Hacia una nueva ética en los negocios:

preparados para evitar el crímen económico y cibernético

32%

Más de un tercio de las organizaciones en Colombia reportan haber sido víctimas del delito económico.

32%

A nivel Global, el crímen cibernético asciende este año al segundo puesto de delitos económicos reportados.

61%

Más de la mitad de los encuestados en Colombia declaran que los defraudadores son actores al interior de la organización.

pwc

www.pwc.com/crimesurvey

Hacia una nueva ética en los negocios:

preparados para evitar el crímen económico y cibernético

Datos a nivel mundial

1 *La amenaza constante de los delitos económicos.*

- El 36% de las organizaciones experimentaron delitos económicos.
- Países desarrollados, así como mercados emergentes fueron víctimas de delitos de este tipo.
- Los métodos de detección de las compañías no responden a tiempo.

¿Qué oportunidades existen en la lucha proactiva contra la delincuencia económica?

El delito económico es un problema mundial.

2 *Los controles deben ser parte de la cultura organizacional.*

- Los fraudes conservan la misma tendencia en cuanto al incremento en el número de delitos, sin importar si fueron cometidos por actores internos o externos.
- Uno de cada cinco encuestados nunca ha llevado a cabo evaluaciones de riesgo de fraude.

¿Sabes cuáles son los riesgos que enfrenta tu negocio? ¿Has identificado las áreas más vulnerables?

Las consecuencias financieras sobrepasan los millones de dólares en algunos casos.

3 *Los delitos cibernéticos aumentan pero la capacidad de respuesta de las empresas no crece a la misma velocidad.*

- La ciberdelincuencia es el segundo delito económico más reportado, afecta al 32% de las organizaciones.
- La mayor parte de las empresas aún no están preparadas, inclusive algunas parecen no entender los riesgos que enfrentan: sólo el 37% de las organizaciones tiene una respuesta ante incidentes cibernéticos.
- El compromiso de las directivas es fundamental, pero menos de la mitad de los miembros de la junta directiva solicitan información sobre el estado de la preparación y respuesta ante ataques cibernéticos.

¿Realmente cuál es el estado de preparación y respuesta de su empresa ante ataques cibernéticos?

Estar preparados es visto como una fortaleza de la empresa.

4 *Falta de alineación entre las directivas y el resto de la empresa.*

- Uno de cada cinco encuestados no sabe que existe un programa de ética y cumplimiento formal en su empresa, ni quiénes son los responsables de su implementación.
- Casi la mitad de los casos de delitos económicos graves fueron perpetrados por actores internos de la compañía.
- Las principales consecuencias de los delitos económicos son el impacto en la moral de los empleados (44%) y el daño reputacional (32%) para las compañías.

¿Su estrategia de negocio está alineada con los valores organizacionales?

Su primer mecanismo de defensa son sus empleados y la cultura organizacional.

5 *El control de lavado de activos continúa sorprendiendo.*

- Uno de cada cinco bancos ha experimentado multas o acciones por parte de los reguladores. La falta de cumplimiento puede dar lugar a responsabilidad civil.
- Más de una cuarta parte de las empresas de servicios financieros no ha llevado a cabo evaluaciones de riesgo de Lavado de Activos y Financiación del Terrorismo.
- La falta de personal con experiencia en la prevención y detección de LA/FT[1] es un problema serio para las empresas.

¿Cómo se encuentra preparada su organización para enfrentar las exigencias de los reguladores?

Los costos de los programas de cumplimiento han aumentado, al igual que los costos asociados al incumplimiento.

1) Lavado de activos y Financiación del terrorismo (LA/FT)

Contenido

Prólogo

Mónica Jiménez
Socia de Advisory
Colombia

El Fraude, el crimen cibernético y la ética empresarial, un desafío para nuestras organizaciones.

Las empresas hoy más que antes buscan su expansión, aumentar su oferta de productos y servicios, y llegar a más personas en distintas regiones y comunidades, un objetivo estratégico que necesita fundamentalmente de la tecnología y que trae consigo riesgos para la organización al ampliar su marco de actuación en entornos diferentes y con nuevas formas de hacer negocios.

Y lo que la realidad nos muestra, es que la delincuencia económica no conoce fronteras y que es un riesgo siempre latente dispuesto a vulnerar la puerta de seguridad de las organizaciones, violando las barreras de control implementadas y convirtiéndonos en víctimas de la misma.

Es importante comprender que la tecnología, clave en el proceso de expansión, es una de las áreas donde más se ha incrementado el nivel de vulnerabilidad originado en la permanente innovación tecnológica de los sistemas de información y, en general, en la automatización de los procesos productivos y operativos que facilitan la conexión automática y con ella los fraudes cibernéticos.

Hace unos años la distancia nos protegía de los delincuentes cibernéticos, hoy todo es diferente. El delincuente puede estar sentado junto a nosotros o ser nuestro antípoda, el riesgo no cambia, con la misma velocidad y oportunidad tendrá la posibilidad de convertirnos en su víctima. La diferencia estará en los controles de seguridad cibernética instalados para salvaguardar la información de la organización, los cuales evitarán las transacciones ilegales y el acceso indebido a la información.

Pero no todo radica en la tecnología ni en las herramientas de seguridad; de forma transversal y siendo un tema de discusión profundo y complejo, están la ética y los valores, fundamentos constituidos en el ser humano desde la familia, pero que nosotros como líderes empresariales debemos fomentar en nuestros equipos de trabajo, proveedores y clientes. Dentro de este contexto, no solamente mejoraremos significativamente el cumplimiento de nuestras políticas, sino el cumplimiento de leyes y regulaciones establecidas por órganos de control, supervisión y vigilancia del estado.

Porque es desde allí que crearemos barreras robustas para aquellos “creativos” cibernéticos y no cibernéticos que buscan un enriquecimiento ilícito a través de estas transacciones, y que vulneran nuestros códigos de ética y conducta, en los que creemos y cumplimos.

Nuestra encuesta de Delitos Económicos 2016 muestra claramente cómo se ha incrementado la vulnerabilidad en el ambiente cibernético y cómo se sostienen los indicadores de delincuencia económica alrededor de algunos procesos e industrias que son más sensibles al fraude pero que comparten un factor: la necesidad de contar con mayores esfuerzos para fortalecer una cultura de ética y control en las organizaciones.

El riesgo de fraude es un aspecto que las compañías debemos continuar trabajando, no podemos “bajar la guardia”, debemos analizar permanentemente en dónde están los riesgos más significativos de fraude y cuál es la mejor forma de reducirlos mediante herramientas automatizadas, expertos en el tema y una adecuada formación a nuestros colaboradores.

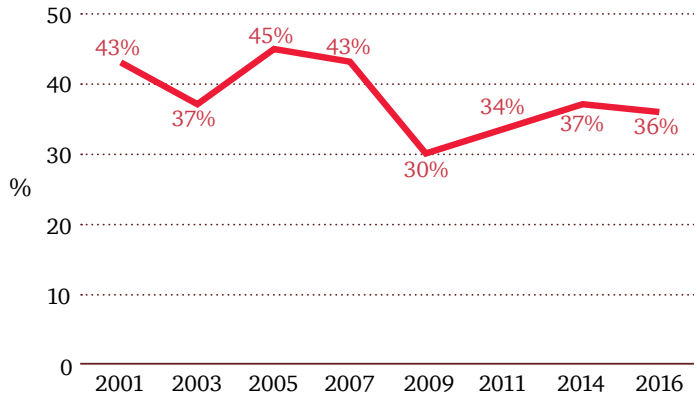
Situación actual del delito económico

2016: El delito económico evoluciona y las medidas de prevención retroceden.

Nos complace presentar los resultados obtenidos en la primera Encuesta Global de Delitos Económicos GCS (por sus siglas en inglés, Global Crime Survey) realizada por PwC Global con la participación de PwC Colombia. La encuesta, desarrollada a nivel global desde el 2001, ofrece gran cantidad de información que nos permitió comparar a Colombia con otras regiones del mundo y según esto, establecer tendencias.

El delito económico presenta un comportamiento en el que más de un tercio (32%) de las organizaciones reportan haber experimentado delitos de esta naturaleza en los últimos 24 meses, así lo indicaron los 118 participantes de la encuesta en Colombia. A nivel global, las respuestas de más de 6000 participantes demostraron una leve disminución en los casos de delitos económicos (1%), primera vez que ocurre desde la crisis financiera de 2008-2009.

Fig 1: Tasa reportada de crimen económico



Encuesta Global 2016

Nuestros hallazgos del GCS indican que 1 de cada 10 delitos económicos son descubiertos por accidente.

En primera instancia, esto podría evidenciar un retorno de la inversión de las medidas preventivas que tomaron recientemente las organizaciones. Pero si se revisan los datos en detalle, esta ligera disminución oculta una preocupante tendencia; el crimen organizado ha cambiado significativamente su forma de perpetrar los crímenes económicos, mientras que los controles y los esquemas de detección de las empresas no reaccionan oportunamente. Esta situación es más preocupante si se tiene en cuenta el aumento en el costo financiero del fraude. El informe de este año muestra como la delincuencia económica ha evolucionado en los últimos dos años, transformándose de diferentes formas dependiendo del sector industrial y de la región.

A pesar de esta continua amenaza, a nivel global se observa una disminución en la efectividad de los esquemas de detección de actividades criminales en términos de control de gestión (detección durante controles corporativos que se ha reducido en un 7%). Además, una de cada cinco organizaciones (22%) a nivel global no ha llevado a cabo ningún tipo de evaluación de los riesgos de fraude en los últimos 24 meses. En Colombia la estadística no está lejos (19%).

La Encuesta Global Anual de CEOs de PwC 2016 muestra que el 67% de los directores ejecutivos perciben más que antes amenazas para el crecimiento de su empresa (8% más que en 2015), con una tendencia preocupante en la que pareciera que muchos aspectos en las organizaciones han sido dejados al azar, una actitud pasiva ante la delincuencia económica que produce efectos desastrosos.

Además la encuesta, tanto a nivel global como local reveló una falta generalizada de confianza en las políticas locales, un fenómeno que no se limita a las regiones o países poderosos.

El mensaje es claro: la prevención, la protección y la respuesta a la delincuencia económica depende de cada una de las organizaciones.

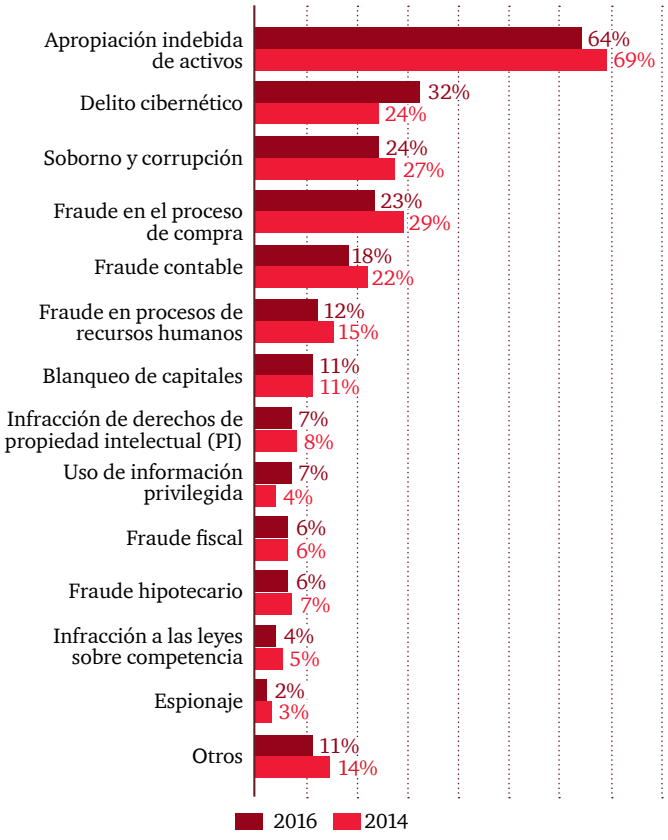
Este año la encuesta se focaliza en tres áreas: Crimen Cibernético, Control de Lavado de Activos, y Programas de Ética y Cumplimiento. Adicionalmente explora ciertos temas, incluyendo la gestión de riesgos asociados a la implementación de la tecnología, la importancia de realizar negocios de manera responsable y la integración de la conducta ética en la toma de decisiones.

Este informe identificará las formas idóneas para evitar los delitos económicos, ayudando así a contrarrestar esta tendencia basándose en el cumplimiento de las responsabilidades legales.

Se observa la misma tendencia en todos los delitos económicos a excepción de uno que va adquiriendo ventaja.

Los delitos económicos más comunes reportados por los encuestados son:

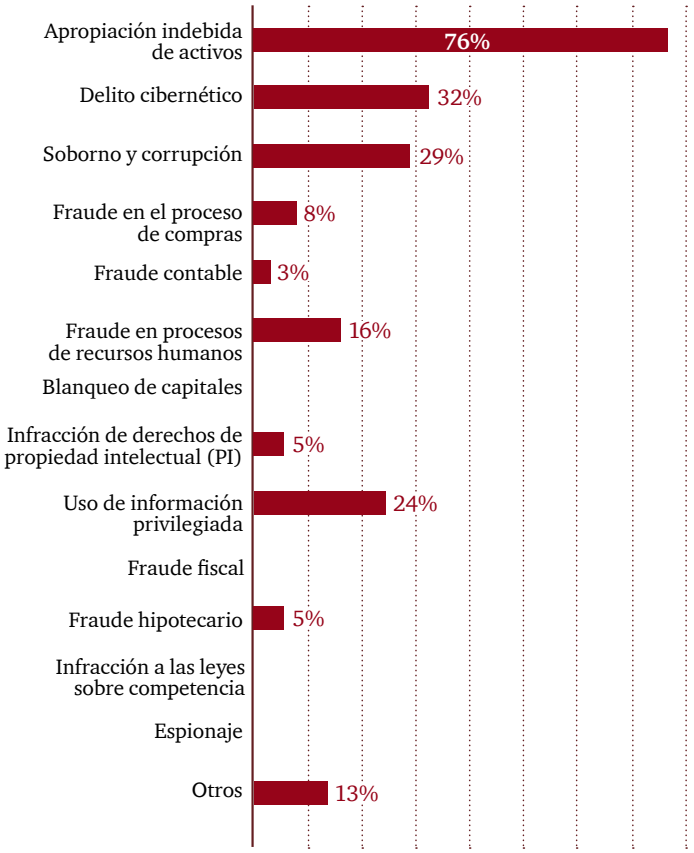
Fig 2: ¿Qué tipos de delitos económicos ha sufrido su organización durante los últimos 24 meses?



Encuesta Global 2016

De las empresas que han experimentado delitos económicos la malversación de activos tiene el mayor porcentaje a nivel Colombia, el cual corresponde a un 76% contra un 64% a

Fig 3: ¿Qué tipos de delitos económicos ha sufrido su organización durante los últimos 24 meses?



Encuesta Colombia 2016

nivel global. A diferencia de la cifra global donde el fraude contable tiene un 18%, en Colombia es tan solo del 3%. El lavado de activos no es considerado un delito relevante en Colombia, caso contrario al "insider trading" o el fraude por uso de la información privilegiada; en Colombia se considera un delito al 24% y a nivel global al 7%.

El soborno y corrupción, y el fraude en compras han sido históricamente fuertes a nivel Latinoamérica, sin embargo demostraron un descenso este año respecto a las estadísticas de 2014. Un delito que ha demostrado un continuo crecimiento es el crimen cibernético, el cual se posiciona este año en el segundo puesto, tanto a nivel latinoamericano como a nivel Colombia.

Fig 4: Los 3 de delitos económicos más reportados en 2016

Encuesta Global 2016

Encuesta Colombia 2016

La apropiación indebida o malversación de activos ha sido tradicionalmente considerado como el fraude más fácil para detectar, por lo tanto su prevalencia en nuestra encuesta global es generalmente predecible. Sin embargo, a nivel global desde 2011, hemos visto una tendencia a la baja en el reporte de este delito. En Colombia el porcentaje de esta acción es el mismo que a nivel Latinoamérica (76%).

El soborno y la corrupción han mantenido su posición dentro de los top 5 de fraudes reportados a nivel Latinoamérica. Si comparamos el porcentaje de 2015, entre Colombia y Latinoamérica, el porcentaje en Colombia es mayor en 9 puntos (29% Colombia vs 20% Latinoamérica).

Teniendo en cuenta la disminución en la detección de actividades criminales en términos de control de gestión y el aumento de la ciberdelincuencia, debemos preguntarnos: ¿son estos crímenes cada vez más difíciles de detectar o somos cada vez menos conscientes de los riesgos que enfrentan nuestros negocios? Y además, la pregunta más importante: ¿qué debemos hacer al respecto?

Con un promedio del 20% de los encuestados a nivel global que cree que es probable que sus organizaciones experimenten estos delitos económicos en los próximos 24 meses, es el momento adecuado para retomar el tema.

El delito económico, un problema global con diferente intensidad según la región

Región	Delitos económicos reportados 2016	Delitos económicos reportados 2014
África	57%	50%
Europa Occidental	40%	35%
Norte América	37%	41%
Europa Oriental	33%	39%
Asia	30%	32%
América Latina	28%	35%
Medio Oriente	25%	21%
Global	**36%**	**37%**

Encuesta Global 2016

Mientras la mayoría de las regiones reportaron cifras más bajas en cuanto al delito económico, África y Europa Occidental mostraron incrementos significativos en la encuesta de 2016. Los principales protagonistas que ocasionan el aumento en las tasas de delincuencia económica en África fueron: Sudáfrica (69%, sin cambios desde 2014) seguido por Kenia (61%, un 17% sobre el porcentaje de 2014) y Zambia (61% con respecto al 35% en el 2014). En Medio Oriente, aunque el incremento no fue tan significativo, los encuestados en Arabia Saudita por ejemplo, reportaron cifras que se duplicaron del 11% en el 2014 al 24% en el 2016.

En Europa Occidental, Francia (68%) y el Reino Unido (55%) protagonizaron los incrementos de la región. Ambos aumentaron aproximadamente un 25% con respecto al 2014. El de Francia se debe a una mayor cantidad de fraudes por causas externas, en su mayoría por la ciberdelincuencia, situación que casi se duplicó pasando de 28% en 2014 al 53% en 2016. En el Reino Unido, el porcentaje aumentó un 83%.

A nivel regional, mientras que la mayoría ha experimentado un aumento de incidentes de ciberdelincuencia, Europa del Este reportó una caída del 2% (10% inferior a la media mundial). La ciberdelincuencia tampoco figura en los tres principales tipos de delitos económicos de África, Asia Pacífico y Europa del Este. Estas regiones tienen más casos en temas de soborno, corrupción y fraude en compras, respecto al promedio global.

Mientras que la mayoría de países desarrollados han experimentado altos niveles de regulación local por delitos informáticos, lavado de dinero y soborno, y corrupción; el control ha tenido que evolucionar y trascender fronteras dado

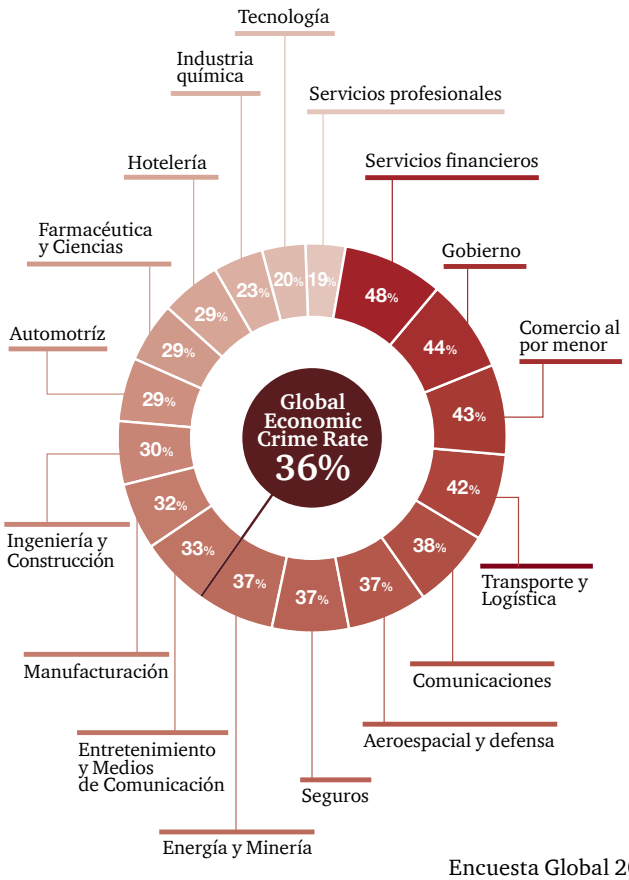
que las actividades delictivas también lo están haciendo. Esto ha impulsado la cooperación internacional en leyes y regulaciones de este tipo.

Existe la oportunidad para todas las organizaciones, sin importar su tamaño o diversidad geográfica, de tener una visión global y una aplicación de normas internacionales a sus esfuerzos para luchar contra los delitos económicos.

¿Cómo está afectando la delincuencia económica a la industria?

Los servicios financieros tradicionalmente han demostrado ser la industria más amenazada por este delito económico, ya que son el canal financiero de todas las industrias.

Fig 5: ¿Qué industrias están en riesgo?



Encuesta Global 2016

Se añade un problema, con la evolución del mercado hacia soluciones integradas de negocio, muchas organizaciones están realizando actividades que tradicionalmente son efectuadas por los bancos. Numerosas empresas de servicios no financieros como el automotriz, comercio minorista y los sectores de consumo y comunicaciones, por nombrar sólo unos pocos, están creando alianzas con compañías de servicios financieros o están obteniendo sus propias licencias bancarias. Gracias a esto los estafadores ahora tienen muchas más posibilidades de cumplir su objetivo.

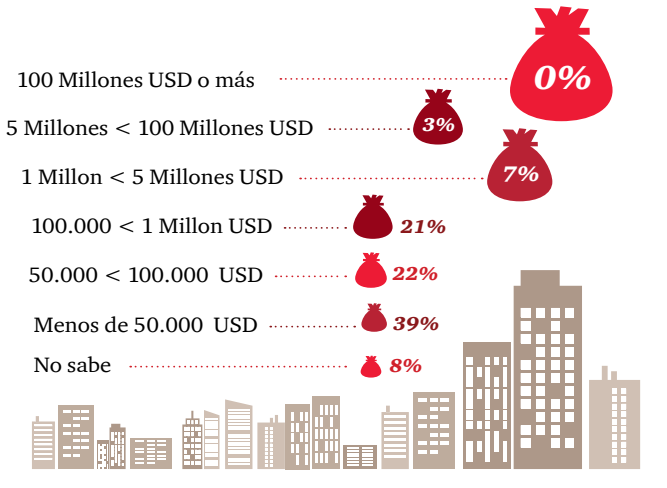
Mientras que la industria de servicios financieros, en virtud del alto entorno regulado, ha construido a lo largo de las décadas mecanismos de control sofisticados, metodologías de detección y herramientas de gestión de riesgos, los nuevos actores mencionados anteriormente entran al escenario por su cuenta en la gestión de los riesgos en un panorama de continuo cambio.

Daños financieros y colaterales en aumento

Mientras más de la mitad de las organizaciones encuestadas a nivel Latinoamérica (61%) informaron haber perdido hasta USD 100.000 a causa de delitos económicos en los últimos 24 meses, el 31% experimentó pérdidas entre $100 mil y $100 millones.

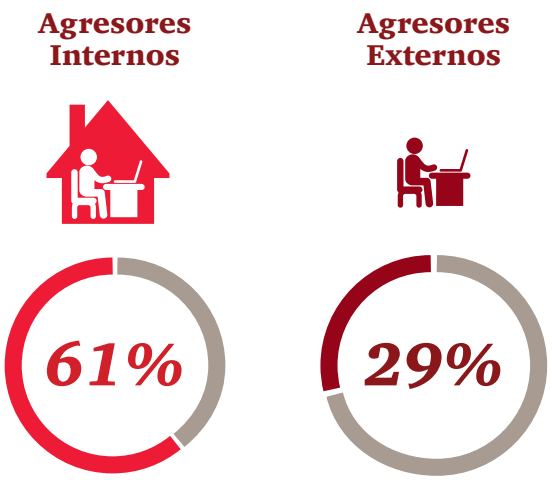
El verdadero costo de la delincuencia económica para la economía mundial es difícil de estimar, en especial cuando se tiene en cuenta que la pérdida financiera real a menudo sólo es un pequeño componente de las consecuencias de un incidente más grave, como por ejemplo pérdida en relaciones comerciales, medidas correctivas, intervenciones por investigación, multas reglamentarias, honorarios legales, entre otros. Todas estas tienen un impacto en el resultado final y los costos pueden ser enormes, aunque en gran parte inestimables.

Fig 6: En términos financieros, aproximadamente cuál es la pérdida económica en América Latina de los últimos 24 meses



Perfil del defraudador

Según las estadísticas latinoamericanas los empleados que operan al interior de la organización son los que tienen el perfil principal del defraudador, aunque las cifras han disminuido en forma importante con respecto a los reportes de años anteriores (55% en comparación con 70% en 2014). En Colombia la cifra de este año es más alta que la de Latinoamérica (61% vs 55%).



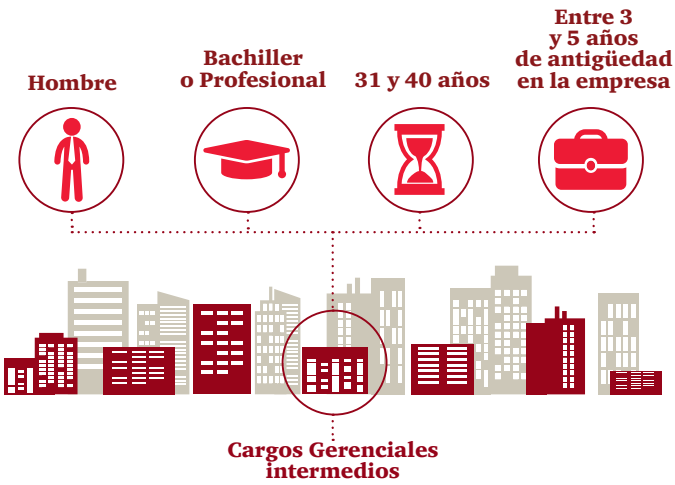
Encuesta Colombia 2016

En Latinoamérica la tendencia se inclina a que aproximadamente la mitad de los agresores internos son mandos medios y superiores, sin embargo los directivos de mandos medios o intermedios han contribuido en mayor medida a realizar el fraude interno. Este aspecto sumado a una debilidad potencial en los controles internos en donde simplemente se trata de completar requisitos en lugar de convertirse en un proceso efectivo que haga parte de una cultura organizacional, son factores que permiten que el fraude ocurra. En Colombia, por ejemplo, el 19% de los encuestados nunca ha llevado a cabo la evaluación del riesgo de fraude y además el 29% únicamente realiza una evaluación anual.

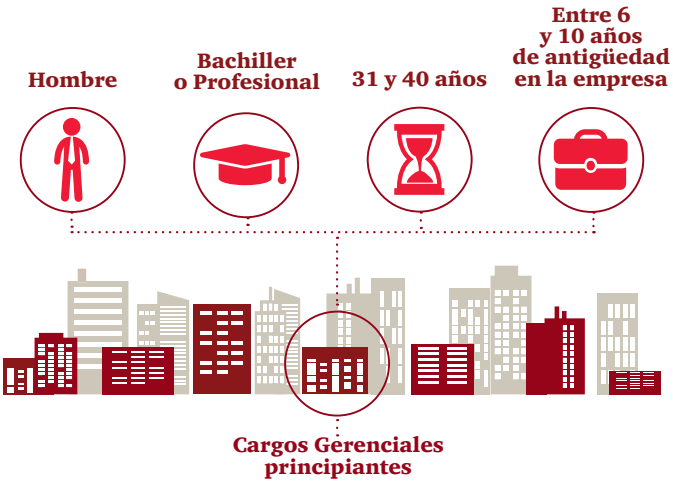
A diferencia de América Latina, donde el perfil del defraudador se inclina por personas entre 3 y 5 años de antigüedad en la empresa; en Colombia el perfil del defraudador oscila entre 6 y 10 años de antigüedad.

Ahora más que nunca las organizaciones tienen la oportunidad de restructurar sus mecanismos de control y volver a los fundamentos creando una cultura de controles y de conciencia sobre la existencia del riesgo, en lugar de actividades que funcionen por inercia. Además, demostrar un comportamiento de cero tolerancia en caso de prácticas deshonestas puede ayudar a las organizaciones a evitar pérdidas debidas al fraude interno.

Fig 7: Categoría del perfil del defraudador en las organizaciones en los últimos 24 meses. América Latina Vs Colombia



Encuesta América Latina 2016



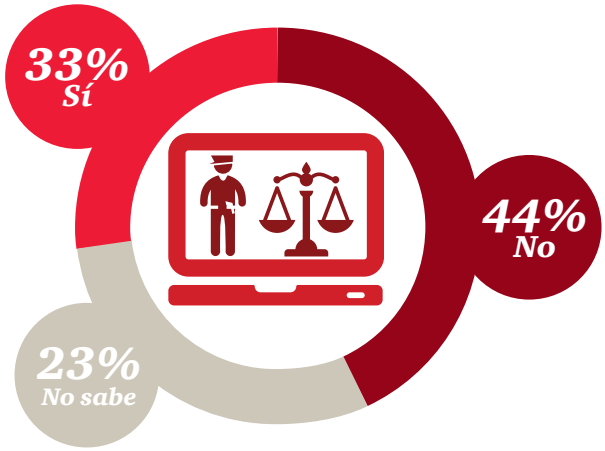
Encuesta Colombia 2016

Percepciones sobre los reguladores

Al preguntar a los encuestados su opinión sobre si los organismos gubernamentales cuentan con los recursos suficientes para investigar y declarar juicios a delitos económicos de manera adecuada; a nivel global, un rotundo 44% respondió negativamente, mientras que otro 28% considera que sí y otro 28% dice no tener el conocimiento para responder. En Colombia los resultados no son muy alejados, un porcentaje de 44% negativo, 33% positivo y 23% no tiene el conocimiento para responder a la pregunta.

Esta métrica se debe a varios factores, algunos de estos son el tamaño o porcentaje de la delincuencia económica en cada país y el grado en que las fuerzas del orden dan o restan importancia a áreas como la delincuencia informática.

Fig 8: ¿Cree que los agentes gubernamentales cuentan con la capacitación y recursos necesarios para investigar y perseguir delitos económicos?



Encuesta Colombia 2016

Listado de los primeros 15 países que consideran que los agentes gubernamentales no cuentan con la capacitación y recursos necesarios para investigar y perseguir delitos económicos

1	Kenia	79%
2	Sudáfrica	70%
3	Turquía	60%
4	Filipinas	58%
5	Bulgaria	58%
6	Polonia	58%
7	Ucrania	57%
8	México	56%
9	Zambia	55%
10	Nigeria	54%
11	Australia	52%
12	Estados Unidos	52%
13	Francia	51%
14	Venezuela	50%
15	India	49%

Encuesta Global 2016

Convertir la probabilidad de que ocurra un delito en una oportunidad para crecer.

A lo largo de nuestro informe nos hemos centrado en las respuestas más significativas en cuanto a las áreas estratégicas y oportunidades de mejoramiento en los negocios, pero ¿qué significan realmente estos datos en el futuro de su negocio? Como lo hemos discutido, las próximas secciones estarán dedicadas a las tres áreas estratégicas y críticas: el ciber-crimen, anti lavado de dinero, y ética y programas de cumplimiento. Los resultados de esta encuesta no sólo pueden ayudar a descubrir tendencias y banderas rojas potencialmente problemáticas, sino también ser útiles como indicadores de áreas significativas que generan oportunidades para las organizaciones con visión futurista. Estar prevenido es estar preparado para el éxito.

Ciber-crimen:

Aunque se presume que los activos militares son altamente seguros, los hackers han encontrado deficiencias en los sistemas de seguridad considerados de "bajo riesgo"; lo cual puede ser fácilmente usado para rastrear el destino de sus suministros.

Cuando la conectividad está omnipresente, también lo están las amenazas

La tecnología digital continúa transformando al mundo de los negocios, pero también la exposición de las organizaciones a las oportunidades y/o amenazas. Por lo tanto, no es de extrañar que la ciberdelincuencia siga aumentando, ubicándose como el segundo tipo de crimen reportado en la Encuesta Global de Delitos Económicos de este año.

La realidad en el año 2016 es que así como cualquier tema comercial que se extiende y tiende a abarcar contenido digital, los delitos económicos no son una excepción. En una red de negocios internacionales que se encuentra en continua conexión y que incluye diversos terceros como proveedores de servicios, socios, gobierno y reguladores, el panorama digital de las organizaciones puede verse comprometido de diversas maneras. El riesgo cibernético es un concepto que abarca más de lo que tradicionalmente percibimos como una computadora. Hemos visto un fuerte aumento de ataques cibernéticos que incluye temas como el Internet de las cosas ("IoT" siglas en inglés Internet of Things) incluyendo hasta aparatos domésticos y vehículos.

Es esta la paradoja de los medios digitales, las empresas hoy en día son capaces de expandirse y alcanzar más territorios más rápido que nunca, gracias a las conexiones digitales modernas, herramientas y plataformas que pueden conectarse en tiempo real con clientes, proveedores y socios. Al mismo tiempo, la delincuencia cibernética se ha convertido en una poderosa fuerza que está limitando ese potencial.

La amenaza cibernética que puede afectar a las empresas es precisamente lo que preocupa a sus directivos. El elevado nivel de preocupación sobre la creciente invasión de la ciberdelincuencia se confirma en la Encuesta Global Anual de CEOs de PwC 2016, en donde cada seis de diez directivos expresaron que los ciber-ataques y la velocidad de la tecnología son las principales amenazas a ser consideradas.

Los resultados de la encuesta de este año apuntan a un hecho inquietante; demasiadas organizaciones están dejando como primeros agentes a intervenir a sus equipos de IT sin el adecuado seguimiento por parte de la alta dirección, y es aún más preocupante la composición de estos equipos, la cual es fundamentalmente defectuosa y por lo tanto afecta a las organizaciones.

Fruto de nuestro trabajo como Firma en temas de estrategia digital y ejecución en empresas a nivel mundial, hemos identificado prácticas que distinguen a los líderes en esta era digital. La principal de ellas es una actitud proactiva en temas de ciber-seguridad y privacidad. Para ello es necesario que todos en la organización – desde la junta directiva, la alta dirección, los mandos intermedios y los trabajadores lo vean como su responsabilidad.

El ciber-crimen, en un mundo de negocios en continua conexión, a nivel Global continúa en ascenso ubicándose en el segundo lugar de delitos económicos reportados.

El ciber-crimen alcanza el segundo lugar delitos económicos reportados

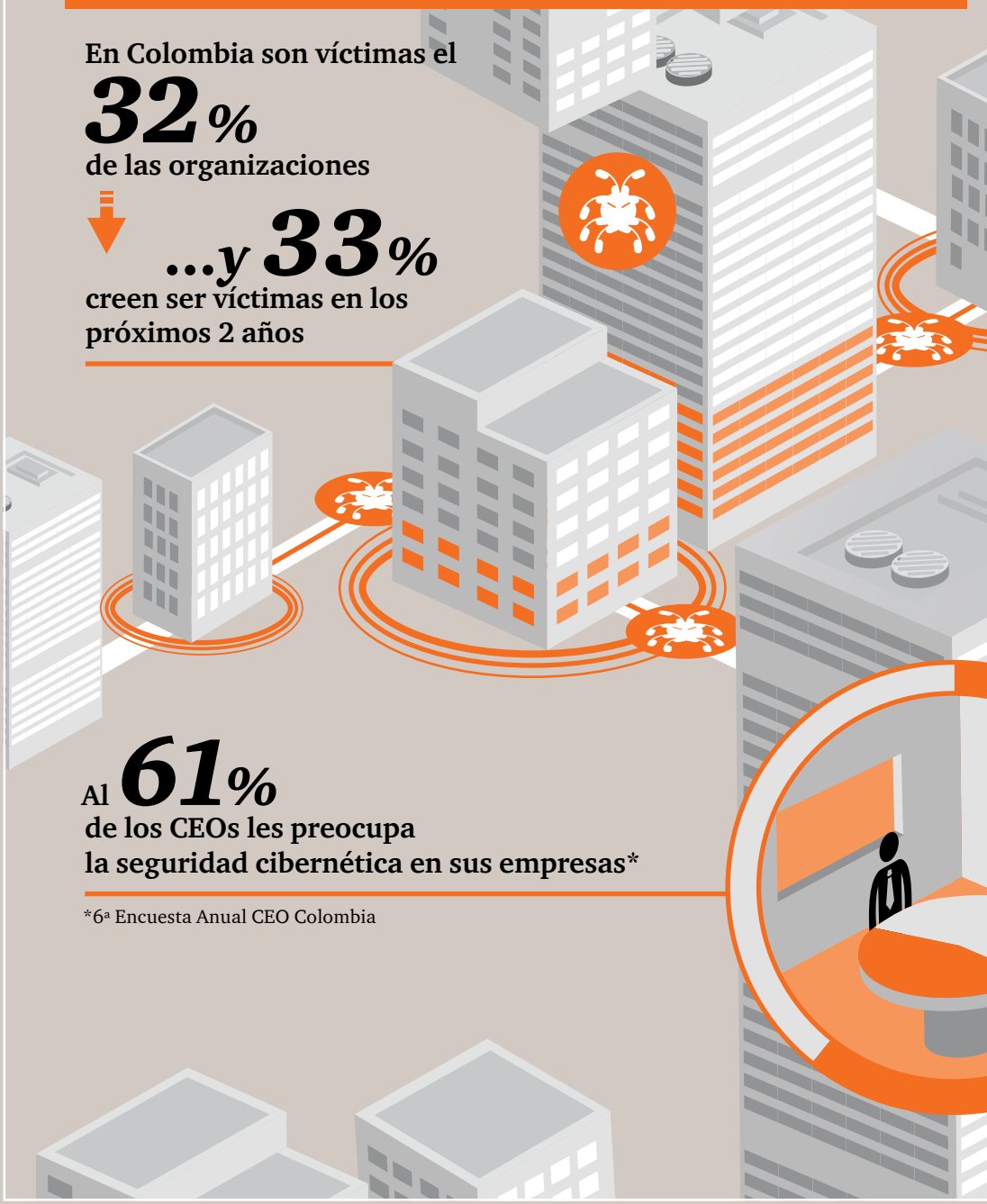
En Colombia son víctimas el

32%

de las organizaciones

...y 33%

creen ser víctimas en los próximos 2 años



Al **61%**

de los CEOs les preocupa la seguridad cibernética en sus empresas*

*6ª Encuesta Anual CEO Colombia

Tan solo el 32%

de las organizaciones en Colombia tienen un plan de respuestas ante el ciber-crimen

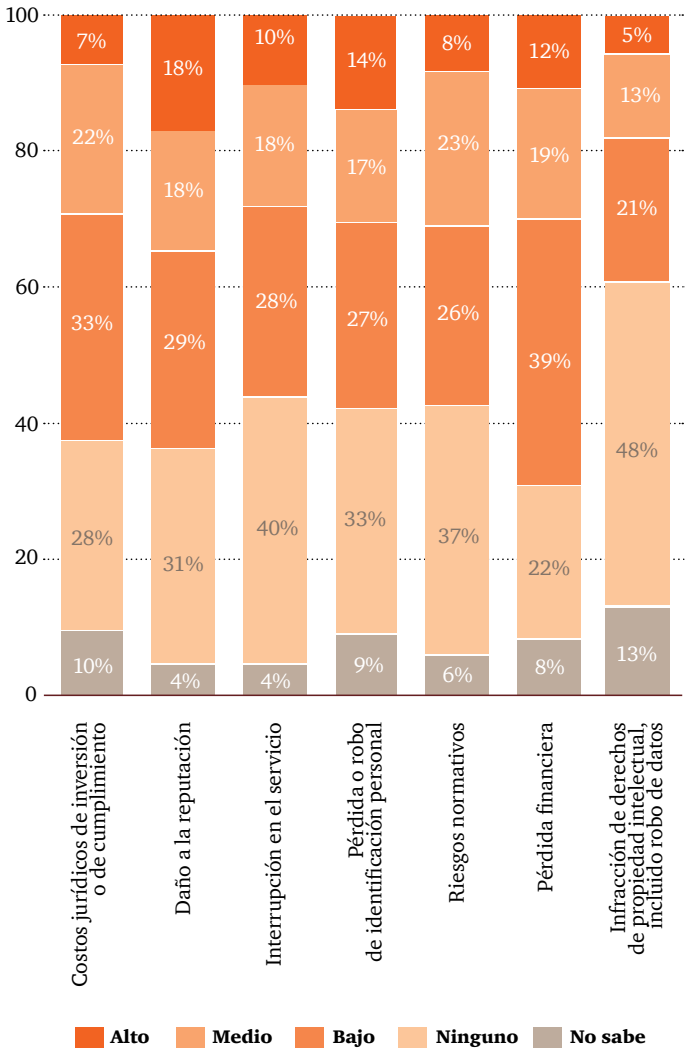
La mayoría de las empresas no están adecuadamente preparadas, incluso no entienden los riesgos que enfrentan.

¿Su plan de respuesta ante ataques cibernéticos está adaptado a la realidad?

Hallazgos clave: El ciber-crimen continúa en ascenso

El resultado de nuestra encuesta de ciberdelincuencia a nivel global es mucho más alto que en años anteriores, subiendo del cuarto al segundo lugar dentro de los tipos de delitos económicos reportados. De hecho, ha sido el único delito económico que presentó incremento. Este año en Latinoamérica, la ciberdelincuencia se ubica en el quinto lugar.

Fig 9: Si el ciber-crimen ha afectado a su organización en los últimos 24 meses, cómo mide usted el nivel de impacto en los siguientes aspectos:



Encuesta Latinoamérica 2016

Las pérdidas pueden ser altas, a nivel global la encuesta demuestra que aproximadamente 50 organizaciones reportan pérdidas superiores a $5 millones de dólares. De estas, aproximadamente un tercio reportaron pérdidas a causa del crimen cibernético de más de $100 millones de dólares.

En Latinoamérica el impacto en cuanto a reputación fue considerado el más perjudicial, seguido por la pérdida o robo de información personal, pérdida financiera, interrupciones del servicio, riesgos regulatorios, costos jurídicos de inversión o de cumplimiento, e infracción de derechos de propiedad intelectual, incluido el robo de datos.

En Colombia, la amenaza es preocupante. El porcentaje de personas que respondió no haber sido víctima de delitos cibernéticos es del 64%, por lo tanto pueden llegar a estar comprometidos sin saberlo. Una tendencia que hemos comprobado es que los hackers pueden estar en las organizaciones o continuar relacionados con ella por largos periodos sin ser detectados.

Los agresores también son conocidos por realizar ataques de distracción para ocultar los verdaderos actos delictivos, que son los realmente dañinos. Las técnicas de distracción incluyen evitar que el atacado pueda acceder al servicio, mientras que el verdadero objetivo del ataque se desarrolla de manera lenta y difícil de detectar.

Por lo general los delincuentes lanzan ataques contra los sistemas que no proporcionan ningún valor para ellos, esto se hace simplemente para desviar la respuesta a incidentes mientras que en el fondo los atacantes están infiltrando la información real que estaban buscando.

Dos tipos de ciber-crimen existentes: ¿qué significan para usted?

Hemos recorrido un largo camino desde los días de aquellos hackers que realizaban robos de tarjetas bancarias. Ha habido un aumento y sofisticación en la detección de la identidad (o de procedencia) de un atacante. Aun así, el hecho es que la competencia entre los criminales y las empresas es tan agitada como siempre, para las empresas es una batalla constante.

En los últimos años los delitos económicos cibernéticos han evolucionado hasta tal punto que se pueden segmentar en dos categorías distintas: quienes roban dinero y quebrantan la reputación, y quienes roban la propiedad intelectual y arrasan con toda la empresa:

• **Fraude cibernético:** La ciberdelincuencia como robo de ID y robo de tarjetas de pago, son los eventos que tienden a acaparar los titulares en las noticias con millones de dólares en pérdidas y la mayor cantidad de víctimas. A pesar de sus consecuencias, rara vez representan una amenaza existencial para las empresas.

• **Ciberespionaje para la obtención de propiedad intelectual y obtención de riquezas (IP)[3]:** La delincuencia económica más crítica que enfrentan las organizaciones es la de espionaje cibernético internacional, el robo de propiedad intelectual o secretos comerciales, información sobre productos o estrategias de negociación, entre otros. Los profesionales cibernéticos llaman a tales infracciones "eventos de extremo impacto[4]", y por buenas razones: los daños podrían extenderse a los miles de millones de dólares e incluyen la destrucción de una línea de negocio, una empresa o incluso un ecosistema económico más grande. Este tipo de ataques no sólo son difíciles de detectar, sino que pueden no estar en el radar de amenazas para una empresa.

¿Qué industrias corren peligro frente al delito informático?

Hoy en día todas las industrias corren el riesgo de sufrir un delito informático, incluso las menos pensadas. Acorde a la Encuesta Global de Seguridad de la Información realizada por PwC, en 2015 el sector que sufrió el mayor incremento de delitos informáticos fue el de retail[2], aunque el financiero continúa siendo uno de los más atacados.

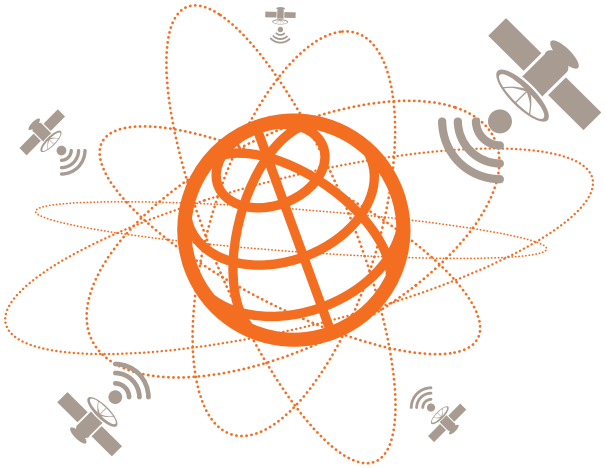
2) Retail: Minorista
3) Traducido del ingles " Transfer-of-wealth/intellectual property (IP) attacks" o en español Propiedad intelectual (PI)
4) Traducido del inglés "Extinction-level events,"

Vectores de amenaza: Las cinco categorías

Estados-Nación
La amenaza incluye espionaje y guerra cibernética.
Víctimas: el gobierno, agencias, infraestructura, energía y organizaciones con variedad de información IP.

Uso de Información privilegiada
No solo sus empleados, también terceras partes quienes tienen acceso a información confidencial y que no están directamente bajo su control.

Terroristas
Siendo relativamente una nueva amenaza, el riesgo incluye la interrupción y guerra cibernética.
Víctimas: el gobierno, agencias, infraestructura y la energía.



Crimen organizado
Las amenazas incluyen el robo de información financiera o de información e identificación personal (a veces con la complicidad de quienes usan información privilegiada).
Víctimas: instituciones financieras, minoristas y compañías médicas.

Hacktivistas*
Las amenazas incluyen interrupciones o daños en la reputación.
Víctimas: organizaciones de alto perfil y los gobiernos o cualquier tipo de organización.

* Acrónimo de hacker y activismo

Mientras que el daño a largo plazo, tanto para la entidad como para la economía, es potencialmente más alto si se trata de ataques de transferencia de riqueza, el impacto en regulación y medios de comunicación que surge del robo de tarjetas de crédito o información de identificación personal puede ser enorme.

¿Estamos preparados?

A pesar de la preocupación de las directivas por el tema, no parece haber una conexión entre las acciones efectivas y necesarias para hacerle frente. Mientras que en Latinoamérica el 45% y en Colombia el 51% de los encuestados respondió que había posibilidad de percibir un mayor riesgo, nuestro estudio encontró que las empresas aún no están lo suficientemente preparadas para hacer frente a las amenazas informáticas actuales.

Fig 10: ¿Cómo ha cambiado su percepción de los riesgos de ciber-crimen en su organización en los últimos 24 meses? (Latinoamérica)

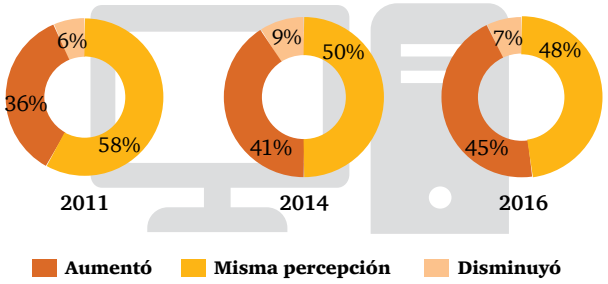
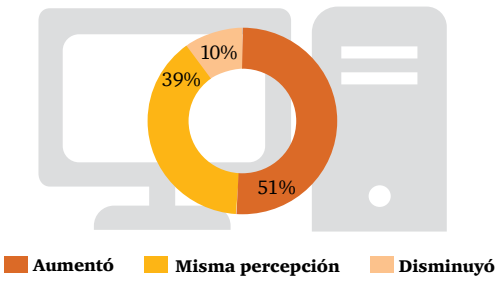


Fig 11: ¿Cómo ha cambiado su percepción de los riesgos de ciber-crimen en su organización en los últimos 24 meses? (Colombia)

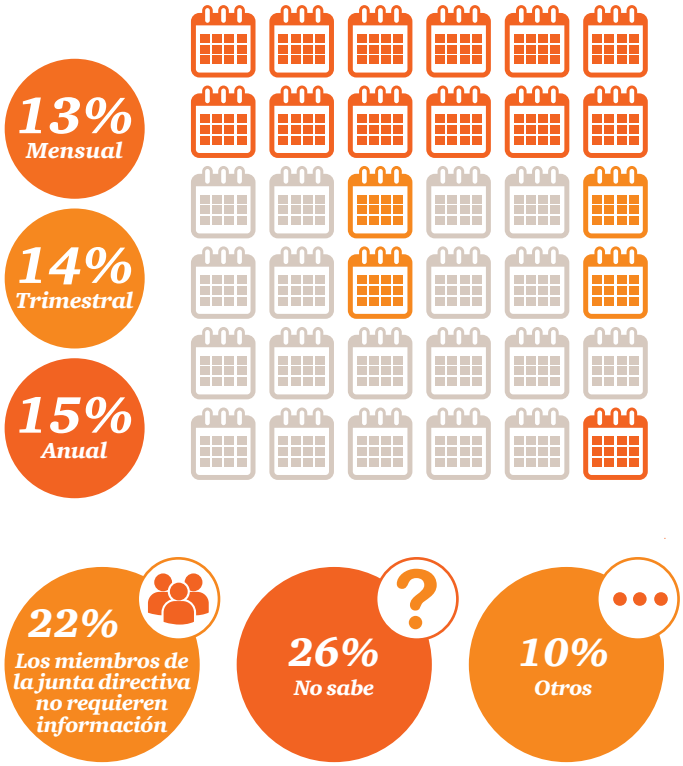


La responsabilidad de corregir las vulnerabilidades cibernéticas comienza en los cargos superiores y juntas

directivas. Sin embargo, nuestro estudio indica que muchas juntas directivas no son lo suficientemente proactivas respecto a estas amenazas, estas demuestran una ausencia general de preparación ante estos sucesos y en general no entienden el tema de la era digital en su organización lo suficientemente bien como para evaluar adecuadamente los riesgos.

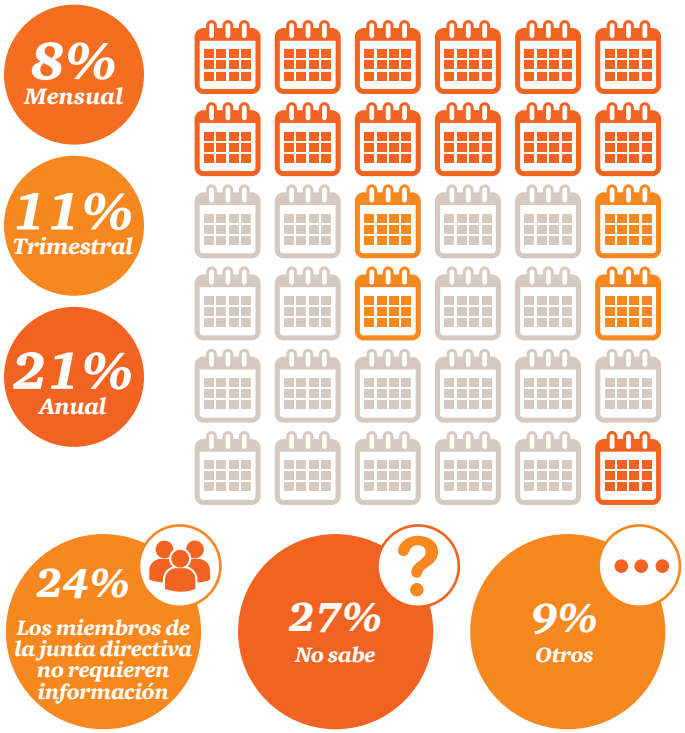
Sorprendentemente, en Colombia menos de la mitad de los miembros de juntas directivas (40%) solicitan información sobre el estado de preparación de sus empresas ante ataques cibernéticos, sólo el 32% de los encuestados tiene un programa de respuestas ante incidentes en caso de crímenes cibernéticos, y uno de cada tres no tiene ningún programa y no pretenden tener alguno, pues la mitad no creen necesitarlo.

Fig 12: Con qué frecuencia los miembros de la junta directiva solicitan información sobre el estado de preparación de la organización para afrontar crímenes cibernéticos. (Latinoamérica)



Sólo el 37% de los encuestados a nivel global, la mayoría de ellos parte de la industria de servicios financieros que es fuertemente regulada, cuenta con un plan de respuesta a incidentes. Tres de cada diez no tienen ningún plan en absoluto, y de estos casi la mitad no creen necesitar uno.

Fig 13: Con qué frecuencia los miembros de la junta directiva solicitan información sobre el estado de preparación de la organización para afrontar crímenes cibernéticos. (Colombia)



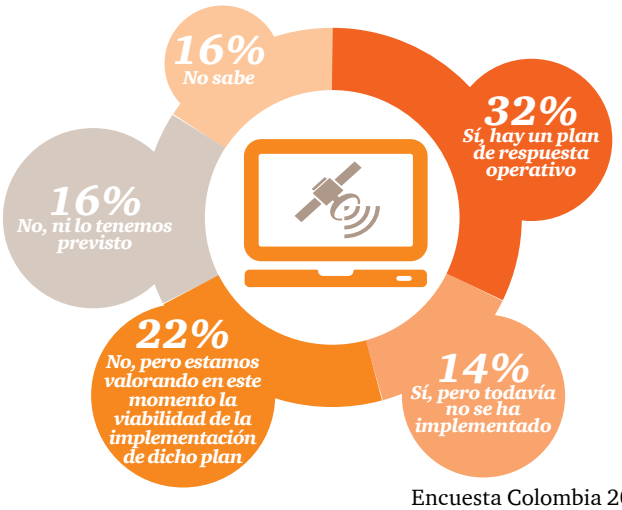
En Colombia el porcentaje de respuestas a planes para lidiar con el ciber-crimen es relativamente parecido al porcentaje a nivel global; 37% global vs 32% Colombia. Sin embargo en Colombia el 22% de los encuestados aceptan no tener planes pero sí están evaluando la posibilidad de tenerlos, contrario al 17% de opinión a nivel global.

Es importante destacar que no contar con un plan de respuesta a incidentes implica que la capacidad de contención oportuna de un evento de seguridad es poco probable y por consiguiente el impacto será mayor en la organización.

Hoy en día es necesario que las organizaciones cuenten con tecnología y personal capaz de monitorear mediante esquemas de correlación de eventos lo que sucede en sus plataformas tecnológicas. Además que puedan identificar incidentes, contenerlos y responder eficientemente, minimizando posibles pérdidas financieras por interrupción operativa, fuga de información o daños a su reputación.

Por otra parte, es necesario contar con esquemas y herramientas de ciber inteligencia que permitirán aportar un valor sin igual a los equipos de respuesta a incidentes respecto a predicciones de posibles ciber-ataques, basados en patrones o comportamientos reportados en la internet y en cualquier parte del mundo.

Fig 14: ¿Dispone su organización de un plan de respuesta ante incidentes relacionados con ciberataques?



Encuesta Colombia 2016

En caso de que ocurra una crisis cibernética, sólo un tercio de las empresas en Colombia dice tener personal plenamente capacitado para actuar inmediatamente. De estos, el 72% pertenecen al departamento de IT. En Colombia mientras IT tiene un papel fundamental que desempeñar en la detección e intento de desviar un ataque, hay que destacar que menos de la mitad de los equipos de respuesta y acciones inmediatas incluye a miembros de los más altos niveles de dirección (24%). Del departamento legal un 26% y de recursos humanos 14%. En Colombia incluso, la atención por parte de altas directivas es inferior que a nivel global, que es del 46% y la de Latinoamérica que es del 27%. En cuanto al uso de investigadores en tecnología forense en Colombia y en Latinoamérica el porcentaje es tan solo del 8%...

Fig 15: Primeros agentes que intervienen en caso de fraude o tentativa de fraude en Colombia

Datos Colombia

Estos resultados sugieren que muchas organizaciones en su afán por enmendar el impacto del incumplimiento y de asegurar un funcionamiento de sus sistemas para poder continuar operando, corren el riesgo de pasar por alto evidencias potencialmente cruciales que tarde o temprano podrían dificultar su capacidad para evaluar el impacto y entender cómo se produjo el incumplimiento. Esta podría ser una de las razones por las cuales algunos hackers permanecen vinculados en las redes sin ser detectados.

Una respuesta apresurada y sin coordinación también puede limitar la capacidad de la organización para investigar todas las áreas que han sido realmente atacadas, especialmente cuando los hackers consideran utilizar técnicas como la explicada, atacar lo que no es realmente importante.

Todo lo anterior obstaculiza la capacidad de la empresa para entender completamente el impacto del ataque y puede producir una inadecuada comunicación, tanto en actores internos como externos de la organización y/o a partes interesadas, incluidos los medios de comunicación. Esto podría conducir a un daño de reputación, clasificado en la encuesta de este año como el impacto más perjudicial de un ataque cibernético.

Por último, es importante tener en cuenta que el área de tecnología en las organizaciones tiene como principal objetivo garantizar la adecuada operación de la tecnología que apoya a sus procesos de negocio. Es especialmente preocupante que las áreas de TI estén siendo referencia para atender eventos de seguridad y que no se cuente con un área formal de Seguridad de la Información que cuente con la estructura adecuada para responder a la tendencia de ciber-ataques y nuevas vulnerabilidades. Principalmente se ha percibido en Colombia, apartando el sector financiero, estructuras básicas o inexistentes de áreas de Seguridad de la Información.

Los ciber-ataques hoy en día no están focalizados en el sector financiero, también ha habido una creciente serie de casos en el sector salud y en el sector de la educación. En estos sectores, la posesión no autorizada de información personal pasa a tener mayor impacto en las instituciones y en sus clientes que los casos relacionados con fraude de tarjetas de crédito y dinero electrónico.

Responda estas simples preguntas: ¿Qué tiene mayor impacto para usted, que le realicen una transferencia electrónica de dinero no autorizada o que se publique su historia clínica donde puedan conocer su estado de salud? ¿Qué es más grave para usted según su criterio?, ¿cuál de las situaciones puede ser compensada y cuál no?

La importancia de una defensa permanente

Las amenazas cibernéticas y cómo mitigarlas son responsabilidad de toda la empresa, todos tienen un papel crucial que desempeñar. Sin embargo, aunque hemos visto grandes avances en la preparación de respuestas a posibles ataques cibernéticos desde nuestra última encuesta global, la mayoría de las empresas todavía no están preparadas adecuadamente, ya sea para comprender los riesgos que enfrentan o para anticipar y gestionar los incidentes de manera efectiva.

Muchas organizaciones están sufriendo pérdidas cibernéticas debido a que las funciones básicas no se cumplen. Desde una participación insuficiente o falta de preparación para reaccionar a estos casos por parte de la junta directiva, hasta configuraciones incompletas del sistema y los controles inadecuados sobre aquellos terceros con acceso a la red. De esta manera las empresas sufren errores que a menudo dejan la puerta cibernética entreabierta a intrusos.

Es de vital importancia que las juntas directivas incorporen temas de ciberdelincuencia en sus evaluaciones de riesgos de rutina, que comuniquen el plan en todas las líneas de organización y que discutan específicamente con el departamento de IT en qué momento quieren ser alertados de una violación.

Las amenazas cibernéticas deben ser comprendidas y planificadas como cualquier otra amenaza potencial de negocio o interrupción de actividades (como actos de terrorismo o un desastre natural). Además deben contar con un plan de respuesta en caso de amenaza, funciones y responsabilidades claras, con seguimiento y planificación de escenarios.

Es por eso que las empresas líderes están integrando ejercicios de gestión de crisis como elemento central de su estrategia de respuesta de ciberseguridad e incidentes, además de realizar ejercicios regulares que examinan escenarios específicos de presión para sus planes de respuesta y para identificar las lagunas o deficiencias.

"La innovación tecnológica permite a las empresas mayor competitividad, sin embargo si no realizamos un adecuado análisis de riesgos en ITE, esta innovación nos deja en mayor exposición a delitos cibernéticos".

Mónica Jiménez, Socia Advisory, PwC Colombia.

Una crisis corporativa cibernética es uno de los temas más complejos y desafiantes que una organización puede enfrentar. Las infracciones cibernéticas requieren comunicaciones sofisticadas y estrategias de investigación, incluyendo capacidades analíticas y forenses que deben ejecutarse con precisión, agilidad y cabeza fría.

Aunque potencialmente desalentador, el aumento gradual de la preparación tiene su lado positivo: se puede ver como una prueba de esfuerzo de organización que puede y debe conducir a mejoras en sus procesos. En el panorama de riesgo de hoy, una empresa preparada para manejar una crisis cibernética también puede ser una ventaja competitiva e incluso su mecanismo de supervivencia.

Las amenazas informáticas y su mitigación son responsabilidad de toda la organización

Ejecutivos:

- Garantizar que la calidad de la información sea recibida y asimilada.
- Implementar programas de concientización respecto a la seguridad del usuario.
- Desarrollar una estrategia basada en seguridad.

Auditoría y Riesgo:

- Asegurar el completo entendimiento de los riesgos y amenazas informáticas.
- Llevar a cabo procedimientos de due diligence para mitigar riesgos asociados a terceros.
- Analizar riesgos asociados a los sistemas operativos (no financieros).
- Abordar cuestiones básicas de auditoría informática.

Legal:

- Conocer la evolución del marco regulatorio respecto a seguridad informática y la privacidad de los datos.
- Monitorear las decisiones tomadas por los supervisores en respuesta ante incidentes de seguridad informática.
- Estar atentos a factores que podrían afectar la seguridad informática.

IT:

- Llevar a cabo evaluaciones forenses.
- Ser conscientes de las transformaciones constantes del panorama de amenazas y ataques.
- Realizar pruebas de los planes de respuesta.
- Analizar los planes de respuesta ante incidentes.
- Implementar procesos de monitoreo efectivos.
- Emplear nuevas estrategias como simuladores de ataques informáticos, entre otros.

Contactos

Mauricio Arias
Socio de Tecnología
+57 (1) 668 4999 Ext. 206
mauricio.arias@co.pwc.com

Victor Pittol
Cybersecurity & Privacy Manager
+57 (1) 668 4999 Ext. 204
pittol.victor@co.pwc.com

Ética y Cumplimiento:

Manejar el equilibrio entre la confianza y el cumplimiento puede ser la diferencia entre mantener o perder los mejores talentos. En un mundo donde los mercados están en continua evolución, es vital contar con una estrategia donde esté alineada la ética y el cumplimiento con los riesgos del negocio.

Alineando riesgos y responsabilidades con valores y estrategia

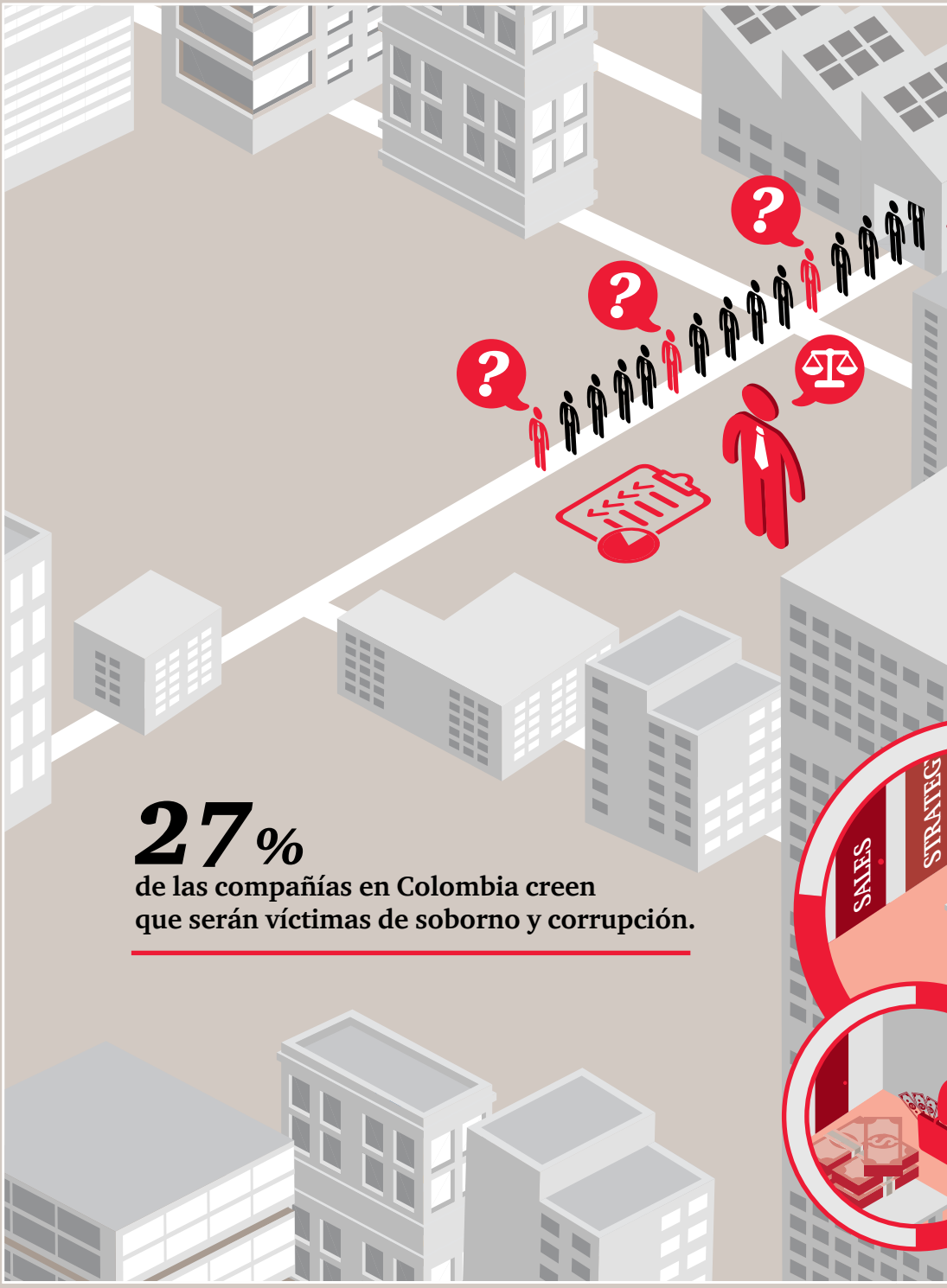
Los resultados de nuestra encuesta muestran que no sólo se trata del incremento del número de delitos económicos, sino de la complejidad de los riesgos relacionados con dichos delitos y el rol que la tecnología juega. Esto no es una sorpresa en un entorno empresarial caracterizado por la creciente globalización, el refuerzo en la vigilancia contra los delitos y el aumento en la demanda por una contabilidad pública.

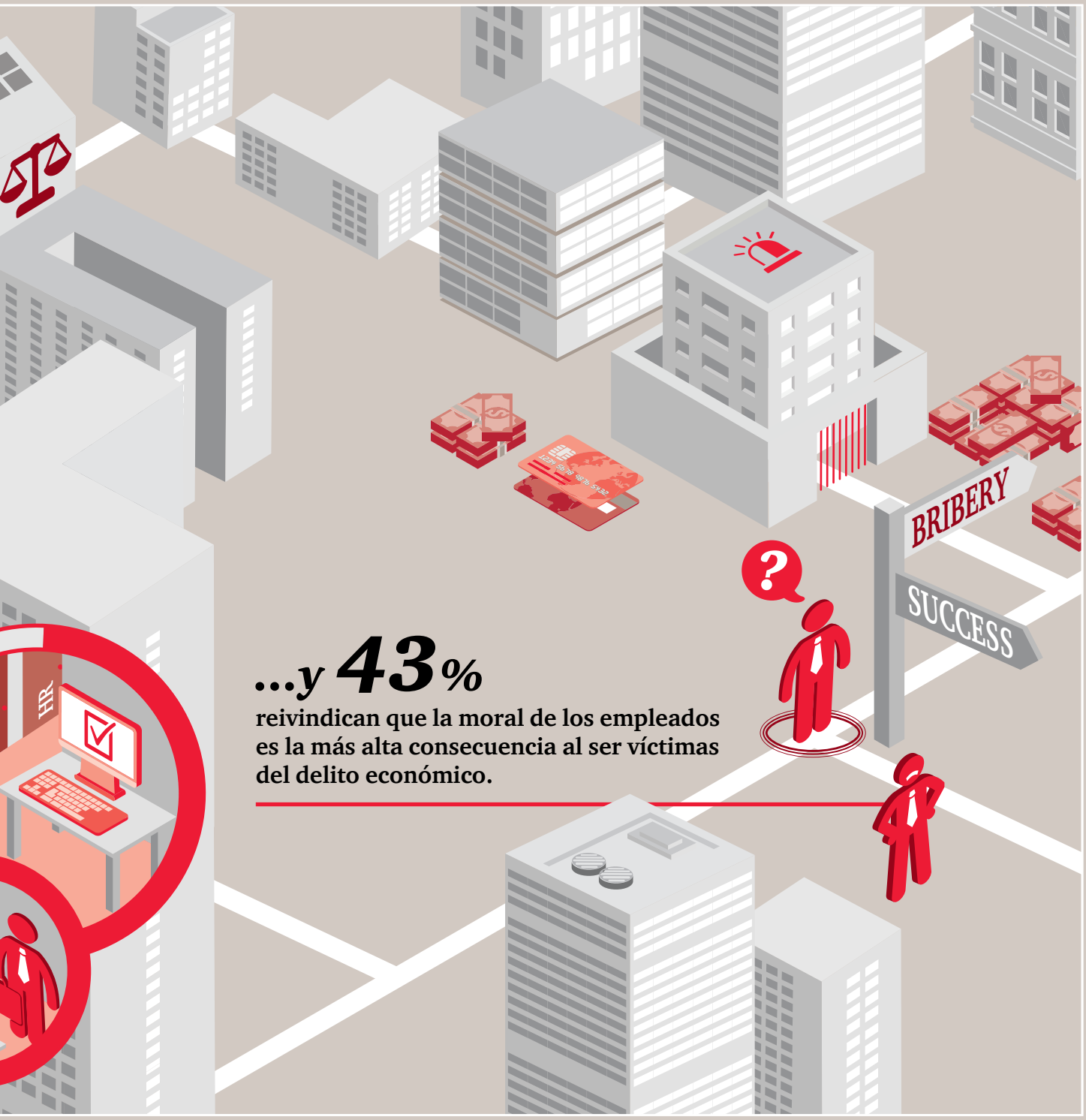
Es por eso que la capacidad de las empresas para identificar y mitigar los riesgos de cumplimiento tiene que evolucionar a un ritmo rápido. Dentro de los aspectos que se deben tener en cuenta está que el enfoque ante el riesgo, basado en la ética y el cumplimiento, comience con una comprensión de cuáles son los riesgos de fraude económico más probables en la empresa y en dónde están sus debilidades a nivel de cumplimiento. Teniendo claro ese panorama, se puede crear un sistema eficaz que mitigue esos riesgos y brinde las herramientas para alcanzar los objetivos del negocio. Sin embargo, 19% de las organizaciones en Colombia no ha llevado a cabo una evaluación de riesgos de fraude en los últimos 24 meses.

Mientras en Latinoamérica el número de encuestados que reportaron haber sufrido crímenes económicos permanece constante a través de los años (28% en 2015), en Colombia es superior (32% en 2015). Al analizar en detalle los resultados de la encuesta en cuanto a tipo de crímenes, se evidencian algunas diferencias: la mayoría de los fraudes "tradicionales" en Latinoamérica tales como la apropiación indebida de activos, fraude contable, soborno y corrupción, se mantienen o han caído en porcentaje desde 2014, mientras que en otros delitos, en particular el delito cibernético, el blanqueo de dinero y el uso de información privilegiada, hemos evidenciado el aumento en porcentaje. La disminución en algunas cifras de esta encuesta global alimenta una sensación de falta de seguridad, de ahí que exista el riesgo de que las empresas no se den cuenta del valor de invertir en programas de ética y cumplimiento.

De hecho, muchas organizaciones prefieren recortar costos en contratación o capacitación de empleados, o simplemente dar más responsabilidades a su equipo de cumplimiento existente para incluir funciones adicionales. Este puede llegar a ser un error de cálculo estratégico, pues en muchas industrias y zonas geográficas los riesgos de delincuencia económica no están disminuyendo y un pensamiento corporativo sin visión y a corto plazo puede ser peligroso. El punto es que si bien los riesgos y amenazas son siempre cambiantes, la naturaleza de un programa de cumplimiento exitoso es uno que puede prever y tratar un panorama de riesgos en evolución.

Las personas responsables quieren trabajar en compañías responsables.





...y 43%

reivindican que la moral de los empleados es la más alta consecuencia al ser víctimas del delito económico.

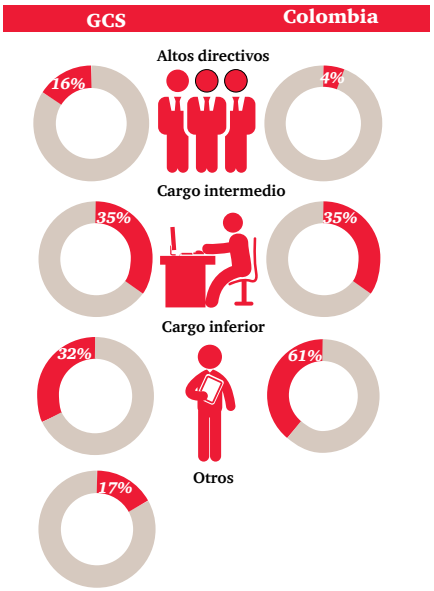
Hallazgos clave: ¿Se trata acaso de una desconexión?

Esta desconexión se puede ver con solo considerar los incidentes que se publican en medios de comunicación por los cuales las organizaciones multinacionales se ven implicadas, incluso aquellas que cuentan con programas de ética y cumplimiento. ¿Acaso estos incidentes indican que tales programas no van alineados con el cambio y los riesgos del negocio? ¿Acaso están enviando mensajes contradictorios? ¿Hay una razón más profunda que explique esta desconexión?

Los resultados apuntan a una brecha entre la percepción de lo que los directores ejecutivos de las empresas y la junta directiva dicen y lo que realmente está sucediendo en el negocio, en particular entre los de nivel alto y medio. Según nuestra encuesta a nivel global, los mandos medios siguen siendo los más propensos a cometer fraude, siendo vulnerables a sentir que los valores dentro de sus empresas no son claros y a creer que los programas de incentivos no son justos. En Colombia los más propensos a cometer fraude, a diferencia de las cifras globales, son las personas en el cargo de "junior management" (cargos gerenciales principiantes).

La 19ª Encuesta Global Anual de CEOs de PwC corrobora las brechas entre la intención y la ejecución. Las principales amenazas que enfrentan las organizaciones, según la respuesta de los directivos, son el soborno y la corrupción, factores que pasaron de 51% a 56%. La falta de confianza en los negocios fue a su vez otra amenaza reportada, lo que subraya la importancia de tener un programa sofisticado y creíble de ética corporativa.

Fig 16: Considerando el delito económico más grave que ha sufrido su organización en términos de pérdida monetaria en los últimos 24 meses ¿Qué cargo se perfilaría como el principal defraudador?



Asegurar que se cumplan los programas de cumplimiento

¿Cómo las empresas pueden asegurar que los programas de cumplimiento se pongan en práctica? ¿Cómo se incentiva al cumplimiento? ¿Cómo se mide? A continuación se presentan cuatro áreas clave de enfoque para la mejora de la eficacia de los programas de ética y cumplimiento.

- Las personas y la cultura: El mantenimiento de un programa basado en valores, medición y premiación o incentivos a quienes lo cumplen.
- Funciones y responsabilidades: Asegurarse de que sean claras, correctas y que estén alineadas con los riesgos actuales.
- Las áreas de alto riesgo: Mejorar la aplicación, la auditoría o testeo al programa de cumplimiento en los mercados de alto riesgo.
- Tecnología: Mejor uso de herramientas de detección, prevención y análisis de datos.

Cinco pasos para contar con un programa de cumplimiento más efectivo

1. Asegúrese de que el programa este en línea con la estrategia corporativa y comuníquelo.
2. Evalúe y replantee su función como oficial de cumplimiento y sea consciente del proceso de adaptación constante en un entorno donde el riesgo y las amenazas cambian.
3. Asegúrese de que todos los dueños de los procesos entiendan el programa de cumplimiento a nivel macro y en detalle y la importancia de que debe ser aplicado en toda la organización. Asimile y comunique el alcance de sus propias responsabilidades.
4. Recuerde que las políticas y las capacitaciones en temas de valores no son suficientes: el compromiso creíble y coherente en toda la organización es esencial.
5. No pretenda querer reducir el tamaño de los riesgos cuando por el contrario están aumentando.

Las personas y la cultura: Su primer mecanismo de defensa

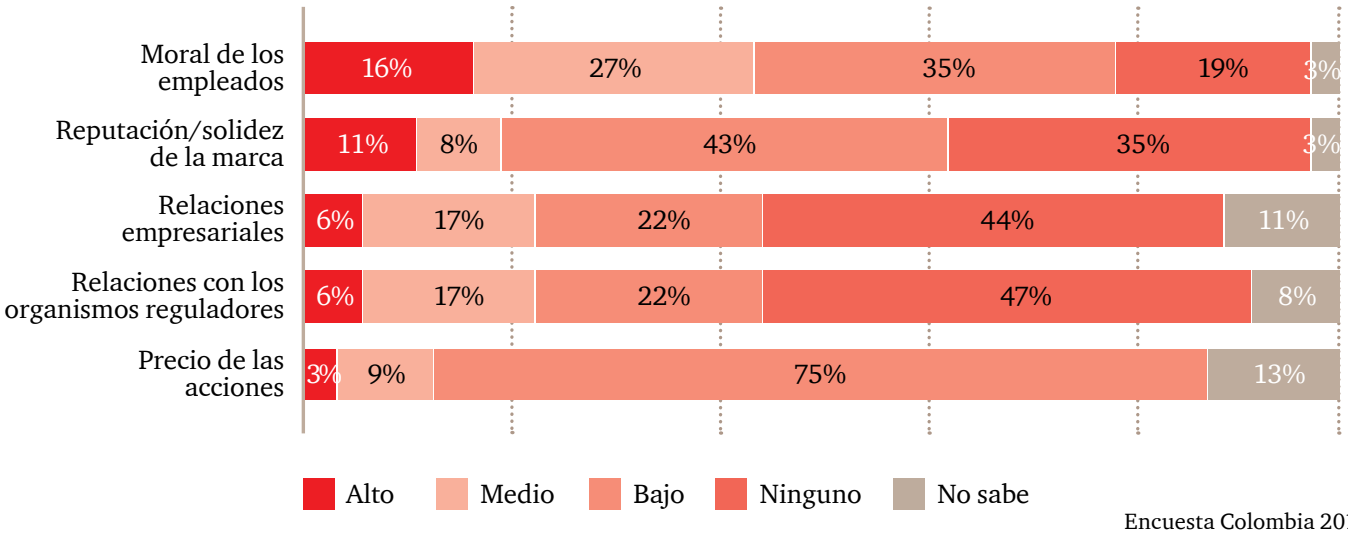
El delito económico es siempre una mala decisión impulsada por el comportamiento humano, por lo tanto es lógico pensar que el comportamiento de la gente es la solución al problema. Esto significa que el tema no es tan sólo inculcar principios y procesos claros para los empleados, sino también crear una cultura donde el cumplimiento está atado a los valores y a la estrategia general de la organización.

Nuestros entrevistados afirman que el mayor daño organizacional que han experimentado como resultado de la delincuencia económica no se ve reflejado principalmente en el precio de sus acciones ni en las relaciones con los reguladores. En Colombia se refleja en mayor proporción en la moral de los empleados con un 43% (medio y alto impacto) y en la reputación con un 19%. Esto pone en consideración la importancia de los valores claros en una estrategia de negocios exitosa.

"Una investigación reciente de PwC y London School of Business en el tema de fomento de ética en el sector de servicios financieros, muestra que un enfoque de "mano dura" por parte de la dirección en temas de rendimiento genera un ambiente de miedo, que a su vez conduce a conductas poco éticas.
El estudio encontró que la ansiedad provocada por la "cultura de exigencias a nivel de rendimiento" reduce la capacidad de las personas de tomar buenas decisiones y a menudo las lleva a tener un mal comportamiento."

Publicación: "Stand out for the right reasons"
PwC and London Business School research, June 2015.

Fig 17: ¿Qué impacto ha tenido el delito económico que ha sufrido su organización en los últimos 24 meses en cada uno de los siguientes aspectos?



Encuesta Colombia 2016

Un programa de cumplimiento basado en valores es algo más que pretender tener equipos fuertes. Se trata también de atraer a los mejores y a los más brillantes de su organización. Las personas responsables quieren trabajar para empresas responsables y son quienes ponen en práctica sus creencias y las predican dando ejemplo.

Un programa de cumplimiento bien diseñado y apoyado por un enfoque de comportamientos éticos puede ofrecer un beneficio claro para la estrategia del negocio.

Para ser eficaz, en su programa de cumplimiento debe existir un código de conducta actualizado, una política y un entrenamiento. Fundamentalmente debe haber coherencia entre los valores, el comportamiento y la toma de decisiones.

En lugar de atacar uno a uno los incidentes, el enfoque debe ser hacia las capacitaciones de las personas que integran la compañía explicando con argumentos cómo y por qué se deben tomar las decisiones correctas en algunas circunstancias.

Brechas de percepción:

Un tema persistente en nuestros resultados de la encuesta es el de las brechas o lagunas en cuanto a la percepción, que puede conducir a resultados no deseados.

Estas pueden dividirse en 3 categorías básicas:

- La brecha entre lo que la junta directiva cree y promueve, y lo que la gente dentro de la organización ve realmente y realiza día a día.
- La brecha entre las intenciones y el hecho de cumplir con ellas.
- La brecha entre la alta y media dirección en cuanto a supervisar el cumplimiento.

La necesidad de este enfoque se basa en los resultados de la encuesta global en donde la alta dirección estuvo involucrada en los fraudes económicos (como Asia Pacífico, América del Norte y Europa Occidental). En estos casos, uno de sus incentivos más grandes fue la presión para lograr metas.

Entienda y mida las brechas existentes

Casi todos los encuestados, tanto a nivel global como en Colombia, coincidieron en que su organización contiene valores organizacionales claramente establecidos y bien entendidos (86%), respuesta en particular de los directores ejecutivos y directores financieros. Sin embargo, nuestra encuesta global identificó áreas en donde el gerente senior y los directivos no percibían lo mismo que los mandos medios. Esto se refleja en los resultados; mientras el 90% de los directores ejecutivos creen que los valores son claros y comprendidos, el porcentaje se reduce a 84% a nivel de gerentes.

En nuestra experiencia, la brecha entre lo que dicen y piensan los líderes de alto rango y los mandos medios es muy significativa. Este hecho puede crear un vacío que, aún con las mejores intenciones, puede convertirse en comportamientos poco éticos.

Fig 18: ¿En qué grado está de acuerdo o no con las siguientes afirmaciones sobre su organización en cuanto a su ética empresarial y cumplimiento normativo?

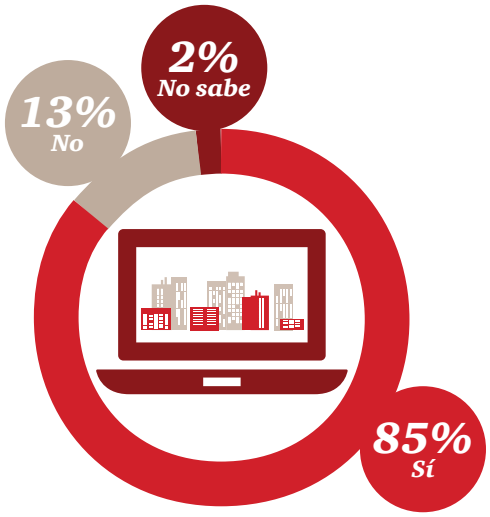
Encuesta Global 2016

Alineando roles con responsabilidades: ¿Quién está a cargo?

Nuestra encuesta reveló que un número significativo de empresas no tiene una estructura de cumplimiento formal. En algunos casos esto puede suceder por el tamaño reducido de las empresas. El 15% de los encuestados en Colombia dijo que no conocía un programa formal de ética y cumplimiento en su empresa.

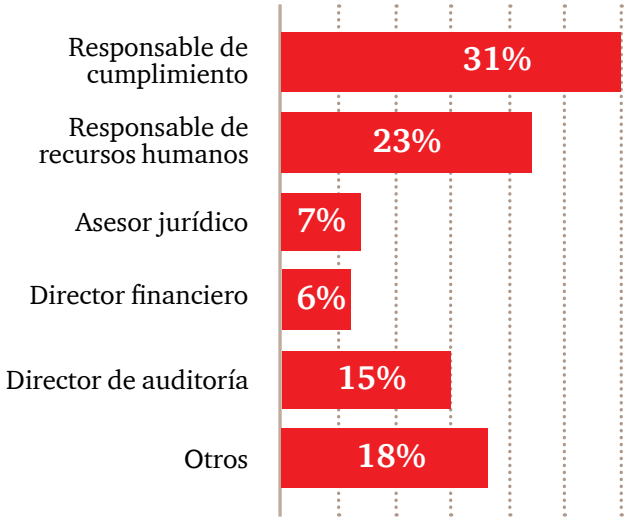
En Colombia podemos analizar que el 85% de las organizaciones que dice tener un programa oficial de ética empresarial y programa de cumplimiento, realmente no tiene muy clara la responsabilidad de verificar que los programas sí se lleven a cabo.

Fig 19: ¿Cuenta su organización con un programa formal de ética empresarial y cumplimiento normativo?



Encuesta Colombia 2016

Fig 20: ¿Quién es responsable del programa de ética empresarial y cumplimiento normativo en su organización?



Encuesta Colombia 2016

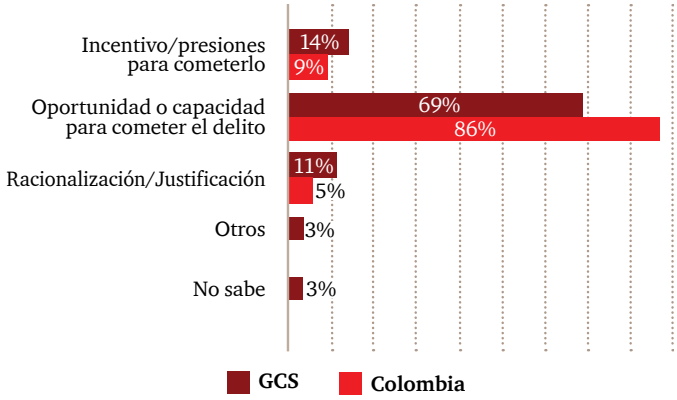
¿Quién es el responsable? Adoptando enfoques de riesgo

Es importante que todas las personas del negocio, no sólo los profesionales de cumplimiento, comprendan sus roles, funciones y responsabilidades para así asegurar que el negocio está alineado con los programas de ética y cumplimiento. Aun así, muchas empresas presentan un grado de confusión acerca de quién tiene la responsabilidad o quién es el dueño de los procesos.

¿De quién es la responsabilidad de entender los riesgos y determinar el riesgo? Las funciones de los encargados de cumplimiento son la supervisión y orientación. Sin embargo, en algunas organizaciones hay una tendencia a considerar el cumplimiento como una especie de póliza de seguro.

En Colombia los actores internos son quienes principalmente cometen actos de fraude económico. La principal causa es la oportunidad o habilidad para cometer el crimen. El porcentaje en Latinoamérica y en Colombia es mayor que a nivel global, 72% y 86% respectivamente contra 69%.

Fig 21: ¿Qué factor cree que ha contribuido a que los delitos económicos sean realizados por los agentes internos?



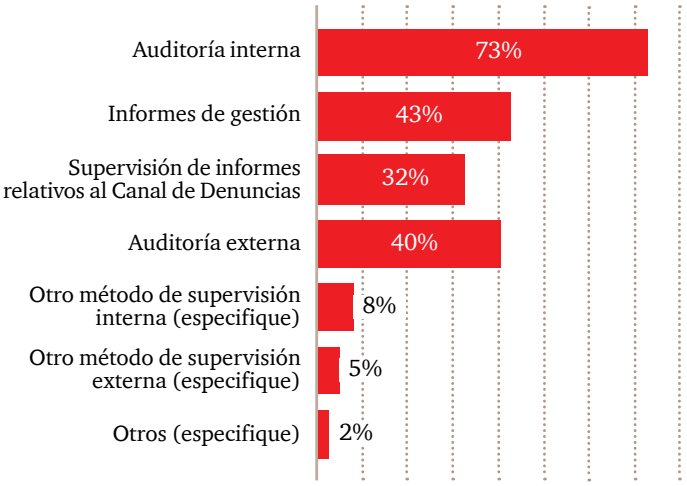
Encuesta Global Vs Colombia

En resumen, todos los miembros de la empresa deben trabajar bajo las mismas reglas en cuanto al cumplimiento. Las organizaciones con visión futurista se posicionan y se identifican como una "comunidad de cumplimiento" en donde la ética y el cumplimiento se convierten en el factor central de las funciones y responsabilidades del negocio.

La oportunidad (para el crimen) golpea la puerta. ¿Alguien está escuchando?

Los tres elementos que conforman el triángulo del fraude son: oportunidad, racionalización/justificación y presión para llevar a cabo el crimen. En Colombia, de quienes indicaron haber sufrido delitos económicos a causa de actores internos en la organización, el 86% consideran que la oportunidad es el factor principal de ocurrencia.

Fig 22: ¿Cómo se asegura su organización de que el programa de ética empresarial y cumplimiento normativo es eficaz?



Encuesta Colombia 2016

Se considera que la detección del fraude* es más fuerte en Colombia que a nivel global, en términos de denuncias por medio de hotlines "whistleblowing hotline", con un porcentaje de 11% en Colombia contra 5% a nivel Global.

* percepción de fraude en términos de pérdidas financieras.

¿Cuál es la mejor opción para prevenir la delincuencia económica? Una gran mayoría opina que se deben favorecer entornos de control más fuertes. En Colombia el 73% de los encuestados cree que quien garantiza la eficacia de sus programas de cumplimiento es el departamento de auditoría interna.

Aunque la auditoría interna es una pieza importante para la eficacia de un programa de cumplimiento, no significa que sea suficiente para asegurarlo. Por otra parte, el perfil de riesgo de fraude ha cambiado (por ejemplo hubo aumento de nuevos fraudes, como la delincuencia cibernética), y la incidencia de algunos tipos de fraude está aumentando o persiste en algunas organizaciones.

Por ejemplo, en las organizaciones con más de 1.000 empleados a nivel global siguen siendo más probables los fraudes en compras, soborno o corrupción (5% y 2% respectivamente superior al promedio global), mientras que los esquemas de fraude parecen encontrar una manera de sobrepasar los controles establecidos.

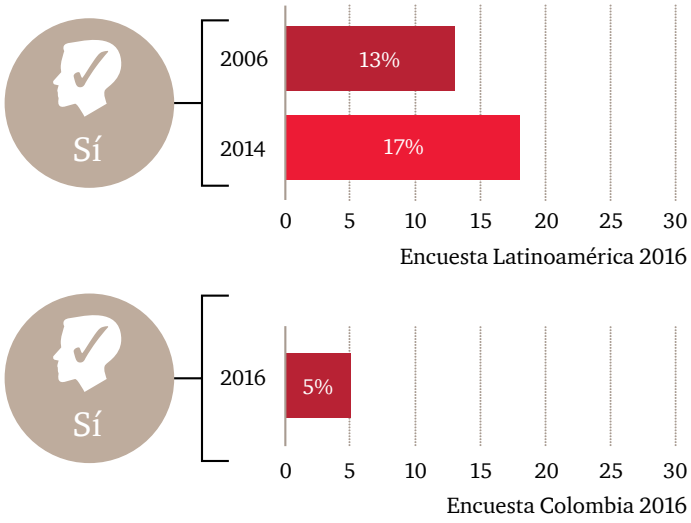
Dado a que la prevención debe tener un lugar ideal en la toma de decisiones, los mecanismos realizados por auditoría interna deben estar integrados con los informes de gestión de las directivas y un monitoreo en tiempo real de las operaciones del negocio, para que los temas sean detectados y prevenidos a tiempo. Nuestros encuestados del sector financiero a nivel global, en particular sobre los informes de gestión, los consideran clave para garantizar la efectividad de los programas de cumplimiento, con un 60% que corroboran el uso de ellos.

En Colombia, el 43% de los encuestados considera que los informes de gestión son clave para garantizar la efectividad de los programas de cumplimiento y al igual que en la encuesta global, el 8% de los encuestados dice estar utilizando otros tipos de monitoreo interno más prometedores que los enfoques de supervisión interna tales como el análisis predictivo o análisis de datos, que son más difíciles de ser atacados.

Implementando en áreas de alto riesgo: El truco está en los detalles

Inculcar el comportamiento ético dentro de una organización global exige una comunicación consistente y la presentación de informes de gestión. Adicionalmente se debe considerar que los países y sus respectivas divisiones de riesgo no son las mismas, de ahí la importancia de crear un programa de cumplimiento global adaptado a la realidad de cada territorio.

Fig 23: Porcentaje de organizaciones que han recibido una petición de pago de soborno



Se debe asumir la existencia del riesgo transnacional de soborno y corrupción. Los reguladores están cada vez más dispuestos a crear conciencia sobre la responsabilidad de alejar el comportamiento poco ético de las organizaciones, para asegurarse de que todas sus personas están haciendo lo correcto todo el tiempo.

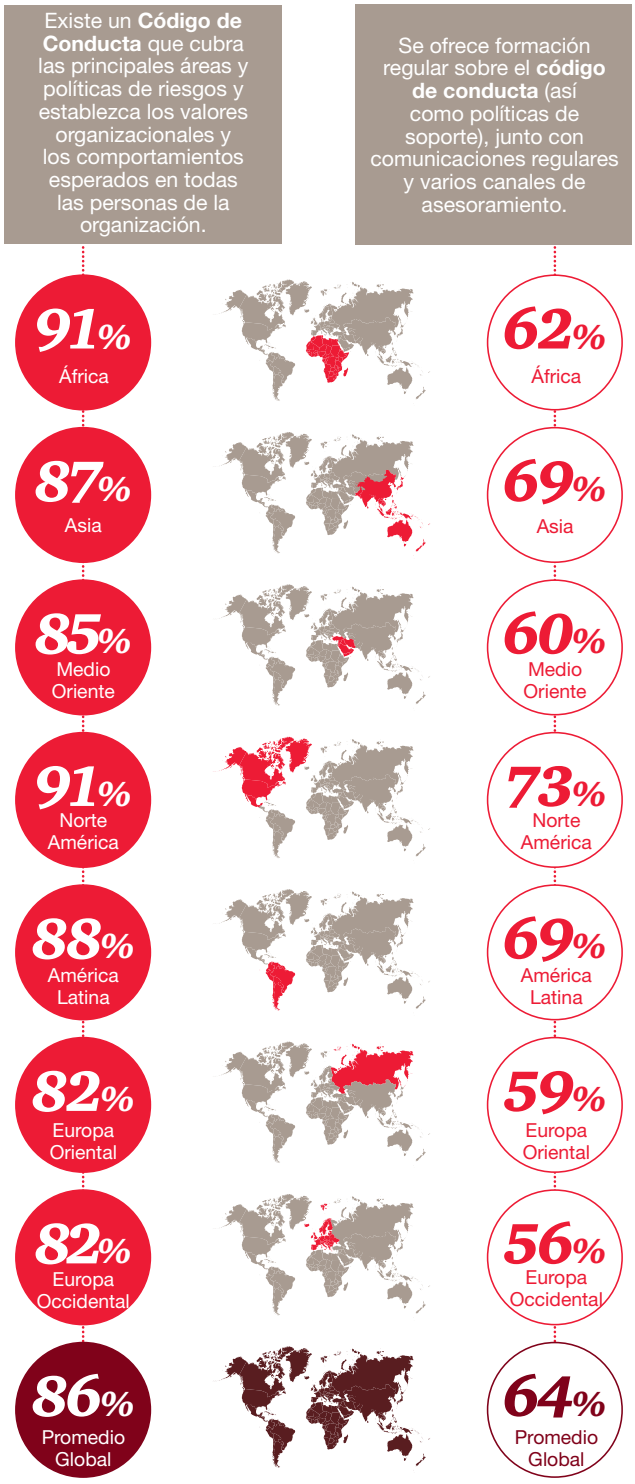
¿Cómo responden las organizaciones a este riesgo? Tener un código de conducta es un punto de partida, sin embargo los empleados muchas veces no saben cómo utilizarlo en su día a día para la toma de decisiones, lo cual genera debilidades para mitigar el riesgo de cumplimiento. El código de conducta y las políticas empresariales necesitan ser divulgadas a través de capacitaciones y comunicaciones realizadas periódicamente, donde se recompense y se reconozca la toma de buenas decisiones y se genere conciencia respecto a los procedimientos disciplinarios contra quienes toman malas decisiones.

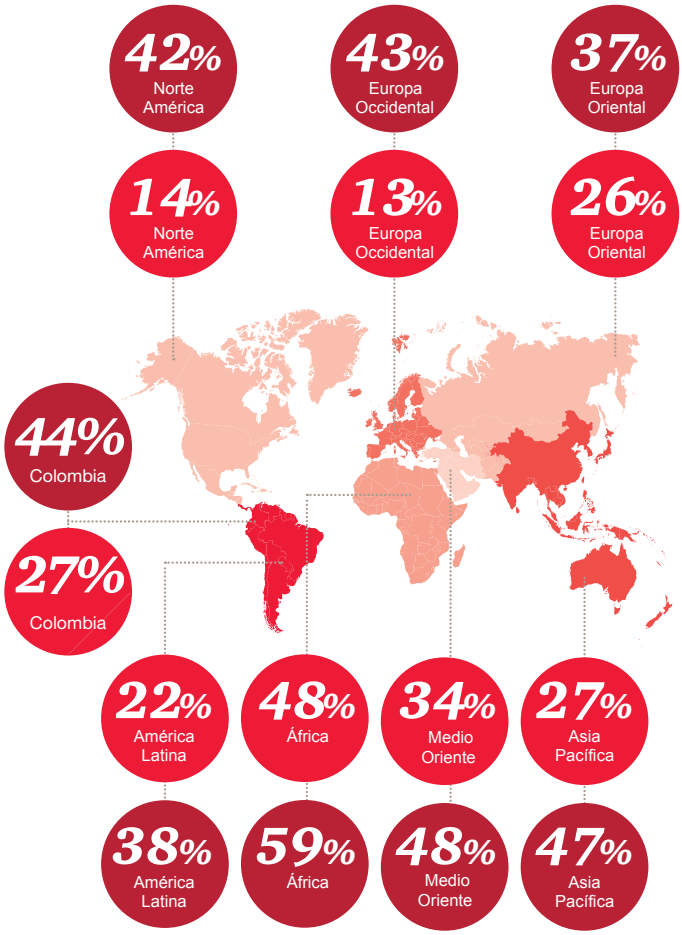
Aunque el 86% de las organizaciones a nivel mundial declaran que su organización cuenta con un código de conducta vigente, sólo el 64% afirma que proporcionó entrenamiento o capacitaciones periódicas y asesoramiento regular sobre el mismo. La discrepancia fue particularmente aguda para los encuestados de África, Europa Occidental, Oriente Medio y Europa del Este.

En general, el 91% de los encuestados a nivel global de la alta dirección declararon que el soborno no es una práctica legítima. Estos resultados fueron consistentes a través de todas las regiones y todos los sectores. Sin embargo, aún se identifican un gran número de incidentes reportados en muchas zonas a nivel global, incluso cada vez hay un mayor número de organizaciones que esperan experimentar casos de soborno y corrupción durante los próximos 24 meses.

Las regiones que creen que es más probable experimentar el soborno y la corrupción en los próximos 24 meses son África, Medio Oriente y Asia Pacífico. Asimismo, son estas las regiones que dicen que van a invertir en programas de cumplimiento en los próximos 24 meses (59%, 48% y 47%, respectivamente). Sin embargo, invertir no siempre soluciona los problemas. Las organizaciones necesitan asegurarse de que están utilizando las herramientas, tecnologías y técnicas adecuadas para obtener el retorno de la inversión en temas de cumplimiento.

Fig 24: Capacitaciones y código de conducta





- Encuestados que creen que en los próximos 24 meses existe probabilidad de que su organización sufra como delito económico el soborno y/o la corrupción.
- Encuestados que planean incrementar la inversión en sus programas de cumplimiento en los próximos 24 meses.

El 91% de los encuestados opina que la alta dirección en sus empresas es clara en expresar que el soborno es una práctica ilegítima.

Esta cifra se repite en todas las regiones y sectores, sin embargo se evidencia un gran número de incidentes reportados. Además, en varias regiones y organizaciones, se espera experimentar soborno y corrupción en los próximos 24 meses.

Encuesta Global 2016

La tecnología: No es la cura pero sí una fuerte medicina

Hoy en día existen varias herramientas sofisticadas, incluyendo el *Big Data Analytics* o Análisis de Datos Masivos, capaces de proporcionar un monitoreo mayor y más eficiente de las operaciones, lo cual puede ayudar a un cumplimiento más efectivo de las mismas usando una gran variedad de datos, algunos estructurados y otros no.

Sin embargo, a excepción de los sistemas de monitoreo de transacciones, los cuales son principalmente utilizados por los clientes del sector financiero, muy pocas organizaciones están utilizando estos tipos de tecnología para ayudar a detectar y prevenir los delitos económicos. Actualmente sólo el 8% de los encuestados a nivel global dice utilizar otro tipo de enfoque en control interno como el análisis de datos.

Pero cuidado, las organizaciones pueden cometer errores relacionados con la tecnología y pueden verse impulsados a desconectar los procesos de evaluación de riesgos. Algunos recurren al exceso de monitoreo en distintos aspectos, descuidan la atención a otras áreas y sin saberlo duplican sus gastos en diferentes herramientas. Otros siguen un enfoque de cumplimiento con requisitos ineficientes y no utilizan los datos correctos, provocando el abandono de análisis de datos antes de demostrar su validez.

Hemos observado que la mejor manera para empezar no es el monitoreo de la Big Data, el objetivo es enfocarse en el detalle de los datos de la evaluación de riesgos y contar con información consistente y comparable, actividades que suenan sencillas pero no lo son.

El modelo óptimo abarca cómo mitigar los riesgos a los que se enfrenta la organización y cómo presentar informes por unidad de negocio, por geografía o terceros. Para lograr esto se necesitan tres aspectos:

- Un método coherente para la definición de riesgos
- Transparencia en la medición de riesgo
- Una plataforma de datos común

Contactos

Monica Jiménez
Socia de Advisory
+57 (1) 634 05 55 Ext. 10202
monica.jimenez@co.pwc.com

Jorge Ropero
Gerente Forense
+57 (1) 634 05 55 Ext. 10438
jorge.ropero@co.pwc.com

Estos requisitos combinados con un gobierno centralizado y un modelo operativo, pueden ayudarle a comenzar a evaluar qué tan efectivas son sus transacciones de monitoreo actuales y a centrarse en las verdaderas amenazas para su empresa. En conclusión, el enfoque no debe centrarse en la tecnología como tal, sino más bien en los alcances que esta nos permite. Los datos por sí solos nunca serán una solución, pero utilizados eficazmente puede ofrecer a las compañías la clave para enfrentar sus riesgos de cumplimiento.

Control de lavado de activos:

¿Cómo responder al entorno regulatorio que cambia rápidamente?

El lavado de dinero destruye valor, facilita la delincuencia económica y las actividades ilícitas como la corrupción, el terrorismo, la evasión de impuestos, el tráfico de drogas y la trata de personas. Facilita la transferencia de fondos necesarios para cometer los delitos anteriormente nombrados que resulta perjudicial para la reputación de una organización.

Se estima que entre el 2 y el 5% del PIB mundial es lavado de dinero a través de transacciones ilícitas en el mundo, lo que representa aproximadamente $1-2 billones de dólares. Sin embargo, según la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDC), menos del 1% de los flujos financieros ilícitos son incautados por las autoridades.[5]

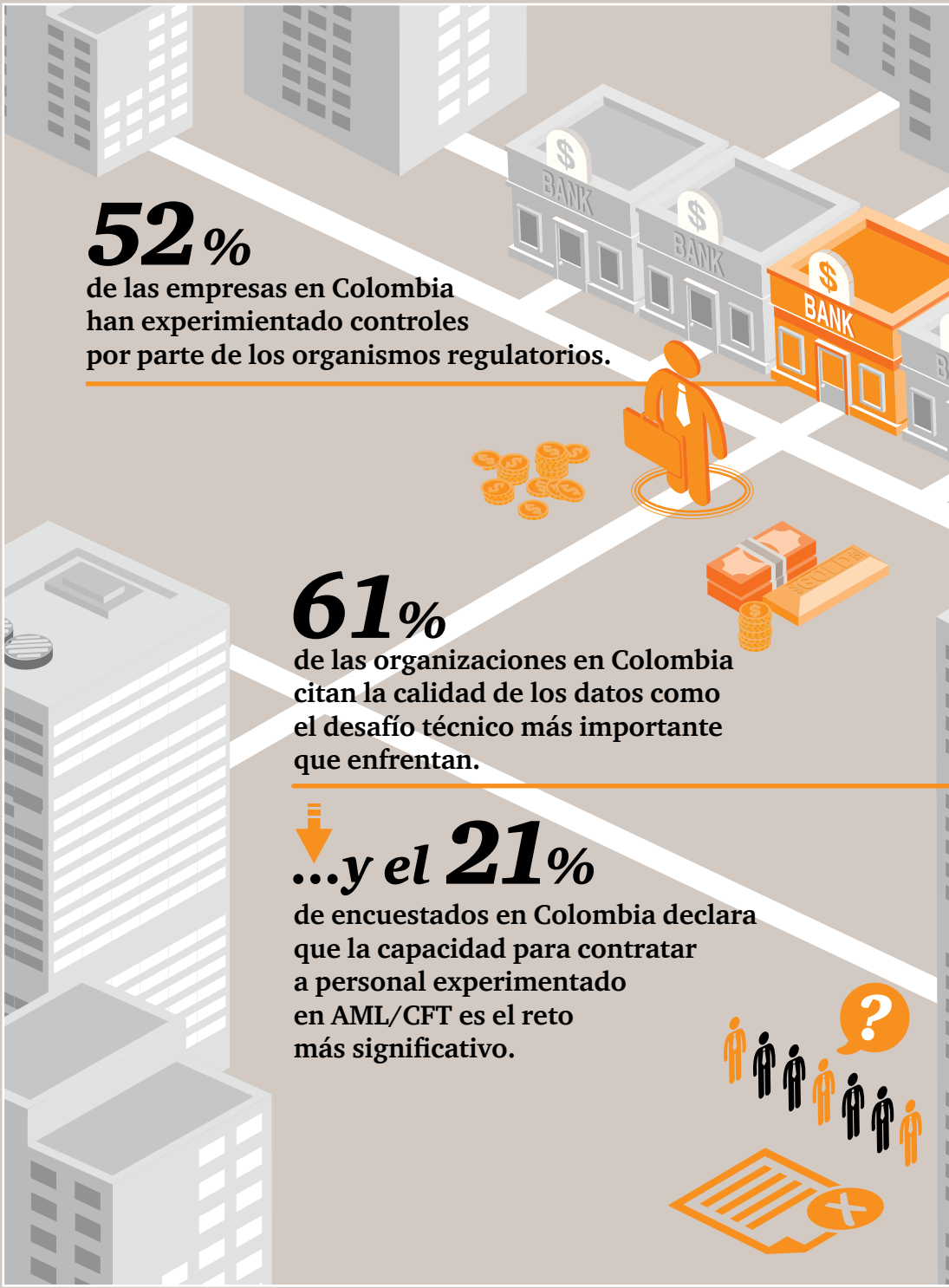
Con el aumento de ataques terroristas, lavado de dinero y financiación del terrorismo, el interés de los gobiernos a nivel mundial en cuanto a estos temas aumenta. En los últimos años, sólo en los EE.UU, casi una docena de instituciones financieras han recibido altas multas y sanciones por este tipo de violaciones. Hay fuertes indicios de que varios países aplicarán igualmente regulaciones sustantivas y de observación como lo ha realizado EE.UU

El foco de atención por parte de las autoridades no es sólo a los servicios prestados por instituciones financieras. Cualquier organización que facilite las transacciones financieras, incluyendo instituciones que permitan servicios monetarios no bancarios como el pago de servicios por medios digitales / móvil, seguros de vida, etc., están del mismo modo bajo la lupa de los organismos de vigilancia y prevención de lavado de dinero (AML). Es alarmante pero no sorprendente que muchos de estos nuevos participantes parecen aún no estar al tanto de los requisitos que deben cumplir o de los programas de cumplimiento que necesitarían.

Como las regulaciones a nivel mundial profundizan cada vez más en complejidad y alcance, el costo del cumplimiento continúa en crecimiento. Según nuevas cifras de WealthInsight, el gasto global en cumplimento de AML espera aumentar a más de $8 billones en 2017[6] (una tasa de crecimiento anual compuesta de casi 9%). Muchos se resisten al gasto a pesar de los costos y sanciones.

5) Tomado de "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes" por la oficina de Naciones Unidas contra las drogas y el crimen © 2011 Naciones Unidas. Reimpreso con el permiso de Naciones Unidas.
6) Estadísticas facilitadas por WealthInsight

El aumento de estándares regulatorios conlleva un incremento en las acciones legales.



¿Cómo su organización confronta el control de los organismos reguladores?

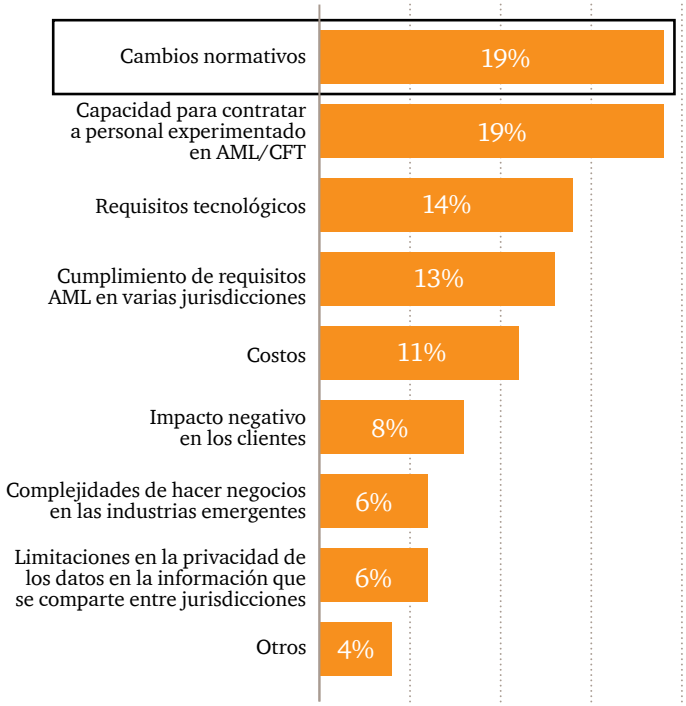
AML ENTES DE VIGILANCIA Y REGULADORES

- **Circular Externa 100-000005** expedida por la Superintendencia de Sociedades, y cuyo objetivo principal es la implementación de un sistema de autocontrol y gestión del riesgo del lavado de activos (LA) y financiación del terrorismo (FT): organismo cuya misión actual es promover políticas para luchar contra el lavado de dinero y la financiación del terrorismo monitoreando temas de LA y tendencias FT y estableciendo normas internacionales. El GAFI estableció " Cuarenta Recomendaciones " - un estándar mínimo global de un sistema de prevención de lavado de dinero efectivo, adoptado en la actualidad por 34 países miembros como parte de su normativa sobre blanqueo de dinero y legislación.
- **Consejo de Seguridad de las Naciones Unidas**, adopta resoluciones que incluyen listas de personas contra quienes han sido impuestas sanciones, tales como organizaciones terroristas. Estas listas son utilizadas por los gobiernos para apoyar medidas en contra de la actividad terrorista.
- **The Office of Foreign Assets Control (OFAC)**, entidad dependiente del Departamento del Tesoro de EE.UU que mantiene y administra una serie de sanciones económicas de Estados Unidos y de embargos.

Hallazgos clave: Regulación basada en la examinación

El aumento de las normas reguladoras incrementa la acción legal

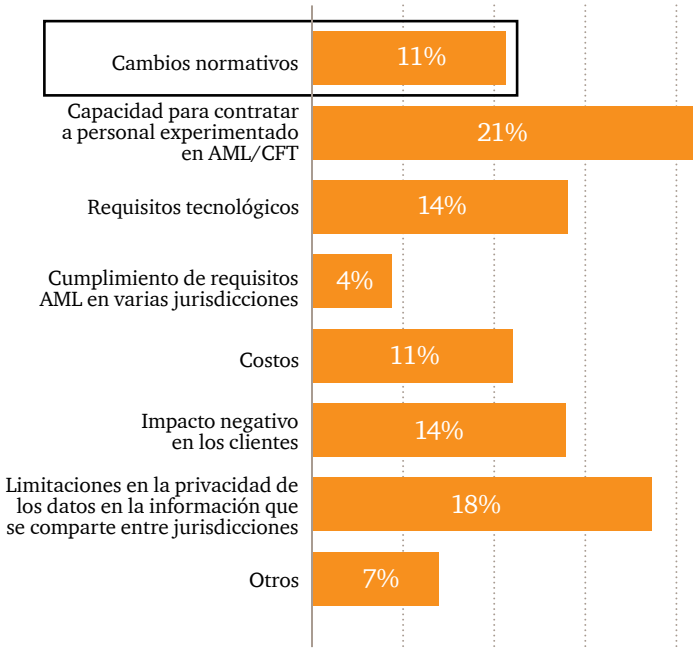
Fig 25: Retos más significativos en relación al cumplimiento de requisitos AML/CFT



Encuesta Global 2016

Nuestra encuesta muestra que el nivel de esfuerzos para cumplir la normatividad en cuanto al lavado de dinero y la lucha contra la financiación del terrorismo (CFT), son medidas que han creado desafíos tanto para las instituciones financieras como para otras industrias, incluso creando programas de cumplimiento AML más sofisticados y robustos.

Fig 26: Retos más significativos en relación al cumplimiento de requisitos AML/CFT



Encuesta Colombia 2016

Algunos gobiernos han impuesto multas y en algunos casos han iniciado acciones penales en contra de las instituciones financieras por no haber implementado suficientes controles para monitorear sus operaciones globales.

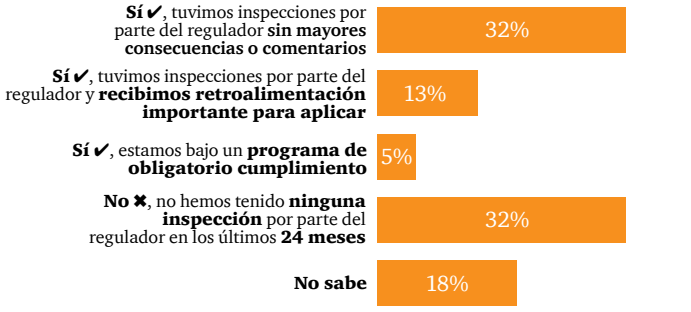
¿Implementación desigual?

Mientras que la mayoría de los Estados-Naciones cuentan con algún mecanismo para inspecciones del control de lavado de activos (AML), el grado de rigurosidad de estas varía sustancialmente.

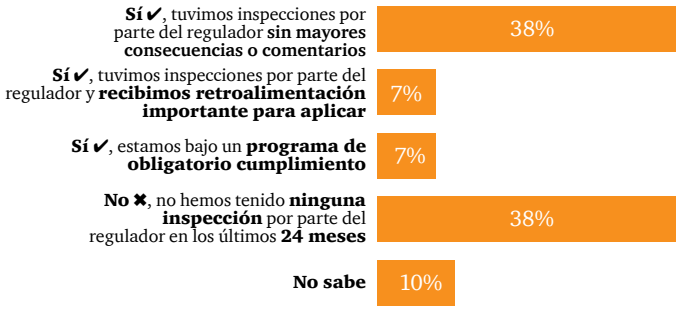
Estados Unidos y unos pocos países desarrollados cuentan con personal encargado de examinar todo lo relacionado con control de lavado de activos y sus posibles sanciones. Sin embargo, muchos países recurren al uso del personal encargado de las evaluaciones de cumplimiento o análisis de riesgo de la compañía y no especialistas, efectuando inspecciones con menos frecuencia.

Algunas instituciones financieras se han convertido en foco de atención de las entidades reguladoras en sus países debido a las prácticas comerciales ilícitas que realizan y con frecuencia se presentan confusiones respecto a donde una compañía puede operar legítimamente si está bajo sanciones en cualquier otro lugar.

Fig 27: Medidas regulatorias



Encuesta Global 2016



Encuesta Colombia 2016

Otro desafío para las organizaciones que luchan por cumplir las normas globales de LA/ FT es que las expectativas de regulación están reemplazando cada vez más los requisitos legales concretos. Esto es más frecuente en las áreas con procesos donde se exige una debida diligencia del cliente y en donde el monitoreo de transacciones es más constante.

Los reguladores al examinar aplican estándares basados en las prácticas de otra institución. Esta llamada "regulation by examination " (regulación basada en la examinación) desafía el enfoque de riesgo que aplican las organizaciones al creer conocer y dominar el riesgo.

GAFI: Un nuevo enfoque en la eficacia

GAFI ha cambiado su estándar de evaluación de las normas ALD / CFT* en donde el enfoque se basa más en la eficacia que en la técnica y donde se miden todas las organizaciones por criterios similares.

Este nuevo enfoque debería conducir a algunos países en desarrollo a realizar cambios en sus prácticas de aplicación y por ende llevar a las instituciones a adaptarse a la eficacia incluso transnacional, si la institución opera en diferentes países.

Sin embargo, también podría generar brechas en la percepción del significado de "eficacia" entre los mercados desarrollados y emergentes.

*Anti-Lavado de Dinero y Control de la Financiación del Terrorismo.

Independientemente del propio país, las organizaciones deben considerar cómo están regulados los temas LA/FT a nivel mundial por 3 razones:

- GAFI: establece las normas internacionales para la gestión y ejecución del riesgo LA/FT. Por lo tanto, forma la base de los reglamentos nacionales y las obligaciones de los bancos y otras instituciones reguladas.
- OFAC: junto con otras reglamentaciones como la inglesa, Her Majesty's Treasury (HMT), administra sanciones económicas y por su diseño se centra en el movimiento de bienes, servicios y fondos en el extranjero y a través de las fronteras.
- Es casi imposible para las instituciones financieras evitar las leyes de las jurisdicciones que administran las principales monedas mundiales como el dólar estadounidense, la libra esterlina y el euro. Tan solo el acto de incurrir en el lavado de una simple transacción en los EE.UU o con dólares estadounidenses o de contactar a una persona en los EE.UU por teléfono o correo electrónico; es suficiente para considerarse como un nexo ilícito y ser perseguido por las autoridades en los EE.UU.

Cada vez más las regulaciones de los principales centros financieros como Hong Kong, Singapur, Londres y Nueva York, están exigiendo a las instituciones la incorporación de los más altos estándares tanto a nivel internacional como en sus países de origen.

Todos estos acontecimientos imprevisibles, que cambian rápidamente, pueden conducir a una especie de inercia estratégica. Una cosa es muy clara, se requiere de la objetividad y la experiencia adecuada para elaborar programas de cumplimiento ante el delito financiero.

¿Qué significa toda esta información para su empresa?

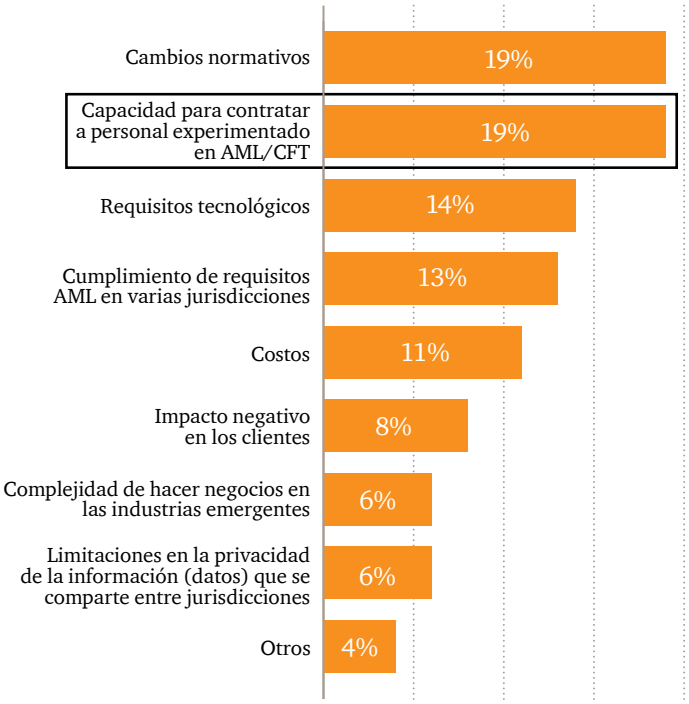
Teniendo en cuenta la globalización de estándares AML/CFT, es importante recordar que usted será juzgado por el más alto nivel de cumplimiento de los estándares internacionales. Aquí hay tres puntos de acción a considerar:

- **Manténgase actualizado en cuanto a la reglamentación.** Mire más allá del cumplimiento de las leyes de hoy. Focalícese hacia el futuro y examine cómo estructurar adecuadamente el cumplimiento de las tendencias legislativas. Concéntrese en tener una función o un encargado viable dentro de su organización que realice un seguimiento de la normatividad.
- **Lleve la delantera sin necesidad de ser quien sigue al otro.** Estar en el medio del pelotón lo expone al riesgo de caer detrás de la curva de regulación. Enfóquese en ser estratégicamente ágil e innovador para mantenerse en la cima de los cambios regulatorios.
- **Aprenda de los errores de otros.** Pocas organizaciones son conocidas por investigar activamente la causa o raíz de los problemas significativos como si son identificadas por los reguladores. La remediación a menudo sirve como una solución rápida para hacer frente a los hallazgos, sin embargo, el costo de remediar las violaciones a menudo pesa más que las penas impuestas por los reguladores. Como la mayoría de las transacciones tienen un componente financiero multinacional, es una buena práctica siempre que sea posible, realizar autoevaluaciones en AML/CFT y establecer requisitos "en toda la empresa" para garantizar la coherencia, incluso en otros países donde su empresa opera.

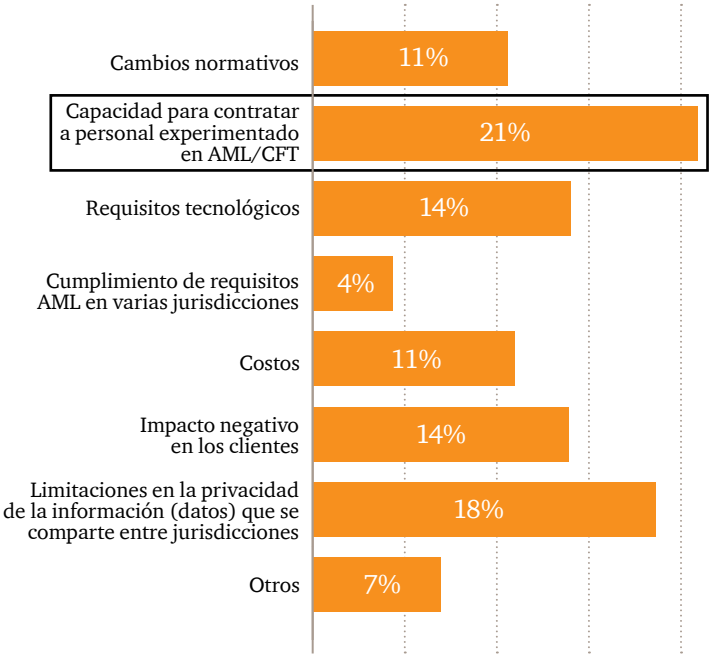
Sus empleados, sus procesos

Quienes fueron encuestados tanto a nivel global como en Colombia afirmaron que la contratación de personal con experiencia es el desafío más importante que enfrentan en cuanto a temas AML. Por desgracia, la oferta de talento sigue cayendo detrás de la demanda. La competencia por encontrar perfiles altos es significativa, tanto para los servicios financieros como para empresas de servicios no financieros.

Fig 28: Retos más significativos en relación al cumplimiento de requisitos AML/CFT



Encuesta Global 2016



Encuesta Colombia 2016

Algunas organizaciones están afrontando el reto de capacitar al personal interno de la compañía con un enfoque significativo en AML/ CFT y soborno.

Fig 29: Medidas implementadas para cumplir con el aumento de expectativas normativas.

Encuesta Global 2016

Encuesta Colombia 2016

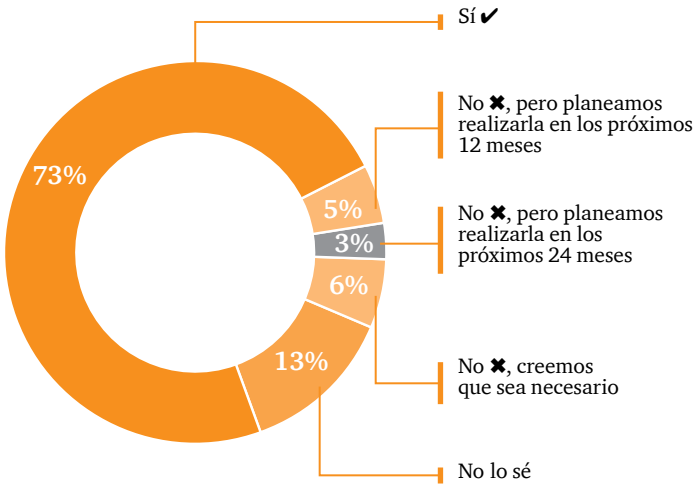
Las evaluaciones de riesgo son críticas. Durante la última década, el refuerzo en controles ante el lavado de dinero en los sistemas financieros ha obligado a los delincuentes a buscar nuevas maneras de cometer sus delitos. Es por eso que las evaluaciones de riesgo son cruciales, lo que permite a su organización identificar y abordar el lavado de dinero y la financiación del terrorismo, enfrentando cuando y con quien hace usted negocios.

A pesar de las claras ventajas, más de una cuarta parte de las empresas de servicios financieros que participaron en la encuesta a nivel global, o bien no están actualmente llevando a cabo una evaluación del riesgo AML/CFT o no lo saben. En todos los sectores, en Colombia el porcentaje es inferior que a nivel global, el 13% frente al 27%.

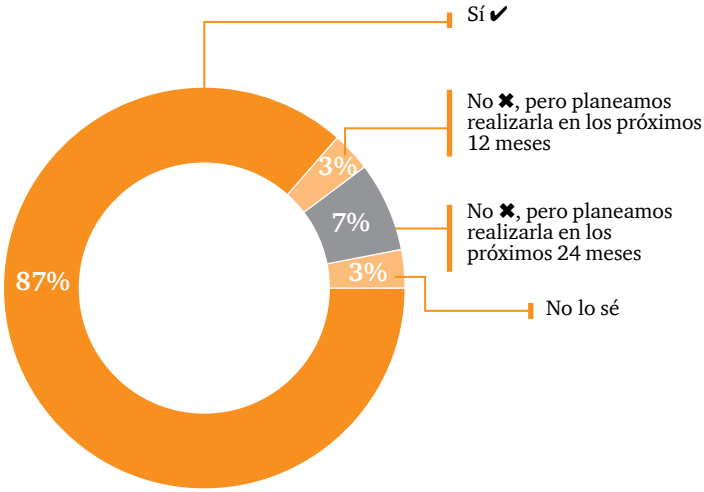
A medida que la sofisticación de quienes lavan dinero sigue aumentando, implementar estas medidas es un tema que no se puede posponer. Por ejemplo, el Trade-based money laundering (Lavado de dinero basado en el comercio o TBML), es un complejo sistema que se basa en proporcionar datos falsos que permite a los delincuentes transitar transacciones por todo el mundo como si fuesen legítimas. Este método es cada vez más difícil de detectar a través de los sistemas de monitoreo de transacciones tradicionales.

Retomando el tema, las evaluaciones de riesgo deben realizarse de forma periódica. Ellas deben estar estrechamente en sintonía con cambios de circunstancias como el entorno, los estándares globales y la regulación en los países donde la empresa opera. Cabe destacar que las evaluaciones deben incluir la elaboración de perfiles para corroborar que no tienen relación con temas como el lavado de dinero ni la financiación del terrorismo. Estos aspectos son parte del estándar global recomendado por el GAFI y los reguladores para frenar las amenazas.

Fig 30: Porcentaje de organizaciones que han llevado a cabo evaluaciones de riesgo AML/CFT.



Encuesta Global 2016



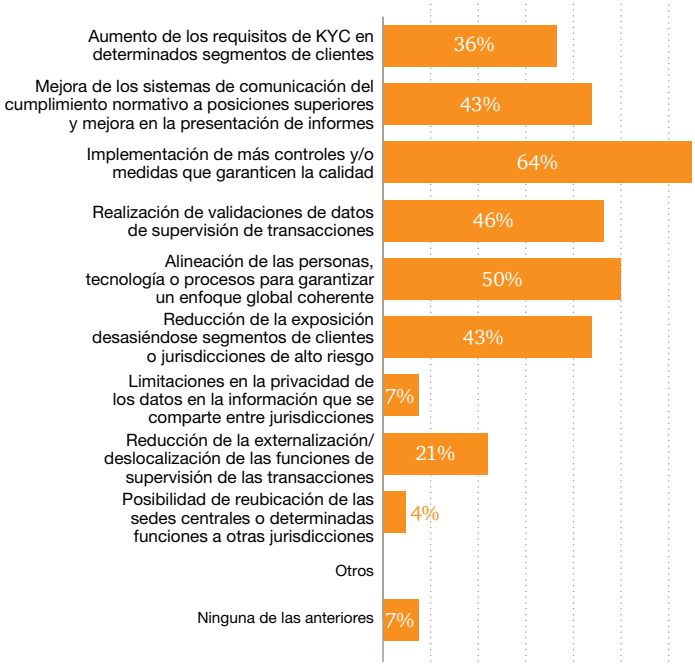
Encuesta Colombia 2016

Conozca su cliente hoy y mañana. La transparencia en cuanto al conocimiento de su cliente debe ir más allá que la mera identificación y verificación de la información que proporcionan. Debe ser un acto dinámico, continuo y es esencial para mantener el monitoreo de señales de alerta y actividades sospechosas. Especial atención se debe prestar a las relaciones y transacciones comerciales de los clientes sobre todo cuando se hacen negocios con personas que residen en países con regulaciones débiles o insuficientes en términos de AML.

Fig 31: Actividades implementadas para reducir los riesgos de AML/CFT

Encuesta Global 2016

Fig 32: Actividades implementadas para reducir los riesgos de AML/CFT



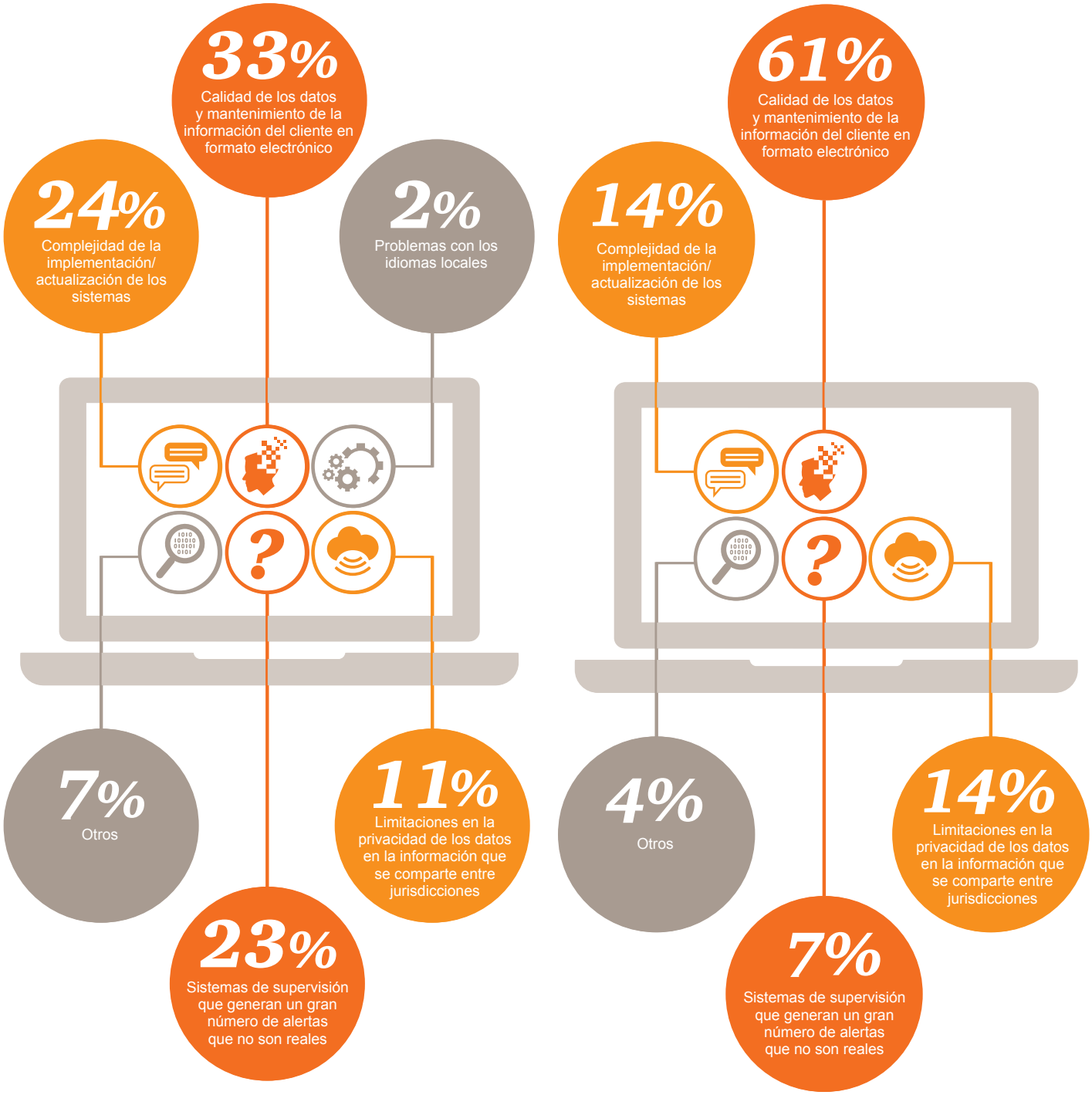
Encuesta Colombia 2016

Tecnología

Las empresas de todo tipo de industria parecen estar en aprietos en temas de tecnología para mitigar este riesgo. En particular, la mayoría de las organizaciones de servicios se enfrentan al obstáculo de "reestructurar " sus programas AML en un panorama de regulación mundial y en evolución constante. Sin embargo, muchas se ven obstaculizadas por sistemas de monitoreo que se consideran extremadamente costosos.

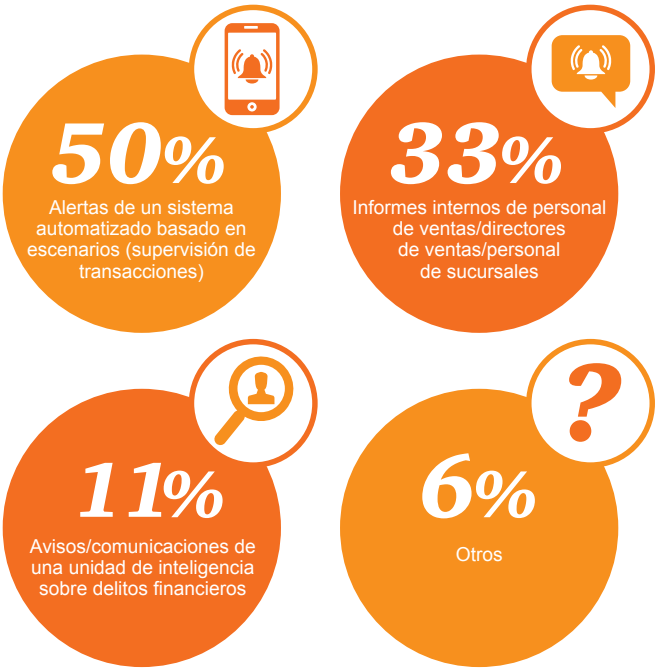
Desafortunadamente, el costo y la complejidad de la implementación de algunas de las nuevas plataformas más sofisticadas y analíticas con algoritmos de vanguardia que pueden ayudar a pasar de una herramienta básica a un enfoque más estratégico y eficaz no es asequible para muchos. Las personas encuestadas pertenecientes a servicios financieros parecen ser muy conscientes de estos desafíos de sistemas. A nivel global, el 33% de los encuestados de todos los sectores industriales y el 61% a nivel Colombia, citan a la calidad de datos como el desafío técnico más importante que enfrentan.

Fig 33: Sistemas AML/CFT: Reto más significativo



Agravando aún más el problema, las alertas para identificar temas de lavado de activos no parecen estar funcionando correctamente. Aunque en Colombia el porcentaje es superior, el informe global declara que sólo la mitad de los eventos sospechosos de lavado de dinero o financiación del terrorismo está siendo detectados por los sistemas de monitoreo de transacciones. Las tipologías actuales de AML podrían no estar alcanzando los matices y estructuras complejas necesarias para identificar las transacciones de alto riesgo.

Fig 34: Métodos de identificación de actividades sospechosas.



Encuesta Global 2016

Encuesta Colombia 2016

Invertir en nuevos modelos analíticos no es hasta el momento un fenómeno generalizado en todas las empresas. Esto podría ser un indicio de que las instituciones no están viendo una relación positiva en cuanto a costo-beneficio.

¿Qué puede hacer una empresa para dar el salto hacia nuevas tecnologías?

A menudo los cambios son producidos luego de una eventualidad o una remediación producto de sanciones regulatorias. También se pueden dar por fusiones o adquisiciones, u otro tipo de transacciones que revelan que los antiguos sistemas no son sanos. Otra causa puede ser un nuevo competidor que entra en el mercado y cambia el panorama y las reglas del juego.

A veces es simplemente una cuestión de la organización que se da cuenta de que el retorno esperado de la inversión y el hecho de cambiar de tecnología es mayor que el costo de inversión y mantenimiento.

Incluso puede haber beneficios al obtener nuevas tecnologías. Más allá del cumplimiento AML, se pueden mejorar programas anti- soborno, evitar sanciones, reforzar los controles y el monitoreo frente al fraude, mejorar los controles financieros e investigaciones y potencialmente fortalecer su gestión global.

Contactos

Ana María Villarreal
Associate Partner
+57 (1) 634 0555
ana.milena.villarreal@co.pwc.com

Andrea Paola Moreno
Risk Advisory Services
+57 (1) 634 0555 Ext. 10414
paola.moreno@co.pwc.com

Estadísticas de participación

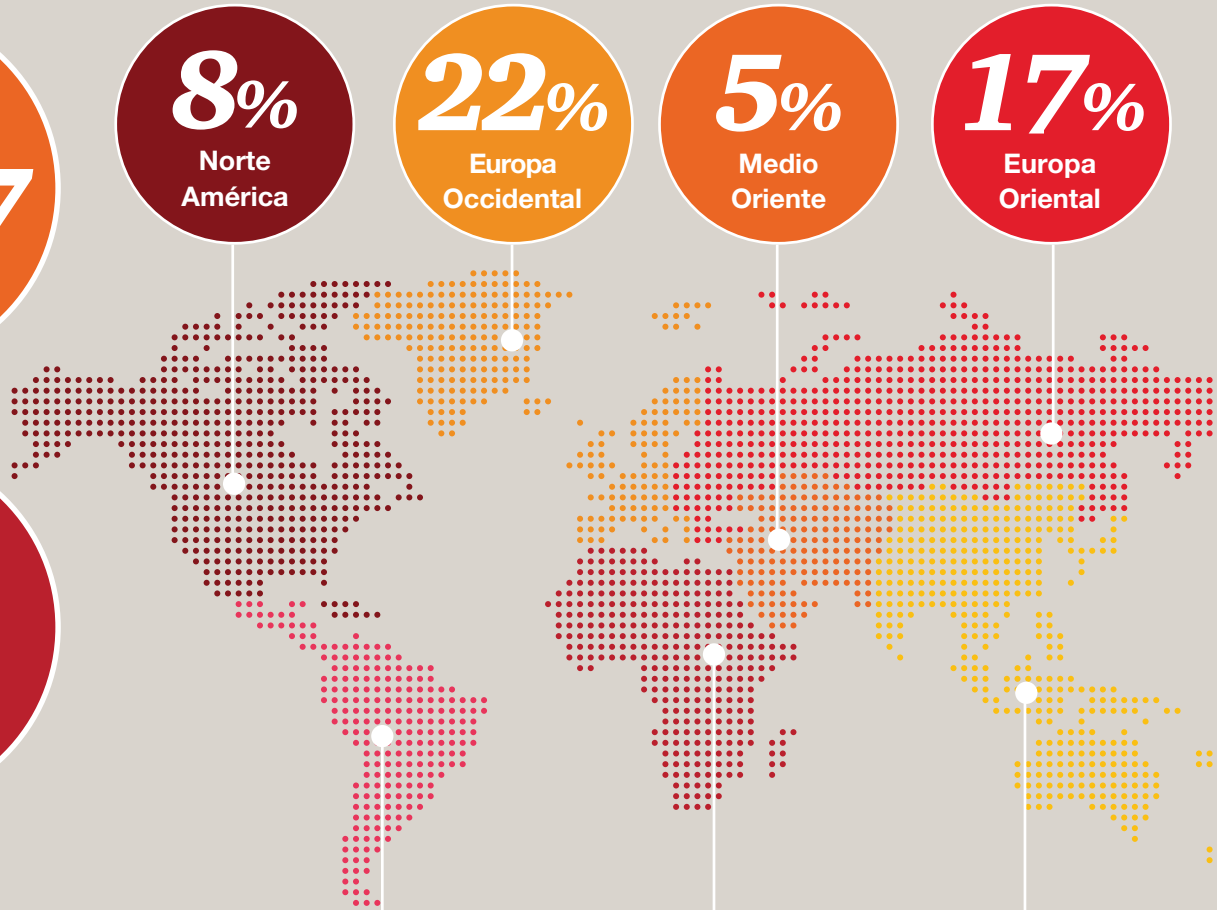
Estadísticas de participación

6,337 completaron la encuesta

Paises **115** participantes

Encuesta realizada en **17** idiomas

Participación por región



- **8%** Norte América
- **22%** Europa Occidental
- **5%** Medio Oriente
- **17%** Europa Oriental
- **18%** América Latina
- **10%** África
- **20%** Asia

Global

Encuestados

45%
Presidente/Miembro de la Junta Directiva y Directores

70%
de respuestas por parte de quienes trabajan en finanzas, altos ejecutivos, auditoría, cumplimiento y riesgo

54%
de encuestados que trabajan en organizaciones de más de 1.000 empleados

37%
de las empresas encuestadas cotizan en bolsa

30%
Jefe de unidad de negocio o departamento

59%
de empresas encuestadas son multinacionales

Sectores industriales

35%
Industrial

24%
Financiero

14%
Consumo

7%
Tecnología

6%
Servicios Profesionales

14%
Otros

Encuesta Global 2016

Estadísticas de participación

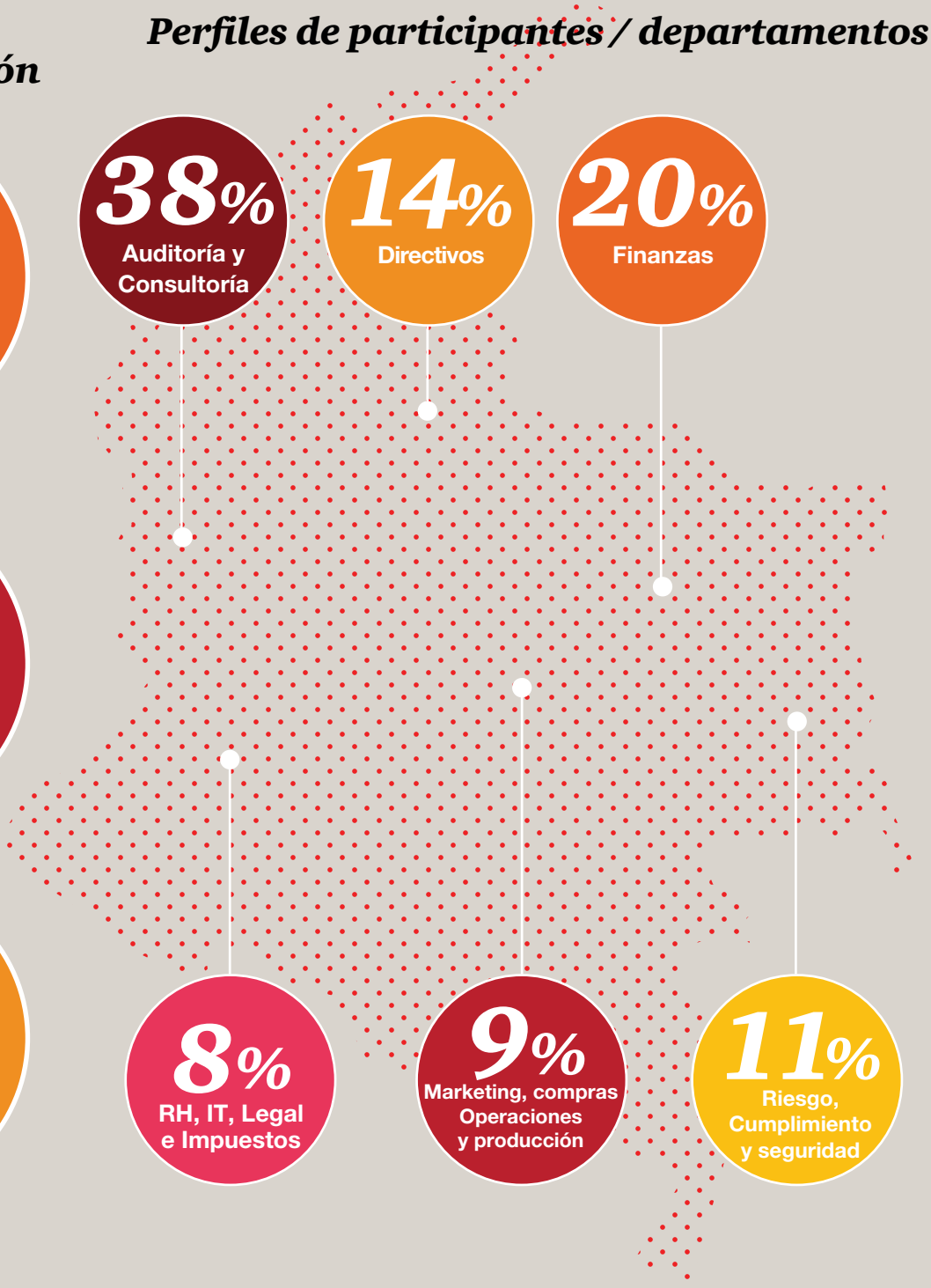
Estadísticas de participación

118 completaron la encuesta

26% Sector Financiero

74% Sector No financiero

Perfiles de participantes / departamentos



Colombia

Encuestados

79%
de respuestas por parte de quienes trabajan en finanzas, altos ejecutivos, auditoría, cumplimiento y riesgo

50%
de encuestados que trabajan en organizaciones de más de 1.000 empleados

26%
de las empresas encuestadas cotizan en bolsa

48%
de empresas encuestadas son multinacionales

Sectores industriales

39% Industrial

29% Financiero

5% Consumo

3% Tecnología

5% Servicios Profesionales

19% Otros

Encuesta Colombia 2016

Información acerca de la encuesta

La página web www.pwc.com/crimesurvey ha sido diseñada para complementar la encuesta a nivel global y profundizar en datos tales como:

- ***Metodología de la encuesta***
- ***Terminología***
- ***Datos comparativos entre países***
- ***Información adicional acerca de los participantes***

Además, los datos de la encuesta se presentan en una herramienta innovadora que permitirá a los visitantes del sitio la posibilidad de personalizar su análisis de los datos para sus necesidades específicas.

Contactos

Survey Leadership Team

Trevor White
Partner, South Africa
t: +27 (31) 271 2020
e: trevor.white@za.pwc.com

Mark Anderson
Partner, United Kingdom
t: +44 (0) 207 8042564
e: mark.r.anderson@uk.pwc.com

Didier Lavion
Principal, United States
t: +1 (646) 471 8440
e: didier.lavion@us.pwc.com

Editorial Board Members

Alex Tan
Executive Director, Malaysia
t: +60 (3) 2173 1338
e: alex.tan@my.pwc.com

Claudia Nestler
Partner, Germany
t: +49 (69) 9585 5552
e: claudia.nestler@de.pwc.com

Martin Whitehead
Partner, Brazil
t: +55 (11) 3674 2141
e: martin.j.whitehead@br.pwc.com

Antoinette Lau
Partner, China
t: +86 (21) 2323 5533
e: antoinette.yy.lau@cn.pwc.com

Dinesh Anand
Partner, India
t: +91 9818267114
e: dinesh.anand@in.pwc.com

Survey Management Team

Moazam Fakey
Senior Manager, South Africa
t: +27 (11) 797 4750
e: moazam.fakey@za.pwc.com

Anjali Fehon
Forensics Strategy Leader,
United States
t: +1 (973) 236 4310
e: anjali.t.fehon@us.pwc.com

Survey Colombian Team

Mónica Jiménez
Partner Advisory, Colombia
t: +57 (1) 634 0555 Ext. 10202
e: monica.jimenez@co.pwc.com

Jorge Ropero
Forensics Manager
Colombia
t: +57 (1) 634 0555 Ext. 10438
e: jorge.ropero@co.pwc.com

Editorial Team

Santiago Uribe
Clients & Markets Senior Manager
t: +57 (1) 634 0555 Ext. 10436
e: santiago.uribe@co.pwc.com

María Paula Jiménez
Forensics Senior, Colombia
t: +57 (1) 634 0555 Ext. 10211
e: paula.jimenez@co.pwc.com