados a "pensar" y "obrar éticamente", con comportamientos que son valorados y propagados en el ambiente organizacional y en la sociedad, donde los beneficios redunden para todos.

¿Cómo podemos ayudar?

Le ayudamos en la construcción y refuerzo de su programa de cumplimiento y estructura de gobierno corporativo al:

- Diagnosticar e implementar los requerimientos legales con respecto a los riesgos de fraude, corrupción, lavado de activos y financiación del terrorismo LA/FT.
- Diseñar una capacitación hecha a la medida para sus empleados y contrapartes con respecto a los asuntos de antisoborno, anticorrupción y LA/FT.
- Asistirle en la evaluación de su actual estructura de Gobierno Corporativo, optimizando sus procesos, políticas y normativas.
- Evaluación y diseño del esquema de la cultura organizacional.
- Definición y/o restructuración de valores corporativos.



Finalmente, ¿Por dónde comenzar?

Cuando considere el actual panorama de fraude y de prevención del mismo, aquí tiene algunas preguntas prácticas para saber por dónde comenzar:

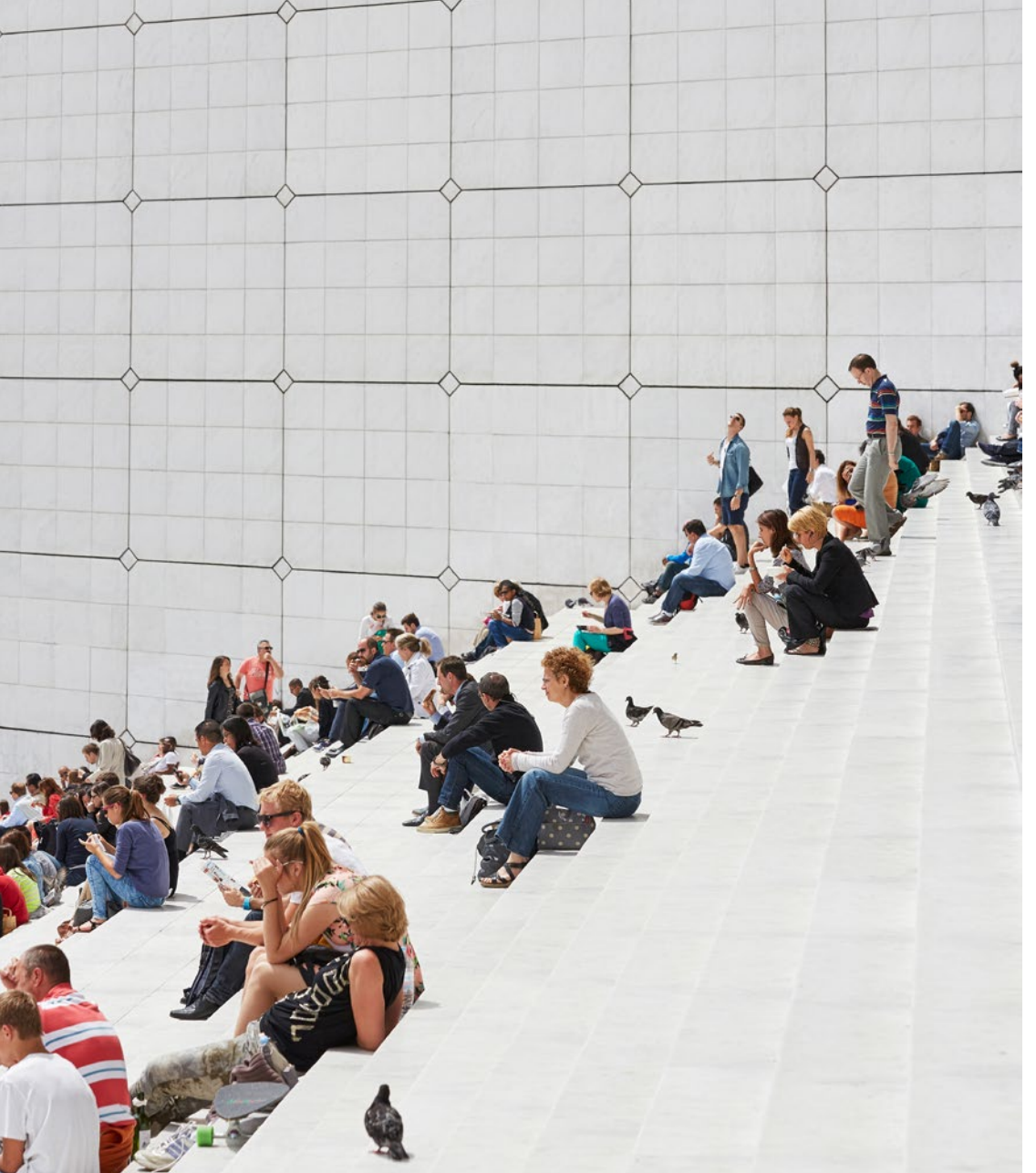
- ¿Ha llevado a cabo una evaluación de riesgo de fraude en toda la empresa, que le permita identificar sus escenarios de riesgos y vulnerabilidades al fraude?
- ¿Está teniendo en cuenta, en sus actividades para mitigar el fraude, los roles y responsabilidades de los cargos de la alta gerencia; los potenciales riesgos asociados con su poder de decisión y la posible capacidad de saltarse los controles internos existentes?
- En la lucha contra el fraude ¿se está enfocando solo en el fraude externo?
- ¿Qué tan involucrada se encuentra la junta y/o comité de auditoría en la supervisión de las actividades para detectar eventos de fraude, corrupción y/o lavados de activos en la compañía?
- ¿Cuenta con un programa integrado de cumplimiento y ética empresarial que incluya procedimientos para prevención, detección de fraude y corrupción? ¿Cómo se compara su programa con el de sus colegas?
- ¿Tiene su compañía un programa robusto de capacitación en materia de fraude, corrupción y lavado de activos, que se ajuste a las necesidades y tamaño de la organización?
- ¿Está encontrando un equilibrio adecuado entre la inversión en tecnología, así como en la cultura organizacional?
- ¿Ha disminuido el número de sus revisiones internas o recortado los recursos que antes se dedicaban a los programas para la prevención de fraude?
- ¿Tiene su organización un sistema de denuncias que se ajusta al tamaño de la compañía?
  - ¿Es confiable para cualquier interno/externo que quiera denunciar?
  - ¿Cómo se está gestionando?
  - ¿Qué resultados arroja?
  - ¿Cómo se están adelantando las investigaciones derivadas de las denuncias?
- En una crisis ¿conoce el protocolo de respuesta, los roles y responsabilidades de quienes deben intervenir?

Contactos de la red PwC

Mónica Jiménez
Socia Líder Advisory
+57 1 634 05 55 Ext. 10202
monica.jimenez@co.pwc.com

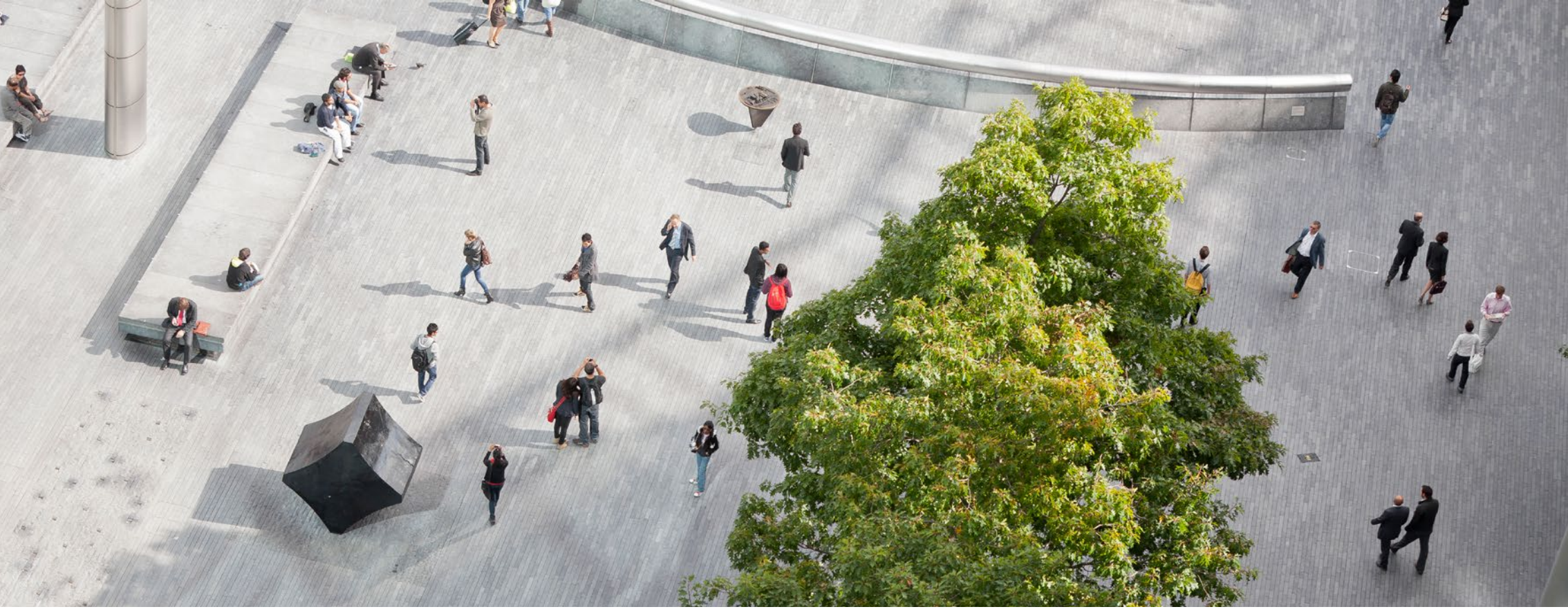
Jorge Ropero
Gerente Servicios Forenses
+57 1 634 05 55 Ext. 10438
jorge.ropero@co.pwc.com

Diego Fernando Vargas
Gerente Servicios Forenses
+57 1 634 05 55 Ext. 10226
diego.f.vargas@co.pwc.com



Acerca de la encuesta

La Encuesta Global sobre Fraude y Delitos Económicos de 2018 – PwC fue diligenciada por 7.228 encuestados de 123 territorios. Del total de encuestados: el 52% eran ejecutivos senior de sus respectivas organizaciones, el 42% representan a las compañías que cotizan en bolsa y el 55% representan organizaciones con más de 1.000 empleados.



www.pwc.com/co

PwC ayuda a las organizaciones y personas a crear el valor que están buscando. Somos una red de firmas presente en 158 países, con más de 236.235 personas comprometidas a entregar calidad en los servicios de Auditoría, Impuestos y Consultoría. Cuéntanos lo que te importa y encuentra más información visitando nuestra web: www.pwc.com.