Poniendo la lupa sobre los delitos económicos:

La preparación devuelve el foco a las oportunidades

33%

de las organizaciones en Venezuela reportaron haber sido víctimas de algún delito económico

32%

El Cibercrimen escala posiciones a nivel global, al ser el segundo tipo de delito económico más reportado

10%

Uno de cada diez delitos económicos son descubiertos por accidente.

pwc

www.pwc.com/crimesurvey

Principales observaciones

1 *Los delitos económicos son una tenaz amenaza*

- Una de cada tres organizaciones (36%) sufrieron delitos económicos.
- Tanto los mercados emergentes como los desarrollados se vieron afectados.
- Los métodos de detección de las compañías no están a la altura de la amenaza.

¿Qué oportunidades hay disponibles para contrarrestar proactivamente los delitos económicos?

Los delitos económicos son un problema diversificado a nivel mundial

2 *Los controles deben estar arraigados en la cultura organizacional*

- Se cierra la brecha entre perpetradores de fraude internos y externos.
- 1 de cada 5 encuestados nunca ha llevado a cabo una evaluación de riesgos de fraude.

¿Cuáles son los riegos de su organización? ¿Identifica usted activamente las áreas vulnerables?

En algunos casos los daños financieros alcanzan los cientos de millones de dólares estadounidenses

3 *Las amenazas cibernéticas aumentan y la preparación de los negocios no les sigue el paso*

- El cibercrimen pasó a ser el 2do delito económico más reportado, afectando al 32% de las organizaciones.
- La mayoría de las compañías no se encuentran preparadas adecuadamente o tan siquiera entienden los riesgos que enfrentan: solo el 37% de las organizaciones tienen un plan de respuesta a incidentes cibernéticos.
- El compromiso de los líderes es fundamental; sin embargo, menos de la mitad de los miembros de la junta directiva solicitan información acerca del estado de preparación cibernética de sus organizaciones.

¿Cuán realista es su plan de respuesta ante los ciberataques?

Se puede considerar la preparación ante los ciberataques como una prueba de esfuerzo organizacional

4 *Desconexión entre lo establecido por la dirección y la realidad en los niveles inferiores*

- 1 de cada 5 encuestados desconoce la existencia de un programa formal de ética y cumplimiento en sus organizaciones, y muchos se encuentran confundidos acerca de la titularidad del mismo.
- Casi la mitad de los delitos económicos graves fueron perpetrados por actores internos.
- Los principales daños citados se relacionan con la moral de los empleados (44%) y la reputación de la organización (32%).

¿Su estrategia de negocios se encuentra alineada y liderada por sus valores organizacionales?

Las personas y la cultura son su primera línea de defensa

5 *La prevención de la legitimación de capitales continúa causando confusión*

- 1 de cada 5 bancos ha sufrido acciones correctivas por parte de algún regulador.
- Más de un cuarto de las firmas de servicios financieros no ha llevado a cabo evaluaciones de riesgos de legitimación de capitales (AML, por sus siglas en inglés) y de financiamiento del terrorismo (CFT, por sus siglas en inglés) en todas sus operaciones alrededor del mundo.
- 33% de los encuestados citaron a la calidad de la información como un importante desafío técnico.
- La falta de personal con experiencia en AML y CTF es un gran problema.

¿Cuál sería el resultado de su organización ante una inspección de los entes reguladores?

El costo del cumplimiento (y del no cumplimiento) continúa creciendo

Contenido

Prefacio

En los temas de ocupación de los CEO, el concepto de riesgo en los negocios se ha extendido del panorama tradicional, a uno que involucra un espectro mucho más complejo de amenazas. Y es que la promesa de oportunidades se ve confrontada ante la diversidad de los riesgos, y la sustentabilidad del negocio supeditada a factores más diversos.

En paralelo: los delitos económicos amplían sus caminos hacia los negocios, el cumplimiento regulatorio se incrementa y con ello el costo. No es una historia nueva, es la consecuencia de la aceleración en el ritmo de los negocios, y la necesidad de triunfar en un mercado vertiginoso.

Nuestro informe lo reta a ajustar el lente sobre los delitos económicos y a reenfocar su rumbo hacia oportunidades relacionadas con una preparación estratégica.

Este trabajo ha sido desarrollado para que todo aquel expuesto a un riesgo en los negocios conozca las generalidades del crimen. Esta definición de conjunto engloba a toda la organización, y la razón de ello es porque el crimen muta tanto como cambian los negocios, y lo que hoy es una amenaza para un departamento mañana lo será para otro. En consecuencia, el análisis de los delitos económicos necesita ser incorporado como herramienta para la toma de decisiones en su día a día, y preparar a su compañía para afrontarlo representa hacer un ejercicio de planificación continua.

Lo que hará la diferencia entre lograr sus metas o que lo hagan aquellos quienes atentan contra su organización, será ajustar la visión de su compañía y elaborar estratégicamente planes para su crecimiento y defensa, basados en su perfil específico de oportunidades y amenazas.

Roberto Sánchez V.
Socio líder de Servicios
de Asesoría en Riesgos

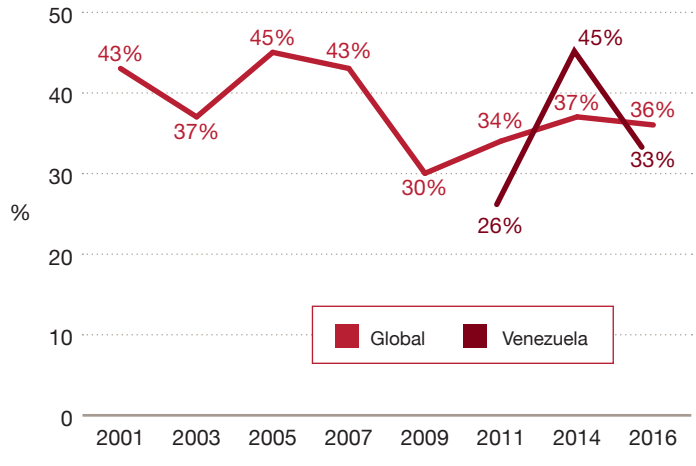
Evolución económica del crimen

2016: Evolucionan los delitos económicos, las medidas preventivas se quedan atrás

Según lo informado por más de 6.000 personas que respondieron la Encuesta Global de Delitos Económicos 2016 de PwC, en los últimos 24 meses más de un tercio de las organizaciones han sufrido delitos económicos.

Los resultados de este año muestran la primera disminución de los delitos económicos desde la crisis de 2008-2009, aunque marginal, de solo de un 1%. A primera vista, esto podría ser evidencia de que las inversiones en medidas preventivas hechas por las organizaciones en los últimos años han dado frutos. Sin embargo, si examinamos los datos con mayor detenimiento, comenzamos a sospechar que esta pequeña disminución enmascara la preocupante tendencia que los delitos económicos evolucionan, y los programas de detección y control no son capaces de seguirles el paso. Adicionalmente, esta disminución no necesariamente refleja reducción en su impacto financiero, ya que las pérdidas de cada fraude se encuentran en alza.

Fig 1: Tasa reportada de delitos económicos



El informe ilustra como en los últimos dos años los delitos económicos han evolucionado, mutando su forma dependiendo del sector industrial y de la región.

Pese a esta creciente amenaza, hemos visto una disminución en la detección de actividades criminales a través de los métodos bajo control de la gerencia, con una caída del 7% en la detección por medio de los controles corporativos. Lo que más resalta en este aspecto, es que 1 de cada 5 organizaciones (22%) no ha realizado una evaluación de riesgo en los últimos 24 meses. Si miramos esto en el contexto de los hallazgos de la 19a Encuesta Global Anual a los CEO, en la que dos tercios de los directores ejecutivos estuvieron de acuerdo con que hoy las amenazas al crecimiento son mayores que en el pasado (un marcado incremento comparado con la tasa del 59% de 2015), estamos ante la presencia de una preocupante tendencia: dejar demasiado al azar. De hecho, nuestros hallazgos indican que 1 de cada 10 delitos económicos son descubiertos por accidente.

Nuestros hallazgos indican que 1 de cada 10 delitos económicos es descubierto por accidente.

Hoy más que nunca un enfoque pasivo ante la detección y prevención de los delitos económicos es una receta para el desastre. Poniendo en manifiesto este hecho, nuestra encuesta descubrió una generalizada falta de confianza en los organismos encargados de hacer cumplir las leyes, fenómeno que no se encuentra circunscrito a una región o nivel de carga económica.

El mensaje está claro: la carga de prevenir, proteger y responder ante los delitos económicos recae exclusivamente en las propias organizaciones.

Nuestra encuesta de este año se enfoca en tres áreas claves: Cibercrimen, Programas de cumplimiento y Prevención de legitimación de capitales y ética, pero también explora algunos temas comunes como el manejo de los riesgos asociados a la adopción de nuevas tecnologías, lo que significa conducir responsablemente su organización en un -cada vez más extenso- panorama de negocios, así como la integración de conductas éticas a la toma de decisiones.

Además de resaltar las áreas específicas de delitos económicos que requieren atención, enfatizamos en aquellas cosas en las que se puede mejorar, como sería implementar medidas más sofisticadas y efectivas que, además de reducir estos riesgos, aportan los beneficios de un negocio más consciente a las amenazas y seguro de sus defensas ante un mundo cambiante.

El panorama venezolano

Este año, la participación en nuestra Encuesta Global de Delitos Económicos 2016 por parte de las organizaciones en Venezuela superó cualquier expectativa, alcanzando el tercer lugar de participación global y el primero en la región de centro y surámerica. Semejante participación, nos permite evaluar las semejanzas y diferencias que podamos tener con los resultados globales, y particularmente con la región.

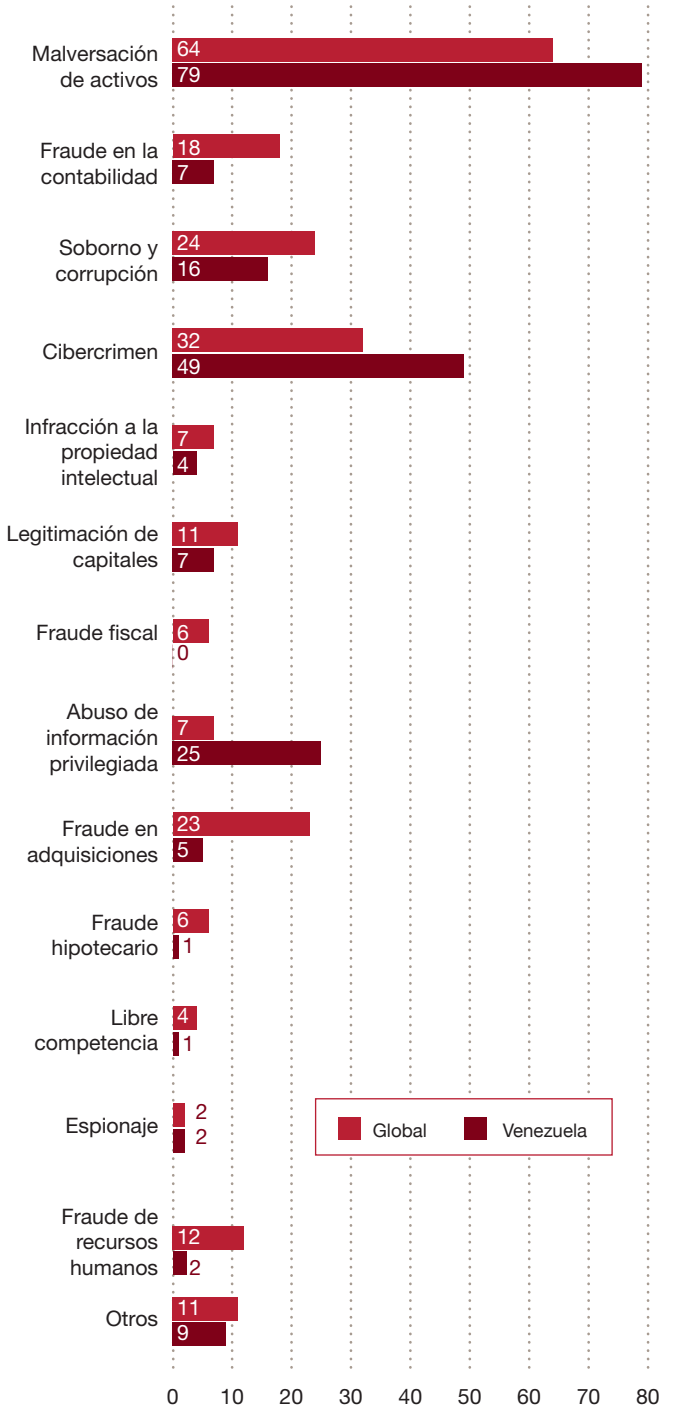
Las organizaciones en Venezuela no escapan del flagelo económico, donde una de cada tres organizaciones reportaron haber sido víctima de algún tipo de delito en los últimos 24 meses. Este número significa una marcada reducción en cuanto al porcentaje reportado en nuestra edición del 2014, cuando el 45% de las organizaciones en nuestro país reportó haber sufrido algún tipo de delito económico, pudiendo obedecer al panorama económico local, la contracción del mercado o la desaceleración de las inversiones en el país, pero también puede tener una lectura interesante: Este año, la encuesta incrementó su participación en sectores que históricamente no lo hacían.

Aunque los delitos tradicionales siguen a la delantera, un enemigo omnipresente avanza

En la siguiente figura se muestran los delitos económicos más generalizados reportados por nuestros encuestados en 2016: Mientras que este año, a nivel global, todos los principales tipos de delitos considerados "tradicionales" (malversación de activos, soborno y corrupción, fraude en las adquisiciones y fraude contable) presentaron un leve descenso respecto a las cifras de 2014, el cibercrimen ha tenido un crecimiento sostenido desde que debutara en nuestra encuesta en 2011, posicionándose actualmente en el segundo lugar. Cabe destacar que para el 2014 este flagelo ya ocupaba el segundo lugar en Venezuela según nuestra encuesta, y actualmente se afianza en esta posición con un incremento de nueve puntos porcentuales para alcanzar un notable 49% de incidencia entre quienes manifestaron haber sufrido algún tipo de delito económico en los últimos 24 meses.

Pero este no es el único problema que hoy aqueja a las empresas venezolanas, ya que los delitos tradicionales están teniendo comportamiento diferenciados con respecto a los resultados globales, particularmente en la malversación de activos y uso de información privilegiada, en donde ha ocurrido un repunte.

Fig 2: Tipos de delitos económicos experimentados

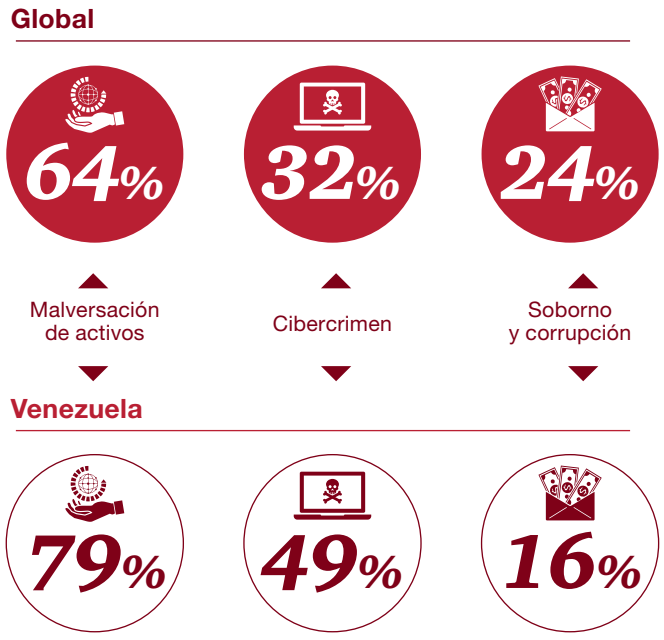


Lo que también llama la atención es la caída abrupta de las afirmaciones de los encuestados sobre haber sido víctimas del soborno y la corrupción, mejorando sensiblemente con respecto a los resultados del 2014 y mejorando los resultados globales.

Los 3 delitos económicos más comunes reportados en 2016

Aunque históricamente a la malversación de activos se le ha visto como el fraude más fácil de detectar, por lo que su presencia año tras año en nuestra encuesta es generalmente predecible, desde 2011 hemos visto una tendencia a la baja en las tasas reportadas de este delito a nivel global.

Fig 3: Los tres delitos más comunes reportados



Lo anterior podría ser consecuencia de un endurecimiento de los controles organizacionales y de que las empresas han mejorado en la prevención de los delitos económicos tradicionales, pero también podría ser el resultado de la evolución de los tipos de fraude a unos con mayor impacto como el cibercrimen.

A la luz del descenso en la tasa de detección a través de los medios bajo el control de la gerencia y ante una mayor incidencia de cibercrimen, debemos preguntarnos si estos delitos se han vuelto más difíciles de detectar o es que simplemente cada vez estamos menos conscientes de las amenazas cambiantes a las que se enfrentan nuestros negocios, y aún más importante: ¿qué debemos hacer al respecto?. Considerando que en promedio 20% de nuestros encuestados cree que sus organizaciones podrían sufrir de los principales delitos económicos en los próximos 24 meses, éste es el momento correcto para reconsiderar.

Delitos económicos: Son un problema global, pero no son los mismos en todos lados

Region	Delitos económicos reportados en 2016	Delitos económicos reportados en 2014
Africa	57%	50%
Europa Occidental	40%	35%
América del Norte	37%	41%
Europa Oriental	33%	39%
Asia y el Pacífico	30%	32%
América Latina	28%	35%
Medio Oriente	25%	21%
Venezuela	**33%**	**45%**
Global	**36%**	**37%**

Mientras que algunas regiones reportaron tasas más bajas de delitos económicos, y que se mantuvo la tendencia mundial, África, Europa Occidental y el Medio Oriente mostraron incrementos significativos en nuestra encuesta de 2016. Los principales propulsores de las altas tasas reportadas en África fueron Suráfrica (69%, sin cambios desde 2014), seguida por Kenia (61%, con un aumento del 17% respecto a la tasa de 2014) y Zambia (61%, con un aumento del 35%), mientras que en el Medio Oriente, los encuestados de Arabia Saudita reportaron tasas de delitos económicos de más del doble del 11% reportado en 2014, alcanzando el 24% en 2016.

En Europa Occidental llevaron la delantera Francia (68%) y Reino Unido (55%), ambos con un aumento de un cuarto respecto de 2014. En Francia, el significativo incremento en los delitos económicos es atribuible al aumento de los fraudes externos, predominantemente cibercrimen, el cual casi se duplicó pasando del 28% en 2014 al 53% en 2016. En el Reino Unido, el incremento se puede atribuir a la duplicación del número de encuestados que reportaron casos de soborno y corrupción en respuesta a mayores regulaciones (en la forma de la Ley Antisoborno del Reino Unido) y, en consecuencia, a una mayor conciencia de este delito.

El Reino Unido también experimentó un incremento del 50% en los incidentes reportados de cibercrimen.

A nivel regional, América Latina reportó una disminución del 7% en cuanto a la incidencia de los delitos económicos en comparación con los resultados del 2014 (8% por debajo del promedio mundial). Del mismo modo, el soborno y la corrupción y el fraude en las contrataciones públicas registraron un descenso del 5% y 7%, respectivamente. Sin embargo, el cibercrimen escala una posición y supera al soborno y la corrupción y al fraude en las contrataciones públicas para posicionarse como el segundo tipo de delito económico reportado en la región.

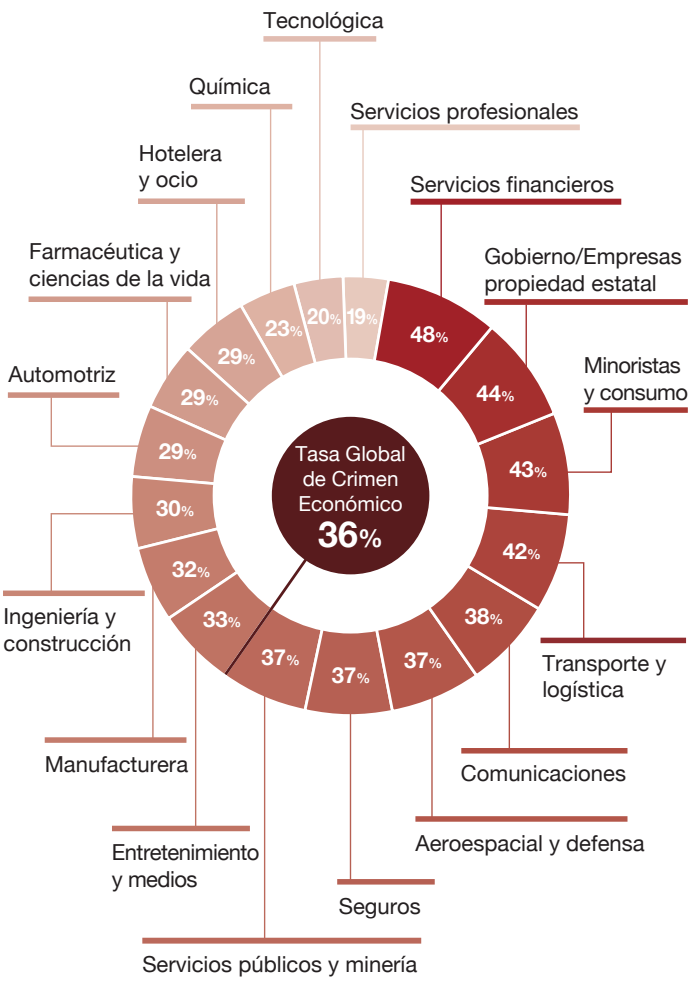
En tanto que en la mayoría de los países desarrollados se ha incrementado la atención regulatoria (particularmente en áreas sensibles como el cibercrimen, la legitimación de capitales, el soborno y la corrupción), la naturaleza trasnacional de las actividades criminales ha desdibujado las fronteras e impulsado un mayor nivel de cooperación internacional en reglamentación y cumplimiento.

Si evitamos caer en generalizaciones, estas estadísticas demuestran que los delitos económicos son un asunto mundial bastante diversificado, tanto en tipo de delito como a través de los mercados emergentes y desarrollados. El entender estas diferencias puede ayudar a las organizaciones a enfocar sus esfuerzos de prevención en las áreas correctas, sin perder la perspectiva de adoptar una visión global y aplicar normas internacionales a sus esfuerzos para combatir los delitos económicos.

¿Cómo afectan a su industria los delitos económicos?

Por ser los que apoyan las necesidades económicas de todas las demás industrias, los servicios financieros han sido, a través del tiempo, los más amenazados por los delitos económicos.

Fig 3: ¿Cuáles industrias se encuentran en riesgo?



Sin embargo, conforme el mercado evoluciona hacia soluciones de negocios integradas, muchas organizaciones no financieras ahora se encargan internamente de las necesidades económicas de su clientela, o han concebido modelos de negocios y servicios que asemejan a los prestados por las instituciones financieras.

Numerosos negocios en los sectores automotriz, comunicaciones, minorista y consumo, por solo nombrar algunos, además tienen acuerdos conjuntos con compañías de servicios financieros o licencias bancarias propias, dándole a los estafadores que "siguen el dinero" más vías para lograr sus objetivos.

Mientras que la industria de servicios financieros, en virtud de su altamente regulado ambiente, ha establecido a lo largo de las décadas sofisticados mecanismos de control, metodologías de detección y herramientas de gestión de riesgo, en general a las empresas que podríamos denominar como "híbridas" les va a tocar lidiar como principiantes con estos riesgos, y eventualmente con el panorama de cumplimiento debido a la rápida evolución en el que ahora se encuentran los organismos reguladores en identificar a estos nuevos jugadores del negocio financiero.

Aumento de la incidencia de delitos económicos en los últimos 24 meses, en sectores de la industria

A medida que las condiciones del mercado cambian, también lo hace el panorama de amenazas. Re-evaluaciones periódicas son clave para prevenir la delincuencia económica

Crecientes daños financieros y colaterales

Las pérdidas pueden ser severas. En Venezuela, poco más de la mitad de los encuestados (56%) reportó pérdidas financieras menores a los USD 50 mil, representando un incremento de 14 puntos porcentuales respecto a la edición del 2014. Sin embargo, 16% de los participantes manifestó haber sufrido pérdidas entre USD 50 mil y USD 100 mil, y otro 16% reportó pérdidas entre USD 100 mil y USD 1 millón, números que se mantienen igual a los reportados durante la edición anterior de la encuesta. Estas son cifras substanciales y representan la tendencia de los costos crecientes de cada ocurrencia de un fraude. Otro punto a destacar en nuestro país es la disminución de la incertidumbre en cuanto al monto de las pérdidas financieras que afrontan las organizaciones, pasando de un 16% de encuestados que no conocían el monto de dichas pérdidas en 2014, a un 11% en la presente edición.

Fig 3: Impacto financiero de los delitos económicos

En términos financieros, ¿aproximadamente cuánto cree usted que su organización puede haber perdido a través de los casos de delitos económicos en los últimos 24 meses?

	Global	Venezuela
100 millones o más USD	1	0
5 millones < 100 millones USD	4	1
1 millón < 5 millones USD	9	0
100.000 to < 1 millón USD	22	16
50.000 to < 100.000 USD	17	16
Menos de 50 000 USD	36	56

Características más probables de un estafador interno venezolano

Es difícil de estimar el verdadero costo de los delitos económicos para la economía mundial, en especial si consideramos que las pérdidas financieras suelen, con frecuencia, ser solo una pequeña parte de las repercusiones de un incidente.

Nuestros encuestados consistentemente señalaron que extensos daños colaterales, como consecuencia de interrupciones del negocio (medidas correctivas, intervenciones de investigación y preventivas, multas regulatorias, honorarios legales y, más importante aún, daños a la moral y la reputación), impactaron significativamente el desempeño a largo plazo del negocio. Por supuesto, este tipo de pérdidas, aunque no siempre son cuantificables, puede en el tiempo eclipsar el relativo impacto a corto plazo de las pérdidas financieras.

Perfil del estafador

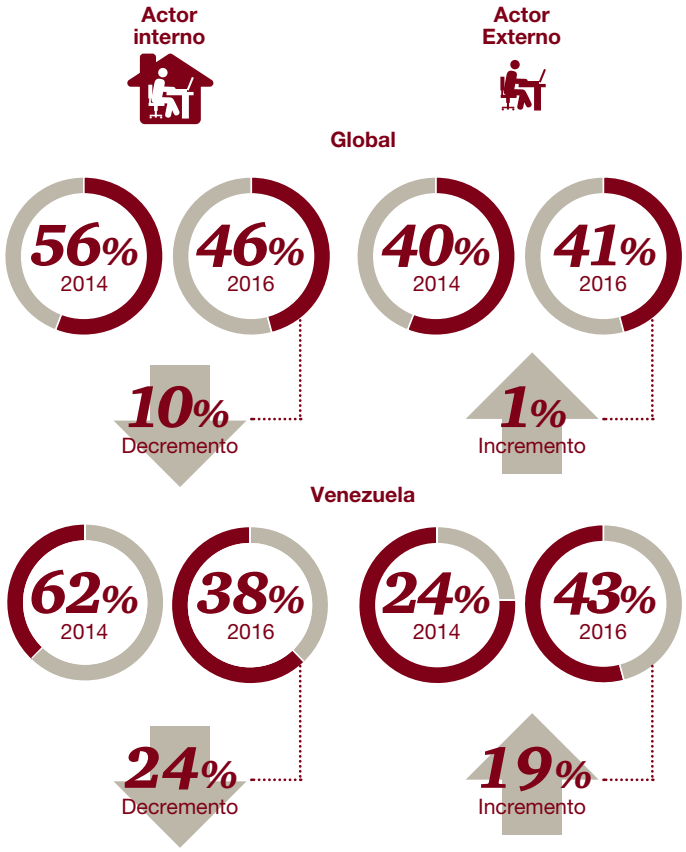
Desde nuestra última encuesta hemos visto como la brecha entre estafadores internos y externos se ha venido cerrando. Aunque todavía más de la mitad de los perpetradores internos pertenecen a las gerencias media y alta, en algunas regiones la subdirección contribuyó también bastante a la comisión de fraudes internos. Esto nos indica una potencial debilidad de los controles internos, en donde las medidas de control solo sirven como meros puntos de revisión en vez de procesos efectivos integrados a la cultura de la organización. Lo anterior se ve reforzado por el hecho de que 22% de los encuestados nunca ha llevado a cabo una evaluación de riesgo y que el 31% solo la lleva a cabo una vez al año.

En algunas regiones (por ejemplo, Europa Occidental), se han incrementado significativamente los fraudes perpetrados por la alta gerencia, los cuales son los más difíciles de detectar y suelen tener mayores repercusiones.

Las historias no son las mismas en todos lados. Si analizamos algunas regiones, los actores internos continúan como los principales perpetradores y en crecimiento en: África (7% mayor que el promedio mundial), Asia y el Pacífico (9% más alto), América Latina (9% más alto), a pesar del significativo descenso en el número de encuestados que dijeron que los actores internos son los responsables de cometer fraude (descenso del 6% - 15% en todas estas regiones desde 2014), lo que demuestra discrepancias entre la percepción y lo que efectivamente está ocurriendo en dicha región.

Por otro lado, los actores externos fueron los mayores responsables de fraude en Europa Oriental (44%), Europa Occidental (49%) y América del Norte (56%) comparado con el promedio mundial de 41%.

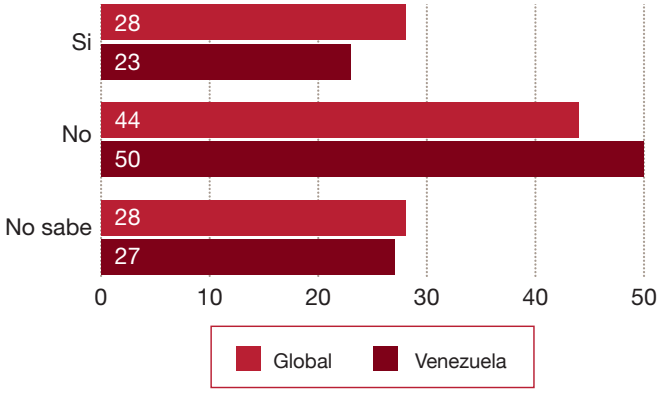
El cambio más substancial en lo que se refiera al tipo de perpetrador se dio en América del Norte con un significativo giro de perpetradores internos a externos.



Opinión sobre los organismos encargados de hacer cumplir las leyes

Preguntamos a los encuestados su opinión acerca de si pensaban que los organimos encargados de ejecutar localmente la ley están adecuadamente dotados de recursos y capacitados para investigar y procesar delitos económicos, y una rotunda mayoría (44% Global y 50% en Venezuela) expresó dudas respecto a este punto, mientras que 28% Global (23% en Venezuela) confía en las instituciones encargadas de ejecutar la ley.

Fig 4: Niveles de confianza en los organismos encargados de ejecutar la ley y hacer cumplir las leyes



Principales 15 países que mostraron desconfianza en los recursos y capacitación de los encargados de ejecutar la ley para combatir los delitos económicos

1	Kenia	79%
2	Suráfrica	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%

Prevenido, apertrechado, adelantado

La constante evolución de los delitos económicos los hacen un problema cada vez más complejo para las organizaciones y las economías como un todo, y el hecho que el ambiente regulatorio también se encuentre en constante cambio trae consigo numerosos retos para los negocios. Con la percepción que no necesariamente los organismos encargados de hacer cumplir las leyes están en capacidad de hacer una diferencia material, la carga de proteger a las organizaciones y a sus grupos de interés de los delitos económicos recae directamente sobre los hombros de la comunidad de negocios.

En las próximas tres secciones (dedicadas a las áreas estratégicamente fundamentales del cibercrimen, la legitimación de capitales y los programas de ética y cumplimiento), discutiremos cómo los números de nuestra encuesta pueden ayudar a descubrir no solo potenciales señales de alerta y tendencias problemáticas, sino también servir como indicadores de máxima importancia en áreas de oportunidad para las organizaciones visionarias, de manera de afrontar los desafíos de un mundo totalmente nuevo. Estar prevenido es estar apertrechado para el éxito.

Cibercrimen

Aunque se supone que los activos militares son de alta seguridad, los hackers han hallado que los proveedores "de bajo riesgo" tienen deficiencias en su seguridad, que puede ser fácilmente explotados y utilizados para rastrear el destino de estos suministros

Una amenaza sin límites

La tecnología digital continúa transformando y alterando el mundo de los negocios, exponiendo a las organizaciones a oportunidades y amenazas, por lo que no nos debe sorprender que el cibercrimen continúe su escalada, alcanzando en la Encuesta Global de Delitos Económicos de este año el segundo lugar como el tipo de delito más reportado.

En 2016 la realidad que arroja nuestra encuesta es que, como cualquier otro aspecto del comercio, los delitos económicos pasaron a ser digitales en cierta medida. En un ecosistema de negocios "hiperconectado" que con frecuencia se extiende a través de varias jurisdicciones, una violación en cualquier nódo del sistema (incluyendo a terceros como proveedores de servicios, socios de negocio o autoridades gubernamentales) puede comprometer en una variedad de formas el panorama digital de la organización.

Mas grave aún, ahora los riesgos cibernéticos abarcan un contexto mayor a lo que nuestra visión tradicional de la tecnología concebía, ya que hemos observado un fuerte aumento en los ataques que involucran a toda esta tendencia denominada "Internet de las cosas", incluyendo automóviles y electrodomésticos.

He aquí la paradoja digital: aunque las compañías de hoy día pueden cubrir más terreno, más rápido que antes y en tiempo real gracias a las nuevas tecnologías, al mismo tiempo el cibercrimen se ha convertido en una poderosa fuerza compensatoria que limita ese potencial, lo cual preocupa a los líderes de negocio por considerar que los puede estar frenando. En la 19a Encuesta Global Anual a los CEO de PwC, seis de cada diez directores ejecutivos clasificaron a las amenazas cibernéticas y a la velocidad del cambio tecnológico como las principales amenazas al crecimiento.

La encuesta de este año apunta al inquietante hecho que demasiadas organizaciones dejan la primera respuesta a sus equipos de TI, sin intervención adecuada o soporte de la alta gerencia y de otros actores claves. Más aún, la composición de estos equipos de respuesta es, con frecuencia, fundamentalmente defectuosa, afectando al final el manejo de los incidentes.

A través del extenso trabajo de nuestra Firma en estrategia y ejecución digital en miles de compañías a nivel mundial, hemos identificado las prácticas que distinguen a los líderes de la era digital, entre las cuales se destaca una postura proactiva en ciberseguridad y privacidad. Lo anterior necesita que todos dentro de la organización, desde la junta y la alta gerencia hasta la gerencia media y los colaboradores, la vean como su responsabilidad.

Sigue aumentando el cibercrimen

La incidencia de cibercrímenes reportados este año por nuestros encuestados es considerablemente más alta, subiendo entre los tipos de delitos económicos del 4to al 2do lugar a nivel Global y 2do lugar en Venezuela, siendo en particular el único delito económico que aumentó en esa categoría. Más de un cuarto de los encuestados dijo haberse visto afectado por el cibercrimen, mientras que de forma inquietante un 18% dijo no saber si fue o no afectado.

Las pérdidas pueden ser elevadas. Un puñado de encuestados (aproximadamente 50 organizaciones a nivel Global) dijeron haber sufrido pérdidas de más de USD 5 millones y de ellos, cerca de un tercio reportó pérdidas relacionadas con el cibercrimen por más de USD 100 millones.

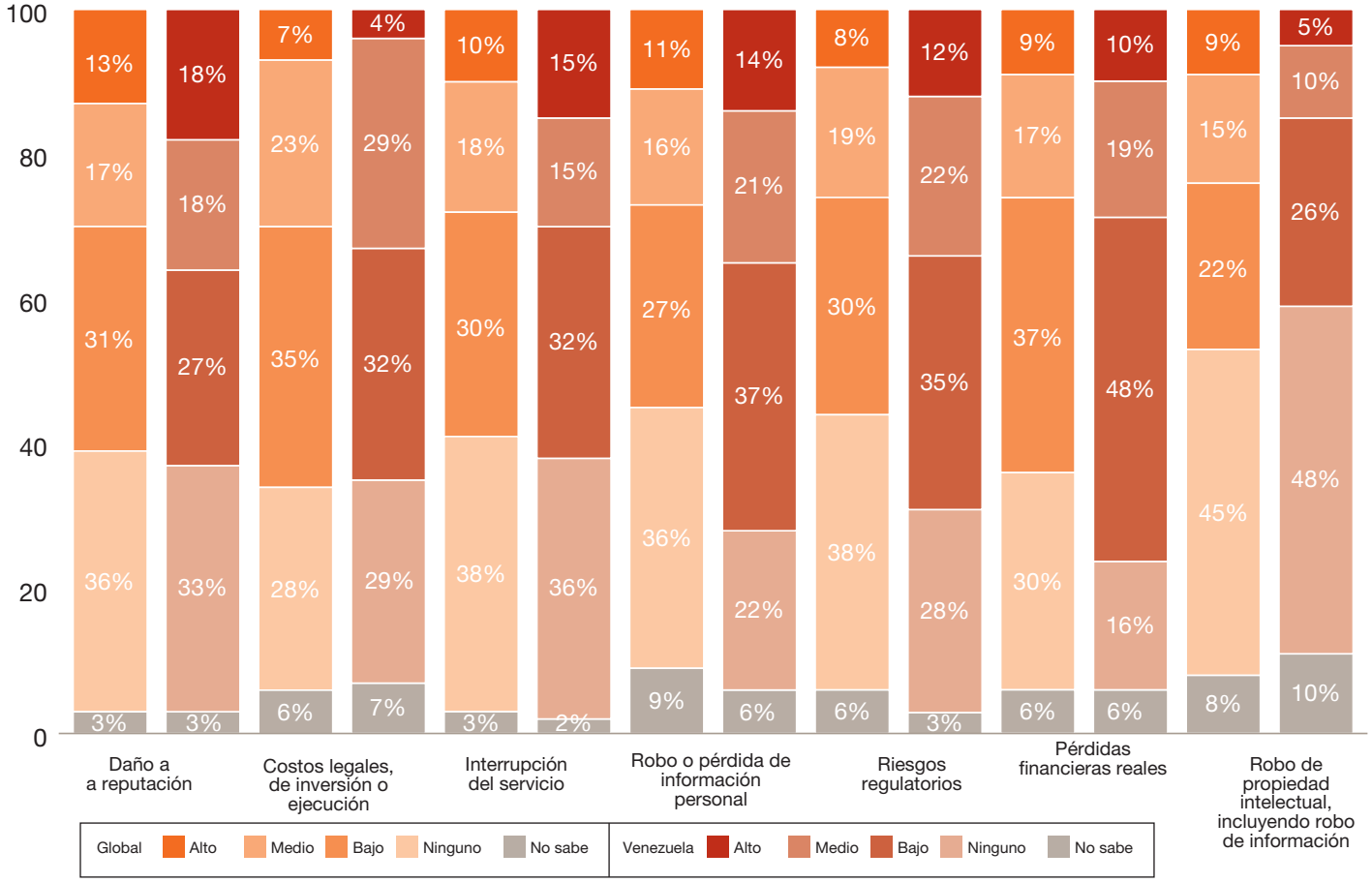
Los encuestados consideraron al daño a la reputación como el impacto más dañino de una violación cibernética, seguido de cerca por los costos legales, de la inversión o de ejecución.

Dada la insidiosa naturaleza de esta amenaza, es probable que del 56% que dijo no haber sido víctima muchos se hayan visto comprometidos sin tan siquiera saberlo, ya que hemos observado la preocupante tendencia de que los hackers se las arreglan para permanecer por largos períodos en las redes de las organizaciones sin ser detectados.

Los atacantes también son conocidos por montar ataques de distracción para ocultar actividades más dañinas. Las técnicas de distracción incluyen el uso de ataques de negación de servicio, distribuidos como medio para distraer y crear mucho ruido mientras el verdadero foco del ataque se desenvuelve lentamente y sin ser detectado.

Por lo general, en estos escenarios los hackers atacan sistemas que no les aportan valor simplemente para desviar a los equipos de respuesta a incidentes mientras que en segundo plano atacan y, disimuladamente, roban la información que les interesa.

Figura 2: Nivel de impacto del cibercrimen (según el informe de incidentes de cibercrimen en las organizaciones)



¿Qué empresas están en riesgo de cibercrimen?

Hoy en día, todas las industrias están en riesgo, incluyendo algunas que en el pasado podrían haberse considerado a sí mismas como objetivos poco probables. De acuerdo a la Encuesta sobre la Situación Global de la Seguridad de la Información de 2016, el sector que registró en 2015 el incremento más significativo en cibercrímenes fue el minorista, mientras que el financiero (aún uno de los más atacados) se niveló con muy poco crecimiento en términos de números de ataques durante los últimos 3 años.

¿Por qué las compañías (y naciones) roban propiedad intelectual?

- En muchos países desarrollados se observa un patrón de violaciones a la propiedad intelectual a gran escala. Estos no son ataques aleatorios a compañías individuales sino parte de una campaña de mayor envergadura estratégicamente organizada.
- Aunque alguna nación pueden estar detrás de algunos de estos ataques a gran escala, esto no es una cuestión de terrorismo (intentos de inutilizar infraestructuras vitales) sino de delitos económicos.
- ¿Por qué robar la propiedad intelectual de otras compañías? Porque es menos costoso en tiempo y recursos que realizar una investigación y desarrollo propio.

Los dos tipos de cibercrímenes y lo que significan para usted

Hemos avanzado mucho desde los días de los hackers adolescentes que robaban tarjetas bancarias. Aunque ha habido un encomiable y significativo incremento de la concientización y sofisticación en la detección de la identidad (o procedencia) de los atacantes, eso no quita que la competencia entre criminales y compañías continúe aún más febril que nunca, y esto para las empresas es una batalla que no podrán ganar permanentemente.

Durante los últimos años, los delitos económicos cibernéticos han evolucionado al punto que se les puede segmentar en dos categorías distintas: el tipo que roba dinero y afecta reputaciones, y el que roba propiedad intelectual y atenta contra el negocio.

- **Fraude cibernético.** Aunque los cibercrímenes monetizables como el robo de identidad y de medios de pago son los que saltan a los titulares (dados sus miles de dólares en pérdidas y múltiples víctimas) rara vez, a pesar de su alto perfil, llegan a representar una amenaza existencial para las compañías.
- **Transferencia de riqueza/ Ataques a la propiedad intelectual.** El delito económico más grave que enfrentan las organizaciones es el espionaje cibernético, el robo de propiedad intelectual (secretos comerciales, información de productos, estrategias de negociación y similares). Los profesionales cibernéticos denominan a estas violaciones como “eventos nivel extinción” y con mucha razón, porque los daños pueden alcanzar los millardos de dólares e incluir la destrucción de una línea de negocio, de una compañía y hasta de un ecosistema económico más grande. No solo estos tipos de ataques son difíciles de detectar sino que pueden no estar siquiera en el radar de amenazas de la compañía.

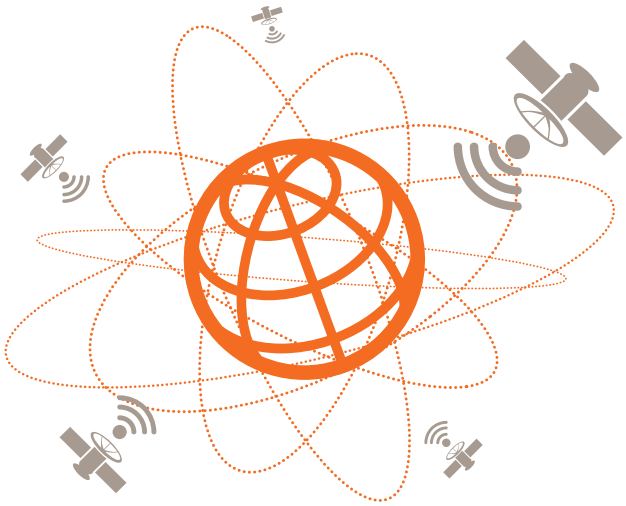
Aunque el daño a largo plazo de los ataques de trasferencia de riqueza (tanto para la entidad como para la economía) es potencialmente mucho mayor, la molestia regulatoria y el escrutinio mediático generados por el robo de tarjetas de crédito o de información personal pueden ser inmensos.

Vectores de amenazas: Las cinco categorías

Naciones
Las amenazas abarcan el espionaje y la guerra cibernética; entre las víctimas se encuentran agencias gubernamentales, infraestructura, energía y organizaciones con abundante propiedad intelectual.

Personas con información privilegiada
No sólo sus empleados sino también terceros de confianza con acceso a datos sensibles quienes no se encuentran bajo su control de manera directa.

Terroristas
Todavía una amenaza relativamente incipiente, las amenazas abarcan las interrupciones y la guerra cibernética; entre las víctimas se encuentran agencias gubernamentales, infraestructura y energía.



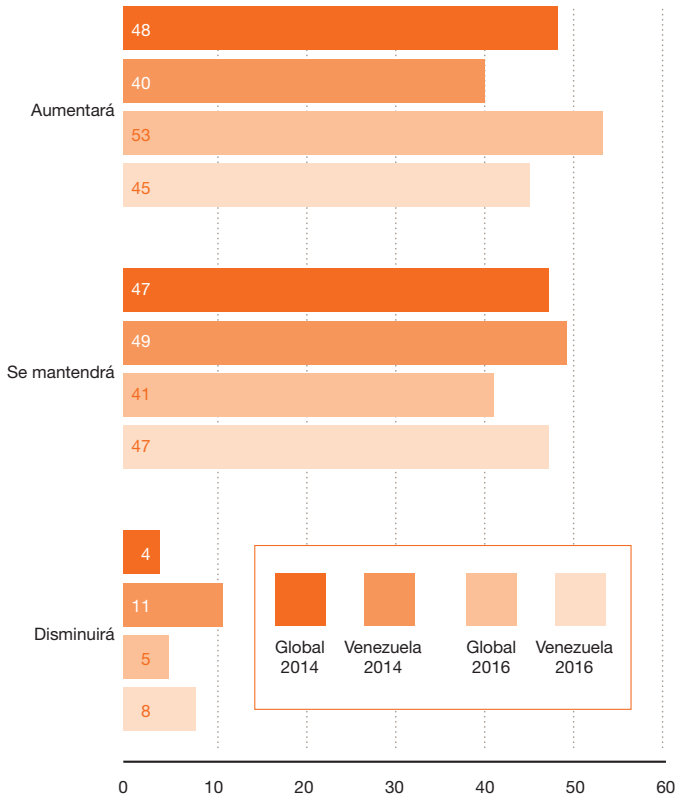
Sindicatos del crimen organizado
Las amenazas abarcan el robo de información financiera o de identificación personal (a veces con distorsiones de mercado de personas con información privilegiada); entre las víctimas se encuentran instituciones financieras, minoristas, empresas médicas y de hotelería.

Hackers activistas
Las amenazas abarcan las interrupciones del servicio enfocadas en la política o el daño a la reputación; entre las víctimas se encuentran organizaciones de alto perfil, gobiernos e incluso individuos.

¿Preparados o no?

Más de la mitad de los encuestados (53%, 10% de aumento desde 2014) observan un aumento del riesgo de las amenazas cibernéticas, tal vez debido a una mayor cobertura por parte de los medios. Sin embargo, nuestra encuesta sugiere que las compañías no están preparadas de manera adecuada para enfrentar las actuales amenazas cibernéticas.

Figura 2: Percepción de los riesgos del cibercrimen



La responsabilidad de corregir las vulnerabilidades cibernéticas comienza en los estratos más altos de la empresa. Sin embargo, nuestra encuesta sugiere que muchas juntas no son suficientemente proactivas en relación con las amenazas cibernéticas.

Por lo general, no entienden muy bien la información sensitiva de su organización a fin de evaluar los riesgos de manera adecuada, a pesar de que en diversos países las juntas tienen una responsabilidad fiduciaria con los accionistas cuando se trata de riesgos cibernéticos (Por ejemplo, la Comisión

de Valores de Estados Unidos ha emitido una alerta que los exámenes futuros considerarán las capacidades de respuesta cibernética de las compañías[1]) . Asombrosamente, menos de la mitad de los miembros de las juntas realmente solicitan información sobre el estado de preparación cibernética de su organización.

Solo el 37% de los encuestados a nivel Global (40% en Venezuela), la mayoría perteneciente a la industria regulada de servicios financieros, cuentan con un plan de respuesta a incidentes totalmente operativo. Tres de cada diez encuestados no tienen ningún plan, y de ellos, casi la mitad considera que no lo necesita.

Figura 3: Frecuencia de las solicitudes por parte de la junta de información sobre el estado de preparación cibernética

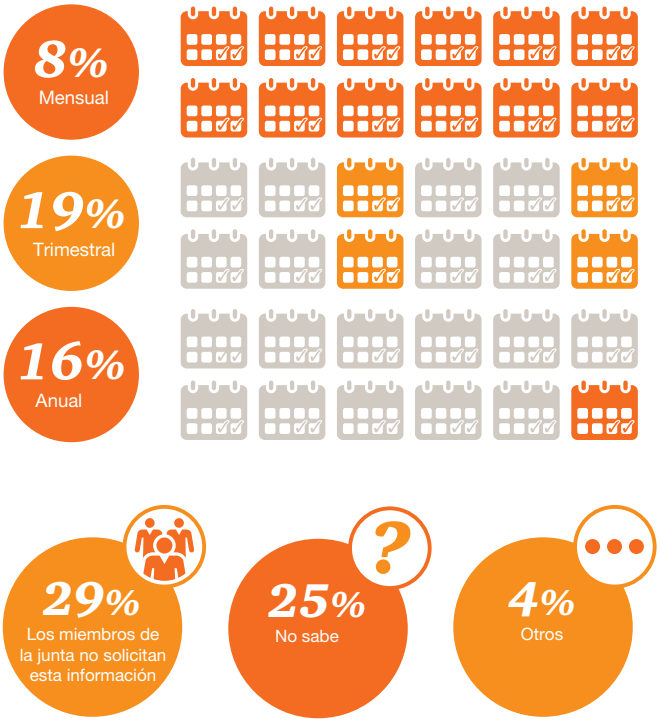
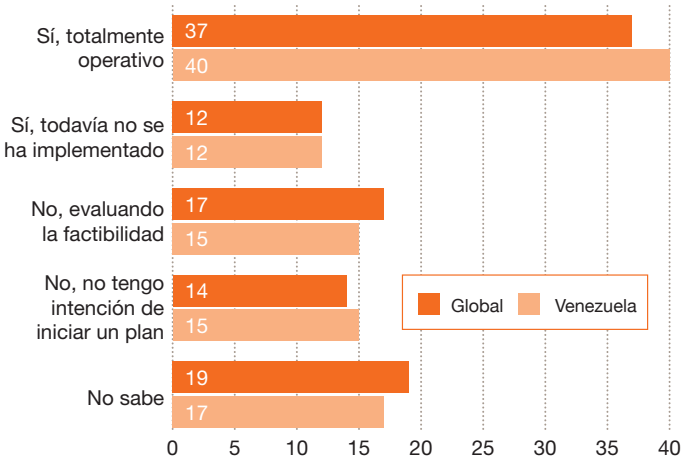


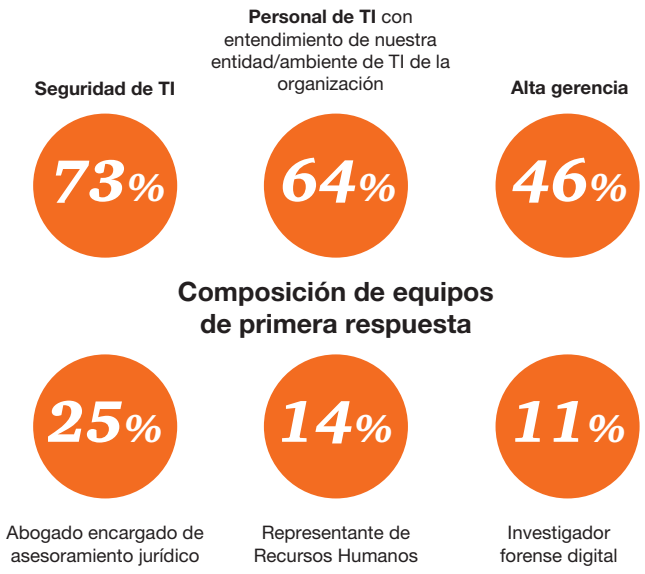
Figura 4: ¿Las organizaciones cuentan con un plan de respuesta a incidentes para enfrentar los ataques cibernéticos?



1) https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

En caso de presentarse una cibercrisis, solo cuatro de diez compañías cuentan con personal "totalmente capacitado" para actuar como equipos de primera respuesta, de los cuales la inmensa mayoría (73%) son personal de TI.

Figura 5: ¿Las organizaciones han seleccionado equipos de primera respuesta contra el cibercrimen?



Si bien es cierto que TI desempeña un papel primordial al detectar e intentar desviar un ataque, cabe destacar que menos de la mitad de los equipos de primera respuesta estaban integrados por miembros responsables de la gestión de alto nivel de la crisis: alta gerencia (46%), legal (25%), Recursos Humanos (14%), entre otros. Solo uno de cada diez equipos de respuesta a incidentes incluía investigadores forenses digitales.

Estos resultados sugieren que muchas organizaciones, en un comprensible apuro por contener la violación y levantar sus sistemas para que funcionen nuevamente, corren el riesgo de pasar por alto una posible evidencia crucial. Posteriormente, esto podría comprometer su capacidad para imponer castigos y, lo que es aún más importante, entender cómo ocurrió la violación.

En el futuro inmediato, una respuesta poco coordinada también podría limitar la capacidad de la organización para investigar todas las áreas que han sido realmente objeto de violaciones, sobre todo si se toma en cuenta el uso frecuente de las técnicas de desviación de los hackers.

Finalmente, la precipitación excesiva en responder a un ataque puede obstaculizar la capacidad de una compañía para comprender de manera cabal el impacto holístico de la violación y comunicarse de manera apropiada con los grupos de interés internos y externos, incluyendo los medios. Esto podría ocasionar un daño a la reputación; ubicándose en la encuesta de este año como el impacto más perjudicial de una violación cibernética.

Detectando una violación: gestión de crisis

¿Qué ocurre cuando detecta una violación? Es fundamental disminuir el intervalo entre la detección eficaz y la respuesta, e interrumpir los impactos de negocio perjudiciales tan pronto como sea posible. Después de convocar a sus equipos de primera respuesta a una crisis y cibernética, a continuación mencionamos algunas medidas que puede adoptar:

- Recaudar los principales hechos sobre la violación y averiguar si todavía continúa. Debido a la creciente complejidad de las redes, puede ser difícil identificar como un actor hostil podría haber tenido acceso a la red. Las sofisticadas herramientas analíticas de datos y forenses, algunas de las cuales se pueden obtener a través de expertos externos y otras mediante encargados de ejecutar la ley, son cruciales para esta fase.
- Considerar que a veces un ataque detectado puede ocultar incursiones más profundas en su organización y que en algunas situaciones detectar una violación y comenzar a frenar el daño puede demorarse semanas y no horas.
- Decidir si es necesaria (y en qué medida) la participación de los organismos encargados de ejecutar la ley y si son locales o federales. Existen diversos factores que se deben tomar en cuenta y dependerán del tipo y escala del ataque. (Éste es un tema importante ya que casi la mitad de los encuestados dudan de la capacidad por parte de gobierno para investigar el cibercrimen).
- Considerar los riesgos secundarios. Por ejemplo, una simple violación a un correo electrónico puede revelar secretos a los adversarios. En caso de violación de las redes, y si la compañía utiliza voz sobre protocolo de internet (VOIP, por sus siglas en inglés)/servicios telefónicos en red, es probable que los teléfonos también se vean comprometidos.
- Finalmente, cuando ocurre una violación, recuerde que una investigación cibernética sigue siendo esencialmente una investigación y por lo tanto se aplican los principios de una investigación criminal. Al enfocarse en detener un ataque continuo y estar nuevamente en línea, es fundamental no destruir evidencia involuntariamente que podría ayudar a esa investigación y a prevenir el próximo ataque.

La importancia de una defensa de múltiples niveles

Toda la empresa es responsable y desempeña un papel crucial en las amenazas cibernéticas y las mitigaciones. Sin embargo, a pesar de que hemos presenciado avances importantes relativos a la sofisticación y la preparación cibernética desde nuestra última encuesta, la mayoría de las compañías todavía no están preparadas adecuadamente para entender los riesgos que enfrentan ni para anticipar y manejar los incidentes de manera efectiva.

Demasiadas organizaciones están sufriendo pérdidas cibernéticas porque no comprendieron los conceptos básicos. Desde una participación insuficiente por parte de la junta (o preparación/conocimiento), a deficientes configuraciones de los sistemas y controles inadecuados sobre terceros con acceso a la red, las compañías están sufriendo de errores no forzados, frecuentemente dejando la puerta cibernética entreabierta a los intrusos.

Es fundamental que las juntas incluyan el cibercrimen en sus evaluaciones rutinarias de riesgo, comuniquen el plan a todos los niveles de las líneas organizacionales y discutan de manera específica con el departamento de TI en qué momento desean recibir alertas de una violación.

Se deben entender y prever las amenazas cibernéticas de la misma manera que cualquier amenaza o interrupción potencial de negocio (tal como actos de terrorismo o desastre natural). Esto se debe realizar mediante un plan de respuesta, roles y responsabilidades, monitoreo y planificación de escenarios.

Por eso, las compañías líderes están integrando los ejercicios de gestión de crisis como un elemento fundamental de su ciberseguridad y estrategia de respuesta a incidentes.

Dichas compañías realizan de manera periódica ejercicios de simulación examinando escenarios específicos y realizan pruebas de presión a sus planes de respuesta, identificando cualquier brecha o deficiencia.

Las amenazas y mitigaciones de TI son responsabilidad de toda la organización

Nivel ejecutivo:

- Establecer una clara estrategia de ciberseguridad.
- Asegurar que se recibe y procesa información de calidad.
- Ejecutar programas de concienciación en materia de seguridad de usuarios.
- Permitir gastos basados en estrategias sobre la seguridad.

Auditoría y riesgo:

- Asegurar un entendimiento y cobertura cabal de los riesgos de tecnología.
- Realizar una debida diligencia por adelantado para mitigar los riesgos asociados con terceros.
- Abordar los riesgos asociados con los sistemas operacionales (no financieros).
- Abordar los asuntos fundamentales de auditoría de TI.

Legal:

- Mantenerse actualizado ante el cambiante ambiente reglamentario.
- Monitorear las decisiones que toman los organismos reguladores en respuesta a los incidentes de ciberseguridad.
- Ser consciente de los factores que pueden invalidar las pólizas de seguro.

TI:

- Realizar evaluaciones de preparación para las investigaciones forenses.
- Ser consciente del cambiante panorama de amenazas y atacar los vectores.
- Probar los planes de respuesta a incidentes.
- Implementar procesos eficaces de monitoreo.
- Emplear nuevas estrategias: simulaciones de ataque cibernético, ludificación de capacitación de seguridad y sesiones de concienciación y análisis de datos de seguridad.

Los planes no son nada — la planificación es todo

Muchas compañías están integrando los ejercicios periódicos de gestión de crisis como un elemento fundamental de su ciberseguirdad y estrategia de respuesta a incidentes. Dichas compañías realizan de manera periódica ejercicios de simulación examinando escenarios específicos y posteriormente realizan pruebas de presión a sus planes de respuesta a incidentes, identificando cualquier brecha o deficiencia.

Lamentablemente, los planes (parafraseando a un general prusiano) casi nunca sobreviven a su primer contacto con la realidad. Usualmente, la realidad presenta circunstancias imprevistas a los equipos de repuesta a incidentes y a los gestores de la crisis.

Una respuesta efectiva a la crisis requiere las destrezas, el conocimiento y la experiencia de una gama de funciones corporativas trabajando en conjunto: legal, recursos humanos, medios y relaciones públicas, comunicaciones, asesoramiento privado, auditoría y riesgo, finanzas, seguridad corporativa, relaciones entre los organismos reguladores y los encargados de ejecutar la ley, relaciones con accionistas, así como también las unidades de negocio de primera línea y la gerencia regional.

El proceso, el "plan para un plan", que proviene de un programa regular de ejercicios es mucho más valioso que el plan elaborado. Éste genera una "memoria muscular" para la respuesta a incidentes, haciendo que el proceso, el ambiente y la toma de decisiones sean más sencillos para los grupos de interés quienes estarán sometidos a presión en una crisis. De esta manera, se pueden concentrar en resolver el problema que se les presenta.

Una crisis corporativa en ciberseguridad es uno de los problemas más complejos y desafiantes que puede enfrentar una organización. Las violaciones cibernéticas requieren comunicaciones sofisticadas y estrategias de investigación, incluyendo capacidades forenses y analíticas significativas, ejecutadas con precisión, agilidad y mente fría

A pesar de que es potencialmente desalentador, incrementar la preparación tiene su lado positivo ya que se puede observar como una prueba de esfuerzo organizacional que puede y debe propiciar mejoras en sus procesos. En el actual panorama de los riesgos, el grado de preparación de una compañía para enfrentar una crisis cibernética también puede ser un indicador de ventaja competitiva y, en última instancia, su supervivencia.

> *"La falta de conceptos básicos de preparación cibernética puede dejar entreabierta la puerta de la ciberseguridad a los intrusos".*
>
> David Burg, Líder de Ciberseguridad de PwC USA y Global.

Ética y Cumplimiento

Lograr el equilibrio entre la confianza y el cumplimiento puede ser la diferencia entre retener o perder a los mejores talentos. En el mercado actual, que vive en continua evolución, es vital tener una estrategia para alinear la ética y el cumplimiento con los riesgos de negocio

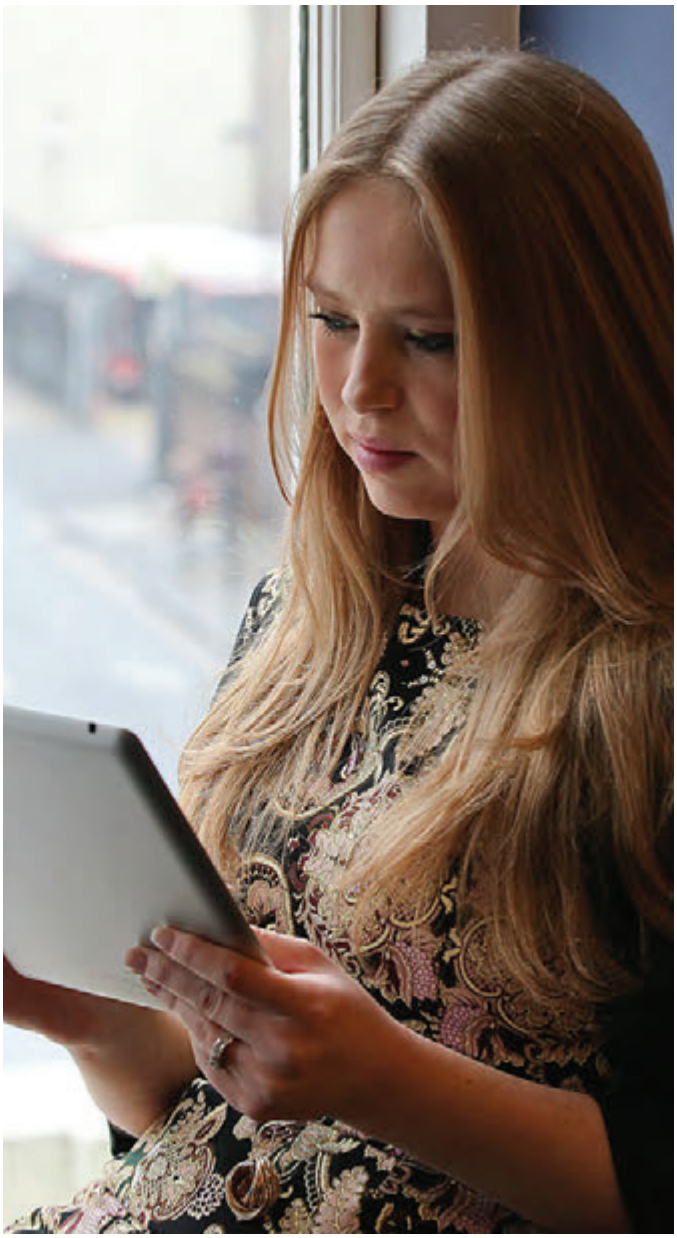
Ética y cumplimiento: alineando los riesgos y las responsabilidades con los valores y la estrategia

Los resultados de nuestra encuesta indican que no solo están aumentando los números de riesgos de delitos económicos, sino también la complejidad de dichos riesgos y el papel que desempeña la tecnología en su evolución. Esto no es extraño en un ambiente de negocios caracterizado por una creciente globalización, cumplimiento supervisado y una mayor demanda de responsabilidad pública.

Por esta razón, su capacidad para identificar y mitigar los riesgos de cumplimiento debe evolucionar a un ritmo rápido. Es esencial contar con un enfoque de ética y cumplimiento basado en el riesgo; un enfoque que parta de un entendimiento holístico de sus riesgos de delitos económicos y un entendimiento de dónde yacen sus debilidades de cumplimiento.

Desde esa posición de claridad, se puede crear un programa efectivo que mitigue dichos riesgos y así alcanzar las metas de negocio. Sin embargo, un alarmante 22% de las organizaciones a nivel Global (23% en Venezuela) no han realizado una evaluación de riesgos de fraude en los últimos 24 meses.

Si bien es cierto que el número de organizaciones que reportan fraude en general (36%) se han mantenido bastante estables en comparación con años recientes, una lectura más atenta de los datos revela matices importantes. La mayoría de los fraudes “tradicionales” (tales como malversación de activos, fraude contable, y soborno y corrupción) han disminuido relativamente con respecto a sus niveles de 2014. Otros delitos, en particular cibercrimen, legitimación de capitales y uso de información privilegiada, han permanecido en el mismo nivel o han aumentado. El cibercrimen ha aumentado en un tercio en sólo dos años (32% vs. 24% a nivel Global).



La modesta caída en algunas de estas métricas relativas a nuestra última encuesta podría estar fomentando una falsa sensación de seguridad. Existe el riesgo de que las compañías no consideren útil invertir más recursos en programas de ética y cumplimiento si no han experimentado un aumento de los delitos económicos.

De hecho, muchas organizaciones han reducido los costos tanto en el número de empleados como en la capacitación, o han ampliado las responsabilidades existentes de su equipo de cumplimiento para incluir deberes adicionales. Esto puede ser un error de cálculo estratégico ya que en muchas industrias y geografías, los riesgos de delitos económicos no están disminuyendo y una memoria corporativa a corto plazo puede ser peligrosa.

El punto fundamental es que mientras los riesgos y las amenazas están en constante cambio, la esencia de un programa de cumplimiento exitoso consiste en prever y abordar la evolución del panorama de riesgos.

Una desconexión

Es necesario considerar los incidentes ocurridos con organizaciones multinacionales que se asumía cuentan con sólidos programas de ética y cumplimiento. ¿Estas fallas indican que dichos programas no siguen el ritmo de los cambiantes riesgos de negocio? ¿Están enviando mensajes contradictorios? ¿O existe una razón más profunda para la desconexión?

Los números apuntan a una brecha de percepción entre lo que suponen y dicen los directores ejecutivos y las juntas y lo que está ocurriendo realmente en el negocio, especialmente entre la alta y media gerencia. De acuerdo con nuestra encuesta, la gerencia media es más propensa a cometer fraude (aunque existen variaciones según la región). Además, es más probable que sienta que los valores no están claramente establecidos o que los programas de incentivos no son justos.

La 19a Encuesta Global Anual a los CEO de PwC confirma este asunto de una brecha entre la intención y la ejecución. Entre las principales amenazas que enfrentan las organizaciones, el porcentaje de directores ejecutivos que mencionó el soborno y la corrupción observó el mayor aumento de 51% a 56%.

Otra amenaza clave reportada fue la falta de confianza en el negocio, destacando la importancia a los equipos de liderazgo de contar con un programa corporativo de ética sofisticado y creíble.

Asegurando un programa de cumplimiento idóneo

¿Cómo la alta gerencia asegura que lo que proclama se está poniendo en práctica? ¿Cómo se incentiva el cumplimiento? ¿Cómo se mide?

A continuación presentamos cuatro áreas de interés clave para incrementar la eficacia de programas de ética y cumplimiento, examinados en el resto de la presente sección:

- Gente y cultura. Mantener un programa basado en valores, midiendo y recompensando los comportamientos deseados.
- Roles y responsabilidades. Asegurar que sean claros y estén alienados de manera correcta con los riesgos actuales.
- Áreas de alto riesgo. Mejor implementación y prueba del programa en mercados y divisiones de alto riesgo.
- Tecnología. Mejor uso de herramientas de detección y prevención, incluyendo importantes análisis de datos.

Cinco pasos hacia un programa de cumplimiento más eficaz

- Asegurar que su programa esté acorde con la estrategia corporativa; y comunicar esta alineación.
- Evaluar y replantear potencialmente la identidad de su función de cumplimiento a fin de que se adapte a un ambiente donde los riesgos y amenazas cambian continuamente.
- Asegurar que todos los titulares de obligaciones de cumplimiento entiendan cabalmente el panorama general de cumplimiento en toda la organización y el alcance de sus propias responsabilidades dentro de la misma.
- Recordar que las políticas y la capacitación sobre valores no son suficientes ya que es fundamental contar con un compromiso creíble y consistente en toda la organización.
- No reducir el personal cuando los riesgos estén en aumento.

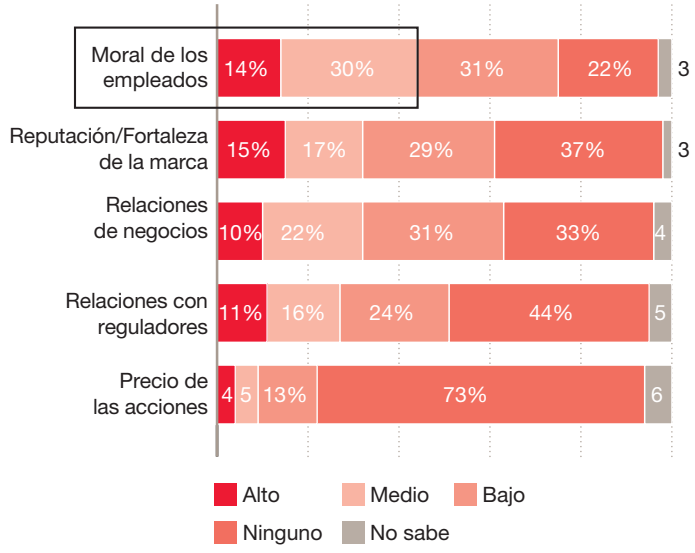
Gente y cultura: su primera línea de defensa

Las decisiones desacertadas impulsadas por el comportamiento humano son la causa principal de los delitos económicos.

Por consiguiente, es evidente que la solución debe comenzar con la gente. Ello significa no solo inculcar claros procesos y principios a sus empleados, sino también crear una cultura donde el cumplimiento esté profundamente arraigado en los valores y a la estrategia general de la organización.

Nuestros encuestados afirmaron que el mayor daño organizacional que experimentaron como resultado de los delitos económicos no se reflejó en el precio de las acciones o incluso en las relaciones con los organismos reguladores. Se reflejó en el daño a la moral del empleado: el 44% de los encuestados experimentaron mediano o alto impacto. El 32% de los encuestados también mencionaron que el daño a la reputación tiene un impacto importante. En ambos casos, la naturaleza de cómo se percibe un negocio, tanto dentro como fuera del mismo, era el área de mayor preocupación. Esto pone de relieve el papel clave que desempeñan los valores en una estrategia de negocios exitosa.

Fig 1: Impacto de los delitos económicos



Un programa de cumplimiento basado en valores también ayuda a atraer y mantener a los mejores y más brillantes talentos a su organización. Las personas responsables desean trabajar para compañías responsables que hagan realidad sus creencias éticas y practiquen lo que predican.

Un programa de cumplimiento bien diseñado, enfocado en respaldar comportamientos éticos, puede ofrecer un claro beneficio estratégico al negocio.

Sin embargo, para que su programa de cumplimiento sea eficaz debe incluir no solo un código de conducta actualizado, una política y algunas horas de capacitación. Esencialmente, debe abordar la profunda conexión entre los valores, los comportamientos y la toma de decisiones.

En vez de intentar abordar o anticipar cada riesgo a medida que se presenta, un enfoque sofisticado consistiría en inculcar en la gente una apreciación subyacente de cómo y por qué se deben tomar las decisiones correctas en ciertas circunstancias.

La necesidad de adoptar este enfoque está fundamentada en nuestros hallazgos de la encuesta que señalan que en las regiones donde la alta gerencia cometía más fraudes económicos (tales como Asia y el Pacífico, América del Norte y Europa Occidental), uno de los mayores motores era el incentivo o la presión por cumplir con una labor (es decir, tomar la decisión equivocada en un momento decisivo).

Tomar en cuenta y medir las brechas (percepción)

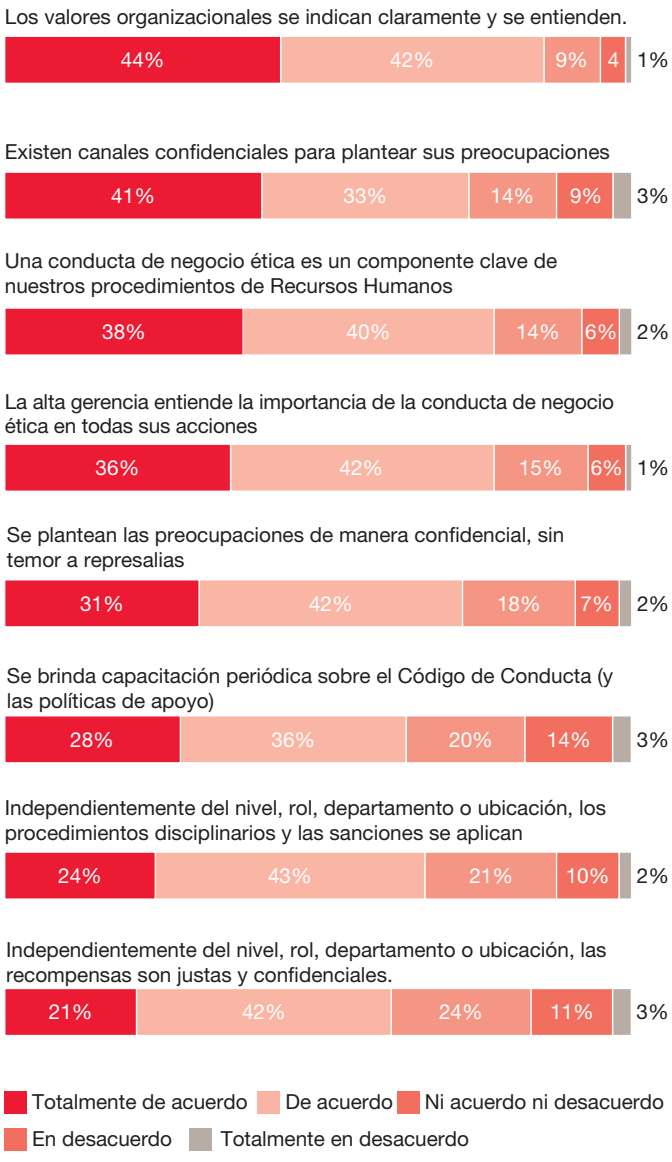
Casi todos los encuestados afirmaron que su organización indicó claramente y entendió los valores organizacionales (86% Global – 87% Venezuela); los directores ejecutivos y directores de finanzas expresaron su opinión de manera rotunda en este sentido. Sin embargo, muestra encuesta identificó áreas donde la alta gerencia y las juntas no percibían las mismas realidades que las de la gerencia media. El 90% de los directores ejecutivos consideraron que los valores eran claros y se entendían; este porcentaje se redujo a 84% para los gerentes.

Brechas de percepción

Un tema recurrente en los resultados de nuestra encuesta es el de las brechas de percepción, que pueden originar resultados no deseados. Estos resultados se pueden desglosar en tres categorías básicas:

- La brecha entre lo que la junta considera y promueve, y lo que la gente dentro de la organización realmente observa, cree y hace diariamente.
- La brecha entre las intenciones y el financiamiento para cumplirlas.
- La brecha entre la alta y media gerencia al supervisar el cumplimiento.

Fig 2: Percepciones de ética y cumplimiento de negocio



Nuestra experiencia nos indica que ésta es una brecha significativa en términos estadísticos, entre lo que la alta gerencia piensa y dice, y lo que la gerencia media percibe, que puede generar un vacío dentro de la organización. A pesar de tener las mejores intenciones, esta situación puede originar actividades poco éticas.

Alineando los roles y las responsabilidades: ¿quién manda aquí?

Nuestra encuesta reveló que aproximadamente uno de cada cinco (18%) encuestados desconocía la existencia de un programa formal de ética y cumplimiento en sus compañías. Y resulta interesante que el porcentaje de directores ejecutivos, miembros de la junta y directores de operaciones que afirmó no tener conocimiento de un programa formal de ética y cumplimiento fue incluso superior, alcanzando un 23%.

Del 82% de las organizaciones que han establecido un programa formal de ética y cumplimiento de negocio, la responsabilidad por dicho programa está muy dispersa entre los roles.

Por lo general, es poco probable que las organizaciones con menos de 1.000 empleados cuenten con un programa formal de ética y cumplimiento. A pesar de que podrían estar haciendo hincapié en las necesidades reales del negocio en lugar de adoptar un enfoque "poco integral", esto puede plantear un desafío, ya que muchas de estas organizaciones están enfrentando un panorama de riesgos similar al de organizaciones más grandes.

Fig 3: ¿Cuántas organizaciones tienen un programa formal de ética y cumplimiento de negocio?

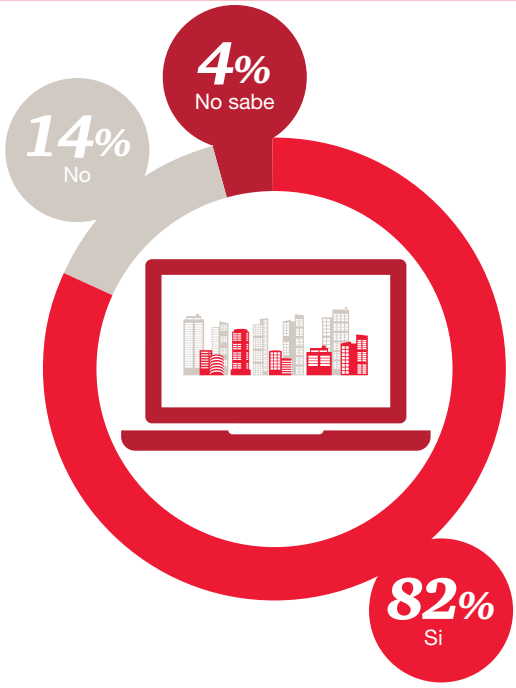
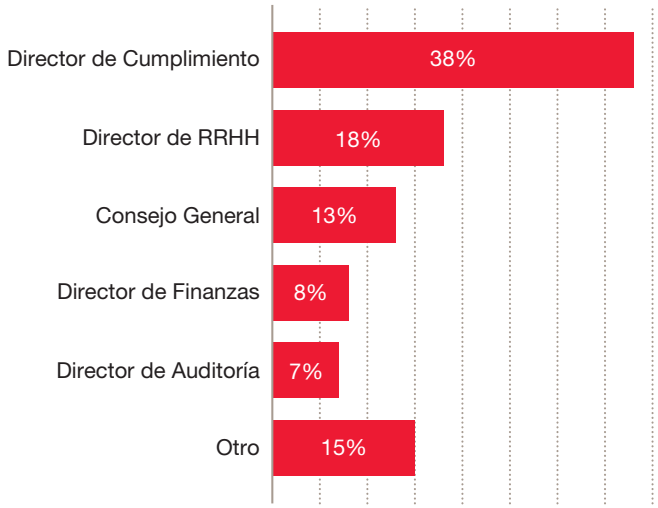


Fig 4: ¿Quién es responsable de los programas de ética y cumplimiento de negocio?



¿Quién tiene la obligación? Adoptar un enfoque basado en riesgos

Es de vital importancia que todas las personas en el negocio, no solo los profesionales de cumplimiento, entiendan sus roles y responsabilidades, asegurando que el negocio esté alineado y que se ejecute su programa de prioridades, ética y cumplimiento. Sin embargo, muchas compañías todavía tienen una cierta confusión sobre quien es el "titular" de esta responsabilidad.

La "titularidad" del programa debe pertenecer a la gerencia de primera línea y de las unidades de negocios, quienes son responsable de entender los riesgos y determinar el apetito de su unidad por dichos riesgos. Por otra parte, la función de cumplimiento está a cargo de la supervisión y orientación. Sin embargo, en algunas organizaciones existe la tendencia de observar el cumplimiento como un tipo de póliza de seguros que les permite asumir una responsabilidad pasiva.

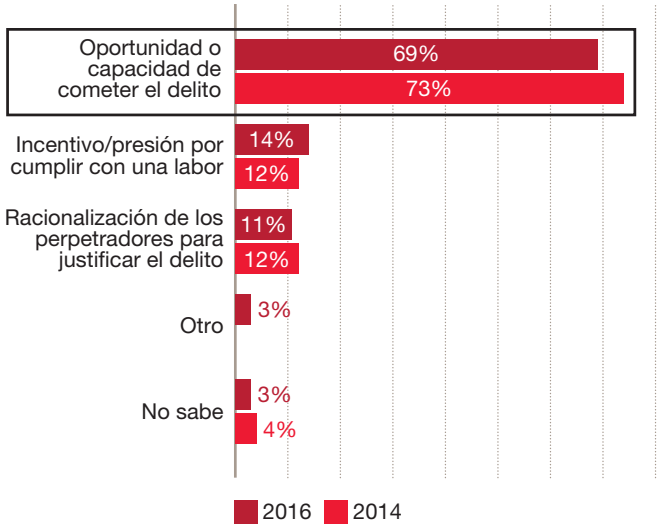
Finalmente, todos los miembros del negocio deben trabajar por obtener los mismos resultados de cumplimiento. Las organizaciones enfocadas en la innovación se posicionan como una "comunidad de cumplimiento" más amplia, en la cual los roles y responsabilidades de la ética y el cumplimiento forman parte de la actividad cotidiana de todos.

Las grandes organizaciones son más susceptibles al fraude en contratación pública y soborno y corrupción.

La oportunidad para delinquir llama a la puerta. ¿Pero quién está escuchando?

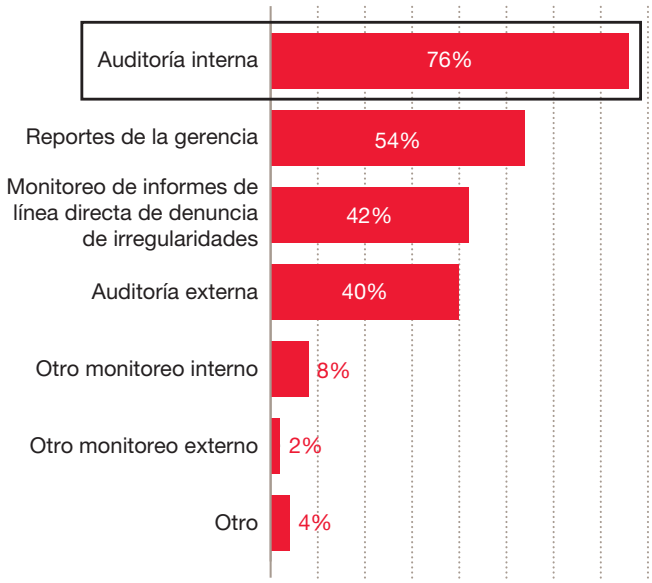
Siete de cada diez organizaciones consideran que la oportunidad es el principal motor de los delitos económicos internos. Esto tiene un peso mucho mayor que los otros dos elementos del triángulo del fraude, que son el incentivo/ la presión por cumplir con una labor y la racionalización del delito.

Fig 5: Factores que contribuyen a los delitos económicos cometidos por actores internos



La gran mayoría parece estar a favor de los ambientes de control más fuertes como un medio para reducir esta oportunidad, pero nuestros resultados preliminares indican que los ambientes de control corporativos hoy son 7% menos eficaces para detectar y prevenir los delitos económicos que hace dos años. Más de tres cuartos de los encuestados (76% a nivel Global y 71% en Venezuela) afirmaron que confían en su función de auditoría interna (AI) como parte de su enfoque para evaluar la efectividad de sus programas de cumplimiento. Aun cuando auditoría interna es una pieza importante del marco de evaluación de la efectividad de un programa de cumplimiento, no es por si misma suficiente para asegurar el cumplimiento, ya que sus intervenciones son tanto periódicas como históricas.

Fig 6: Evaluación de programas de ética y cumplimiento de negocio



Asimismo, el perfil de riesgo de fraude ha variado (por ejemplo, el aumento del cibercrimen), la incidencia de algunos tipos de fraude está aumentando o persiste en ciertos tipos de organizaciones.

Por ejemplo, las grandes organizaciones (con más de 1.000 empleados) son susceptibles al fraude en contrataciones públicas y al soborno y corrupción (7% y 3% mayores, respectivamente, que el promedio global) a medida que los esquemas de fraude esquivan los marcos de control establecidos. De hecho, algunos enfoques de monitoreo han adquirido notoriedad y son susceptibles de elusión.

En vista de que la prevención debe ocurrir idealmente en el momento de tomar decisiones estratégicas, los mecanismos de auditoría interna se deben integrar con los reportes de la gerencia y el monitoreo en tiempo real del negocio, a fin de que los problemas se detecten y prevengan a tiempo. Nuestros encuestados del sector financiero indican que los reportes de la gerencia son un factor clave para asegurar la efectividad de los programas de cumplimiento: el 60% utiliza esta herramienta.

Actualmente, sólo el 8% de los encuestados indican que están utilizando otros enfoques de monitoreo interno más prometedores tales como análisis de datos o análisis predictivos, los cuales son más difíciles de eludir.

Implementación en áreas de alto riesgo: el diablo está en los detalles

A fin de inculcar un comportamiento ético dentro de una organización global se requiere una mejor capacitación, comunicación continua y reportes gerenciales. Pero este comportamiento también debe incluir el entendimiento de que los riesgos de un país y los de una división no son exactamente los mismos, incluso en las áreas de alto riesgo. Por lo tanto, se debe implementar un sofisticado programa de cumplimiento global articulado perfectamente con las realidades locales.

Pongamos como ejemplo el conocido riesgo transaccional de soborno y corrupción. Los organismos reguladores han demostrado cada vez más su voluntad de responsabilizar a las compañías de un comportamiento poco ético que ocurre lejos de la sede central. Asimismo, la gerencia tiene que asegurarse que toda su gente esté actuando de manera correcta todo del tiempo.

¿Cómo responden las organizaciones al riesgo? Tener un código de conducta reconocido es un punto de partida, pero si los empleados no saben cómo usarlo en su toma de decisiones cotidiana, esto es poco eficaz para mitigar los riesgos de cumplimiento. El código y otras políticas se deben integrar a través de la capacitación, las comunicaciones frecuentes, la recompensa y el reconocimiento cuando se toman buenas decisiones, y aplicar los procedimientos disciplinarios cuando se toman malas decisiones.

A pesar que el 86% de las organizaciones a nivel mundial (88% en Venezuela) afirmaron que disponían de un código de conducta, solo el 64% (73% en Venexuela) indicó que la capacitación se impartía periódicamente y estaba respaldada por una comunicación y asesoramiento regulares. Esta diferencia era particularmente abrupta para los encuestados de África, Europa Occidental, Medio Oriente y Europa Oriental.

Fig 7: Porcentaje de organizaciones con exigencias reportadas de soborno

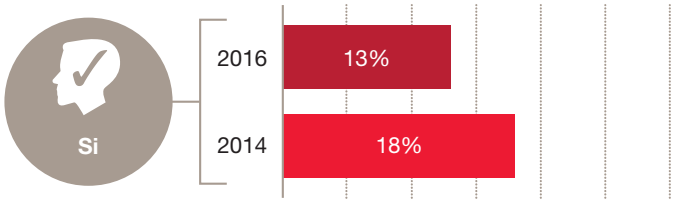
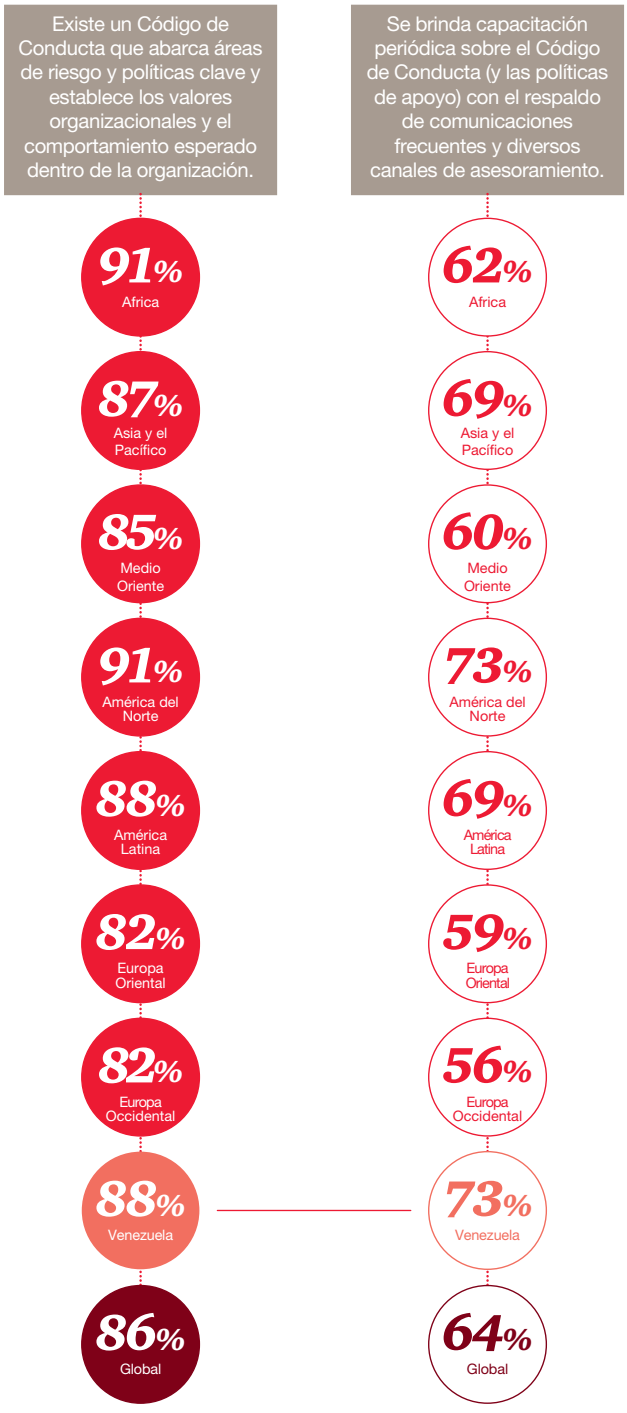


Fig 8: Estadísticas relativas a los correspondientes códigos de conducta y capacitación en las organizaciones



Existe un Código de Conducta que abarca áreas de riesgo y políticas clave y establece los valores organizacionales y el comportamiento esperado dentro de la organización.
Se brinda capacitación periódica sobre el Código de Conducta (y las políticas de apoyo) con el respaldo de comunicaciones frecuentes y diversos canales de asesoramiento.

En líneas generales, el 91% de los encuestados a nivel Global (85% en Venezuela) estuvieron de acuerdo con la declaración que la alta gerencia expresó sobre que el soborno no es una práctica legítima. Esto fue consistente en todas las regiones e industrias. Sin embargo, todavía observamos que se han reportado numerosos incidentes y, en muchas regiones, un número cada vez mayor de organizaciones prevén sufrir soborno y corrupción en los próximos 24 meses.

Fig 9: Estadísticas clave de todas las regiones

Las regiones que consideran muy altas las probabilidades de experimentar soborno y corrupción en los próximos 24 meses – África, Medio Oriente, Asia y el Pacífico - son también las regiones con el mayor número de encuestados que reportaron un aumento planificado en el gasto por concepto de cumplimiento para los próximos 24 meses (59%, 48% y 47%, respectivamente). Sin embargo, un aumento en el gasto no siempre es la solución al problema de fondo. Es necesario que las organizaciones se aseguren de emplear las herramientas, tecnologías y técnicas adecuadas para obtener el máximo beneficio de su inversión en cumplimiento.

Tecnología: no es la panacea, pero sí una poderosa herramienta

Hoy por hoy existen diversas herramientas especializadas - incluyendo análisis de datos masivos (Big-Data Analytics) capaces de ofrecer un monitoreo más efectivo - que pueden aumentar los niveles de cumplimiento en las operaciones mediante la gestión de una variedad de datos estructurados y no estructurados.

Sin embargo, aparte de los sistemas de monitoreo de transacciones (cuyos principales usuarios son clientes del sector financiero), son muy pocas las organizaciones que utilizan este tipo de tecnologías para ayudar en la detección y prevención de los delitos económicos. Actualmente, solo 8% de los encuestados reportó el uso de otras herramientas de monitoreo interno, como el análisis de datos.

Pero cuidado: las organizaciones podrían ser presa de errores tecnológicos. Es probable que algunas organizaciones, guiadas por un proceso de evaluación de riesgos inadecuado, apliquen técnicas de monitoreo exageradas en algunas áreas (con un efecto limitado) y ninguna en otras áreas. Otras organizaciones, por desconocimiento, podrían duplicar sus gastos al utilizar múltiples herramientas. Existen otras que insisten en hacerlo bajo la directiva de "por cumplir" o "porque es lo que debería hacer" - y no siempre recolectan o utilizan apropiadamente los datos que de allí se recolectan, por lo que suelen abandonar precozmente los ejercicios de análisis de datos antes de comprobar su valor.

Hemos observado que el mejor lugar para comenzar no es en el monitoreo de transacciones en el espacio de "Big Data", sino más bien en las evaluaciones de riesgo de los "datos pequeños". Lo más importante es reunir datos consistentes y comparables - algo que parece simple, pero que no lo es.

El modelo óptimo abarca los diversos riesgos que una organización enfrenta y permite reportar por unidad de negocio, ubicación geográfica o por terceros. Para lograr esto son necesarias tres cosas:

- Una taxonomía de riesgo consistente
- Transparencia en la medición de riesgos
- Una plataforma común de datos

Estas condiciones, así como un modelo operativo y de gobierno corporativo centralizado, pueden ayudar a evaluar la amplia gama de iniciativas para monitoreo de transacciones que se emplean en la actualidad - y a concentrarse en torno a aquellas orientadas a las verdaderas amenazas de su empresa. En última instancia, el enfoque no debe limitarse a la tecnología per se, sino a lo que ésta permite realizar. Los datos nunca serán la panacea, pero si se emplean de manera efectiva pueden ofrecer a las compañías una fortaleza adicional para adelantarse a los riesgos de cumplimiento.

Legitimación de capitales y financiamiento al terrorismo

Legitimación de capitales y financiamiento al terrorismo:

¿Cómo responderá a un ambiente regulatorio que cambia tan aceleradamente?

La legitimación de capitales destruye valor. Facilita la comisión de delitos económicos y actividades nefastas como corrupción, terrorismo, evasión de impuestos, y tráfico de drogas y de personas, mediante la posesión o transferencia de los fondos necesarios para cometer estos delitos. Puede ser perjudicial para la reputación de la empresa y sus finanzas.

Se estima que las transacciones de legitimación de capitales en el mundo se encuentran entre 2% a 5% del PIB mundial, aproximadamente USD 2 billones al año. Sin embargo, de acuerdo con la Oficina de las Naciones Unidas contra las Drogas y el Delito (UNODC por sus siglas en inglés), actualmente menos de 1% de los flujos financieros ilícitos son incautados por las autoridades.

Con la creciente notoriedad de los ataques terroristas, la legitimación de capitales y el financiamiento al terrorismo se convirtieron en asuntos prioritarios para los gobiernos del mundo. En los últimos años, solo en los Estados Unidos, se ha penalizado a cerca de una docena de instituciones financieras internacionales por montos entre los cientos y los miles de millones de dólares a causa de actividades de legitimación de capitales o incumplimiento de obligaciones. Estos son indicadores contundentes de que otros países pondrán en práctica igualmente disposiciones sustantivas y medidas para la ejecución de las leyes[2].

Pero no son solo las instituciones que ofrecen servicios financieros. Cualquier organización que facilite transacciones financieras - incluyendo negocios de servicios monetarios no bancarios, tales como servicios de pagos digitales/móviles, aseguradoras y minoristas, por nombrar algunos - forman ahora parte del alcance de la legislación mundial contra la legitimación de capitales (AML por sus siglas en inglés).

Alarmante, más no sorprendentemente, muchos de estos nuevos sujetos obligados no están al día con los requerimientos exigidos o con los programas de prevención exigidos por los gobiernos, y que eventualmente les exigirán.

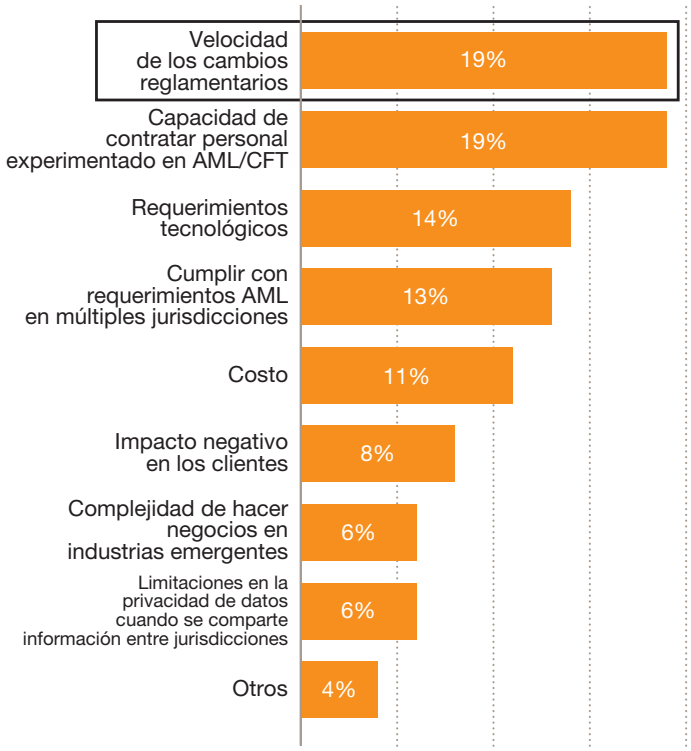
A medida que la normativa se hace más profunda en términos de complejidad y alcance, el costo del cumplimiento sigue aumentando. De acuerdo con nuevas cifras tomadas de WealthInsight, se prevé que el gasto mundial en materia de AML aumente a más de USD 8 mil millones para el 2017[3] (una tasa de crecimiento anual combinada de casi 9%). Pero muchos se resisten a aumentar los gastos en esta área - a pesar del costo de las acciones que se toman para hacer cumplir las leyes y las sanciones masivas producto de su incumplimiento.

[2] De 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes' de la Oficina de las Naciones Unidas contra la Droga y el Delito. © 2011 United Nations.
Reproducido con el permiso de las Naciones Unidas.
[3] Estadísticas facilitadas por cortesía de WealthInsight

Regulación por evaluación

Las acciones correctivas por parte de los reguladores han tenido un repunte importante debido a normas más sólidas. Nuestra encuesta muestra que el nivel de cumplimiento con las medidas contra la legitimación de capitales y el financiamiento al terrorismo (CFT por sus siglas en inglés) ha significado un reto incluso para instituciones financieras que cuentan con los más sólidos y sofisticados programas de cumplimiento en materia de AML.

Fig 1: Retos más significativos para cumplir con los requerimientos AML/CFT



Algunos gobiernos han impuesto multas y en algunos casos han iniciado acciones penales contra instituciones financieras que no han implementado controles suficientes para el monitoreo de sus transacciones globales. Más recientemente, estos mismos gobiernos han reiterado la necesidad de iniciar acciones penales individuales, adicionales a las cuantiosas multas corporativas y convenios que se han impuesto, es decir, buscan identificar las responsabilidades personales detrás de estas faltas. Actualmente, las personas enfrentan el riesgo potencial de ir a prisión si se comprueba su participación en prácticas comerciales ilícitas o incluso por actos significativos de incumplimiento.

Órganos de control y reguladores de la lucha AML

- **Grupo de Acción Financiera en contra del Lavado de Dinero (FATF).** También conocido como el Grupo de Acción Financiera contra el blanqueo de Capitales (GAFI), es un cuerpo intergubernamental cuya misión es establecer políticas y normas para combatir la legitimación de capitales y el financiamiento al terrorismo mediante el seguimiento de las tendencias globales en estas materias; se encarga igualmente de establecer normas internacionales. El FATF estableció "Cuarenta Recomendaciones" - una norma global básica para lograr un sistema efectivo antilavado de dinero. Actualmente, 34 países miembros adoptan estas recomendaciones como parte de su legislación en materia de legitimación de capitales.
- El **Consejo de Seguridad de las Naciones Unidas** emite resoluciones que contienen, entre otras cosas, una lista de personas en contra de las cuales se han impuesto sanciones, como organizaciones terroristas conocidas. Estas listas son empleadas por los gobiernos participantes para apoyar las medidas en contra de la actividad terrorista.
- **Oficina de Control de Activos Extranjeros (OFAC).** Es una oficina adscrita al Departamento del Tesoro de los Estados Unidos que mantiene y administra una serie de programas de sanciones y embargos económicos.

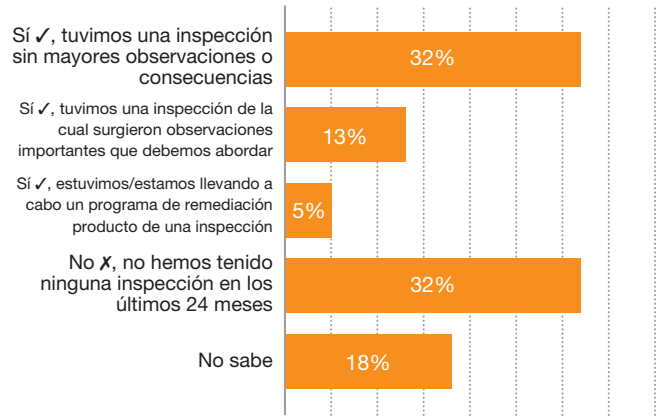
Algunas instituciones financieras han caído bajo el escrutinio de los entes reguladores de un país por realizar prácticas comerciales ilícitas en otro. Comúnmente, surgen conflictos en torno a cuáles son las instituciones del país que pueden intervenir cuando la sanción es impuesta por otros países.

Inspecciones y remediación en aumento

Cuando las organizaciones crecen a través de adquisiciones (como ha ocurrido recientemente), sus vehículos legales, negocios y mercados no se integran de inmediato a los procesos o estándares del grupo. Muchos continúan sufriendo las consecuencias de las acciones o sanciones regulatorias.

Todos estos factores aumentan el perfil de riesgo cuando se trata de aplicar leyes contra la legitimación de capitales y el financiamiento al terrorismo. Nuestra encuesta indica que 18% de los bancos a nivel Global, y 26% en Venezuela, han sido objeto recientemente de acciones correctivas por parte de algún ente regulador.

Fig 2: Inspecciones reglamentarias



Otro reto para las organizaciones que luchan por cumplir con las normas globales AML/CFT es que las expectativas reglamentarias sustituyen cada vez más a los requisitos legales. Esto es más evidente en áreas como la debida diligencia ("due diligence") de clientes y el monitoreo de transacciones, en las que los examinadores pudieran aplicar una norma en una institución basada en las prácticas de otro país o sector.

Esta llamada "regulación por evaluación" pone en tela de juicio el conocido concepto de enfoque basado en riesgos, que se prevé las organizaciones y sus principales interesados apliquen.

El cumplimiento global va más allá de respetar las leyes de una sola jurisdicción. Independientemente de la jurisdicción de origen, las organizaciones deben considerar los asuntos de AML/CFT como aspectos que son regulados desde una perspectiva global, debido a tres razones:

a) El GAFI establece normas internacionales para el manejo de riesgos y cumplimiento AML/CFT. De esta forma, constituye la base para las regulaciones nacionales (y las obligaciones de los bancos y otras instituciones reguladas).

b) La OFAC, junto con otras tesorerías nacionales, como Her Majesty's Treasury (HMT) (el Tesoro de Su Majestad), administran programas de sanciones económicas (y por diseño se enfocan en el movimiento de bienes, servicios y fondos hacia el exterior y a través de las fronteras).

c) La existencia de rígidas y exigentes leyes y prácticas de investigación por parte de las jurisdicciones que administran las principales monedas mundiales, como el dólar estadounidense, la libra esterlina y el euro. El mero acto de realizar una sola transacción en los Estados Unidos o con dólares estadounidenses, o de contactar a una persona en los Estados Unidos por teléfono o correo electrónico, es suficiente para establecer un vínculo y despejar el camino para iniciar juicios en los Estados Unidos.

Los marcos regulatorios de los principales centros financieros (p. ej. Hong Kong, Singapur, Londres y Nueva York) convergen cada vez más en el sentido de exigir a las instituciones la incorporación de los más altos estándares, tanto en el ámbito internacional como en sus jurisdicciones de origen.

Tomados en conjunto, estos rápidos e impredecibles desarrollos pueden llevar a una especie de inercia estratégica a medida que las instituciones intentan predecir el panorama regulatorio al que se enfrentarán en el futuro. Hay una cosa que está más que clara: se requerirá mucho criterio al momento de diseñar los programas de cumplimiento contra delitos financieros.

¿Qué significa todo esto para su organización?

Con la globalización de las normas AML/CFT es importante recordar que usted y su organiuzación puede ser juzgado con base en los más altos estándares internacionales de cumplimiento. A continuación se mencionan tres líneas de acción que debe considerar:

1) **Manténgase al día en materia regulatoria.** Vaya más allá del cumplimiento mecánico de las leyes actuales. En lugar de ello, mire hacia adelante y evalúe de qué forma prepararse para cumplir con las próximas tendencias legislativas. Concéntrese en contar con una función viable dentro de su organización que mantenga un seguimiento de las regulaciones pendientes en esta área.

2) **Sea un líder, no un seguidor.** Encontrarse en medio de un grupo lo expone al riesgo de quedar rezagado en la curva regulatoria. Concéntrese en ser estratégicamente ágil e innovador para así mantenerse a la vanguardia de los cambios en las normativas.

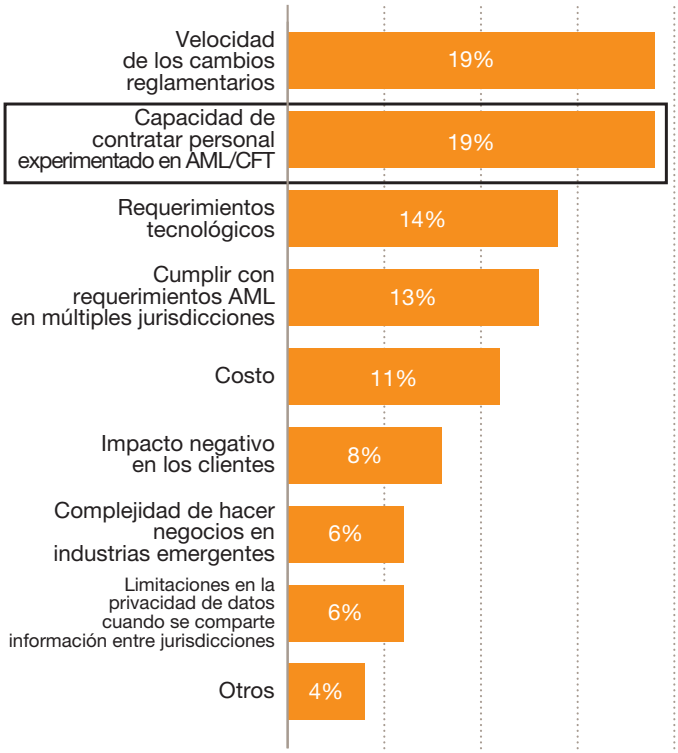
3) **Aprenda de los errores ajenos.** Son pocas las organizaciones que investigan la causa primordial de los asuntos significativos identificados por los entes reguladores. La remediación suele servir como una solución rápida para abarcar las observaciones producto de una inspección reglamentaria; sin embargo, el costo de remediar las violaciones suele superar las penalizaciones impuestas por los entes reguladores. Dado que la mayoría de las transacciones tienen un componente financiero multinacional, es recomendable, siempre que sea posible, guiarse por el estándar más alto de cumplimiento global y someterse a autoevaluaciones AML/CFT más rigurosas. Establezca requerimientos corporativos para garantizar la consistencia en todas las localidades.

¿Qué significa todo esto para su organización?

Según los encuestados, los retos más importantes que deben enfrentarse en el área de legitimación de capitales son: contratar personal con experiencia (19% Global – 22% Venezuela), y administrar la incertidumbre generada por la velocidad de los cambios reglamentarios (19% Global – 13% Venezuela).

Infortunadamente, la oferta de talento sigue estando por debajo de la demanda. Los niveles de rotación entre personal del área AML y el personal de cumplimiento son altos, y la competencia por hacerse de personal de élite es significativa tanto para las empresas del sector financiero como para las de servicios no financieros.

Fig 3: Retos más significativos para cumplir con los requerimientos AML/CFT



Algunas organizaciones están abordando el reto del talento mediante la capacitación de sus propios recursos, con un enfoque significativo en AML/CFT y recursos antisoborno.

Fig 4: Medidas implementadas por la gente para abordar las expectativas reglamentarias

Las evaluaciones de riesgo son críticas

Durante la última década, la aplicación de medidas de control más competitivas en material de prevención contra la legitimación de capitales en los sistemas financieros formales, ha obligado a los delincuentes a buscar nuevas maneras de "movilizar" las ganancias producto de sus delitos. Es por ello que es necesario realizar evaluaciones de riesgo de forma regular, lo que le permitirá a su organización identificar y manejar los riesgos que enfrenta en materia de legitimación de capitales y financiamiento al terrorismo, donde sea y con quien sea que realice negocios.

A pesar de las evidentes ventajas, más de un cuarto de las firmas de servicios financieros que participaron en nuestra encuesta no está realizando en la actualidad ninguna evaluación de riesgo AML/CFT dentro de su negocio global, o no tiene conocimiento de si lo están haciendo.

Y, a medida que la sofisticación de los legitimadores de capitales aumenta con el tiempo, ésta es una medida que no puede posponerse. La legitimación de capitales mediante operaciones comerciales (TBML por sus siglas en ingles), por ejemplo - un sistema complejo de documentación falsa que permite a los delincuentes obtener y movilizar valores alrededor del mundo bajo la apariencia de comercio legítimo - es cada vez más difícil de detectar mediante los sistemas tradicionales de monitoreo de transacciones.

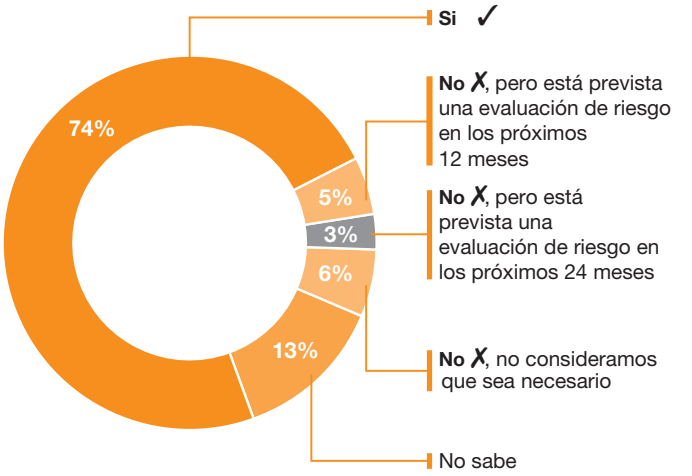
La gente correcta, las aptitudes correctas, los lugares correctos ¿Qué aptitudes necesita?

Cuando su mejor línea de defensa de AML es contar con la gente correcta en las posiciones correctas con las aptitudes correctas, es necesario que sepa lo que busca. Existe una demanda importante de experticia y aptitudes en:

- Estándares y requerimientos globales
- Regulaciones y obligaciones jurisdiccionales
- Ecosistema reglamentario global
- Debida Diligencia con respecto a los clientes
- Pericia técnica en seguimiento de transacciones
- Análisis de datos

Es necesario realizar evaluaciones de riesgo de forma periódica. Estas evaluaciones deben adaptarse a las circunstancias cambiantes, tales como el ambiente operativo, estándares globales y normativa en países en los que se opera. Particularmente, las evaluaciones también deben incluir la clasificación de los clientes dentro de diferentes categorías de riesgo en materia de legitimación de capitales y financiamiento al terrorismo. También es el estándar global recomendado por la CAFI y los entes reguladores para contrarrestar las amenazas.

Fig 5: Porcentaje de organizaciones que realizan evaluaciones de riesgo AML/CFT

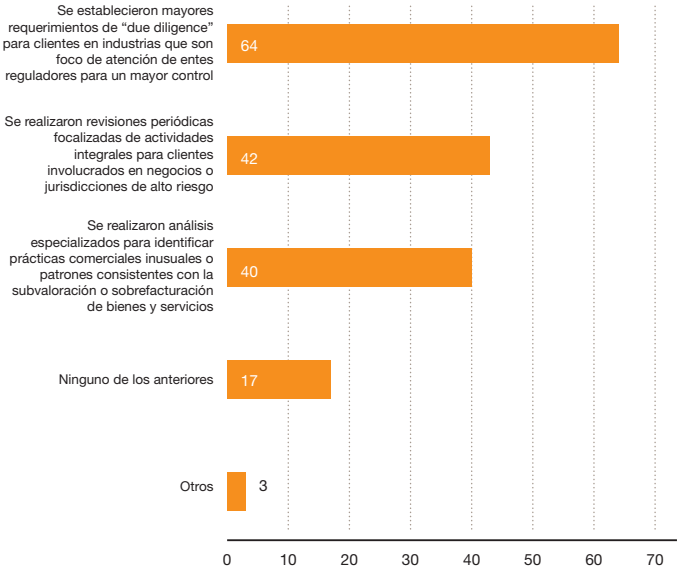


GAFI: Un nuevo enfoque en la efectividad

El GAFI ha cambiado su estándar de evaluación de normas nacionales de AML/CFT de cumplimiento técnico a uno de efectividad, según el cual todas las organizaciones son evaluadas con base en criterios similares.

Este nuevo acento en la efectividad debe impulsar a algunos países en desarrollo a realizar cambios en sus prácticas de cumplimiento, lo cual esperamos se traslade hacia las instituciones y, a su vez, dada la naturaleza global de las iniciativas contra el lavado de dinero, hacia otras jurisdicciones. También podría crear temporalmente una brecha sobre la percepción del significado de "efectividad" entre mercados más avanzados y los que están en vías de desarrollo.

Fig 6: Detección y disuasión de legitimación de capitales mediante operaciones comerciales



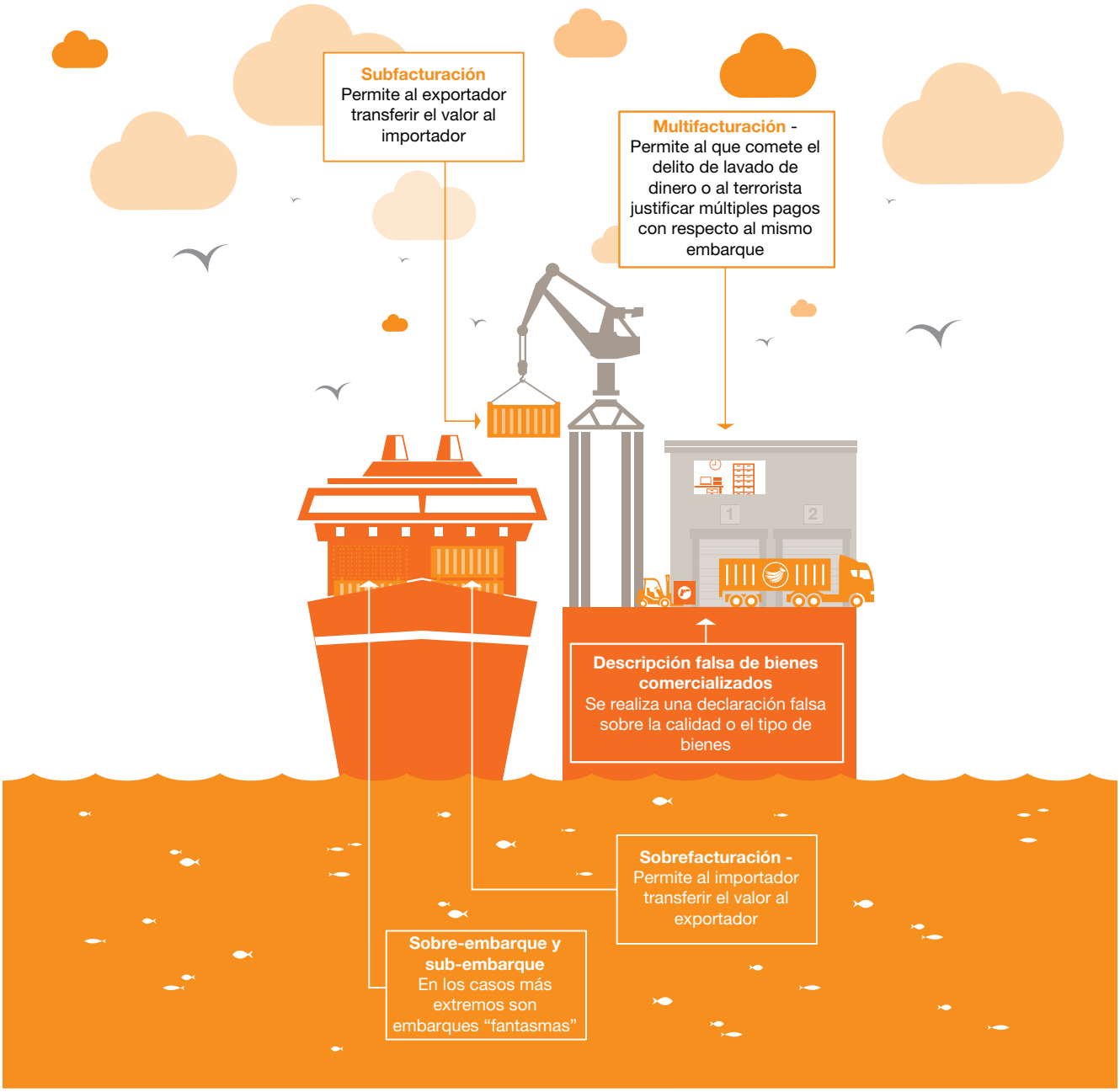
¿Aplicación desigual?

Si bien la mayoría de los paises cuenta con algún mecanismo para las inspecciones AML/CFT, el grado de exhaustividad de tales inspecciones varía sustancialmente.

Los Estados Unidos y algunos otros países desarrollados cuentan con personal examinador dedicado a AML/CFT y sus respectivas sanciones. Pero muchos otros países emplean personas sin especialización alguna para evaluar el cumplimiento o los riesgos, en lugar de personas especializadas en AML/CFT.

En Venezuela, la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) es el ente autorizado para examinar a las instituciones del sector financiero. Sin embargo, encarga a los auditores externos e internos la ejecución de las revisiones de cumplimiento.

Técnicas comunes de TBML



Conozca a su cliente, hoy y mañana

La transparencia en su base de clientes va más allá de la mera identificación y verificación de la información que ellos proporcionan. Debe ser un acto dinámico, no estático.

Es imprescindible mantener un seguimiento continuo de las señales de alarma y cualquier actividad sospechosa. Se debe prestar especial atención a las relaciones y transacciones comerciales de los clientes, especialmente si realizan negocios con personas residentes en países en los que la legislación en materia de legitimación de capitales es débil o insuficiente.

Fig 7: Medidas implementadas para reducir los riesgos AML/CFT

Tecnología

Las empresas que conforman el ecosistema del sistema financiero parecieran estar en aprietos. La mayoría enfrentan el problema de adaptar correctamente sus programas AML a sus negocios cambiantes en un entorno reglamentario global y en constante evolución. Muchas de ellas enfrentan el obstáculo de tener sistemas de monitoreo heredados que están demostrando ser una carga y cuya adaptación, validación y mantenimiento están resultando extremadamente costosos.

Infortunadamente, el costo y la complejidad de implementar algunas de las nuevas y más sofisticadas plataformas de análisis de datos - algoritmos con tecnología de punta que podrían hacer posible la transición de una base transaccional engorrosa hacia un enfoque más estratégico y eficiente - suele ser prohibitivo para muchos. Los encuestados relacionados con servicios financieros parecen estar muy conscientes de estos retos de los sistemas, ya que más de un tercio señala a la calidad de los datos como el reto técnico más importante que afrontan.

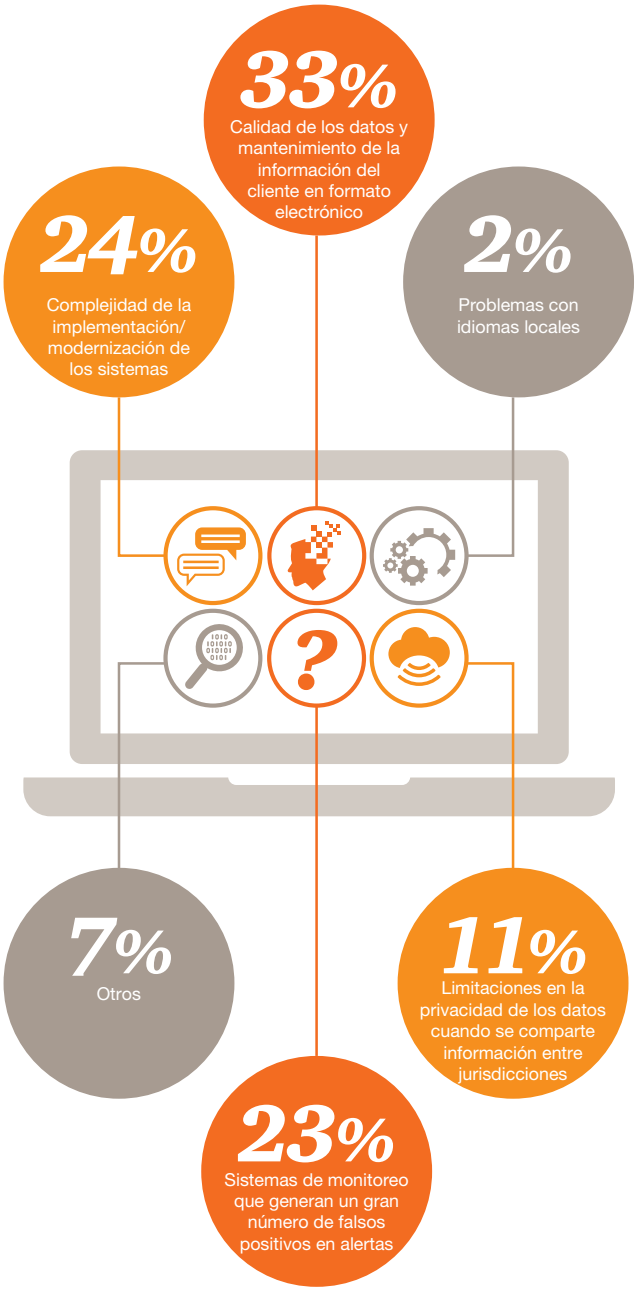
¿Qué impulsa a una empresa a dar el salto hacia una nueva tecnología?

Frecuentemente, este cambio es producto de un evento - remediación debido a sanciones regulatorias, una fusión, adquisición u otra transacción que evidencie que los sistemas actuales ya no cumplen su propósito. También puede ser la consecuencia de la aparición repentina de un competidor en el mercado que cambia los intereses para todos.

Pero algunas veces se produce simplemente porque una organización alcanzó un punto de inflexión en el que se da cuenta que la rentabilidad de saltar hacia una nueva plataforma tecnológica es mayor que el costo de abandonar los sistemas en cuya instalación y mantenimiento han invertido millones de dólares.

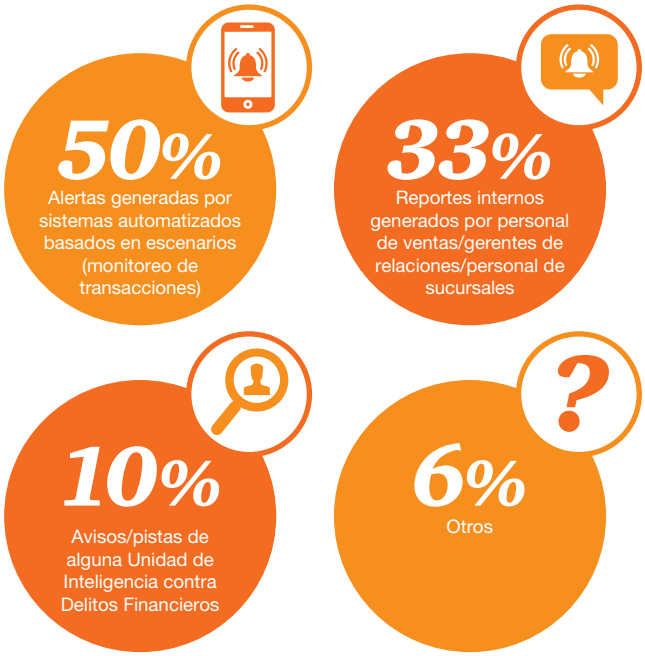
También puede haber otros beneficios en las nuevas tecnologías. Más allá del cumplimiento AML, puede aportar mejoras a otras funciones claves del cumplimiento - incluyendo funciones antisoborno, sanciones de exportación, monitoreo y respuesta ante el fraude, controles e investigaciones financieras - fortaleciendo de esta manera la gobernabilidad.

Fig 8: Retos más significativos relacionados con los sistemas AML/CFT



Para agravar el problema: El rendimiento del monitoreo de AML es deficiente. Solo la mitad de las acciones de lavado de dinero o financiamiento al terrorismo son detectadas por los sistemas de monitoreo de transacciones. Es probable que las tipologías actuales de AML no estén identificando los matices y estructuras complejas necesarias para identificar transacciones de alto riesgo.

Fig 9: Métodos que se emplean para identificar actividades sospechosas



A todos los encuestados se les realizó esta pregunta inicialmente, pero 26% (de 1090) afirmó no haber detectado o reportado alguna actividad sospechosa de AML/CFT. Los resultados que aquí se presentan muestran aquellos que sí detectaron actividad de AML/CFT a través de algún método.

Migrar a nuevos modelos y plataformas analíticas no es, aún, un fenómeno generalizado. Esto podría ser indicativo de que las instituciones reconocen un cierto grado de ineficacia a sus sistemas actuales de detección más que un problema de obsolescencia.

Apéndices

Estadísticas de participación

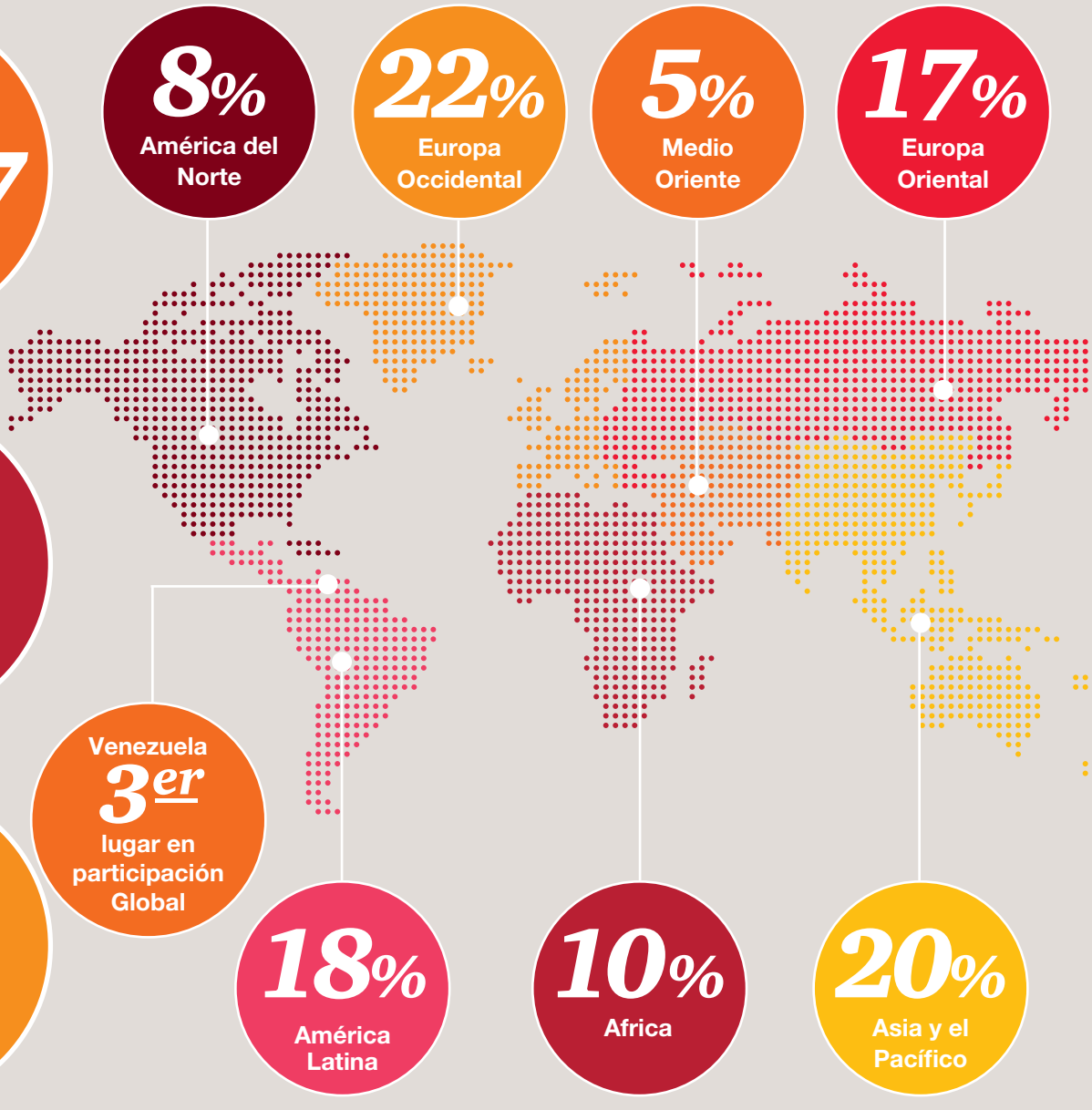
Estadísticas de participación

6.337 completaron la encuesta

En **115** países

Realizada en **17** idiomas diferentes

Participación por región



Encuestados

45%
Alta Gerencia

30%
Jefe de Departmento o Unidad de Negocio

70%
de los encuestados son de las áreas de Gerencia Ejecutiva, Finanzas, Auditoría, Cumplimiento o Manejo de Riesgos

54%
de los encuestados son empleados de organizaciones con más de 1.000 empleados

48%
de las organizaciones participantes tienen más de 10.000 empleados

37%
de la población encuestada representa empresas que cotizan en bolsas

59%
de los encuestados pertenece a organizaciones multinacionales

Sectores

35%
Industrial

24%
Servicios Financieros

14%
Consumo

7%
Tecnología

6%
Servicios Profesionales

13%
Otros

Servicios forenses en Venezuela

El fraude corporativo no está limitado por las fronteras locales, regionales o nacionales. De las regiones altamente industrializadas a los países en desarrollo, donde hay negocios, existe la potencialidad para el crimen corporativo. En particular, las empresas multinacionales enfrentan amenazas multidimensionales.

PwC ofrece un equipo global de especialistas en delitos económicos que puede afrontar el espectro completo de situaciones, desde las cuestiones locales a los desafíos transfronterizos.

Dos mil especialistas en fraudes corporativos de PwC trabajan en 60 países de todo el mundo. Estos profesionales ofrecen conocimientos locales y visión práctica de las diferencias regionales y nacionales en las prácticas de negocios, marcos regulatorios, cultura e idioma.

Nuestro acceso global a estos recursos locales nos permite investigar y analizar eficientemente problemas en países específicos. PwC posee un grupo de especialistas preparado para satisfacer sus necesidades.

Nuestra amplia gama de soluciones se extiende mucho más allá de servicios vinculados a fraudes corporativos para ayudar a nuestros clientes en todo el mundo en tiempo real.

Investigaciones • Línea de denuncias • Revisión y administración de licencias • E-Discovery •Ciberseguridad • Programa anti-fraude y evaluaciones de riesgo • Soborno y corrupción • Inteligencia Corporativa

Servicios forenses en Venezuela

Roberto Sánchez V.
Socio líder del servicio
+58 (212) 700 6222
roberto.sanchez@ve.pwc.com

José Miguel Chirinos
Socio GRC
+58 (212) 700 6246
jose.chirinos@ve.pwc.com

Edwin Orrico
Gerente líder del servicio
+58 (212) 700 6151
edwin.orrico@ve.pwc.com

Colaboradores

Equipo Líder

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

Mark Anderson
Socio, Reino Unido
t: +44 (0) 207 8042564
e: mark.r.anderson@uk.pwc.com

Didier Lavion
Director, Estados Unidos
t: +1 (646) 471 8440
e: didier.lavion@us.pwc.com

Miembros de la Junta Editorial

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

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

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

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

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

Equipo gerencial de la encuesta

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

Anjali Fehon
Líder de Estrategia Forense,
Estados Unidos
t: +1 (973) 236 4310
e: anjali.t.fehon@us.pwc.com

Equipo de mercadeo de la encuesta

Gemma Peart
Gerente de Mercadeo Global, Reino Unido
t: +44 (0) 771 1589 331
e: gemma.peart@uk.pwc.com

Kate Glenn
Líder de Mercadeo Forense,
Estados Unidost: +1 (202) 312 7542
e: kate.n.glenn@us.pwc.com

Líderes de servicios forenses

Andrew Gordon
Líder Global, Reino Unido
t: +44 (0) 20 7804 4187
e: andrew.gordon@uk.pwc.com

Andrew Palmer
Líder EMEA, Reino Unido
t: +44 (0) 20 7212 8656
e: andrew.palmer@uk.pwc.com

Erik Skramstad
Líder EE.UU & APA, Estados Unidos
t: +1 (617) 530 6156
e: erik.skramstad@us.pwc.com

Servicios forenses en Venezuela

Roberto Sánchez V.
Socio líder del servicio
+58 (212) 700 6222
roberto.sanchez@ve.pwc.com

José Miguel Chirinos
Socio GRC
+58 (212) 700 6246
jose.chirinos@ve.pwc.com

Edwin Orrico
Gerente líder del servicio
+58 (212) 700 6151
edwin.orrico@ve.pwc.com

www.pwc.com/crimesurvey