# El impacto de los delitos financieros

**Prevención, detección y respuesta**

KPMG en México

**Los delitos financieros no son una amenaza nueva; organizaciones, gobiernos e individuos se ven afectados frecuentemente por estos crímenes, cuyos daños económicos, sociales y de reputación van en ascenso. Según la Asociación de Especialistas Certificados en Delitos Financieros (Association of Certified Financial Crime Specialists, o ACFCS), dichos delitos incluyen: lavado de dinero y financiamiento al terrorismo, fraude, corrupción, y evasión fiscal.**

**La tecnología ha sido una aliada en las estrategias para su prevención y combate; desafortunadamente, los grupos criminales y los delincuentes de cuello blanco también han aprovechado la tecnología y, con ello, los delitos cibernéticos y otras expresiones del crimen financiero se han incrementado exponencialmente.**

**Considerando lo anterior, decidimos ampliar nuestra tradicional encuesta de fraude, incorporando el lavado de dinero, la corrupción, el cibercrimen y las tecnologías financieras emergentes.**

**Esperamos que este esfuerzo ayude a las organizaciones a replantear los esquemas y técnicas de prevención, detección y combate de dichos delitos para que, lejos de verlos como fenómenos aislados con reacciones esporádicas, adopten un sólido programa con un enfoque holístico de riesgos.**

**Shelley M. Hayes**
Socia Líder de Forensic
KPMG en México
y Centroamérica

# Contenido

# Visión integral y esquemas de prevención

## Programas integrales de prevención

Ante los embates de los crímenes financieros, cada vez más sofisticados y frecuentes, las organizaciones y los gobiernos necesitan desarrollar nuevos niveles de conciencia, así como estrategias integrales con énfasis en la prevención.

La existencia de marcos normativos internacionales y de mejores prácticas para el combate al crimen financiero, como la corrupción o el fraude, sugiere que la mayoría de las compañías deben contar con programas, políticas, campañas y entrenamientos para la prevención de estos delitos.

## Programas de prevención insuficientes

A pesar de lo anterior, el presente estudio muestra que menos de la mitad de las empresas en México (42%), mantienen un programa integral de prevención de delitos financieros; 37% lo hace de manera parcial, mientras que 21% ni siquiera cuenta con alguna medida formal para protegerse de estos riesgos.

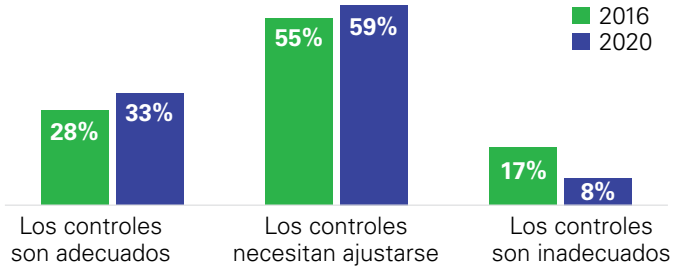
**¿Su empresa cuenta con programas, políticas, campañas y entrenamiento en materia de prevención de delitos financieros?** (Lavado de dinero, fraude, corrupción y ciberseguridad).


Es importante tener presente que ningún programa blinda totalmente a una empresa ante cualquier tipo de riesgo, de modo que si sus principales socios de negocio tienen controles débiles, la organización se expone a riesgo de contagio.

## Ajustes a los controles

Asimismo, tan solo 33% de las compañías consideran que los controles que actualmente tienen implementados son adecuados para mitigar los riesgos de delitos financieros.

**¿Considera que los controles actualmente implementados en su empresa son adecuados para mitigar los riesgos de delitos financieros que pudieran presentarse?** (Lavado de dinero, fraude, corrupción, delitos cibernéticos).




Cabe señalar que los controles requieren ser sometidos regularmente a pruebas de estrés para conocer su nivel de confianza, detectar de forma oportuna áreas de mejora y realizar los ajustes correspondientes.

## La cadena es tan fuerte como el más débil de los eslabones

Aunque el capital humano es de las principales fortalezas de las empresas, un colaborador es susceptible de convertirse en el más débil de los eslabones en un contexto de control. Las organizaciones deben tener en cuenta que, generalmente, las computadoras y programas no fallan; cuando se rompe la cadena suele ser principalmente por un error o acto humano. No es posible corromper una máquina, pero a una persona sí.

## La figura del Oficial de Cumplimiento

Por lo anterior, y a fin de cuidar al más débil de los eslabones en la organización; es decir, al capital humano, diversas legislaciones sugieren incorporar dentro de la estructura corporativa la figura del Oficial de Cumplimiento: aquel individuo responsable de la vigilancia activa tanto del cumplimiento regulatorio como de la efectiva mitigación de riesgos.

Los resultados muestran que más de la mitad de las compañías (52%) no cuentan con la figura de Oficial de Cumplimiento o alguna función similar.

**¿En su empresa existe la figura de Oficial de Cumplimiento u otra función equivalente, encargada específicamente de gestionar los riesgos de delitos financieros?**


Estas cifras contrastan con las recomendaciones de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS, por sus siglas en inglés), la cual recomienda contar con al menos cuatro componentes elementales para un programa de prevención:

- Políticas y procedimientos documentados
- Oficial de Cumplimiento experimentado
- Entrenamiento efectivo y periódico
- Evaluación del nivel de cumplimiento por un tercero independiente

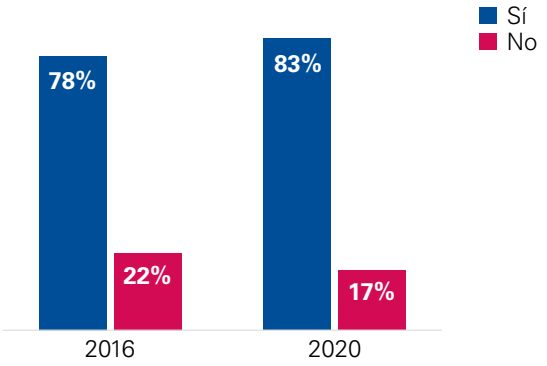
Si alguno de estos elementos falta o falla, la eficiencia del programa puede verse comprometida.

# La evolución del fraude

### Nadie está exento

Independientemente de la industria, las organizaciones han desarrollado algún componente de programas antifraude. El uso de modelos de aprendizaje de computadoras y los procedimientos analíticos predictivos desarrollados para la detección oportuna de patrones de transacciones y comportamientos atípicos han resultado de gran utilidad. Sin embargo, los resultados revelan que todavía 17% de las empresas consideran que no están expuestas a riesgo de fraude. Si bien el porcentaje ha disminuido 5% desde 2016, todavía existe esa falsa percepción de inmunidad en las organizaciones.

### ¿Cree usted que su empresa puede ser víctima de algún fraude?




El fraude sigue siendo uno de los delitos más frecuentes y que más profundamente daña a las empresas y a los individuos. En algunas ocasiones, el fraude, por el tipo de control implementado o por la modalidad en la que se está ejecutando, no es detectado o se detecta muy tarde. Nuestro estudio de 2016 mostró que más de la mitad de los fraudes tomaron 15 meses en ser detectados, lo cual alimenta la falsa creencia de estar a salvo de este delito.

### Fraude interno, externo y en colusión

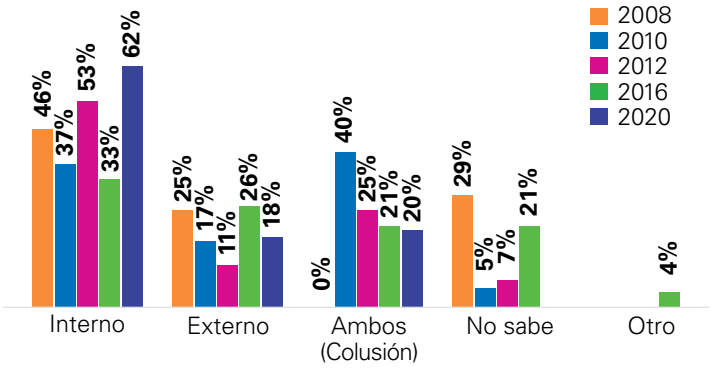
Asimismo, el fraude interno es la principal modalidad de este tipo de crimen financiero, con más de la mitad de los casos en 2012 (53%) y alcanzando 62% en 2020. Esto pone al descubierto una realidad que debe despertar el interés de las organizaciones: frecuentemente, "el enemigo está en casa". Ello puede responder a un ambiente de control interno débil, un entorno laboral hostil y un bajo nivel ético y moral.

**Todavía existe la falsa percepción de que las organizaciones son inmunes a ser víctimas de fraude**

Según el Triángulo del Fraude de Donald Cressey, bastan tres factores: oportunidad, racionalización y motivación, para que una persona cometa algún fraude ocupacional.

Por otra parte, el fraude externo se ha mantenido, durante 12 años, en promedio en aproximadamente 20% de los casos reportados, cifra que también se aplica a los casos de colusión (perpetradores internos y externos), que alcanza 20% en 2020

### ¿Qué modalidad de fraude ha sufrido su empresa?




El presente estudio también muestra que 41% de los defraudadores prefieren actuar solos, y 32% coludiéndose con alguien más al interior de las organizaciones. Los casos de colusión con alguien al exterior a la organización ascendieron a 27%. Si sumamos los porcentajes de ambas colusiones, es decir, una mezcla de colusión interna y externa, obtenemos que 59% de los defraudadores no actúan solos, lo que guarda relación con los resultados publicados por KPMG International, en donde se obtuvo un 62% de casos de colusión.

### ¿El defraudador actuó solo o en colusión?

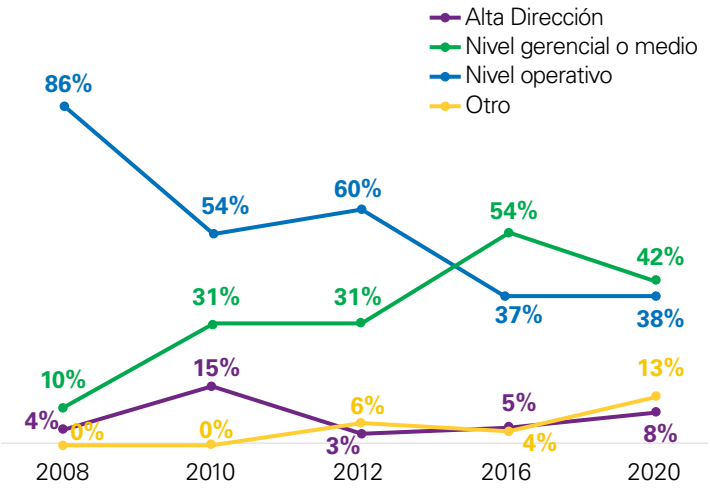

*Empleados con terceros, como exempleados, proveedores, contratistas, clientes, entre otros.

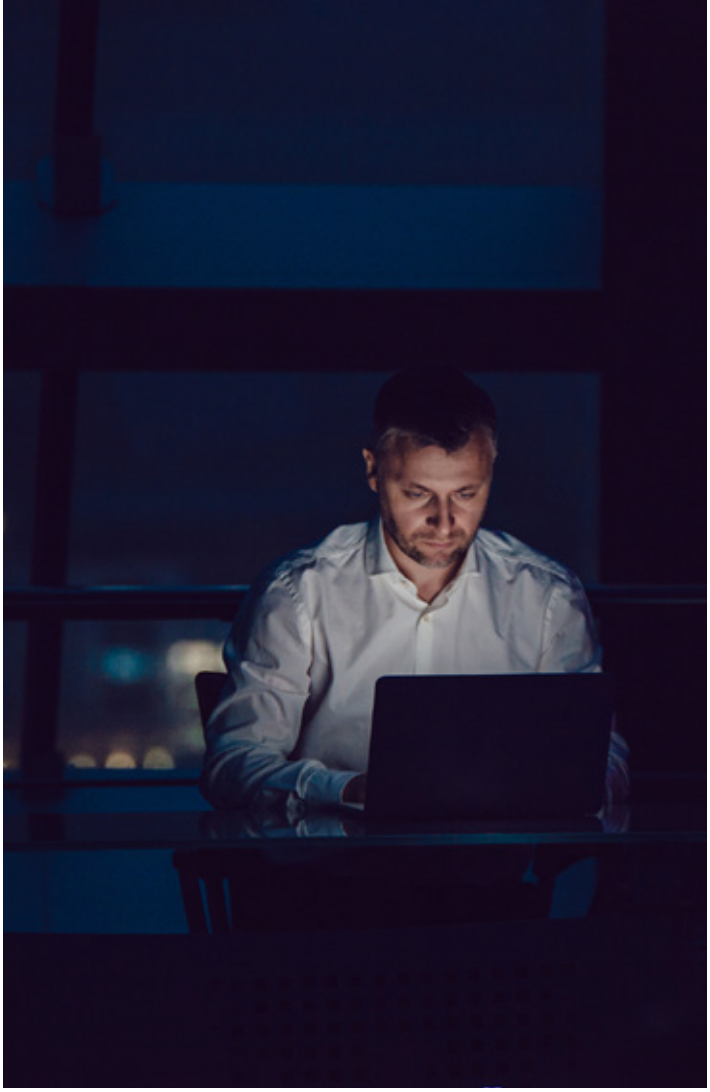
### Nivel jerárquico del perpetrador

Respecto a la posición que ocupaba el defraudador en la organización, el estudio muestra que la mayoría de los fraudes detectados fueron cometidos por personal que ocupaba gerencias o algún otro mando medio (42%).

Podemos ver que a lo largo de los años, los fraudes perpetrados por los niveles operativos han tendido a la baja, mientras que los de gerencia y otros niveles medios, lo han hecho a la alza.

### ¿Qué posición ocupaba el defraudador?

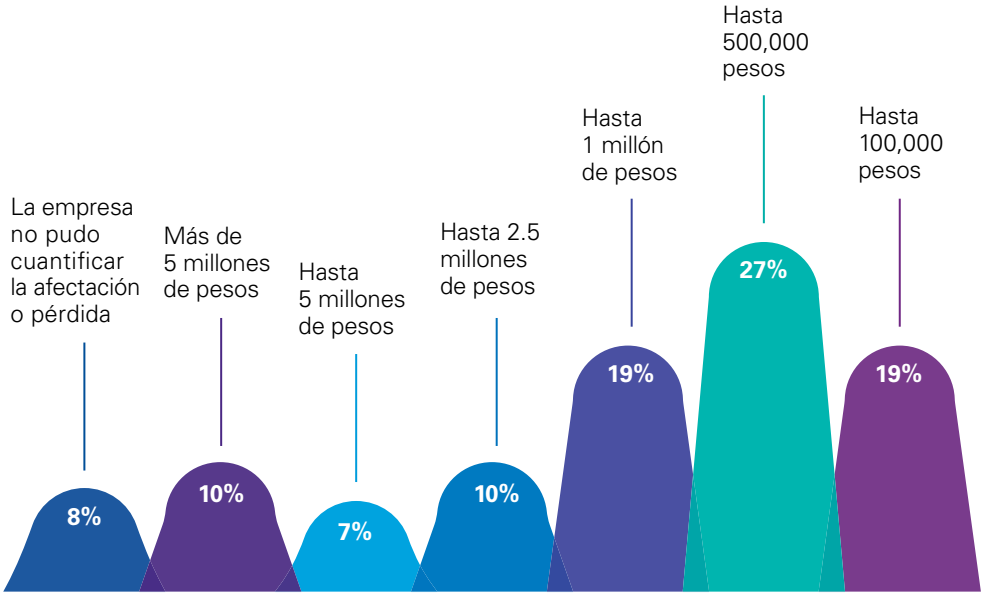


### El costo del fraude

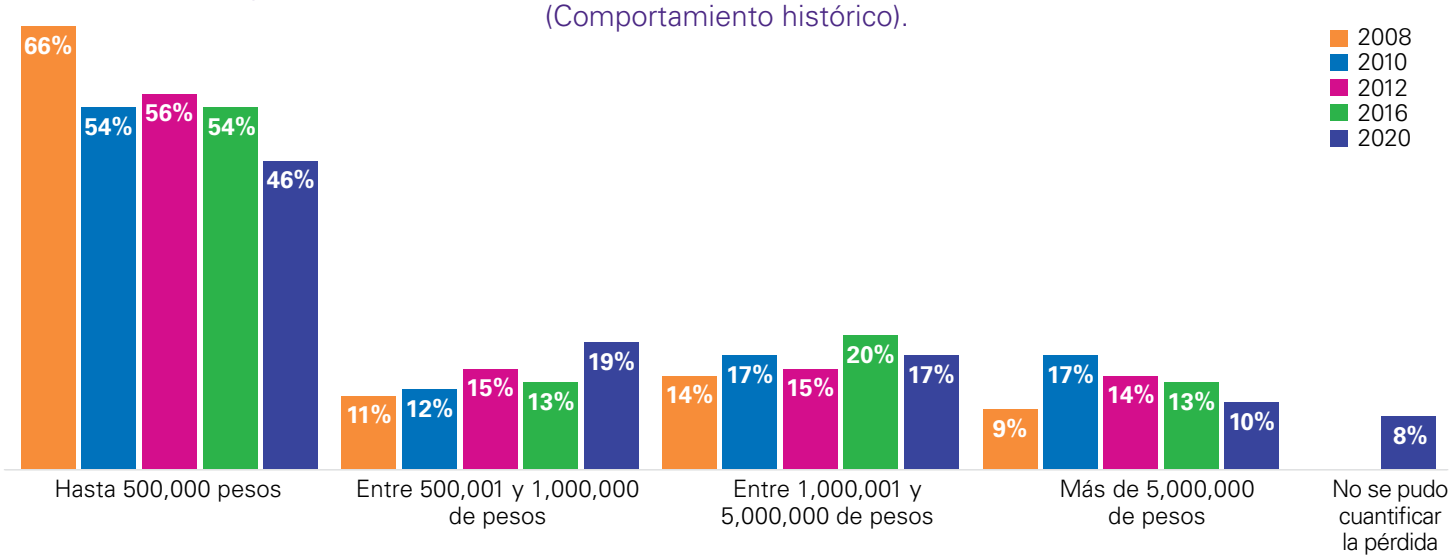
Por otro lado, en promedio, el quebranto de fraude para las compañías se ubica en 1,400,000 pesos por evento, cifra que representa 1% del promedio total de ventas anuales; sin embargo, debemos considerar que 8% de las empresas no pudieron cuantificar la pérdida.

### ¿A cuánto estima que ascendió la afectación económica o la pérdida?



Los fraudes ubicados entre 500,000 y 1 millón de pesos (mdp) son los que más crecimiento han tenido desde 2008, mientras que los que son iguales o menores a 500,000 pesos disminuyeron ocho puntos porcentuales entre 2016 y 2020. Por su parte, los fraudes superiores a los 5 mdp siguen presentando una tendencia importante con 10% de los casos en 2020.

**¿A cuánto estima que ascendió la afectación económica o la pérdida?**
(Comportamiento histórico).




La pérdida estimada de 1% de las ventas anuales, más los costos asociados con procesos legales, de investigación y remediación, de difícil cuantificación como la afectación en la reputación y los daños al ambiente laboral, pueden representar un monto cuantioso para cualquier empresa.

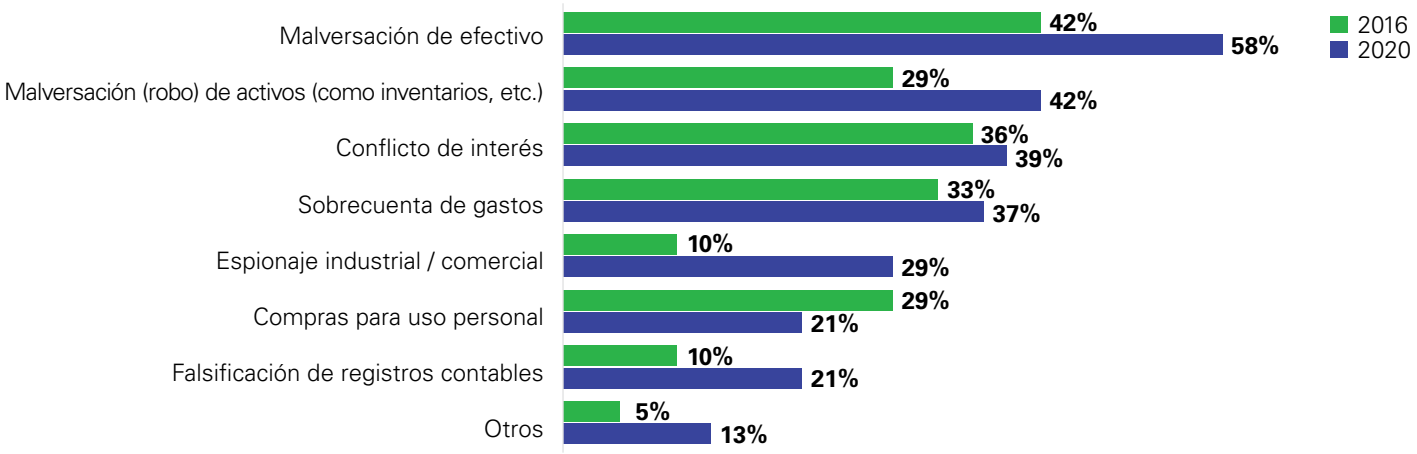
### Modalidad del fraude interno

Con un incremento de 16% (42% a 58% de 2016 a 2020), la malversación de efectivo sigue siendo la principal tipología de fraude interno en las organizaciones, pues es más fácil perderle el rastro. Por su parte, la malversación de otros activos ocupa el segundo lugar, con 42%, habiendo aumentado 13% desde 2016.

La modalidad de conflicto de interés tiene 39% de incidencia; es decir, aproximadamente cuatro de cada diez participantes detectaron una situación de fraude al interior de su organización como consecuencia de esta situación. Este porcentaje indica que existe mayor conciencia sobre la modalidad de fraude producto de conflicto de interés, aunque todavía se requiera mejorar el monitoreo y aplicar las sanciones correspondientes.

En los fraudes relacionados con los registros contables, la sobrecuenta de gastos se incrementó 4%, alcanzando 37% de casos reportados en 2020, y la falsificación de registros contables se duplicó desde 2016, situándose en 21%.

**¿Qué modalidad de fraude interno fue efectuada?**




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Los datos señalan que 14 de los 21 sectores encuestados presentan alguna de estas modalidades de malversación o, en algunos casos, las dos. Los sectores de transporte, salud, manufactura, hotelería y telecomunicaciones lideran el porcentaje de casos de malversación de efectivo. Asimismo, las industrias química y farmacéutica, de electrónicos, alimentos y automotriz, están a la cabeza en casos de fraude por malversación de otros activos. El sector financiero muestra haber avanzado en la prevención y detección de fraudes relacionados con la malversación de efectivo y de otros activos, en contraste con las demás industrias, cuyos controles no son óptimos o carecen de ellos.

> El sector financiero muestra haber avanzado en la prevención y detección de fraudes relacionados con la malversación de efectivo y de otros activos, en contraste con otras industrias

## Modalidad del fraude externo

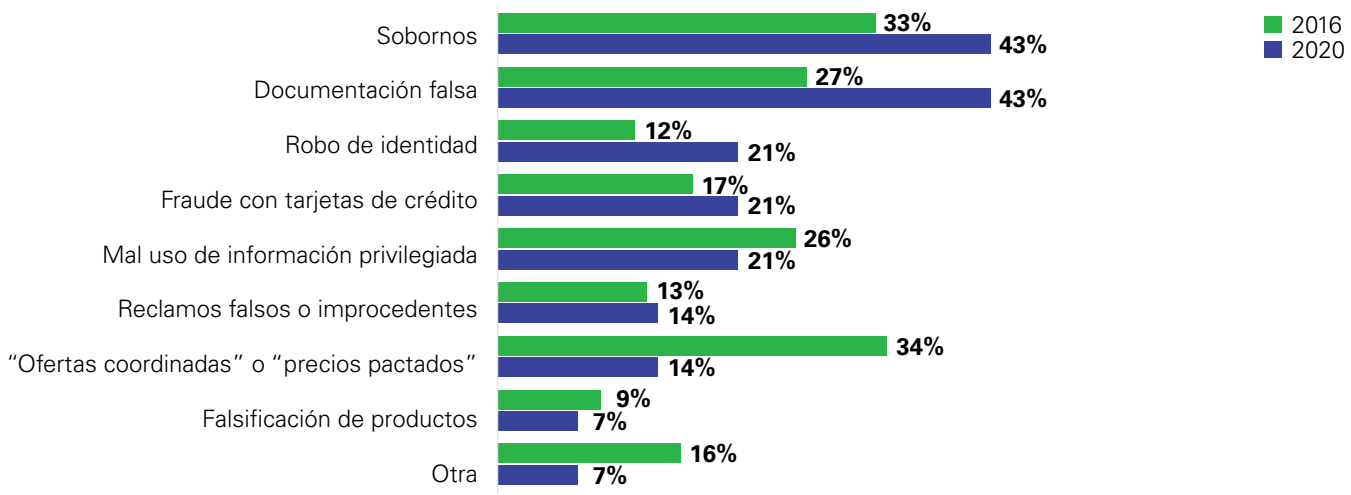
En 2020, las principales modalidades de fraude externo, con una incidencia de 43%, son la documentación falsa y los sobornos. Ambas muestran incrementos considerables con respecto a 2016, de 16 puntos porcentuales en el caso de la primera, y 10% en el de la segunda.

Esto puede ser un indicador de que están estrechamente relacionadas; es decir, se pagan sobornos para que la compañía acepte información falsa, lo que indica que la principal vulnerabilidad de las compañías es la fuerza laboral.

El robo de identidad tuvo un incremento de nueve puntos, mientras que el mal uso de información privilegiada fue la única modalidad que presentó una ligera disminución de 26% en 2016 a 21% en 2020 y los fraudes con tarjetas de crédito mostraron un incremento de 17% a 21%.

En este sentido, casi la mitad de las industrias sufrieron algún fraude perpetrado por individuos ajenos a la empresa. El sector financiero, principalmente, declara haber sido víctima de la documentación falsa y del robo de identidad.

### ¿Qué modalidad de fraude externo fue efectuada?



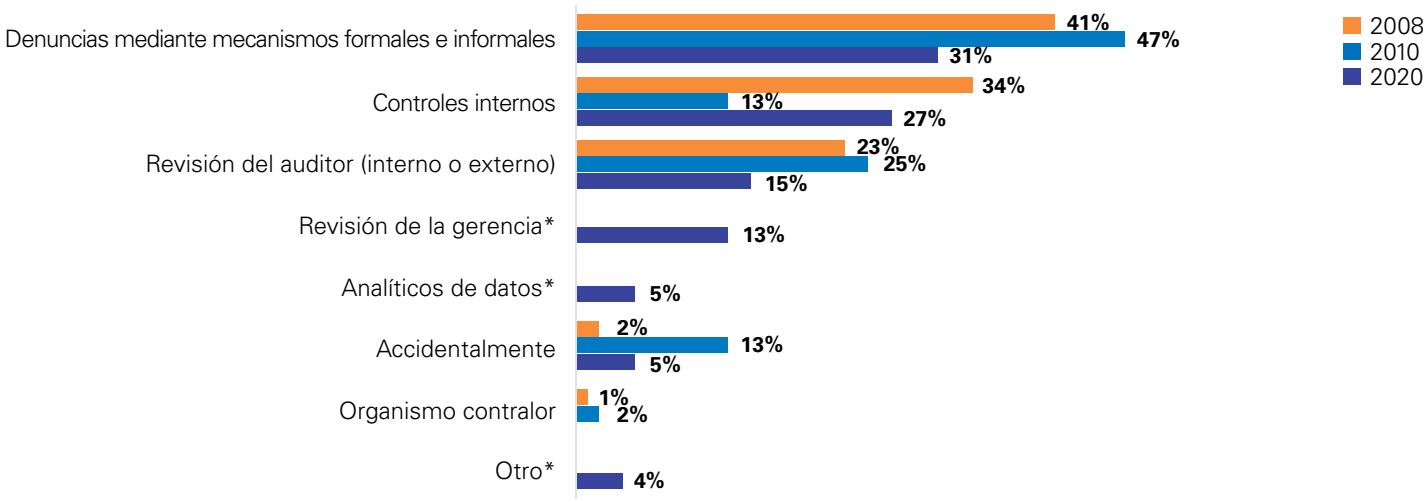

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

## Detección del fraude

Las denuncias siguen siendo la principal fuente de detección, obteniendo un 31% de las menciones, seguidas de los controles internos (27%), y las funciones de auditoría (interna o externa) y revisiones de la gerencia, con 15% y 13% respectivamente.

Resultan útiles las líneas de denuncia operadas por un externo. Además de los resultados del estudio, que equiparan su efectividad a las revisiones de auditoría interna y de la gerencia, la experiencia muestra que son el principal canal por el que se reciben las denuncias.

## ¿Cómo se detectaron los fraudes?

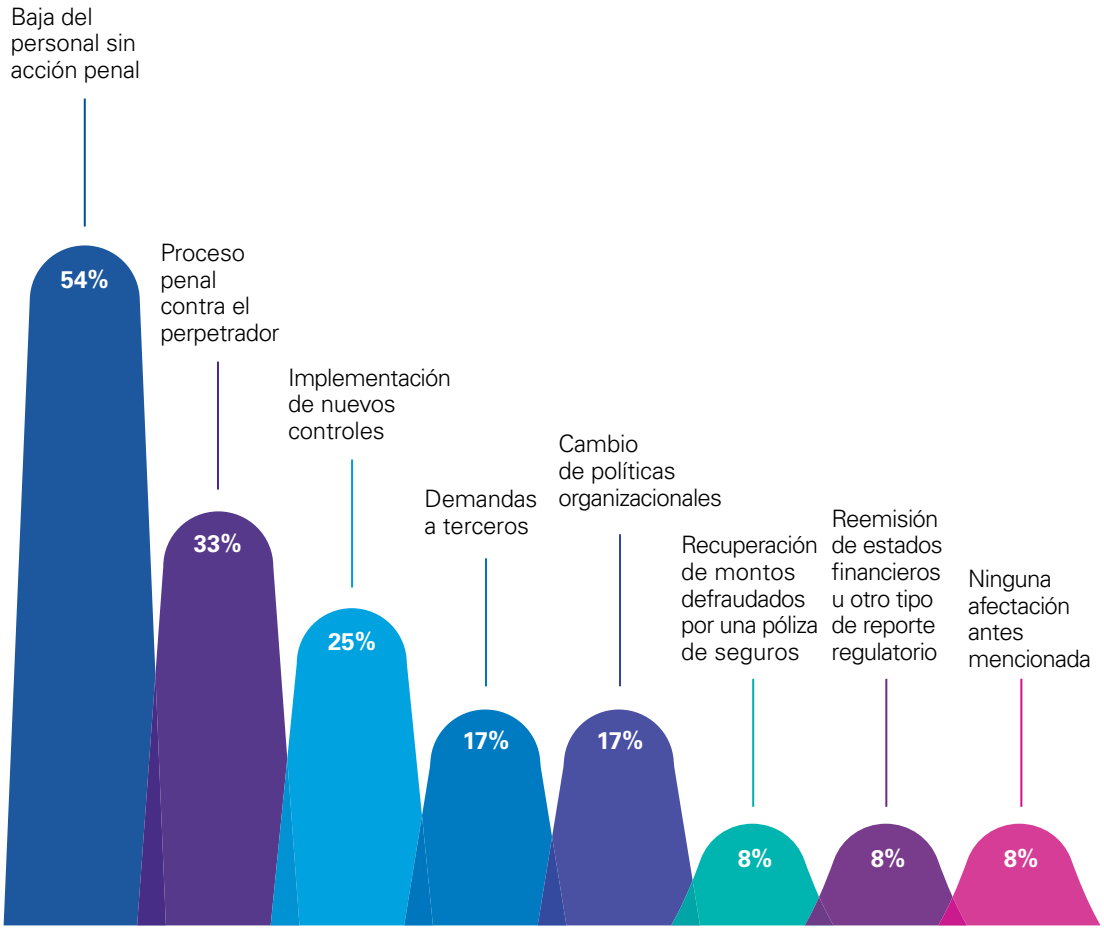



*Estos mecanismos fueron integrados en 2020.

### ¿Qué acciones se toman ante los fraudes?

El presente estudio muestra que, en la mayoría de las ocasiones, ante un caso de fraude, las empresas se limitan a dar de baja al personal implicado, sin iniciar un proceso legal. Solo 33% inició un proceso penal, y una cuarta parte implementó nuevos controles. En cuanto a cambio de políticas organizacionales, solo 17% las llevó a cabo.

## ¿Qué efecto tuvo el fraude en su organización?




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

### Programas antifraude

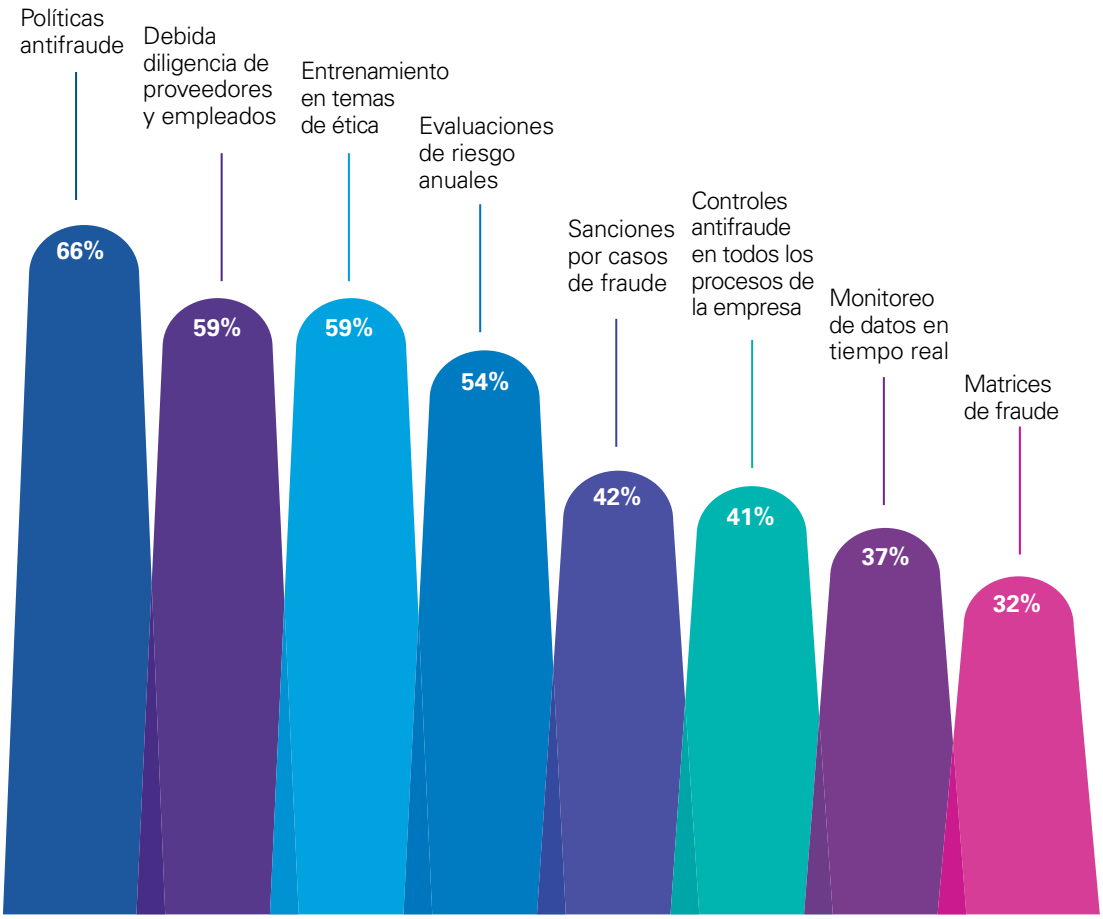
Una estrategia integral de prevención de fraude debe contar con un enfoque holístico. Si bien el fraude es un delito que afecta a todas las organizaciones, aún hace falta mayor compromiso para su combate. Únicamente 41% de las empresas participantes cuentan con un programa integral de prevención, detección y respuesta ante los potenciales casos de fraude.

**¿Su empresa cuenta con un programa integral de prevención, detección y respuesta ante potenciales casos de fraude?**


## La malversación de efectivo y otros activos son las modalidades de fraude interno que más se presentan en las empresas

Al preguntar qué elementos componen los programas de prevención del fraude en las compañías, encontramos que las políticas antifraude son lo más común, al estar presentes en 66% de los casos, seguidas de la debida diligencia a proveedores y colaboradores y del entrenamiento en temas de ética, ambos presentes en 59% de los programas.

**¿Qué elementos componen su programa integral de prevención, detección y respuesta ante potenciales casos de fraude?**




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Solo con un enfoque integral y programas de control e integridad adoptados en toda la organización, será posible disminuir o eliminar la incidencia de este delito que se gesta, en la gran mayoría de los casos, al interior de las empresas.

# Prevención de lavado de dinero y financiamiento al terrorismo (PLD/FT)

## La preocupante realidad en el cumplimiento de las leyes para PLD/FT

Nuestra encuesta revela que cerca de seis de cada diez empresas que respondieron están sujetas a las diferentes regulaciones mexicanas en materia de prevención de lavado de dinero y financiamiento al terrorismo (PLD/FT).

**¿Su empresa es de un sector que está obligado al cumplimiento de las leyes nacionales o internacionales en materia de prevención de lavado de dinero y financiamiento al terrorismo?**


Aunque la mayoría de las compañías están sujetas a dichas leyes PLD/FT, puede haber algunas que, a pesar de estar obligadas a su cumplimiento, consideran que se trata de "un tema de bancos".

## ¿Quiénes son sujetos a las leyes para PLD/FT en nuestro país?

Aunque el sistema financiero y las actividades vulnerables

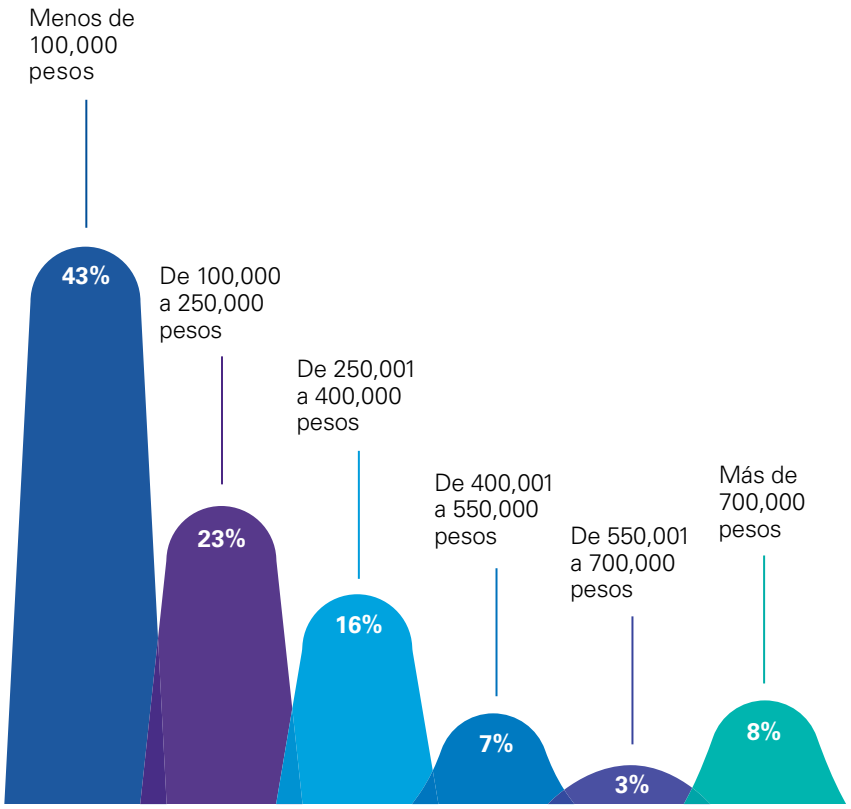
# 31% de las empresas sujetas al régimen PLD/FT no cuentan con un programa de prevención de lavado de dinero

(juegos de apuesta, comercialización de metales preciosos, recepción de donativos, intercambio de activos virtuales y las demás referidas en el artículo 17 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita) mantienen su propio marco normativo, la realidad mostrada por la Evaluación Nacional de Riesgos y por la Evaluación Mutua del Grupo de Acción Financiera Internacional (GAFI) sugiere un gran desafío: mientras no exista un nivel adecuado de conciencia sobre el marco normativo, se seguirán aprovechando estas brechas y utilizando diferentes sectores para fines ilícitos.

## Inversión en programas de PLD/FT

El presente estudio muestra que las compañías invierten en promedio 301,750 pesos anuales en sus programas de PLD/FT, cifra que representa, en promedio, 0.15% de las ventas. Por otra parte, 43% de las compañías invierten menos de 100,000 pesos anuales y solo 8% de las organizaciones invierten más de 700,000 pesos.

**¿Qué monto invierte anualmente en su plan de PLD/FT?**



Algunas de las inversiones elevadas que señala el estudio pueden estar destinadas a sistemas automatizados o a grandes remediaciones regulatorias, pero no necesariamente se está invirtiendo en esquemas prácticos y novedosos que, utilizando la tecnología, permitan robustecer los programas de PLD/FT a un costo asequible.

Un programa efectivo para PLD/FT debe considerar, cuando menos, políticas y procedimientos, sistemas automatizados, estructuras internas, entrenamiento y revisión de un externo independiente. Además, debe ser evaluado continuamente.

## Evaluaciones de los programas de PLD/FT y de los sistemas automatizados

Únicamente 55% de las organizaciones participantes han evaluado sus programas de PLD/FT en los últimos 12 meses, ya sea que la revisión sea hecha por la autoridad supervisora, el auditor interno o por un externo independiente.

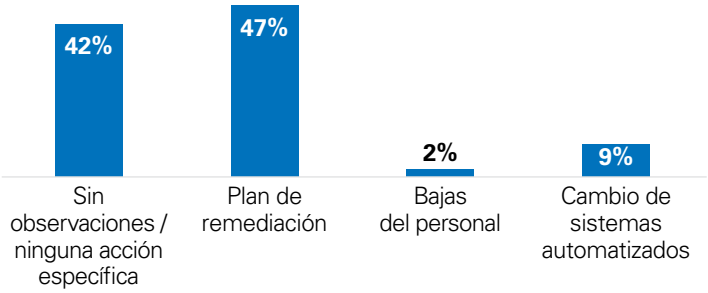
**¿Su programa de PLD/FT ha sido sujeto a evaluación (por la autoridad, por auditor interno o por un externo independiente) en los últimos 12 meses?**


## ¿Quién evalúa los programas de PLD/FT y qué efectos tienen?

Las evaluaciones de terceros independientes lideran la revisión de los programas de PLD/FT con 43%; las efectuadas por un auditor interno ocupan 24%, mientras que las que incluyeron ambas revisiones ocupan 33%.

Al preguntar qué efectos tuvieron en los programas de PLD/FT las observaciones realizadas por el tercero independiente o el auditor interno, 42% de las compañías mencionan que no se derivó en ninguna acción específica o que el resultado fue "sin observaciones", mientras que el efecto más común fue el de los planes de remediación, cuyo resultado ascendió a 47%. Tan solo 9% de los casos derivaron en cambios a los sistemas automatizados y 2% tuvo como consecuencia bajas de personal.

**¿Qué efectos tuvieron en su programa de PLD/FT las observaciones realizadas por el tercero independiente o auditor interno?**




## Pruebas de los sistemas automatizados

Los resultados permiten ver que 51% de los sistemas automatizados de PLD/FT no fueron sometidos a pruebas durante los últimos 12 meses y el 49% restante que sí fue probado, recurrió a un tercero independiente para hacerlo (60%), mientras en los otros casos estuvo a cargo de Auditoría Interna.

**¿Sus sistemas de monitoreo han sido sometidos a pruebas (integridad de datos, recreación de las reglas de negocio, generación de alertas) como parte de las revisiones anuales de cumplimiento?**


Considerando que 55% de las organizaciones manifestaron haber sometido a evaluación sus programas de PLD/FT y 51% sometió sus sistemas a pruebas, puede concluirse que 4% de las pruebas no consideraron los sistemas de monitoreo como parte de la revisión.

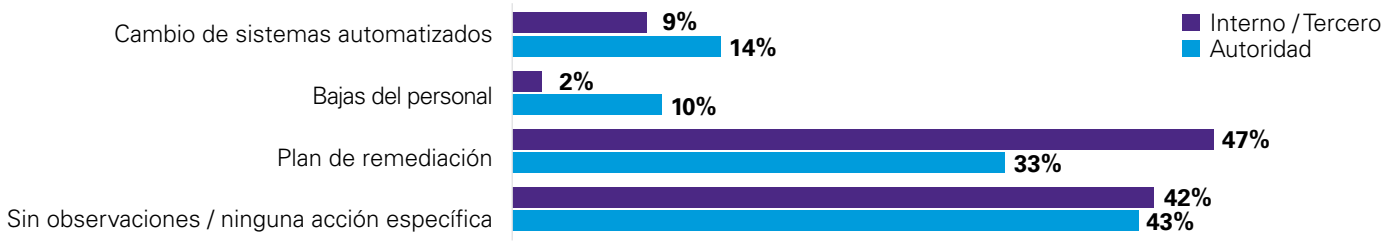
## Supervisión de las autoridades

Otro componente elemental de las estrategias de prevención es el de la supervisión regulatoria. Con los cambios en las

recomendaciones del GAFI publicados en 2012, esta revisión también se realiza basada en riesgos, con la finalidad de que la autoridad pueda, cuando menos una vez, evaluar *in situ* a todas las entidades que tiene bajo supervisión.

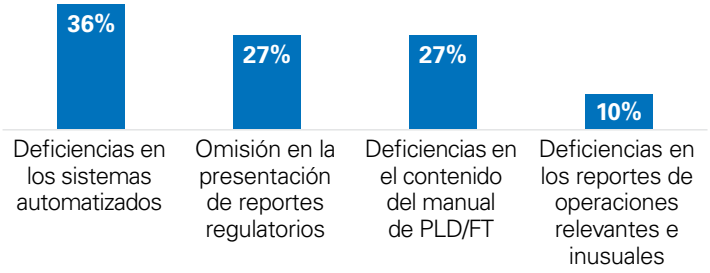
Solo 20% de las empresas participantes han recibido una visita por parte de la autoridad reguladora en los últimos 12 meses, y los resultados, en su mayoría, derivaron en "sin observaciones" (43%) y en planes de remediación (33%).

### ¿Qué efectos tuvieron en su programa de PLD/FT las observaciones realizadas por la revisión interna o de un tercero, así como de la autoridad reguladora?




Por otro lado, 10% de las compañías recibieron alguna multa o sanción en materia de PLD/FT en los últimos 12 meses y las principales razones fueron deficiencias en los sistemas automatizados (36%), seguida de la omisión en la presentación de reportes regulatorios (27%) e insuficiencias en el contenido del manual de PLD/FT (27%).

### ¿Cuál fue la razón principal de las multas impuestas?




> 43% de las empresas sujetas al régimen de PLD/FT invierten menos de 100,000 pesos anuales en sus programas de prevención

### Incremento en los costos regulatorios

El presente estudio revela que 58% de las organizaciones sujetas al régimen PLD/FT consideran que los cambios regulatorios han incrementado el costo del cumplimiento 20%, situación que guarda relación con las tendencias internacionales.

Sin embargo, los altos costos de ser sujeto de multas o sufrir ilícitos lleva a considerar los programas integrales para prevenir estos crímenes como una inversión y un elemento indispensable en la gestión de riesgos.

# El impacto de la corrupción

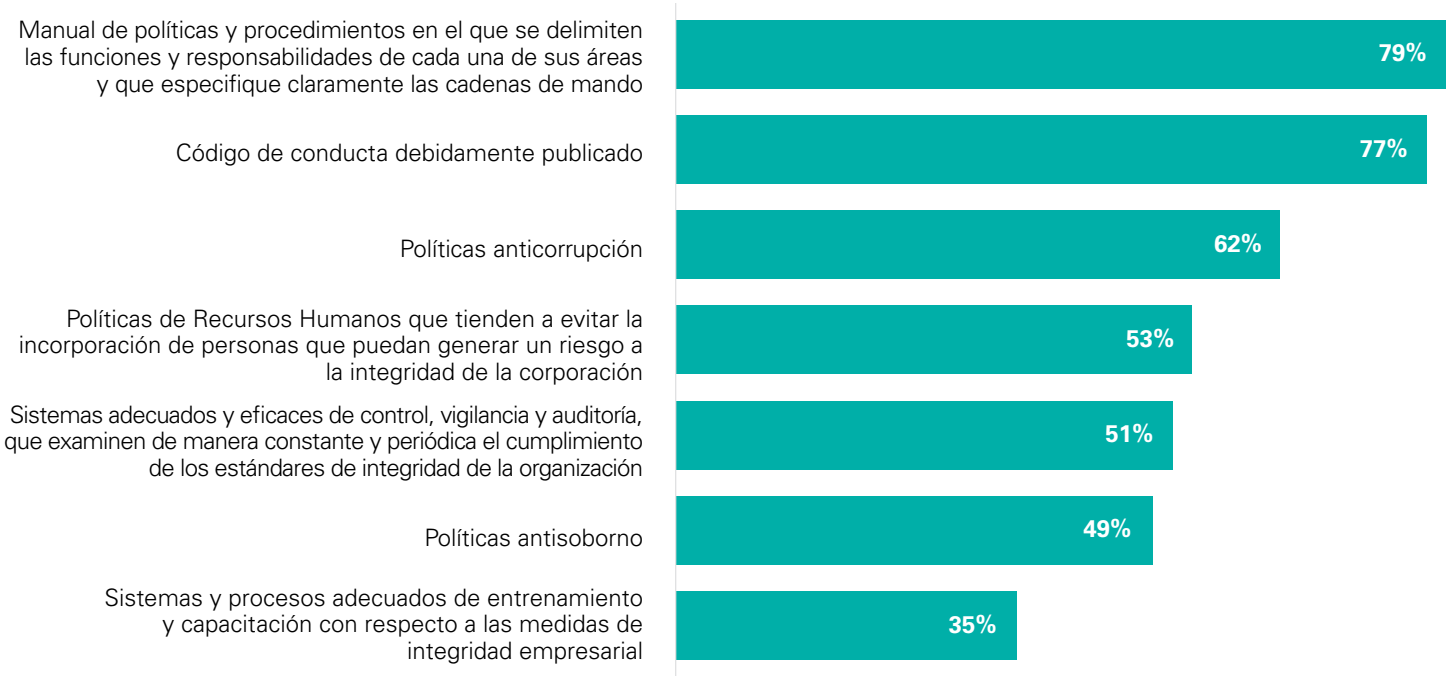
## Panorama general de los programas anticorrupción

Con un costo anual estimado de más de 5% del producto interno bruto (PIB) global,[1] la corrupción sigue creciendo y dispersándose, a pesar de todas las medidas que la comunidad internacional y cada uno de los países han establecido para luchar en contra de este flagelo.

El presente estudio revela que 53% de las empresas sí cuentan con un programa de integridad empresarial (política anticorrupción), ya sea por cumplimiento a las leyes extranjeras o nacionales, en los casos aplicables.

Al preguntar qué elementos conforman su programa de integridad, el resultado más común es el de contar con manuales de políticas y procedimientos en los que se delimitan las funciones y responsabilidades de cada una de las áreas y se especifican claramente las cadenas de mando (79%), seguido de los códigos de conducta debidamente publicados (77%).

### ¿Qué elementos componen su programa de integridad empresarial (política anticorrupción)?




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.
Las opciones de los elementos se tomaron de acuerdo a los descritos en la Ley General de Responsabilidades Administrativas.

Por otra parte, seis de cada diez empresas manifiestan contar con políticas anticorrupción, las cuales delimitan el marco de actuación al interior de estas, y son una declaración escrita de la administración respecto a la prohibición de participar en actos de corrupción.

Asimismo, 53% de las organizaciones cuentan con políticas de Recursos Humanos que buscan evitar la incorporación de personas que presenten un riesgo de integridad, denominadas "conoce a tu empleado" (*know your employee*, KYE). Sin embargo, 49% manifiesta contar con políticas antisoborno. Si no se tiene una declaración formal, escrita de la administración respecto a la prohibición de dar, ofrecer o recibir sobornos, se corre el riesgo de que el talento racionalice la conducta con un simple "yo no sabía" o "nadie me dijo que no podía". Adicionalmente, solo 35% de las empresas manifestaron contar con sistemas y procesos de entrenamiento y capacitación sobre las medidas de integridad.

Cuando no existe una correcta difusión por parte de la administración de las medidas existentes, estas pierden efectividad. Además, es necesario contar con entrenamiento continuo en el marco de un efectivo programa de integridad empresarial.

## Líneas éticas o de denuncia

Las líneas éticas o de denuncia, en especial las operadas por terceros, son de suma utilidad para los programas de integridad empresarial.

Actualmente, el mantenimiento de una línea ética es obligatorio en algunas jurisdicciones y ciertas corporaciones trasnacionales. En el caso de nuestro estudio, 62% de las empresas manifestó contar con una línea de denuncia; sin embargo, en la mayoría de los casos esta es operada internamente (59%).

La experiencia nos ha mostrado que si bien el mantener una línea interna es útil, no resulta siempre lo más eficiente. En cambio,

[1] United Nations (2018). *The cost of corruption: values, economic development under assault, trillions lost, say Guterres*. Recuperado de: https://news.un.org/en/story/2018/12/1027971.

contar con una operada de manera externa transmite al capital humano y a externos que las denuncias serán recibidas de manera anónima, lo cual brinda confianza para recurrir a este mecanismo. Además, conviene hacer extensiva esta modalidad de denuncia a proveedores y otras partes interesadas.

### ¿Es operada internamente por empleados o externamente por una empresa independiente?


Nuestro estudio muestra que 56% de las líneas éticas con las que cuentan las empresas abarcan tanto a la fuerza laboral como a proveedores, situación que nos muestra un mayor compromiso en el combate a la corrupción, ya que la información que los proveedores pueden proporcionar sobre potenciales actos de corrupción es clave para su temprana atención.

### ¿Abarca tanto a la fuerza laboral como a proveedores?


Las líneas éticas son herramientas que brindan grandes beneficios a las organizaciones. Con la adecuada implementación de las rutas críticas correspondientes, las compañías pueden obtener valor de estos mecanismos.

## Pagos de facilitación

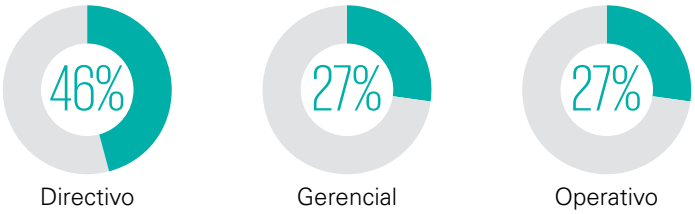
Los pagos de facilitación están prohibidos bajo varias leyes y programas anticorrupción. Sin embargo, 25%* de las empresas tuvieron conocimiento de que en su sector, en los últimos 12 meses, las organizaciones realizaron pagos para facilitar trámites, permisos o transacciones de negocios recurriendo, en la mayor parte de los casos, a un tercero (72%).

Cabe señalar que la corrupción privada es un problema que ha ido creciendo, pues tres de cada diez pagos (26%) realizados tenían como destinatario un particular, lo que expone las fallas que pueden estar teniendo los programas de integridad empresarial.

## ¿Quién realiza los pagos?

Nuestro estudio pudo confirmar que 46% reconoce haber realizado pagos de facilitación desde niveles directivos.

### ¿A qué nivel consideraría o tiene conocimiento de que las empresas de su sector realizan los pagos de facilitación?

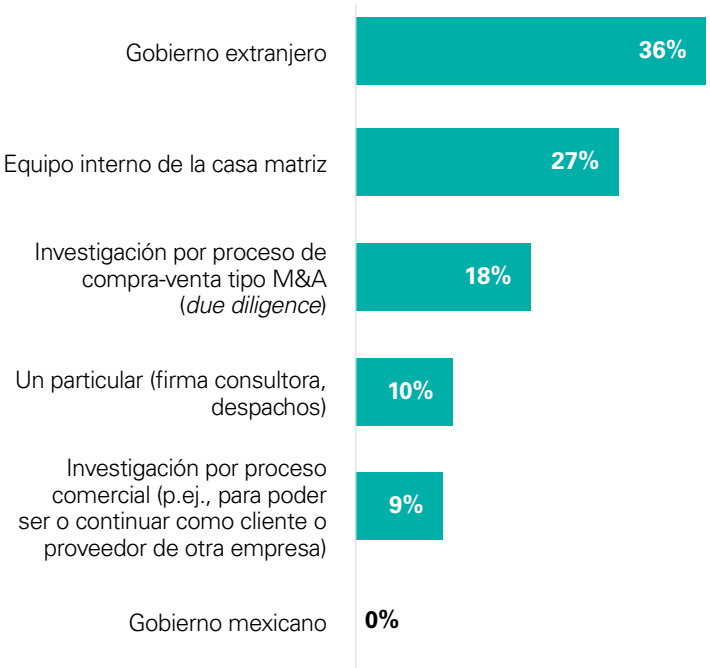



Considerando lo anterior, es necesario que las organizaciones fortalezcan la integridad empresarial e investiguen a fondo cualquier denuncia de posibles actos de corrupción.

## Sujetos a investigación

Por otro lado, 6% de las organizaciones han sido involucradas en investigaciones por corrupción o soborno en los últimos 12 meses. Dichas investigaciones fueron realizadas principalmente por gobiernos extranjeros (36%); el segundo ejecutor de las investigaciones fueron los equipos internos de la casa matriz (27%), muchas de estas ubicadas en el extranjero; en tercer lugar se ubicaron los *due diligence,* o diligencia debida efectuada en un proceso de compraventa, como herramienta elemental para la identificación de riesgos no solo de la corrupción, sino de los delitos financieros en general.

### La investigación fue llevada a cabo por…



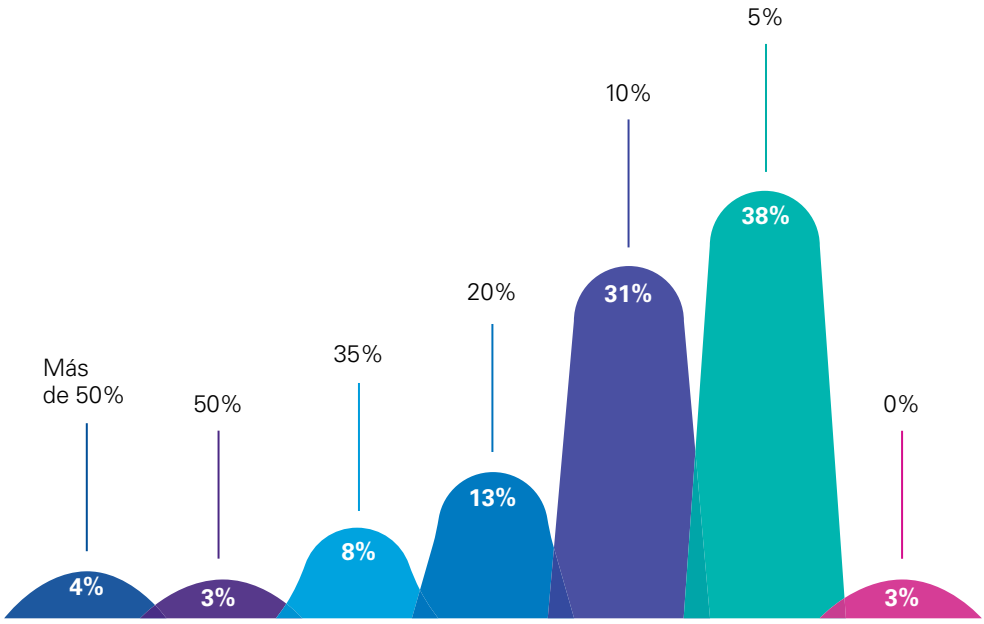

*Derivado de que el procedimiento de levantamiento y análisis de la información fue completamente anónimo, KPMG no tiene manera de conocer quiénes realizan estos pagos.

El alcance extraterritorial de la Ley de Prácticas Corruptas en el Extranjero, de los Estados Unidos (*Foreign Corrupt Practices Act* o FCPA) es una de las mejores armas para combatir la corrupción en el extranjero y la tendencia a realizar investigaciones internacionales está creciendo, ante la imperante necesidad de intercambiar información y llegar hasta las últimas consecuencias.

## El costo de la corrupción

Los datos muestran que 72% de las empresas consideran que la corrupción en nuestro país representa costos para su negocio. Mientras 38% equipara el daño a 5% de las utilidades netas, 31% ubica las afectaciones en 10%, y un alarmante 7% considera que los costos ascienden a 50% o más de dichas utilidades.

**¿Qué porcentaje de la utilidad neta de su empresa estima que se ha visto afectada por el costo de la corrupción que existe en el país?**




En los costos indirectos de la corrupción, 30% de las empresas de nuestro estudio manifiestan haber perdido contratos o licitaciones por no aceptar pagar un soborno.

Considerando los datos mostrados, es posible observar que contar con programas de integridad anticorrupción empresarial no solo favorece a las empresas, sino que influye positivamente en la transformación de la sociedad. El uso de nuevas tecnologías y la implementación de una estrategia integral de combate al crimen financiero, puede permitir robustecer los programas de integridad y con esto, lograr una estrategia de combate a la corrupción más eficaz y eficiente.

En los costos indirectos de la corrupción, 30% de las empresas manifestaron perder contratos o licitaciones por no aceptar pagar un soborno

# La vulnerabilidad ante ciberataques

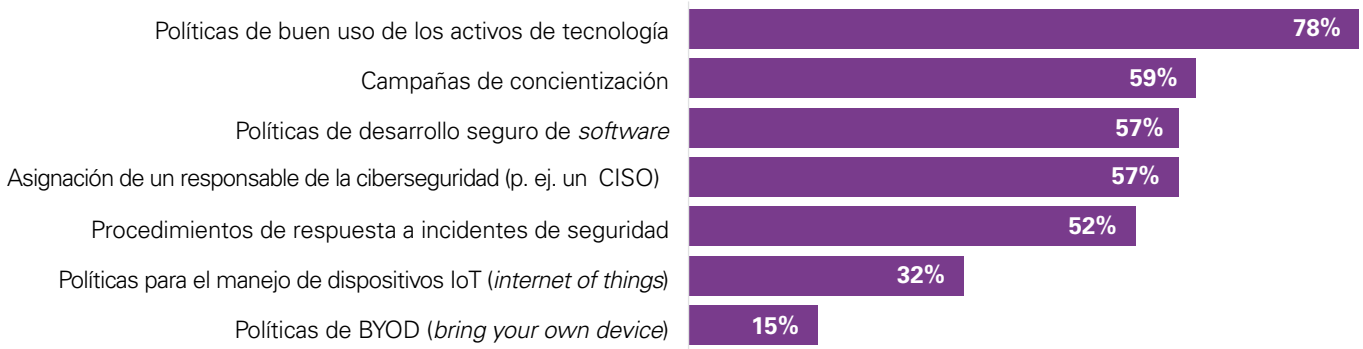
## Situación general de los programas de ciberseguridad

Según datos del estudio *Clarity on Cybersecurity* realizado en 2018 por KPMG en Suiza, 80% de los consejos de administración de las empresas consideran la ciberseguridad como un riesgo operativo; sin embargo, solo 36% menciona el tema en sus reportes anuales.

Asimismo, según el *Estudio Integral de la Función de Auditoría Interna en México* publicado en 2019 por KPMG en México, la ciberseguridad ocupó el primer lugar de "riesgos relevantes" de acuerdo a los auditores internos de las organizaciones encuestadas.

El presente estudio muestra que 63% de las compañías han establecido lineamientos y políticas en materia de ciberseguridad, cuyo principal componente es el de las políticas de buen uso de activos de tecnología (78%). Asimismo, cerca de 60% de las organizaciones cuentan con una persona responsable de la ciberseguridad, como el Oficial de Seguridad de la Información (*Chief Information Security Officer* o CISO).

### ¿Qué clase de lineamientos y políticas tiene en materia de ciberseguridad?

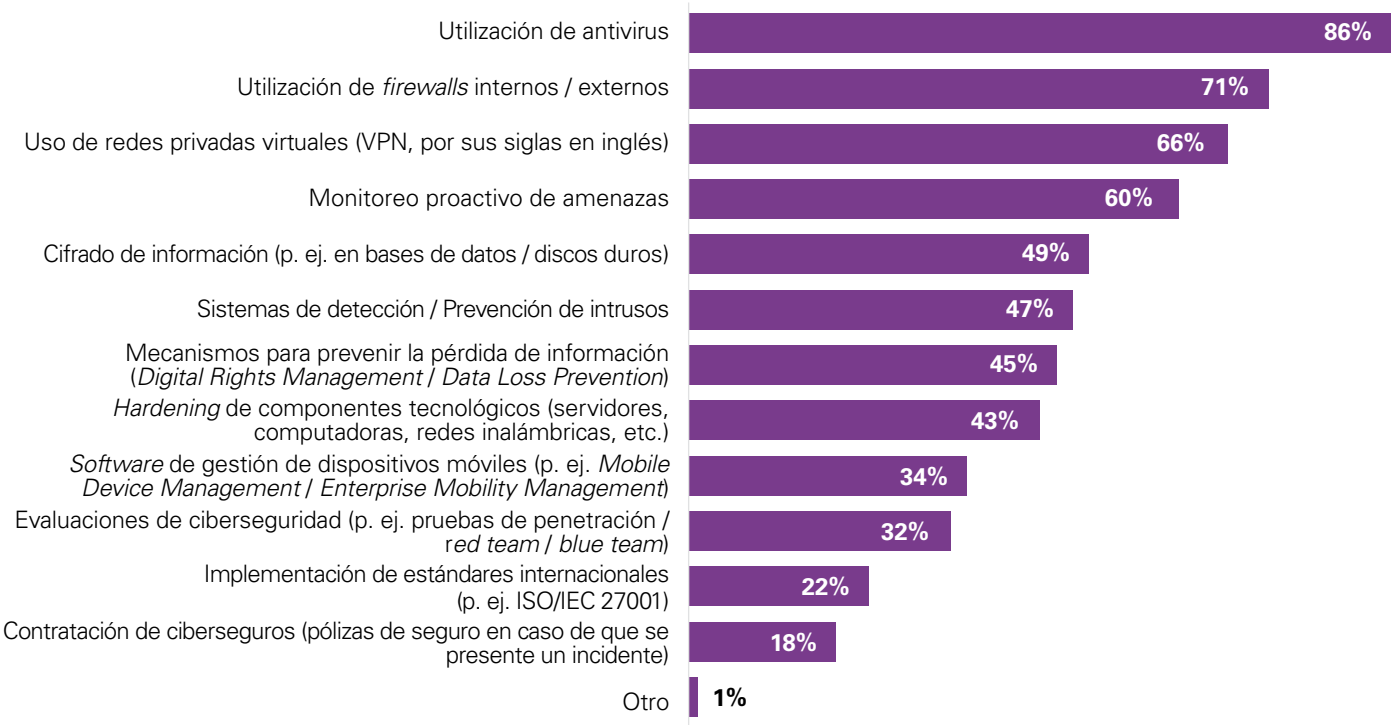



La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

## Controles más comunes

Respecto a los controles para la ciberseguridad, 70% de las empresas manifiestan haber implementado alguno, siendo la utilización de antivirus (86%) el más recurrente, seguido por los *firewalls* internos o externos (71%). Tan solo tres de cada diez compañías afirman haber realizado evaluaciones de ciberseguridad, tales como pruebas de penetración; cabe señalar que dichas pruebas son obligatorias para los bancos y otras entidades del sistema financiero. Por otra parte, solo dos de cada diez entidades contrataron algún ciberseguro, lo que muestra un área de oportunidad en la mitigación de los efectos de estos delitos. Los mecanismos para prevenir la pérdida de información solo estuvieron presentes en cuatro de cada diez empresas.

### ¿Qué clase de controles?




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

## Ciberataques, una realidad creciente

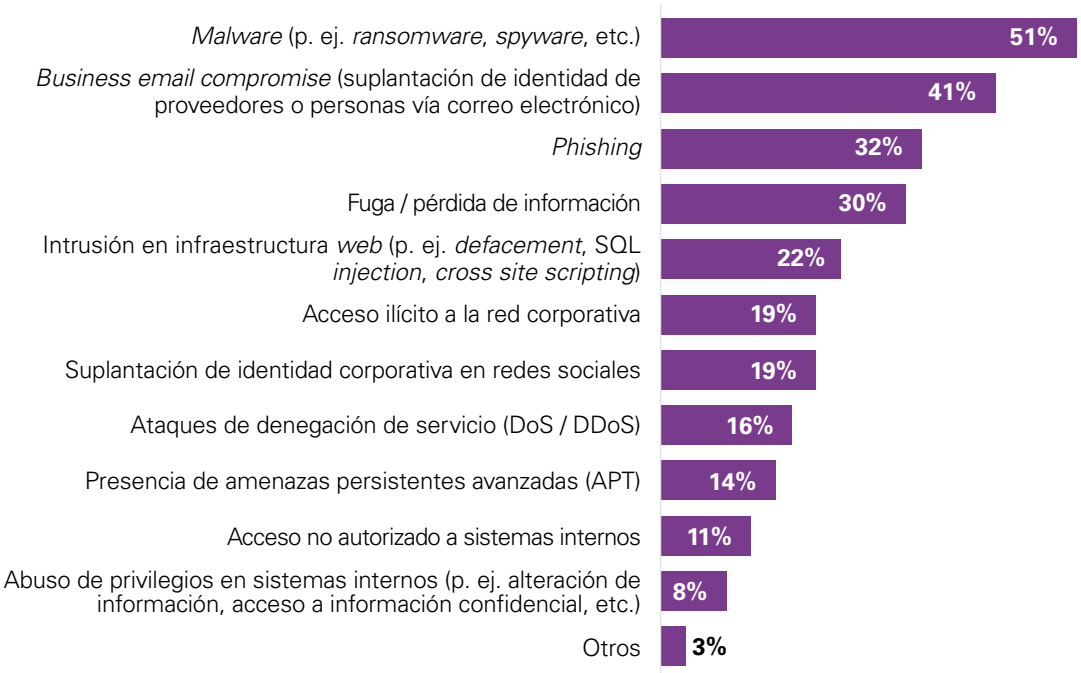
Según un estudio de 2018 realizado por Bromium, *Hyper-connected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually*, el crimen cibernético genera USD 1.5 billones al año; si fuera un país, su PIB sería el número 13 a nivel global.

El presente estudio revela que 23% de las empresas fueron víctimas de algún incidente de ciberseguridad en los últimos 12 meses, siendo la presencia de *malware* o *software* malicioso (51%) el incidente más común, seguido de la suplantación de identidad de proveedores o de personas vía correo electrónico institucional (41%), fenómeno conocido como *business email compromise*.

Con un alarmante 32%, el *phishing* se ubica en el tercer lugar de los incidentes de seguridad, a pesar de que cada vez es más común escuchar y leer advertencias en portales bancarios e instituciones de gobierno sobre esta amenaza.

La fuga o pérdida de información acapara 30% de los incidentes, lo que expone la falta de controles para el manejo de la información privilegiada, confidencial o sensible; por ejemplo, el uso de cifrado en los dispositivos y bases de datos.

### ¿Qué tipo de incidentes?



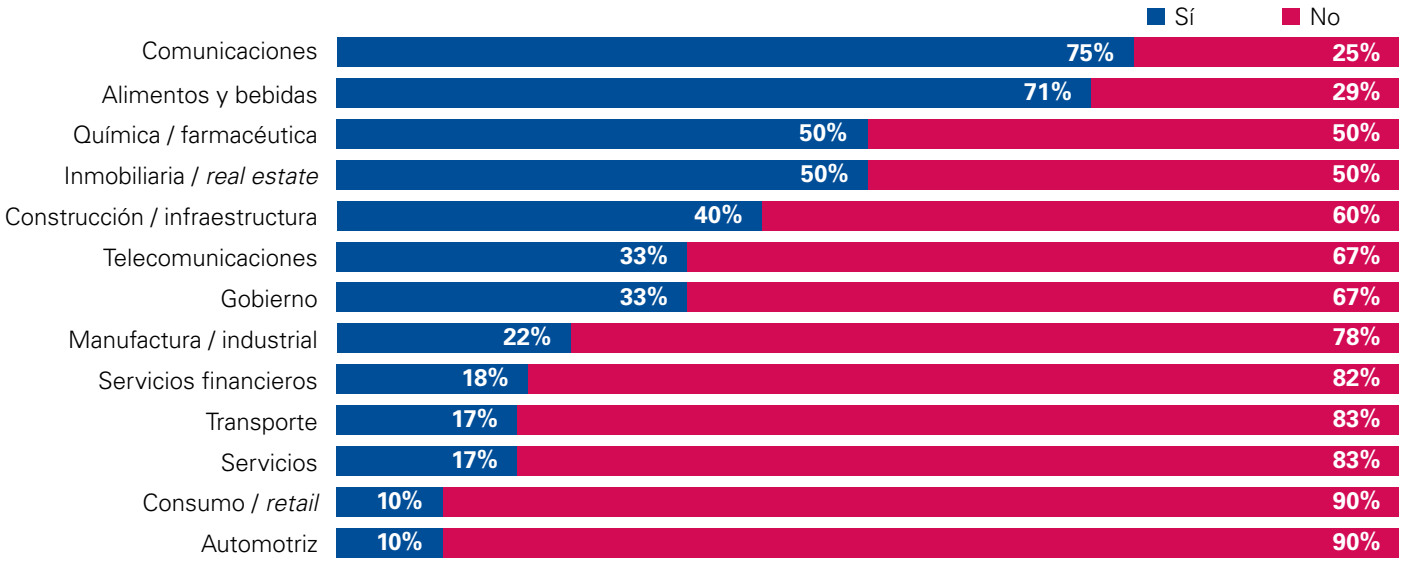

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

> 23% de las empresas fueron víctimas de un incidente de ciberseguridad reciente, siendo el más popular la utilización de *malware*, seguido de la suplantación de identidad de proveedores y personas en los correos electrónicos corporativos

Las amenazas persistentes avanzadas, con una incidencia de 14%, pueden permanecer sin detección por periodos prolongados (meses o años). Bajo esta modalidad, un atacante o grupo de atacantes logra infiltrarse en los sistemas de una organización (generalmente usando técnicas de *phishing*) y observar los procesos, flujos de aprobación y el día a día de la organización. De esta manera obtiene acceso a sistemas y usuarios clave con los que puede realizar operaciones, sobrepasando los controles de segregación de funciones establecidos. El impacto potencial es muy alto.

En este sentido, el sector con mayores incidentes fue el de comunicaciones (75%) y el principal incidente sufrido por este sector fue el de ataques de denegación de servicios (DoS / DDoS), mismo que consiste en que varios sistemas comprometidos, generalmente con un virus, son utilizados para bloquear o negar el acceso a otro sistema, con la finalidad de inhabilitarlo.

## En los últimos 12 meses, ¿su empresa fue víctima de un incidente de ciberseguridad?



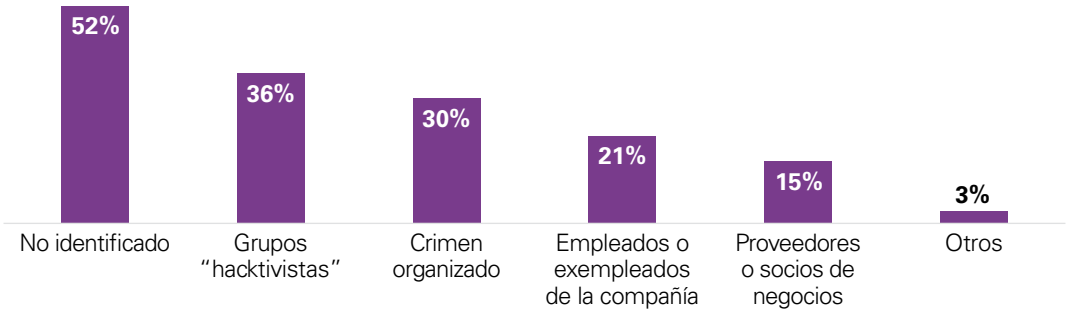

La segunda industria con mayores ataques fue la de alimentos y bebidas (71%), con la modalidad de *business email compromise* (suplantación de identidad de proveedores o personas vía correo electrónico institucional) y el tercer lugar lo ocuparon la industria inmobiliaria (50%) y la química (50%), con las modalidades de *business email compromise* y *phishing* para la primera, e intrusión en infraestructura *web* para la segunda.

En el caso de los servicios financieros, únicamente 18% reportó algún incidente y la principal modalidad fue la del *malware* (57%), seguida por el acceso ilícito a la red corporativa y la intrusión en la infraestructura *web*, ambas con 43%.

Una señal de que es necesario robustecer la estrategia de ciberseguridad en las organizaciones es que en la mitad de los incidentes, no fue posible identificar el origen, mientras que 66% fue causado por grupos del crimen organizado o grupos "hacktivistas".

Por otra parte, 21% fue ejecutado por empleados o exempleados de las compañías, lo que nos muestra una gran falla en el ambiente de control y falta de difusión al interior de las organizaciones.

## ¿Tiene conocimiento del origen del incidente?



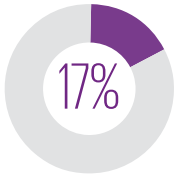

La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Si bien los incidentes de ciberseguridad deberían identificarse lo más rápido posible a fin de accionar los planes de respuesta y minimizar los potenciales daños, 39% de dichos incidentes tomó a las empresas una semana detectarlos, mientras que 36% fueron detectados en un día.

## ¿Cuánto tiempo le tomó identificar el incidente?

Un día

Una semana



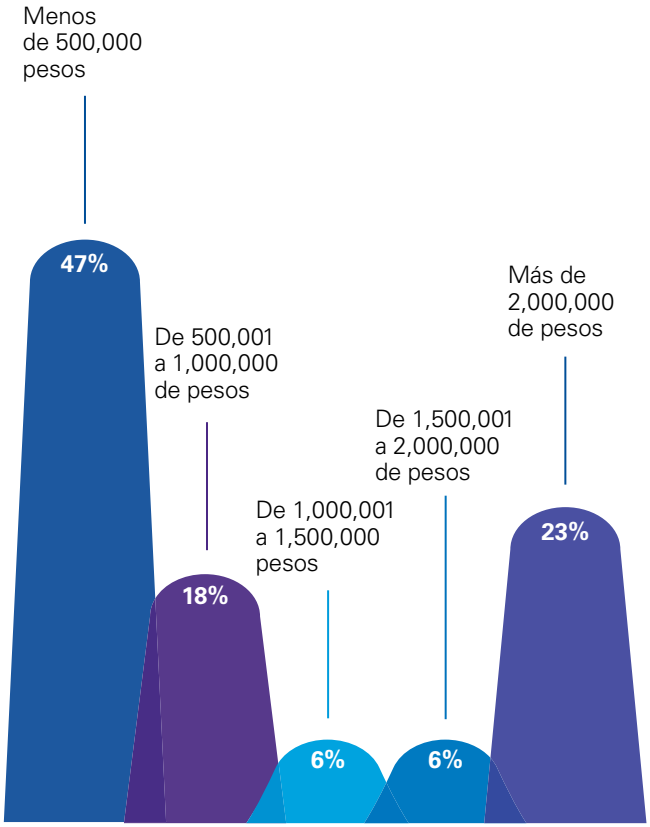
Un mes

Más de un mes

Más de seis meses

**¿Qué repercusiones tienen los ciberataques?**
El presente estudio revela que la mitad de las empresas sufrieron daños económicos; en 22% las afectaciones fueron de índole legal y en 17%, reputacional. Asimismo, cada incidente, considerando, adicionalmente a las pérdidas, los gastos para la atención del evento, tuvieron un costo de más de 1 mdp. Por su parte, 47% de las empresas revelaron afectaciones por debajo de medio millón de pesos, mientras que 23% se ubicó en el extremo contrario, con costos de más de 2 mdp por incidente.

## ¿Cuál fue el costo generado por el incidente?




La principal manera de responder a los incidentes fueron las investigaciones internas (43%), seguidas de investigaciones internas y externas (43%). Sin embargo, 3% de los incidentes permanecieron sin ninguna clase de atención.

## ¿Cómo respondió al incidente?

Investigación interna

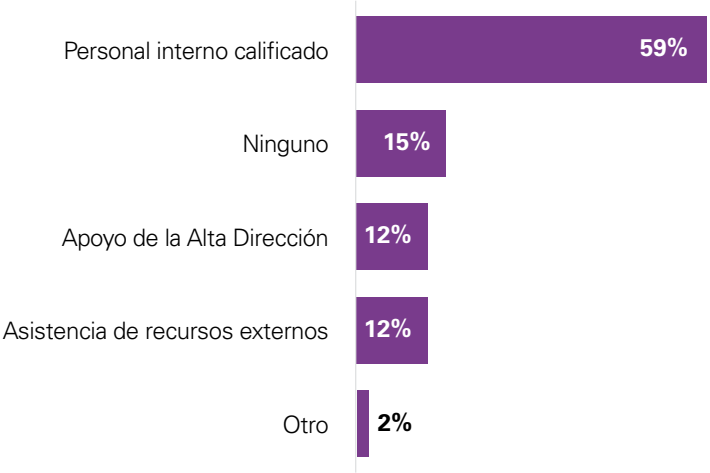
Investigación externa

Ambas

No fue atendido

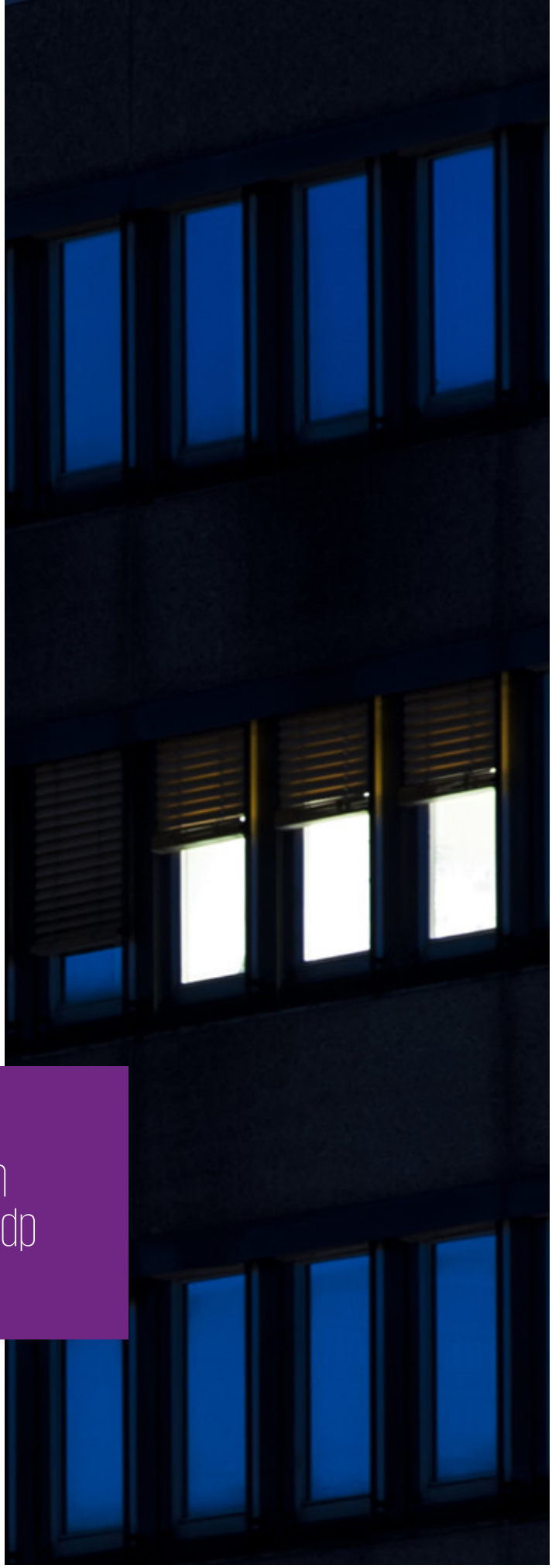
Al igual que en otros delitos económicos, la investigación externa siempre es la más recomendada, ya que permite el desarrollo de una estrategia más eficiente, donde las técnicas de investigación y de recuperación de la evidencia permitirían usar la información para presentar una denuncia en un proceso penal o respaldar un reclamo con la aseguradora. Sin embargo, 59% de las empresas hubieran preferido contar con personal interno calificado para realizar la investigación.

**En general, ¿con qué recursos hubiera querido contar para atender de forma más efectiva el incidente?**




Las amenazas sobre la ciberseguridad son una realidad creciente, ante la que permanecen aún vulnerables las organizaciones. Vale la pena que cada empresa evalúe el costo-beneficio de contar con las herramientas y otros recursos adecuados en el marco de una gestión integral de riesgos, ya sea personal interno calificado que representaría un costo fijo, o bien la asesoría de un externo.

Los incidentes de ciberseguridad representaron un daño económico en promedio para las empresas de 1.2 mdp por cada incidente



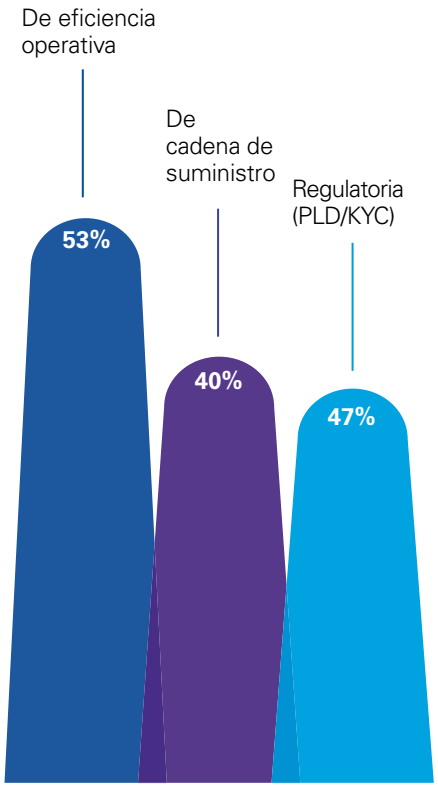
# Nuevas tecnologías y la prevención del crimen financiero

Una visión integral de gestión de riesgos permite reinventar los procesos tradicionales y adoptar las tecnologías emergentes para prevenir el crimen financiero.

La explotación de datos hace posible generar redes más complejas de inteligencia para el análisis de nuevas amenazas, a fin de evitar que se materialicen. Los esquemas de automatización robótica de procesos (*robotic process automation*, RPA), el aprendizaje de computadoras (*machine learning*) y la inteligencia artificial (AI, por sus siglas en inglés), son solo algunos ejemplos de lo que la Cuarta Revolución Industrial nos ofrece.

De acuerdo con el estudio Perspectivas de la *Alta Dirección en México 2020*, 11% de las organizaciones consideran que *blockchain* será una de las iniciativas relevantes para mejorar su competitividad en los próximos tres años. El presente análisis arroja que 53% considera esta solución como la mejor opción para atacar una problemática en la eficiencia operativa, ya que brinda herramientas para la prevención del fraude, principalmente en la cadena de suministro y en la prevención de lavado de dinero, generando la posibilidad de crear registros, contratos inteligentes y herramientas que no pueden ser alteradas y que muestran en tiempo real las transacciones, mismas que pueden hacerse públicas y auditables.

**¿Desarrollaría soluciones *blockchain* para atender qué tipo de problemática?**




La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

En línea con la implementación de las nuevas tecnologías, es relevante destacar que México se ha posicionado como un país referente en la regulación de las denominadas *fintech* (empresas que combinan la tecnología y los servicios financieros), con la publicación de la Ley para Regular las Instituciones de Tecnología Financiera.

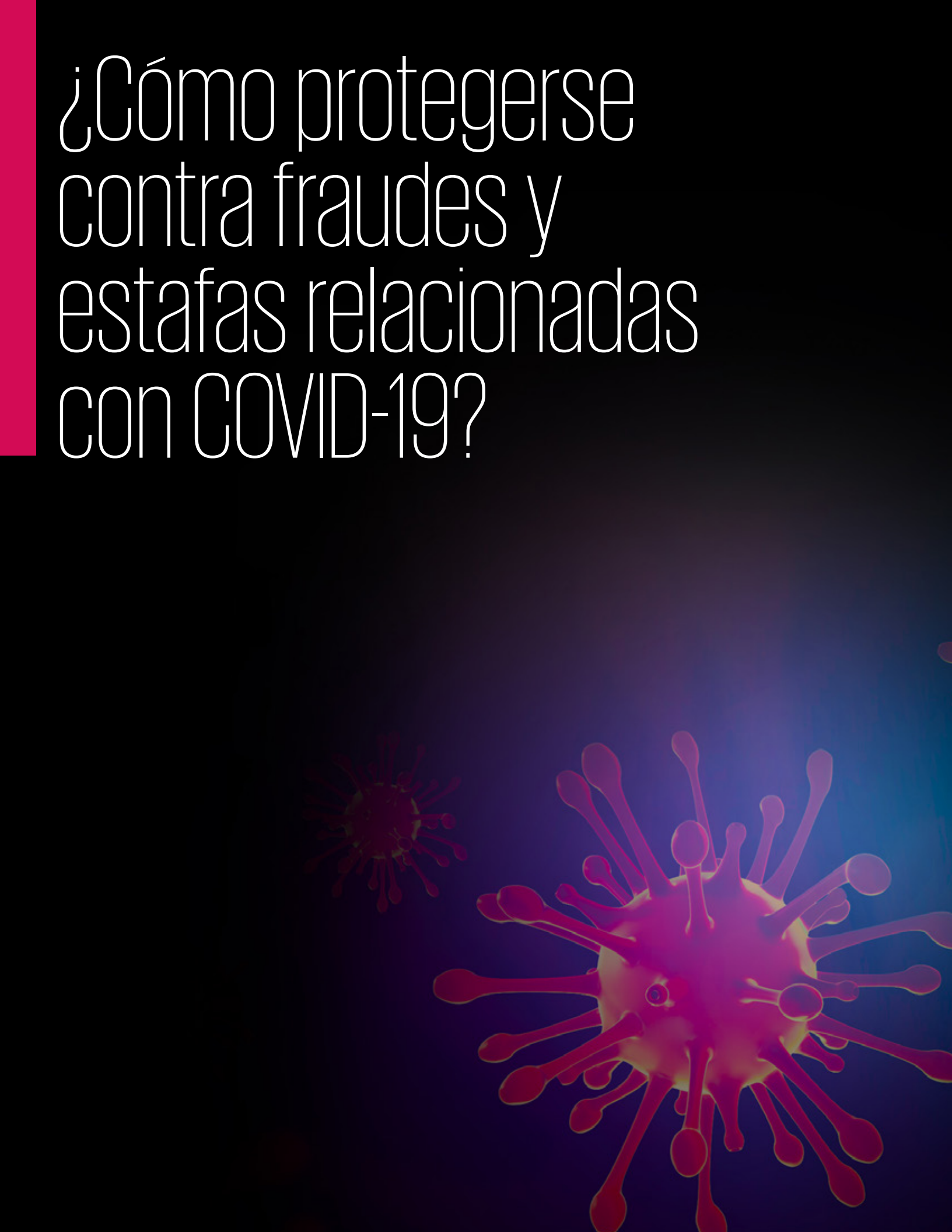
La denominada Ley Fintech se enfoca principalmente en cuatro grandes servicios tecnológicos: *crowdfunding* (financiamiento colectivo); pagos electrónicos, criptoactivos y aplicaciones de programación de interfaces (API, por sus siglas en inglés). Aunque el Banco de México ha procurado tener una posición conservadora respecto al uso de los criptoactivos, la industria de estos nuevos instrumentos sigue creciendo y desarrollándose.

Nuestro estudio muestra que 4% de las empresas han considerado la adopción de los criptoactivos como método de pago, mientras que 3% lo ha considerado para levantar fondos o una combinación de ambas opciones, todo ello en un plazo promedio de 2.6 años. Además, 6% ha considerado alternativas como el *crowdfunding*; 5% la emisión de *initial coin offerings* (ICO) y 5% está evaluando ambas opciones para financiar proyectos.

Si bien no son porcentajes elevados, nos muestra nuevamente que las empresas no han dejado de lado este gran desarrollo tecnológico que presenta múltiples posibilidades de maximizar el valor de los activos reales y de la economía en general.

Sin duda, con los adecuados programas de prevención, detección y respuesta ante crímenes financieros, las organizaciones podrán aprovechar mejor las oportunidades de innovación que van surgiendo en el ecosistema empresarial.

# ¿Cómo protegerse contra fraudes y estafas relacionadas con COVID-19?



La pandemia de COVID-19 ha tenido consecuencias significativas en nuestra sociedad. A partir de esta crisis, la delincuencia organizada elaboró campañas orquestadas a gran escala para defraudar a los clientes bancarios, aprovechando el miedo y la ansiedad relacionados con la contingencia. En estos tiempos difíciles e inciertos, los estafadores aprovechan la incertidumbre que se genera durante una emergencia de salud pública, buscando lucrar con el deseo de recuperar un sentido de seguridad.

En todo el mundo se ha incrementado el número de estafas asociadas a la COVID-19. Los cibercriminales están aprovechando la pandemia para invitar a posibles víctimas a descargar archivos infectados mediante vínculos que no siempre parecen sospechosos. Los delincuentes están sacando ventaja de las búsquedas en internet a gran escala y la curiosidad relacionada con el virus, creando programas maliciosos para ocultarlos dentro de archivos relacionados con dicha enfermedad.

Además, a medida que los gobiernos preparan los paquetes de estímulos económicos como respuesta a la pandemia, y comiencen a brindar apoyo fiscal a sus ciudadanos, es muy probable que se incremente el riesgo de fraude por estafas.

Existen retos importantes para algunos sectores en particular, como los de servicios financieros, productos farmacéuticos, ciencias de la vida y telecomunicaciones. Estos ya han comenzado a dar una respuesta sin precedentes y a resolver las dificultades relacionadas con la continuidad de sus negocios. La demanda supera a la oferta con creces, ya que los clientes preocupados saturan los centros de atención a clientes con llamadas, intentando resolver asuntos relacionados con los tipos de fraude que parecen cambiar cada hora.

## Las estafas relacionadas con COVID-19 incluyen:

### Estafas impulsadas por la tecnología

1) ***Phishing*:** el objetivo de los impostores, quienes afirman ser miembros de renombradas autoridades de salud nacionales e internacionales, como el Centro para el Control y la Prevención de Enfermedades (CDC) de Estados Unidos o la Organización Mundial de la Salud (OMS), es llegar a sus víctimas por medio de correos electrónicos con anexos maliciosos o enlaces a "actualizaciones" sobre la propagación de COVID-19, a nuevas medidas de contención, mapas del brote o información sobre cómo protegerse de la exposición. Una vez abiertos, dichos anexos o enlaces infectan la computadora o el teléfono con algún programa maligno (*malware*) o exponen datos personales confidenciales, números de tarjetas de crédito y otra información, de forma que se transmiten a quien manipulará y sacará ventaja de dichos datos sensibles.

2) **Sitios de internet fraudulentos relacionados con COVID-19:** ya ha habido un incremento importante en el registro de múltiples dominios en internet que llevan el nombre "COVID". Estos sitios falsos parecen ser auténticos sitios de internet creados por organizaciones reconocidas; sin embargo, contienen *malware* diseñado para infectar las computadoras u otros dispositivos, como los teléfonos celulares.

3) **Riesgos relacionados con el correo electrónico del dominio empresarial:** el incremento del trabajo a distancia, acompañado del envío de actualizaciones de información sobre COVID-19 a todos niveles dentro de las organizaciones, han abierto la puerta a los estafadores, quienes dirigen sus ataques a las empresas y a su fuerza laboral. Mediante el uso de correos electrónicos disfrazados de actualizaciones de COVID-19, los criminales informáticos intentan engañar a las víctimas para que compartan su identidad y credenciales, solicitando que inicien sesión en el portal COVID-19 de una empresa falsa. Una vez que el usuario entra con sus credenciales, el estafador obtiene acceso ilimitado a las cuentas empresariales y a la red de la organización donde colabora. Esto facilita la ocurrencia de ataques BEC (Business E-mail Compromise) donde se suplanta la identidad de personal clave de la empresa ante terceros o al interior de la organización, para solicitar desembolsos de dinero o cambios en las cuentas utilizadas para recibir pagos.

4) **Ataques de *ransomware*:** las instituciones de gobierno y las organizaciones privadas están viendo un repunte en ataques de *ransomware*, programa de *software* malicioso que infecta los dispositivos y muestra mensajes exigiendo un pago para restablecer el funcionamiento del sistema. Lo primero que hacen los estafadores en este tipo de ataque, es comprometer la seguridad de los servidores críticos y las terminales conectadas, para luego encriptarlas. El ataque de *ransomware* bloquea el sistema operativo y los archivos del usuario final, haciéndolos inaccesibles hasta que se pague un rescate al atacante, quien suele demandar el pago en criptomonedas (*bitcoins*). A medida que el acceso remoto a las computadoras se convierta en la norma para "trabajar en casa" debido a las medidas de confinamiento, se espera que el incremento de estos ataques paralice la infraestructura de Tecnologías de la Información (TI) de las organizaciones hasta que los delincuentes logren cobrar los rescates correspondientes.

5) **Otras estafas mediante aplicaciones móviles:** los estafadores están desarrollando o manipulando aplicaciones de telefonía móvil que aparentan rastrear la propagación de COVID-19. Sin embargo, una vez instalada, la aplicación infecta el dispositivo del usuario con *malware* que se puede utilizar para obtener información personal, datos confidenciales o detalles de cuentas o tarjetas bancarias.

## Tergiversación por canales de venta

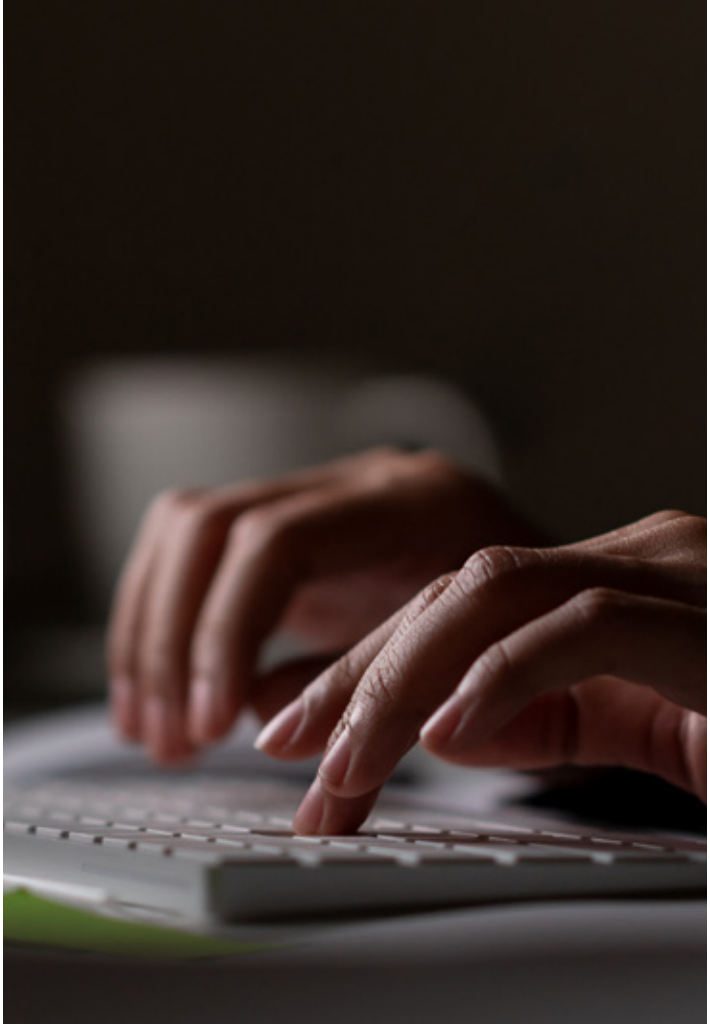
1) **Aplicaciones de educación en línea:** a medida que se cierran las instituciones de educación, los padres se suscriben a un creciente número de aplicaciones de autoaprendizaje en línea, mientras que los estafadores también demuestran ser proactivos en el sector. Se conectan con sus víctimas fingiendo representar aplicaciones educativas de renombre y ofreciendo descuentos atractivos para que el usuario se registre y envíe sus datos bancarios mediante el enlace que ellos proporcionan.

2) **Estafas de suministro:** aprovechando la escasez actual de suministros y la desesperación pública por abastecerse de recursos, los estafadores han abierto aparentes tiendas en línea que venden los suministros médicos de mayor demanda, como máscaras quirúrgicas y desinfectantes para manos. Después de realizar el pago para la "compra" de dichos suministros, los estafadores se embolsan el dinero y no entregan los productos.

3) **Medicamentos falsificados:** debido a la alta la demanda y el bajo suministro de medicamentos esenciales, existe una creciente posibilidad de que se introduzcan medicamentos falsificados en la cadena de suministro de tiendas y farmacias, e incluso en el mercado en línea. El público en general no suele detectar con facilidad la diferencia entre productos auténticos y aquellos que podrían estar falsificados, por lo que existe el riesgo de convertirse en víctima de estos fraudes.

4) **Estafas en pruebas y tratamientos para COVID-19:** el creciente pánico ha generado bandadas de individuos que buscan cómo evitar enfermarse, así como hacerse la prueba de COVID-19 sin que el gobierno se entere (para evitar el aislamiento por cuarentena en instalaciones lejos de su familia, entre otros factores). También hay quienes buscan adquirir tratamientos para COVID-19 por cualquier medio. Por ello, mediante el uso de redes sociales y foros en línea, los estafadores promueven pruebas y tratamientos falsos, entre otros productos para supuestamente prevenir o curar la enfermedad. Estos incluyen promesas de vacunas, medicinas falsas y métodos de tratamiento que no han sido comprobados ni aprobados.

5) **Estafas por supuestos proveedores de servicios médicos:** los criminales se pueden hacer pasar por doctores, enfermeras, paramédicos y administradores de hospitales, entre otros, alegando haber tratado con éxito a un conocido o familiar afectado por COVID-19, exigiendo a las víctimas el pago de dicho tratamiento.



## Inversión y altruismo

1) **Estafas relacionadas con la filantropía:** en tiempos de crisis, las personas suelen sentir la necesidad de ayudar a disminuir el impacto en la comunidad y apoyar a los menos favorecidos. Los estafadores se aprovechan de este deseo, solicitando donativos para organizaciones filantrópicas inexistentes que prometen ayudar a las personas, grupos o áreas afectadas por el virus, o contribuir al desarrollo de una vacuna para combatirlo.

2) **Estafas de inversión:** siguiendo la tradición de una clásica estafa de inversión, este timo tiene la variante de pretender generar ganancias significativas al invertir en una empresa que ofrece servicios o productos que pueden prevenir, detectar o curar la enfermedad COVID-19.

Hay muchas formas de proteger a las empresas de la posibilidad de caer en las manos de los estafadores. El punto más importante para reducir su nivel de vulnerabilidad es garantizar que las personas estén conscientes de las variadas formas en las que los delincuentes intentan aprovecharse de esta crisis de salud mundial.

# ¿Cómo protegerse?

### Conciencia

**1)** Tener cuidado con los correos electrónicos fraudulentos que aseguran provenir de expertos con información vital sobre el virus. No hacer clic en enlaces ni abrir archivos adjuntos de remitentes desconocidos o no verificados, y revisar con atención las direcciones de los correos electrónicos de fuentes que afirman tener información sobre COVID-19. Hay que procurar detectar irregularidades, tales como errores ortográficos o símbolos revueltos. Los estafadores a menudo crean direcciones con diferencias marginales, casi indetectables, respecto a las pertenecientes a las instituciones cuya identidad buscan suplantar.

**2)** Ser cautelosos con las falsas tiendas en línea que utilizan métodos de pago no tradicionales, como un giro postal, transferencia de fondos, tarjetas de regalo o criptomonedas. No utilizar ningún método abreviado de pago proporcionado por un representante. Iniciar sesión en sitios oficiales y verificados al realizar un pago.

**3)** Identificar a los usuarios de alto riesgo (Alta Dirección, Tesorería, Recursos Humanos, entre otros) y contar con medidas adicionales de confirmación de las instrucciones que se reciban de ellos, particularmente de las que no sigan el curso normal de la organización.

**4)** Implementar mecanismos adicionales (por ejemplo, confirmación telefónica de la empresa al proveedor) para atender solicitudes de cambio de cuentas bancarias usadas para pagar a los proveedores.

**5)** Investigar los antecedentes de las organizaciones filantrópicas o la veracidad de las campañas de financiamiento colectivo. Hay que tener cuidado con cualquier empresa, organización civil o persona que solicite donativos en efectivo, por correo, mediante transferencia de fondos u otros canales inusuales.

**6)** Mantenerse informado de las estafas y tendencias de inversión en relación con COVID-19, tales como esquemas que ofrecen descuentos en la compra de productos de *streaming*, o empresas que afirman contar con medicamentos que curan la enfermedad. Comprar solamente medicamentos fabricados para empresas farmacéuticas autorizadas o vendedores conocidos. Incluso en estos casos, siempre verificar los detalles del producto, incluidas las etiquetas, el embalaje, los ingredientes, la fecha de fabricación y caducidad, así como el lugar de manufactura.

**7)** Evitar compartir fotografías en las redes sociales del escritorio o la estación de trabajo, ya que se podría estar compartiendo información confidencial inadvertidamente.

### Controles tecnológicos preventivosa

**1)** Proteger y controlar el acceso remoto a la infraestructura crítica de TI y limitar el acceso a las identificaciones de usuarios internos y externos. Revocar todas las conexiones directas en los servidores fuera de las oficinas. Monitorear el rendimiento del servidor y la red, y configurar las alertas pertinentes.

**2)** Limitar y registrar el uso de aplicaciones que permiten el acceso remoto obliga al restablecimiento forzoso de una contraseña, lo cual crea un doble factor de autenticación en activos críticos de TI.

**3)** Confirmar las actualizaciones de *software*, *anti-malware*, *anti-ransomware* y antivirus instalados en los dispositivos, así como de las actualizaciones de los parches asociados a los sistemas operativos. Evitar la instalación de *software* gratuito en sistemas de TI, ya que puede contener *malware*.

**4)** Conectarse a internet mediante puntos de acceso seguros y de banda ancha. Se recomienda usar una red privada virtual (VPN).

**5)** Evitar utilizar un sitio de internet público para compartir archivos, salvo que la política de la organización lo permita.

### Controles de investigación

**1)** No hay que desestimar ningún incidente o violación a los sistemas, ya que pueden ser indicativos de un problema mayor.

**2)** En caso de un ciberataque, se deberá investigar la causa raíz para protegerse y prevenir cualquier ataque a futuro.

**3)** Utilizar un esquema tipo triaje que permita identificar rápidamente la severidad de los incidentes para tomar medias apropiadas.

> Se debe evitar utilizar un sitio de internet público para compartir archivos, salvo que la política de la organización lo permita

# Metodología e información demográfica

Durante un mes recopilamos las respuestas de más de 200 participantes de diversas industrias, preponderantemente del sector financiero, dada su habitual sensibilidad y familiaridad en el combate a riesgos de fraude y lavado de dinero, así como su robusta gestión de riesgos.

Principalmente respondió la Alta Dirección de compañías del sector privado y de capital mexicano, ubicadas en más de 20 estados de la República Mexicana.

Las respuestas fueron proporcionadas, en su mayoría, por personas a cargo de la Dirección de Finanzas y de Cumplimiento.

## Nivel del participante

38%
**Director**

15%
**Gerente**

11%
**Presidente**

10%
**Vicepresidente**

7%
**Miembro de Comité o Consejo**

2%
**Subdirector**

17%
**Otro**

## Tipo de compañía

72%

**Empresa privada, principalmente de capital mexicano**

23%

**Empresa privada, principalmente de capital extranjero**

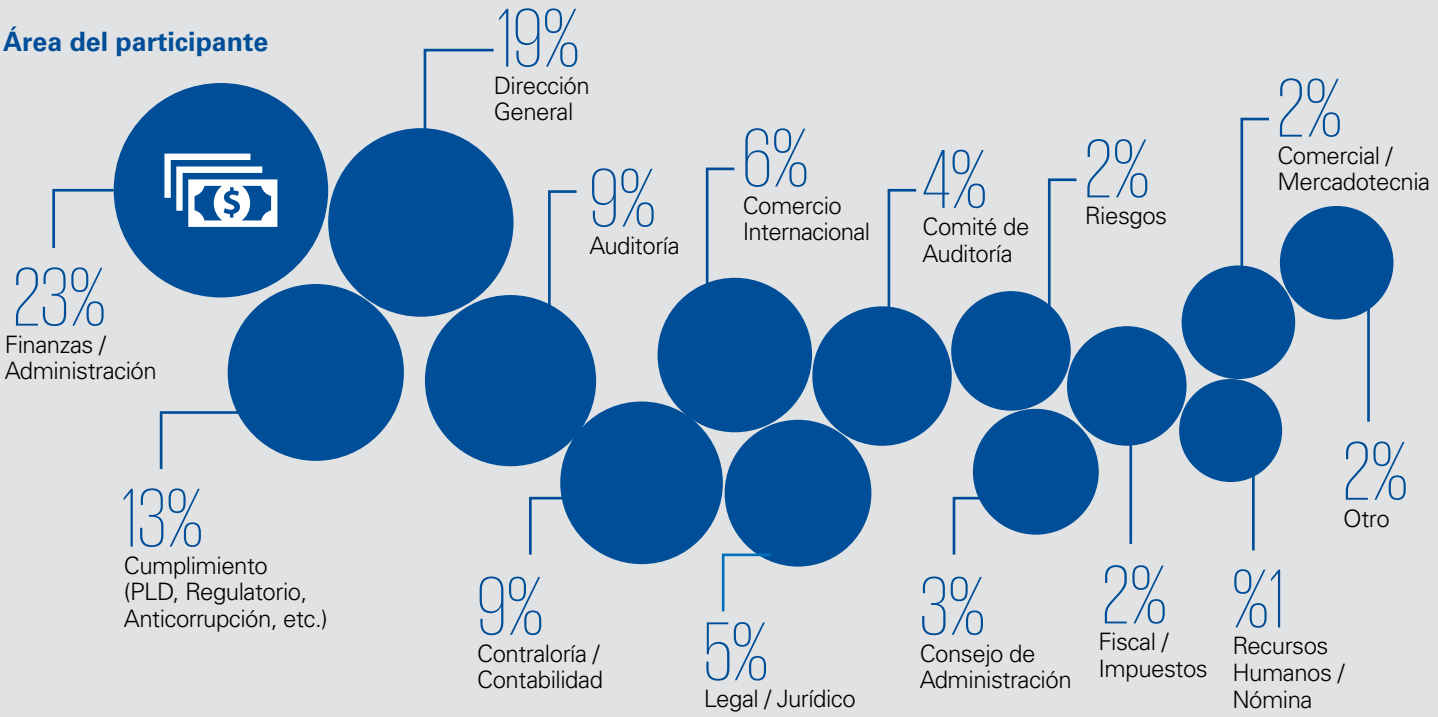
4%

**Organización no lucrativa**

1%

**Entidad gubernamental**

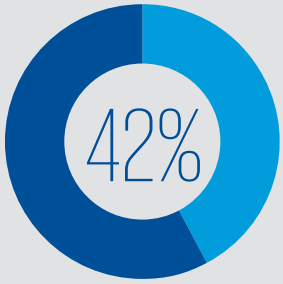
## Área del participante




## Ubicación de la empresa

**46% Ciudad de México**
**9% Jalisco**
**8% Estado de México**
**6% Nuevo León**
**4% Guanajuato**
**3% Querétaro**
**3% Chihuahua**
**3% Morelos**

Con 2% de participación: Puebla, Chiapas, Coahuila, Michoacán y Sonora
Con 1% de participación: Durango, Oaxaca, Guerrero, Hidalgo, Nayarit, Quintana Roo, San Luis Potosí y Tamaulipas




Empresas familiares

## Sector al que pertenece la organización


## Cantidad de personas laborando

**55% De 1 a 500**
**14% De 501 a 1,000**
**9% De 1,001 a 2,000**
**8% De 2,001 a 4,000**
**6% De 4,001 a 10,000**
**8% Más de 10,000**

## Importe de ventas anuales en pesos

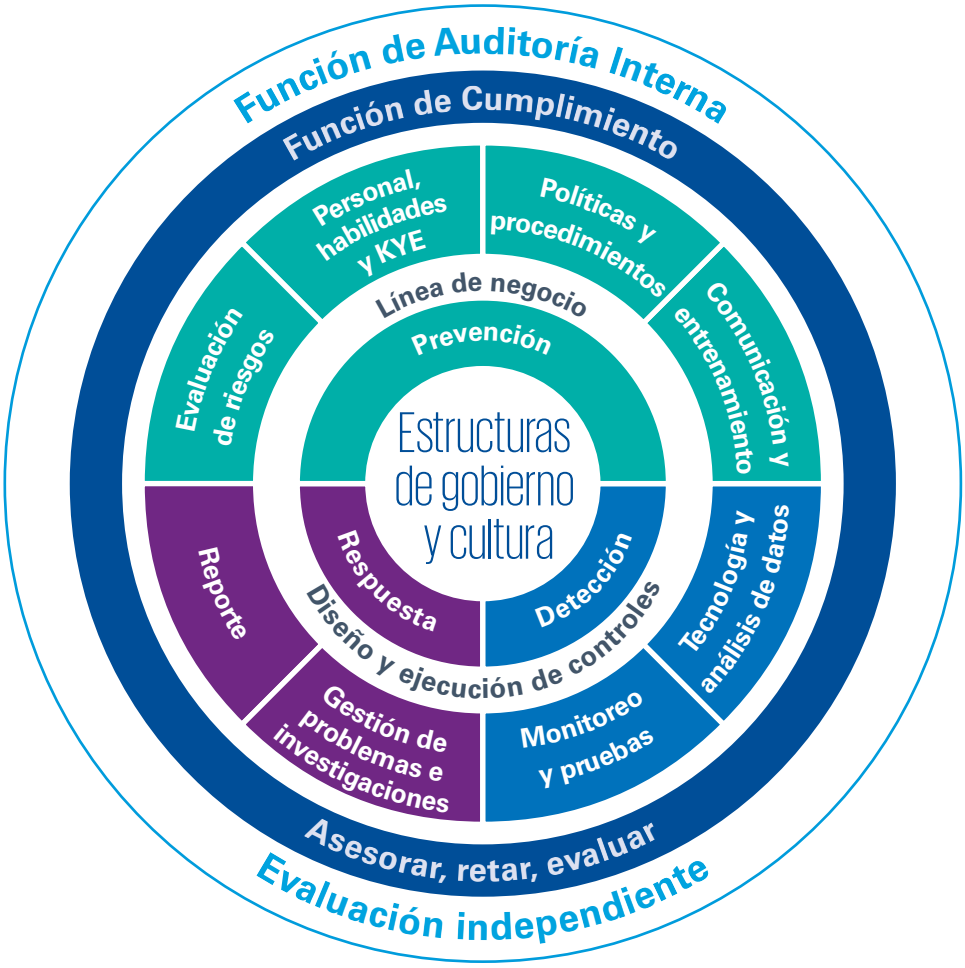
**12% Hasta 4 mdp**
**33% 4 a 100 mdp**
**14% 100 a 250 mdp**
**41% Más de 250 mdp**

# Conclusiones generales

Durante muchos años las empresas han carecido de controles suficientes para combatir crímenes financieros, o han recurrido a estrategias aisladas para hacerlo. Sin embargo, el preocupante número de compañías que aún son víctimas de algún delito financiero o, en ciertos casos, de todos, muestran que es necesario un cambio de visión.

Hemos desarrollado un enfoque de 360 grados para que el análisis de la información vaya más allá de lo tradicional y se pueda generar inteligencia financiera mediante una estrategia eficaz en varias líneas de defensa con sus componentes, aplicados a todas las líneas de negocios y sus respectivos controles.

**Enfoque KPMG**




En nuestra experiencia, las organizaciones requieren frecuentemente de una verdadera reingeniería para maximizar los recursos con los que cuentan y así acceder a un programa integral y eficiente de prevención, detección y respuesta a los delitos financieros.

Una empresa que verdaderamente se compromete a prevenir y luchar en contra de los crímenes financieros, busca ir más allá del cumplimiento teórico y utiliza esquemas de convergencia para aprovechar las estrategias frente a cada uno de los delitos, para contar con un programa integral, práctico y efectivo. Además, es recomendable que esté consciente de que el capital humano puede ser el más débil de los eslabones, pues el *modus operandi* de diversos delitos es desde el interior de las entidades.

Agradecemos a las empresas que participaron en nuestro estudio. Esperamos que este trabajo ayude a las entidades de las diversas industrias y giros a replantear la manera como enfocan sus esfuerzos en el combate al crimen financiero. La lucha es de todos los actores involucrados en este ecosistema, en el que, si alguno falla, la integridad del mismo en general se ve afectada.

Estamos comprometidos a ayudar a que las organizaciones alcancen el más alto nivel de integridad. De este modo, sus programas de combate al crimen financiero podrán ser realmente efectivos. Sin duda, un enfoque holístico será siempre la mejor alternativa.

kpmg.com.mx
800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

# Contactos

**Shelley M. Hayes**
**Socia Líder de Forensic de KPMG en México y Centroamérica**

**José Claudio Treviño**
**Socio de Forensic de KPMG en México**

**Cesar Pérez-Orozco**
**Socio de Forensic de KPMG en México**

La información aquí contenida es de naturaleza general y no tiene el propósito de abordar las circunstancias de ningún individuo o entidad en particular. Aunque procuramos proveer información correcta y oportuna, no puede haber garantía de que dicha información sea correcta en la fecha que se reciba o que continuará siendo correcta en el futuro. Nadie debe tomar medidas basado en dicha información sin la debida asesoría profesional después de un estudio detallado de la situación en particular.

"D.R." © 2020 KPMG Cárdenas Dosal, S.C., la firma mexicana miembro de la red de firmas miembro de KPMG afiliadas a KPMG International Cooperative ("KPMG International"), una entidad suiza. Blvd. Manuel Ávila Camacho 176 P1, Reforma Social, Miguel Hidalgo, C.P. 11650, Ciudad de México. Impreso en México. Todos los derechos reservados.