KPMG

Impacto de los delitos financieros en México 2024

Enfoque holístico ante una problemática cambiante y evolutiva

DELINEANDO ESTRATEGIAS

1 Administración de Riesgos

KPMG México

Contenido

3 Prólogo

4 Panorama integral del fraude

11 La corrupción y su vínculo con los aspectos ASG

14 Panorama e impacto de los ciberdelitos

20 Prevención de lavado de dinero y financiamiento al terrorismo

26 Metodología

27 Conclusiones

Prólogo

A nivel global y local, las organizaciones enfrentan crecientes desafíos ante distintas problemáticas relacionadas con la integridad, la reputación y el impacto financiero. La presencia de delitos financieros como el fraude, la corrupción, así como la creciente sofisticación de los ciberataques y el lavado de dinero, afectan no solo la estabilidad financiera y la reputación de las organizaciones, sino también sus operaciones diarias, planes de crecimiento y permanencia, su estrategia de sostenibilidad y a los derechos humanos.

Ante este panorama, es indispensable que las compañías cuenten con estrategias integrales de prevención, detección y respuesta ante estos delitos, las cuales consideren aspectos ambientales, sociales y de gobierno corporativo (ASG), con un enfoque en derechos humanos, y que permitan atender oportunamente los impactos a nivel interno y externo.

El presente estudio tiene como objetivo analizar en profundidad las consecuencias de estos delitos en las organizaciones en México, explorar mejores prácticas para su prevención mediante un enfoque ASG, y examinar el uso de tecnologías, como la inteligencia artificial (IA), para mitigar potenciales riesgos en el futuro.

Durante agosto de 2024, encuestamos a más de 100 líderes en organizaciones de distintas industrias en 15 estados de la República Mexicana para conocer sus perspectivas sobre cómo prevenir, detectar y responder a los delitos financieros y el impacto que tienen en el ambiente de negocios.

KPMG agradece su contribución, la cual puede motivar a las organizaciones a tener una visión y planes estratégicos a futuro, con base en información reciente y experiencias reales.

Asimismo, le invitamos a conocer y compartir este análisis con sus colegas y grupos de interés, con el fin de detonar conversaciones que inspiren el desarrollo de las organizaciones a nivel nacional y fomenten alianzas estratégicas que garanticen su crecimiento sostenible, con un enfoque en los derechos humanos.

Atentamente,

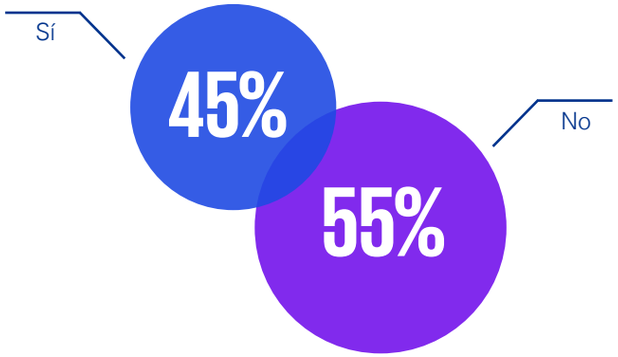
KPMG México

Panorama integral del fraude

Existen distintas definiciones de lo que es un fraude; algunas son emitidas por grupos profesionales como la Asociación de Examinadores de Fraude Certificados (ACFE, por sus siglas en inglés), que son útiles para establecer las bases de este concepto. Para el presente estudio, podemos definir al fraude como una acción malintencionada con el objetivo de obtener un beneficio personal a través del uso inapropiado de recursos o activos de una organización. Esto no solo implica dinero o bienes materiales, ya que actualmente es un concepto mucho más amplio, que abarca, por ejemplo, la información y los datos, los cuales son considerados como un activo intangible sumamente valioso.

Al respecto, 45% de las organizaciones en México reportan haber sufrido el intento o la materialización de un fraude en el último año, lo que pone de manifiesto que se trata de un riesgo latente para cualquier compañía.

En los últimos 12 meses, ¿su empresa ha sufrido el intento o la materialización de un fraude?



Lo anterior se encuentra estrechamente relacionado, como lo veremos a lo largo de esta sección, con los cambios organizacionales, económicos, regulatorios, de capital humano y tecnológicos que se están presentando, los cuales incluyen la sofisticación en las técnicas de fraude.

Modalidad del fraude

En cuanto a la tipología del delito, 35% menciona haber sido víctima de un fraude externo; 32%, de uno interno, y 33% de ambos tipos de fraude.

¿Qué tipo de fraude?

Es oportuno señalar la diferencia entre el fraude interno y el externo. El primero se realiza por parte del personal, e incluso, por las mismas personas propietarias de las organizaciones, mientras que el externo se lleva a cabo por terceros, ya sean clientes, proveedores, grupos criminales o cibercriminales, que buscan vulnerar la seguridad u obtener un beneficio en perjuicio de la organización.

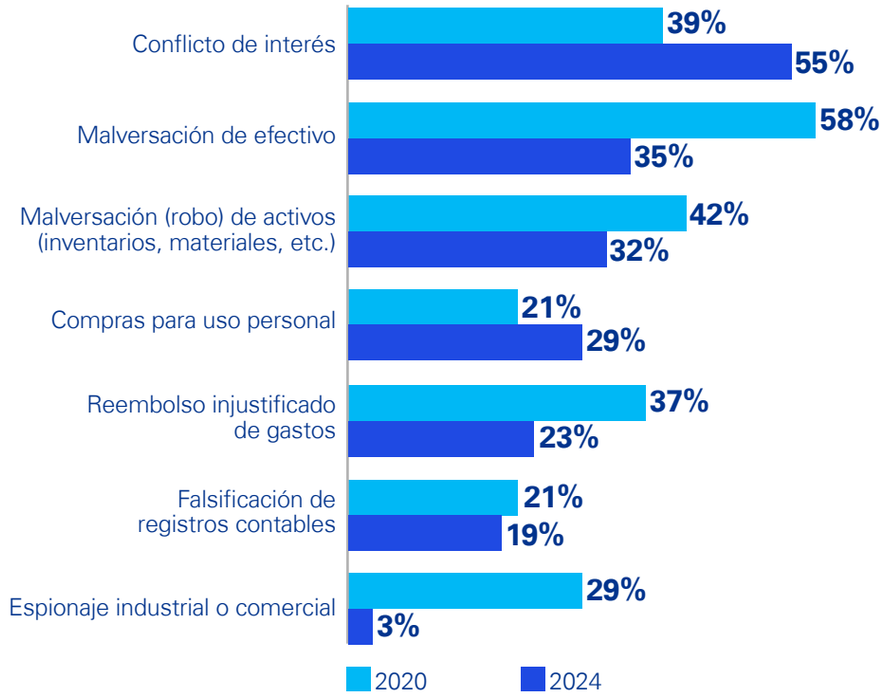
De acuerdo con los datos obtenidos en nuestro estudio de 2020, el fraude interno ha tenido una reducción de 30 puntos porcentuales, mientras que el externo presenta un incremento

de 17 puntos;[1] no obstante, esta cifra no significa que el fraude interno no se siga perpetrando, ya que diversos estudios, como el *Reporte a las Naciones 2024* de la ACFE, muestran que más de la mitad de los casos de fraude interno se cometen por una falta de controles internos en las organizaciones.[2]

[1] *El impacto de los delitos financieros. Prevención, detección y respuesta,* KPMG México, 2020.
[2] *Fraude Ocupacional 2024. Un reporte a las Naciones,* ACFE, 2024.

En relación con los tipos de fraude interno detectados, destacan: el conflicto de interés (55%), la malversación de efectivo (35%), la malversación o robo de activos (32%) y las compras para uso personal (29%).

Tipo de fraude interno que sufrió su empresa

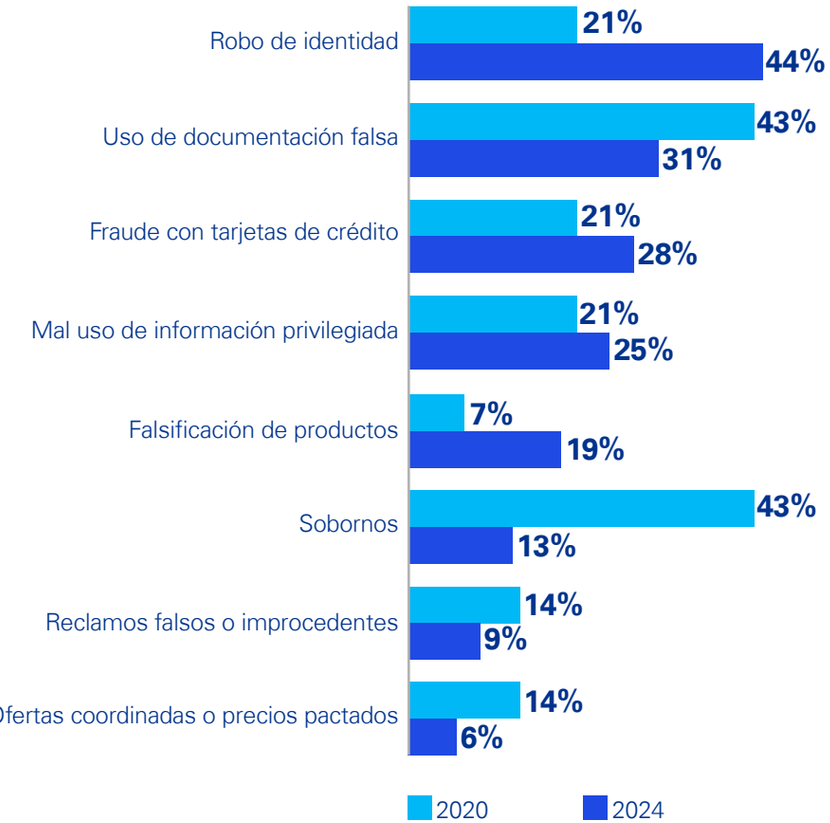


La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

En este sentido, es posible observar un aumento en el número de casos de conflictos de intereses, en comparación con los datos de 2020 (39%), lo que implica que es necesario seguir fortaleciendo los controles internos relacionados y la sensibilización del personal respecto a las conductas éticas esperadas.

En cuanto a los fraudes externos, los principales son: robo de identidad (44%), uso de documentación falsa (31%) y fraude con tarjetas de crédito (28%). Es importante destacar que ciertos tipos de fraude pueden pasar inadvertidos y son reflejo de conductas no éticas, por ejemplo, los fraudes en prácticas anticompetitivas (6%), que, si bien pueden parecer menores, son capaces de generar altos impactos en los mercados a través de controles artificiales de precios o por medio de prácticas monopólicas o concentraciones ilícitas.

Tipo de fraude externo que sufrió su empresa



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

El robo de identidad se ha incrementado 23 puntos porcentuales con respecto a los datos de 2020, lo que puede vincularse con el aumento significativo de los ciberdelitos y fraudes en línea, que se detonaron a raíz de COVID-19 y la creciente digitalización de las operaciones empresariales. Este tipo de fraude puede tener un gran alcance, sobre todo, con el acceso y uso de tecnologías avanzadas como la inteligencia artificial generativa (IAGen), que facilita la generación de contenidos manipulados como videos, fotos, e incluso, voces, que podrían utilizarse para robar información sensible.

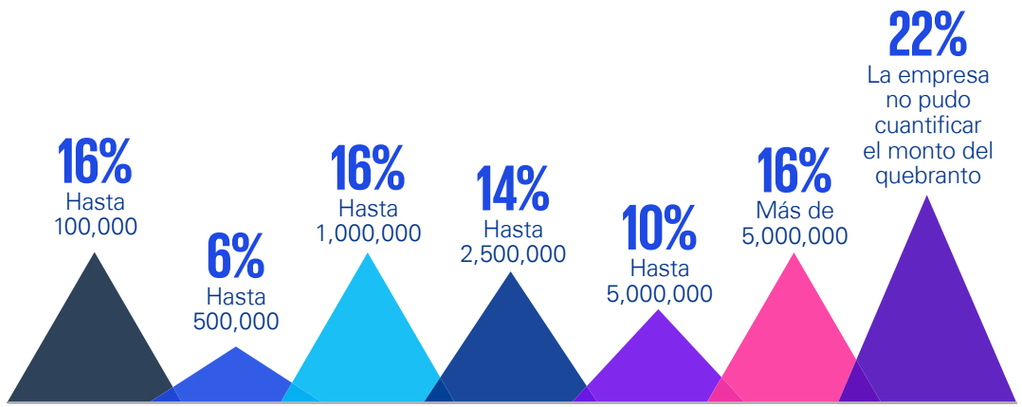
Es importante destacar que los grupos criminales que ejecutan estos delitos suelen investigar, de manera muy puntual, las vulneraciones de la organización o de su personal. Por ejemplo, aprovechan las barreras lingüísticas para confundir, crean situaciones de urgencia y operan en horarios fuera de lo normal, lo que les permite llevar a cabo el ilícito con una mayor probabilidad de éxito.

Por lo anterior, es fundamental que se promueva una activa concientización sobre la responsabilidad de todo el negocio con respecto a la protección de la información y fomentar una cultura de prevención, puesto que estos incidentes pueden tener como consecuencia daños reputacionales, financieros, incumplimiento de leyes y regulaciones, e interrupciones de la operación. Es importante que esta cultura de prevención vaya siempre en línea con el "blindaje" de los procesos internos, con la finalidad de reforzar tanto los controles internos como el entrenamiento de las personas que los llevan a cabo.

Impacto financiero

De las organizaciones que sufrieron algún tipo de fraude, 16% indica que el monto del quebranto ascendió hasta MXN 100,000; 16% reporta hasta MXN 1,000,000, y el mismo porcentaje más de MXN 5,000,000; no obstante, 22% afirma que no fue posible cuantificar el monto del quebranto.

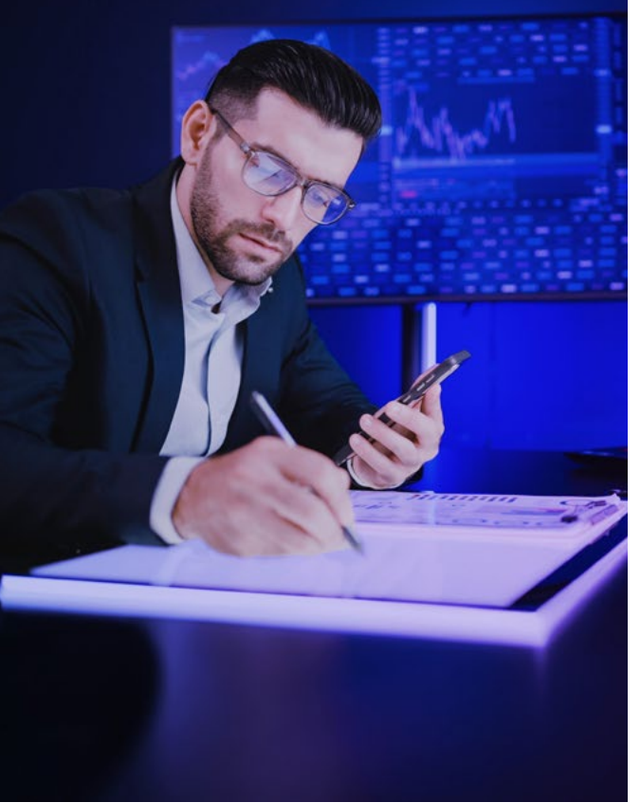
¿A qué monto ascendió el quebranto en pesos (MXN)?



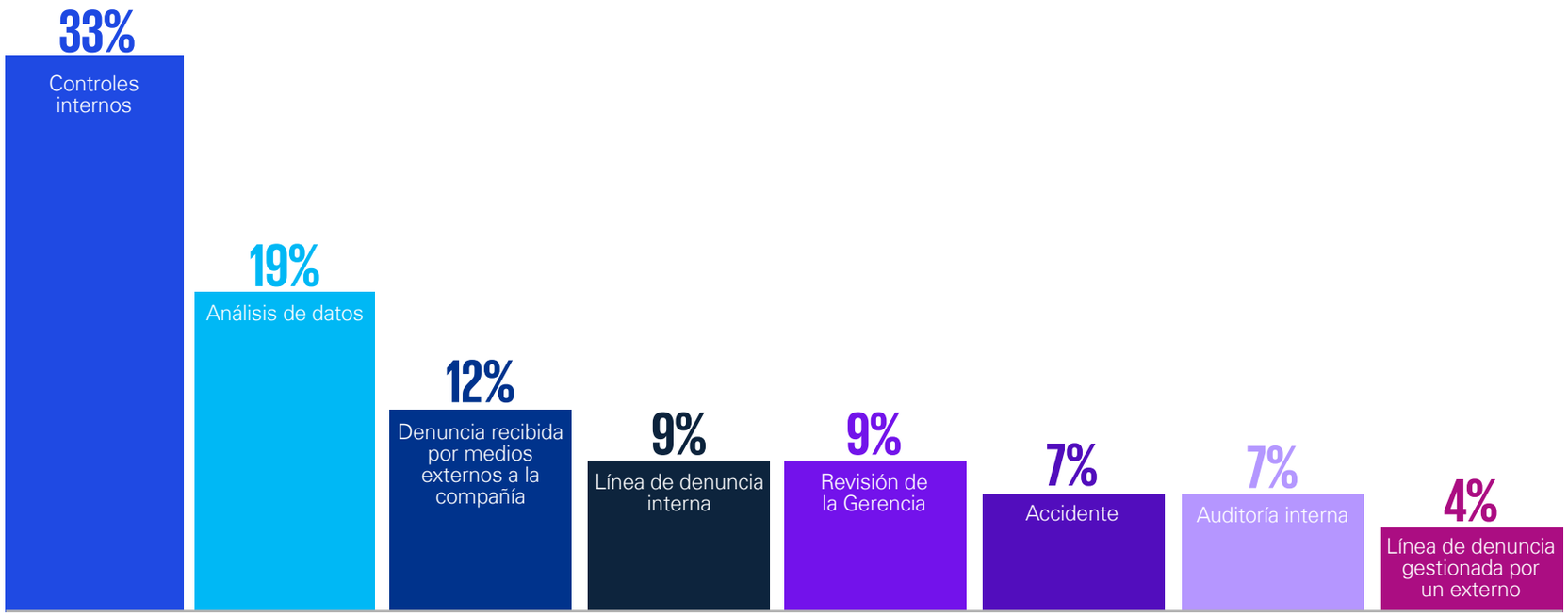
Que 22% no haya podido cuantificar el impacto es sumamente relevante, ya que representa un incremento de 14 puntos porcentuales en comparación a 2020 (8%). Esto puede atribuirse a factores como la falta de investigación y protocolos adecuados para la respuesta a casos de fraude, así como la pérdida o el daño de las pruebas para efectos de cuantificación. Adicionalmente, la falta de inversión en asuntos relacionados con el ciclo de prevención, detección y respuesta impide llevar a cabo las investigaciones pertinentes, lo que hace explicable que un porcentaje relevante no consiga cuantificar el quebranto.

Detección del fraude

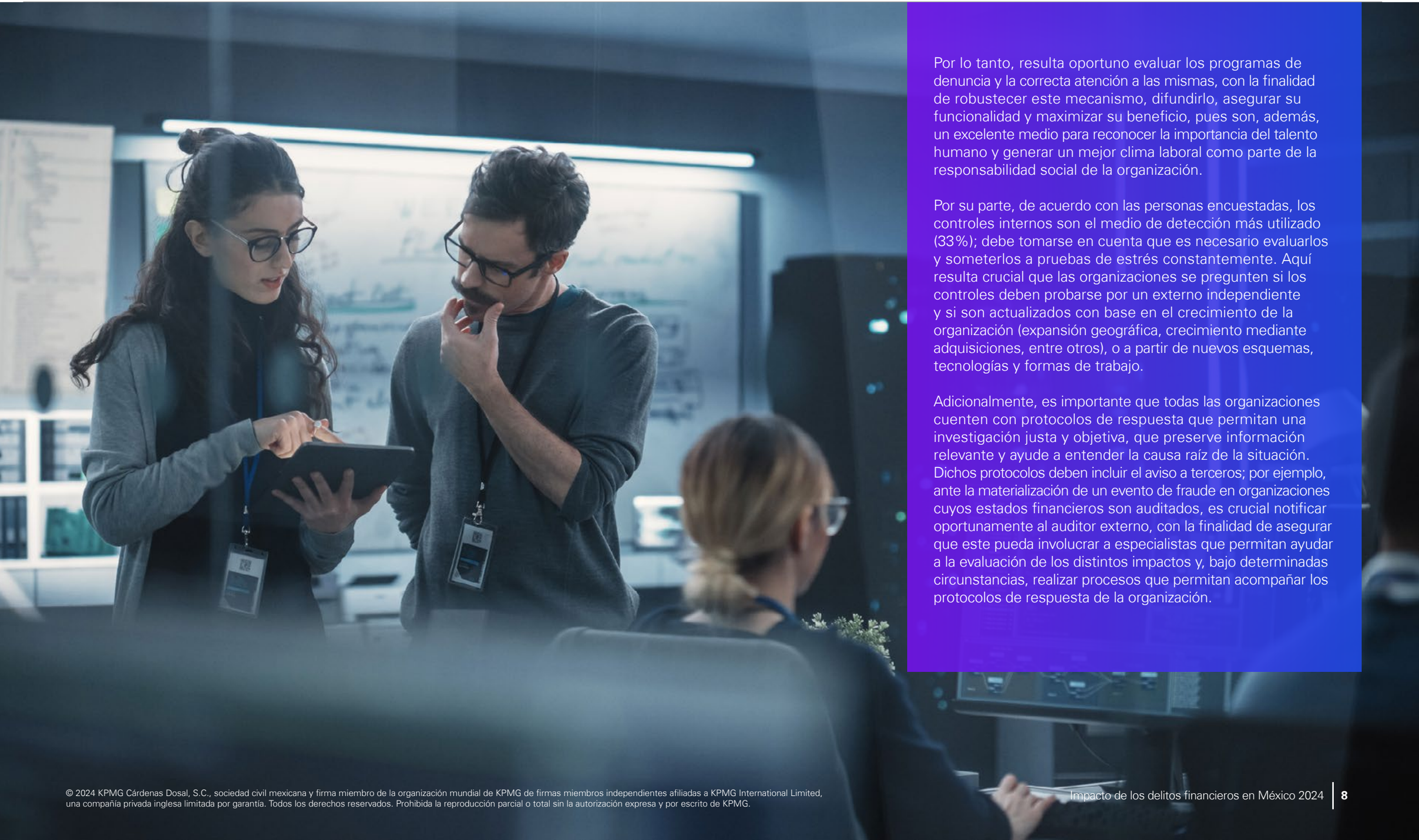
Respecto a los métodos para detectar el fraude, 33% de las organizaciones utilizan controles internos; 19%, análisis de datos; 12%, denuncias recibidas por medios externos, y 9%, líneas de denuncias internas, así como revisiones por parte de la Gerencia.



¿Cuál fue el método aplicado en la detección del fraude?



Existe una tendencia al alza en el uso de herramientas de análisis de datos, porcentaje que se incrementó casi cuatro veces respecto al estudio de 2020 (5%); sin embargo, también resulta relevante que las líneas de denuncia presenten un porcentaje bajo, considerando que este mecanismo suele tener altos niveles de efectividad para detectar casos de fraude, situación que puede ser confirmada por el *Reporte a las Naciones 2024*, que ubica a los *tips* (denuncias) con una efectividad de 43%, e incluso, a los mecanismos de reporte en la *web* y correo electrónico con mayor efectividad que a los reportes a través de vías telefónicas, lo que podría relacionarse con una falta de cultura de denuncia, principalmente motivada por el temor a las represalias.



Por lo tanto, resulta oportuno evaluar los programas de denuncia y la correcta atención a las mismas, con la finalidad de robustecer este mecanismo, difundirlo, asegurar su funcionalidad y maximizar su beneficio, pues son, además, un excelente medio para reconocer la importancia del talento humano y generar un mejor clima laboral como parte de la responsabilidad social de la organización.

Por su parte, de acuerdo con las personas encuestadas, los controles internos son el medio de detección más utilizado (33%); debe tomarse en cuenta que es necesario evaluarlos y someterlos a pruebas de estrés constantemente. Aquí resulta crucial que las organizaciones se pregunten si los controles deben probarse por un externo independiente y si son actualizados con base en el crecimiento de la organización (expansión geográfica, crecimiento mediante adquisiciones, entre otros), o a partir de nuevos esquemas, tecnologías y formas de trabajo.

Adicionalmente, es importante que todas las organizaciones cuenten con protocolos de respuesta que permitan una investigación justa y objetiva, que preserve información relevante y ayude a entender la causa raíz de la situación. Dichos protocolos deben incluir el aviso a terceros; por ejemplo, ante la materialización de un evento de fraude en organizaciones cuyos estados financieros son auditados, es crucial notificar oportunamente al auditor externo, con la finalidad de asegurar que este pueda involucrar a especialistas que permitan ayudar a la evaluación de los distintos impactos y, bajo determinadas circunstancias, realizar procesos que permitan acompañar los protocolos de respuesta de la organización.

Herramientas de prevención, detección y respuesta

Respecto a los principales elementos para prevenir, responder y detectar casos de fraude, 59% menciona que cuenta con capacitación en temas de ética; 50%, con controles antifraude en los procesos, y 43%, con la debida diligencia de proveedores y personal, así como con políticas antifraude y sanciones por este tipo de incidentes; mientras que 16% no cuenta con ningún elemento.

Es importante resaltar que, si bien la mitad de las organizaciones cuentan con controles antifraude, únicamente dos de cada diez utilizan matrices de fraude, las cuales son clave para el análisis de riesgos, lo que podría proporcionar una falsa sensación de seguridad al contar con controles para prevenir este ilícito, pero no tener la certeza del riesgo al que se enfrenta la organización. También llama la atención que cuatro de cada diez directivos manifiesten contar con procesos de debida diligencia a terceros, ya que podría asumirse que esta herramienta no está generando el impacto esperado, al tener como principal tipo de fraude interno al conflicto de interés (55%).

¿Su empresa cuenta con alguno de los siguientes elementos para prevenir, responder y detectar potenciales casos de fraude?

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

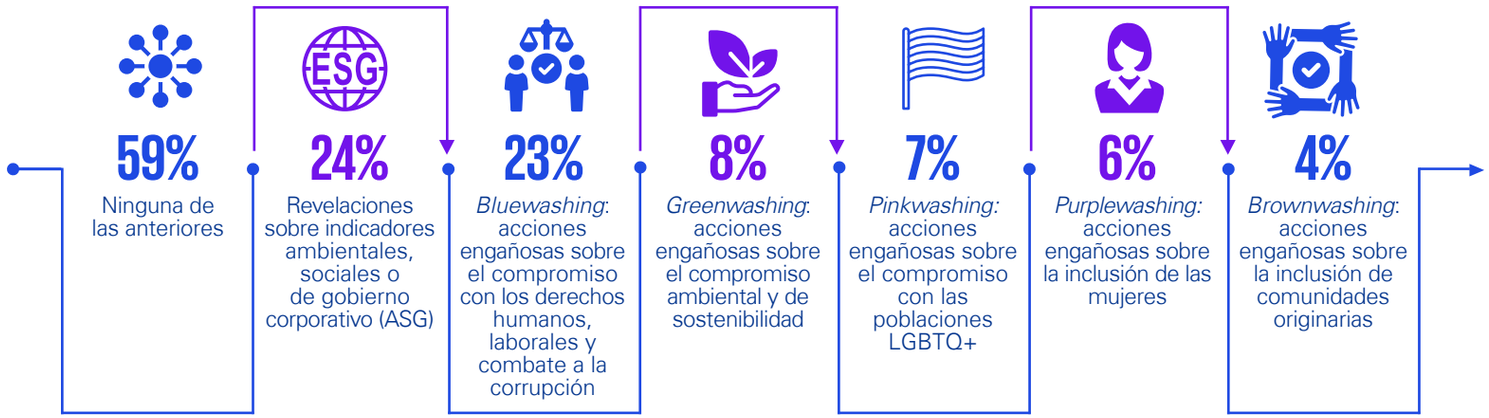
Si bien la capacitación en asuntos éticos es relevante para prevenir el fraude y otro tipo de delitos, también se requiere de entrenamiento, entendido como "la capacitación llevada a la práctica", ya que, en ocasiones, durante el aprendizaje teórico se enfatiza el código de ética y la línea de denuncia, pero cuando es realmente necesario actuar, el personal desconoce los protocolos y cómo utilizar los recursos disponibles eficientemente.

Por ello, es importante que exista un compromiso por parte de la Administración para prevenir el fraude y evaluar de manera periódica el ambiente de negocios y su evolución, así como las nuevas tendencias que la sociedad y terceros exigen, con el fin de incorporarlas a los programas de capacitación y prevención para establecer el estándar en toda la organización.

Desarrollo de competencias en materia ASG

La capacitación para prevenir fraudes relacionados con temas ASG es cada vez más relevante. Al respecto, 24% de las organizaciones afirman que, en el último año, han recibido capacitaciones de revelaciones sobre indicadores ASG, 23% sobre temas de *bluewashing*, 8% sobre *greenwashing* y 7% sobre *pinkwashing*; sin embargo, seis de cada diez (59%) no han recibido capacitación en estas materias.

En los últimos 12 meses, ¿qué capacitaciones ha recibido su organización para prevenir el fraude en las siguientes materias?



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

Que más de la mitad de las organizaciones no hayan recibido capacitación en estos temas es preocupante, considerando la importancia actual de la responsabilidad social y los objetivos de desarrollo sostenible (ODS); es imperativo generar conciencia sobre cómo prevenir estos fraudes para que las estrategias ASG sean viables y accionables.

En este sentido, un factor relevante para que las organizaciones comiencen a integrar la prevención del fraude ASG como parte elemental de las estrategias de crecimiento y sostenibilidad, es el compromiso y la concientización de las personas en posiciones clave. La prevención del fraude ASG debe percibirse como una herramienta para impactar positivamente en el medioambiente, la sociedad y los grupos de interés, no solo como una obligación normativa.

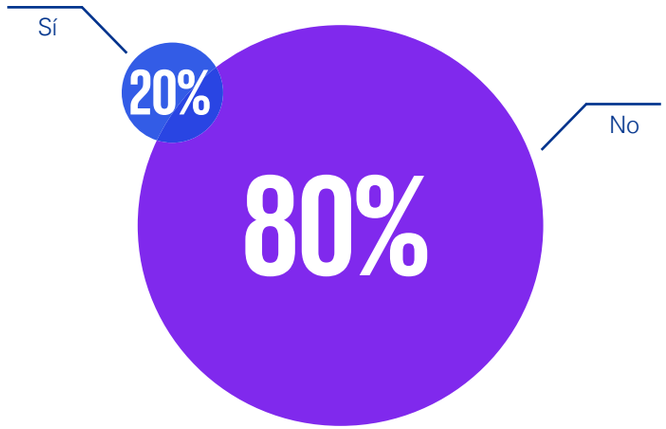
Por lo tanto, es fundamental que se reconozcan los diferentes tipos de fraude relacionados y comprender cómo se pueden materializar e impactar en la organización; es decir, se necesita desarrollar una cultura de prevención del fraude integral, basada en los valores, misión y visión de la organización, y, sobre todo, en su compromiso con los ODS y las prácticas a favor de la diversidad, equidad e inclusión (DEI), para que a través de la capacitación y el entrenamiento continuos, sea posible permear el mensaje en todos los niveles, fortaleciendo la ética y la transparencia.

La corrupción y su vínculo con los aspectos ASG

La corrupción y los flujos financieros ilícitos asociados presentan importantes retos para las organizaciones, particularmente cuando inciden en los compromisos ASG, ya que no solo afectan la operación, sino que también menoscaban los planes de sostenibilidad y los derechos humanos de los grupos vulnerados. Fortalecer los programas anticorrupción resulta imperante para generar entornos de negocio más éticos y sostenibles, dada la relevancia que alcanzan en distintos grupos de interés.

Al respecto, 20% de las organizaciones señalan haber sufrido el intento o la materialización de un acto de corrupción en el último año, lo que subraya la importancia de contar con mecanismos sólidos que integren estrategias ASG para fortalecer la resiliencia del negocio a largo plazo.

En los últimos 12 meses, ¿su empresa ha sufrido el intento o la materialización de un acto de corrupción?

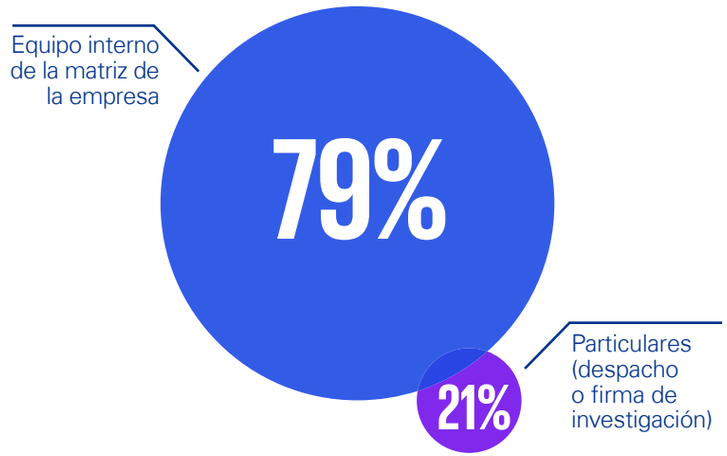


Responsables de la investigación

Sobre dicho incidente, 79% afirma que el equipo interno de la casa matriz realizó las investigaciones correspondientes y 21% lo hizo a través de particulares, por ejemplo, una firma de consultoría especializada. Ante investigaciones cada vez más complejas, es imperativo que los equipos respondan de una manera ética e independiente, que considere todos los posibles efectos que podría tener la materialización del acto de corrupción, tanto en la organización como en los terceros involucrados.

Asimismo, es importante recordar las diferencias en los marcos regulatorios anticorrupción existentes en México y en el extranjero, pues son una base importante para documentar las diversas estrategias de investigación que pueden ser adoptadas por los equipos internos y las consideraciones particulares a incorporar, como el apoyo de especialistas en distintas materias.

Sobre los intentos o actos de corrupción detectados en su empresa, ¿quién realizó las investigaciones correspondientes?



La corrupción y su impacto ASG

En definitiva, la interconexión entre la corrupción y otras problemáticas, como el lavado de dinero o el fraude, incrementa la complejidad de las investigaciones, lo que demanda que las organizaciones implementen mecanismos de respuesta mucho más sofisticados y alineados con los principios ASG, que aseguren la gestión integral de los riesgos y permitan abordar todas las aristas del problema, sin incumplir compromisos ni vulnerar los derechos de los distintos grupos de interés, tanto internos como externos.

La atención oportuna a estos casos es relevante para asegurar el cumplimiento de las leyes y regulaciones anticorrupción nacionales e internacionales, así como para robustecer el marco de prevención, detección y respuesta ante delitos relacionados como la vulneración de los derechos humanos, delitos ambientales, entre otros.

En los últimos 12 meses, ¿tiene conocimiento sobre casos de corrupción en su industria que pudieran estar relacionados con factores ASG?

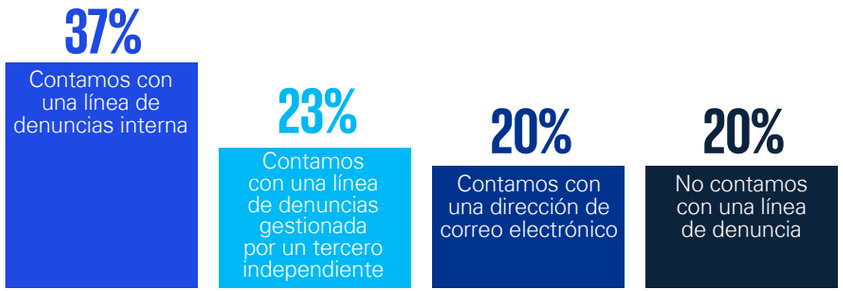
- Sí, con factores sociales (*bluewashing, pinkwashing, brownwashing* y *purplewashing*)
- Sí, con factores ambientales (*greenwashing*)
- Sí, con factores de gobierno corporativo (alteraciones a las revelaciones relacionadas con indicadores ASG)
- No estuvieron vinculados con factores ASG

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

Canales de denuncia para casos de corrupción relacionados con temas ASG

Respecto a los mecanismos para gestionar las denuncias, 37% menciona contar con una línea de denuncia interna; 23% las atiende con ayuda de un tercero independiente, y 20%, mediante una dirección de correo electrónico.

¿Cuál de las siguientes opciones describe mejor cómo su organización gestiona las denuncias?



Para que estos mecanismos sean realmente efectivos, es fundamental fortalecerlos con la difusión y transparencia necesarias; es decir, el personal debe saber que existen, conocer su función y tener la garantía de que su denuncia permanecerá anónima. Asimismo, se debe asegurar que el proceso sea claro y que la información se maneje con discreción, con el fin de crear un entorno de confianza donde el temor a las represalias no sea un obstáculo para la denuncia.

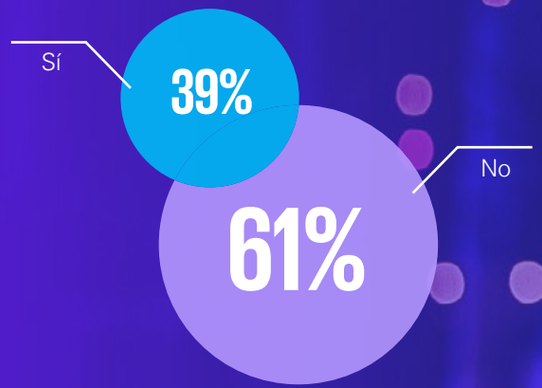
En este contexto, existe un elemento clave para contar con un modelo eficaz de prevención de riesgos de corrupción: la efectividad de los protocolos de respuesta y de comunicación deben incluir métodos claros y justos para asegurar que las investigaciones sean imparciales y estén basadas en hechos comprobables, para evitar que las denuncias puedan ser utilizadas de forma malintencionada, garantizando, en todo momento, que no haya revictimización ni vulneración de los derechos de las personas involucradas.

En este sentido, la capacitación del personal encargado es clave para proporcionar soluciones efectivas. En definitiva, las organizaciones que priorizan la transparencia y la atención efectiva de las denuncias logran marcar una diferencia significativa en la percepción y efectividad de sus programas de prevención.

Panorama e impacto de los ciberdelitos

Datos del estudio *Perspectivas de la Alta Dirección en México 2024* muestran que 35% de las organizaciones consideran los ciberataques como uno de los principales riesgos que podrían ocasionar impactos relevantes en sus estrategias. Esto resulta relevante al hablar de estrategias para combatir dichos ilícitos, pues se alinea con 39% de los participantes del presente estudio que mencionan haber sufrido el intento o la materialización de un ciberataque.[3]

En los últimos 12 meses, ¿su empresa ha sufrido el intento o la materialización de un ciberataque?



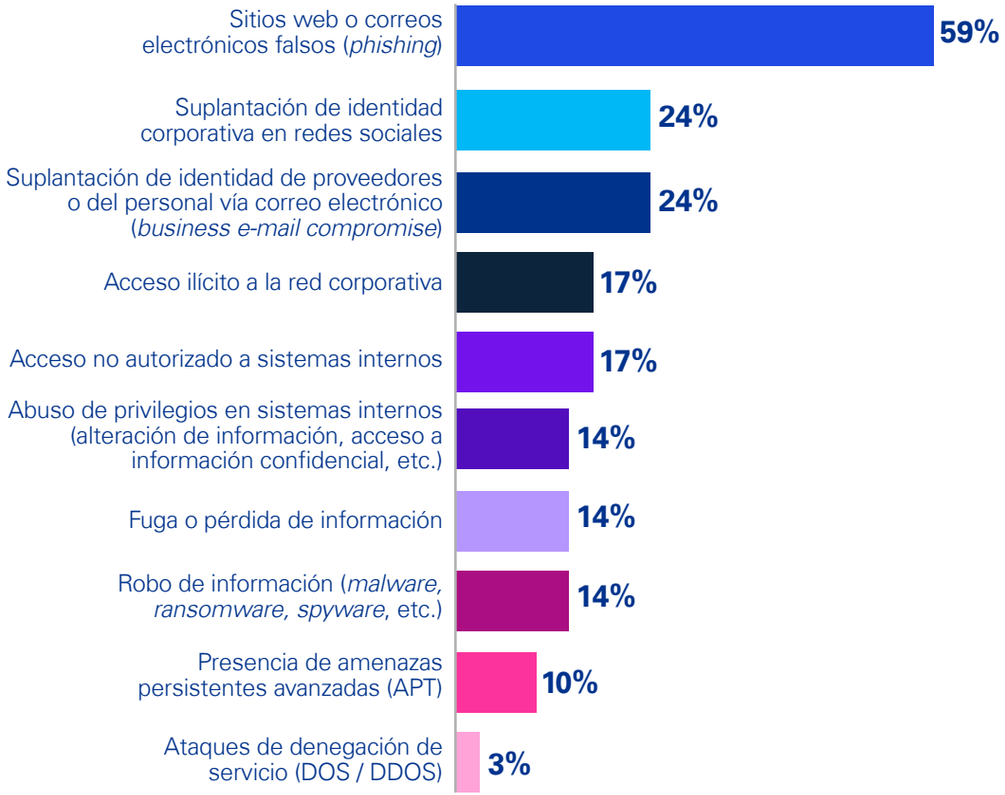
Lo anterior representa un incremento de 16 puntos porcentuales con respecto a la encuesta de 2020 (23%), debido, principalmente, a la sofisticación de las distintas amenazas y su avance tecnológico, que se ha acelerado en los últimos años con la incorporación de la IA.

[3] *Perspectivas de la Alta Dirección en México 2024. Superar los retos y aprovechar las oportunidades*, KPMG, 2024.

Modalidad de los ciberataques

De aquellos negocios que han sido víctimas de un ciberataque, 59% menciona que este se realizó a través de sitios *web* o correos electrónicos falsos, mejor conocidos como *phishing*; 24%, mediante la suplantación de identidad corporativa en redes sociales, y el mismo porcentaje, por la suplantación de identidad de proveedores o personal por medio de correo electrónico.

¿Qué tipo de incidente sufrió o intentaron llevar a cabo contra su empresa?



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

Queda claro que los ciberataques, en particular los relacionados con el *phishing*, representan un riesgo significativo en la actualidad: los casos de este tipo de delito han crecido 27 puntos desde 2020 (32%). Esto se puede relacionar con la falta de capacitación para identificar y prevenir estas amenazas o simplemente con una actitud de descuido, lo que hace imperativa la implementación de programas de entrenamiento y sensibilización continua sobre cómo protegerse de estas amenazas.

Asimismo, a medida que las organizaciones adoptan nuevas tecnologías y esquemas de trabajo, es importante establecer políticas claras y detalladas que regulen el uso adecuado de las herramientas digitales y dispositivos con acceso a información sensible. Estas políticas no pueden limitarse a aquellos activos tecnológicos que son propiedad del negocio, sino que deben extenderse a los dispositivos personales que puedan acceder a dicha información, mediante enfoques como *bring your own device* (BYOD), lo que permitirá a la Administración identificar, prevenir y mitigar los riesgos asociados con posibles ciberdelitos derivados del uso indebido de estos recursos.

Otro aspecto importante es que el personal conozca los protocolos establecidos para responder a este tipo de ataques, ya que a nivel global existen cada vez más regulaciones que obligan a las empresas a revelar dichos incidentes e informar a todas las partes afectadas, incluyendo proveedores, clientes y colaboradores, de manera ágil y transparente, cuando se haya producido una filtración de datos sensibles o el acceso no autorizado a sus sistemas, lo que compromete, sin duda, la reputación del negocio.

Detrás de los ciberataques

De acuerdo con los resultados, 55% de las organizaciones no tienen identificado el origen del incidente; 17% identifica que fue originado por personal que ya no labora en la compañía; 14%, por grupos *hacktivistas*; 10%, por colaboradores internos, y 4% lo relaciona con el crimen organizado.

¿Tiene conocimiento del origen del incidente?

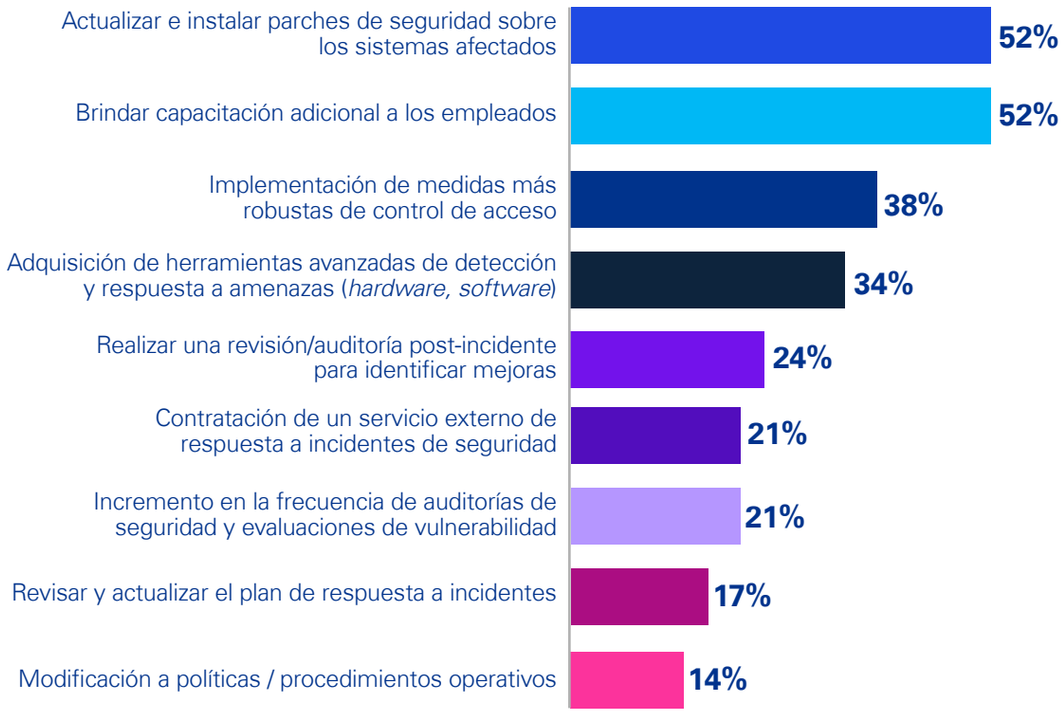
La complejidad para identificar el origen de este tipo de incidentes refleja la importancia de reforzar las estrategias de inversión en protocolos de investigación. Por la naturaleza de los ciberdelitos, las personas que los perpetran pueden ocultar su identidad y ubicación, utilizando herramientas como las redes privadas virtuales (VPN, por sus siglas en inglés), entre otras, por lo que es esencial contar con especialistas que puedan realizar investigaciones exhaustivas y rastrear los incidentes de manera efectiva.

Medidas adoptadas tras el incidente

Sobre las acciones tomadas después del ataque, 52% de las organizaciones actualizaron e instalaron parches de seguridad en los sistemas afectados, y brindaron capacitación adicional al personal; 38% implementó medidas más robustas de control de acceso, y 34% adquirió herramientas avanzadas de detección y respuesta a amenazas.

Por su parte, 24% realizó una revisión o auditoría posterior al incidente para identificar áreas de mejora; 21% contrató un servicio externo de repuesta; otro 21% incrementó la frecuencia de auditorías de seguridad y evaluaciones de vulnerabilidad; 17% revisó y actualizó el plan de respuesta a incidentes, y 14% modificó las políticas o procedimientos operativos.

¿Qué medidas se tomaron luego del incidente?



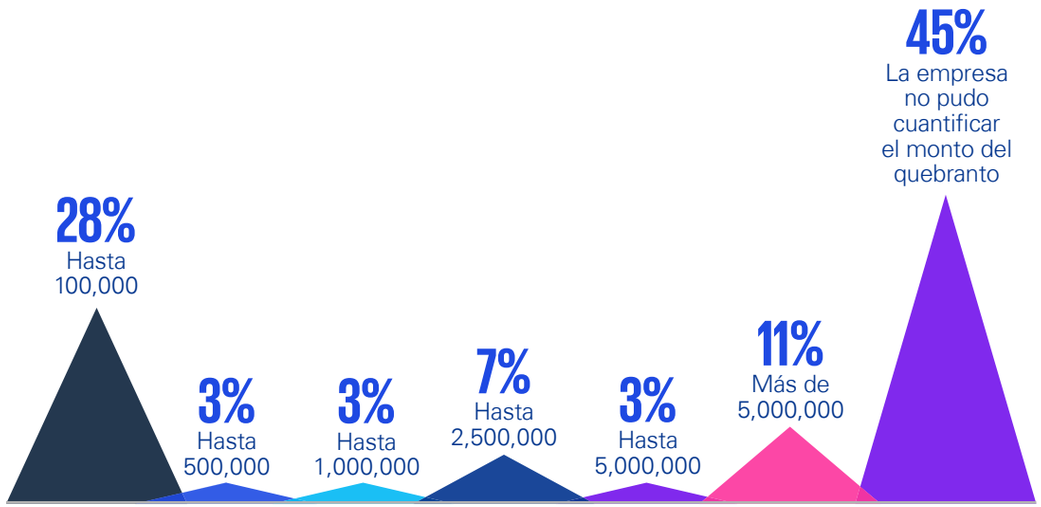
La suma de las variables no es igual a 100% debido a que era posible seleccionar más de una opción.

Como podemos observar, las acciones tomadas tras un incidente cibernético suelen ser reactivas y, por lo tanto, insuficientes para mitigar futuros ataques. El enfoque preventivo es crucial, particularmente en sectores regulados como el financiero, donde las auditorías de seguridad informática son obligatorias; sin embargo, en otros sectores que carecen de regulaciones estrictas, es fundamental reforzar la prevención mediante un adecuado análisis de riesgos, especialmente al implementar nuevas tecnologías, e incluso sobre las existentes, para que se tenga una adecuada protección contra posibles vulnerabilidades.

Impacto financiero

Tras los ciberataques y al evaluar su impacto económico, 45% de las organizaciones no lograron cuantificar los daños, mientras que 28% reporta pérdidas de hasta MXN 100,000; 11%, superiores a MXN 5,000,000, y 7%, de hasta MXN 2,500,000.

¿Cuál fue el impacto económico en pesos (MXN) del incidente?



Estas cifras destacan, al igual que en los incidentes de fraude, la necesidad de implementar herramientas más efectivas y sólidas para la detección y evaluación de los riesgos e impactos causados por este tipo de ilícitos.

Controles de ciberseguridad

Los controles que implementan las organizaciones dependen de la naturaleza de su operación. Al respecto, 51% menciona que realiza el monitoreo proactivo de amenazas internas y externas como control de ciberseguridad; 48% utiliza VPN para el acceso remoto, y 47% cuenta con un plan de recuperación y continuidad del negocio, así como con entrenamientos para su personal; no obstante, 17% no tiene implementado ningún tipo de control de ciberseguridad.

¿Su empresa cuenta con alguno de los siguientes controles de ciberseguridad?

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

En este sentido, el desarrollo de un plan de recuperación y continuidad del negocio requiere de un análisis profundo del tipo de industria y la relevancia de los activos involucrados, ya que sectores como el financiero, por ser altamente regulados, necesitan planes a la medida que consideren los riesgos específicos a los que están expuestas las instituciones. Por ello, es importante realizar una evaluación de riesgos para identificar qué activos, tangibles o intangibles, son críticos en la operación.

Cabe destacar que, para que el plan sea efectivo, deben realizarse pruebas con regularidad, bajo diferentes escenarios de riesgo, por lo que la preparación y actualización son esenciales para evitar fallas, dado que una interrupción puede tener consecuencias significativas, tanto financieras como operativas, particularmente en un entorno digital tan interconectado como el actual.

Asimismo, las organizaciones deben incluir en sus planes de recuperación y respuesta el involucramiento de especialistas en la industria. Así como la tecnología juega un papel transversal en la gestión de otro tipo de riesgos, es esencial que los especialistas fortalezcan los programas de prevención, detección y respuesta ante los ciberdelitos, aportando su conocimiento técnico y comprensión de las vulnerabilidades específicas de cada sector.

En este contexto, ante un entorno altamente digitalizado, resulta alarmante que 17% de las compañías afirmen no contar con controles de ciberseguridad, considerando que gran parte de la tecnología puede estar concentrada en un simple dispositivo móvil, lo que puede aumentar las vulnerabilidades, haciendo imprescindible la implementación de medidas de protección robustas para salvaguardar la información.

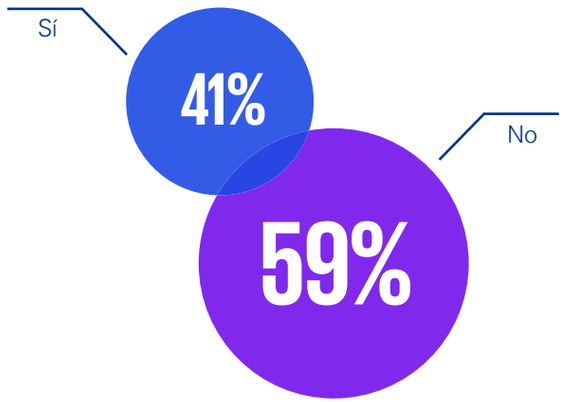
Prevención de lavado de dinero y financiamiento al terrorismo

Sistema financiero

La prevención de lavado de dinero está intrínsecamente relacionada con los compromisos ASG que las organizaciones deben adoptar, particularmente mediante el ODS 16, en el cual una de las metas planteadas es la reducción significativa de las corrientes de flujos ilícitos.

Actualmente, cada vez son más las organizaciones que están sujetas a normatividad en esta materia; por ejemplo, 41% de la muestra afirma que debe adoptar regulaciones en prevención de lavado de dinero (PLD) y financiamiento al terrorismo (FT) por la naturaleza de sus operaciones.

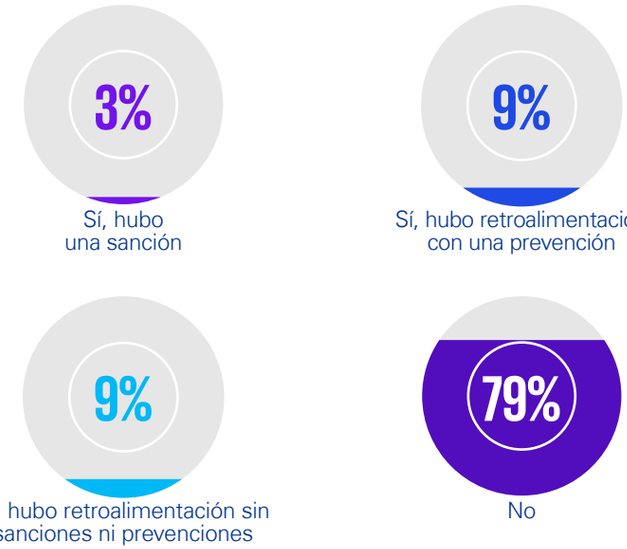
¿Su organización debe adoptar regulaciones específicas en prevención de lavado de dinero del sistema financiero (bancos, casas de bolsa, sofomes, centros cambiarios, transmisores de dinero, *fintech*, entre otras)?



Supervisión y control

Derivado de este porcentaje, 21% menciona haber tenido una visita de inspección, sanción o retroalimentación sobre el programa de PLD/FT por parte de la Comisión Supervisora en el último año; 9% recibió retroalimentación con una prevención; 9% recibió retroalimentación, pero sin sanciones ni prevenciones, y 3% tuvo una sanción.

En los últimos 12 meses, ¿ha tenido visitas de inspección, sanciones o retroalimentación sobre el programa de prevención de lavado de dinero (PLD) y financiamiento al terrorismo (FT) por parte de la Comisión supervisora?



El proceso de detección del lavado de dinero y FT se encuentra regulado y exige que las organizaciones implementen un programa que, entre otras acciones, considere el reporte de operaciones inusuales a la Unidad de Inteligencia Financiera (UIF), a través de sus respectivas comisiones supervisoras, particularmente cuando las actividades de sus usuarios no coincidan con su perfil transaccional conocido o se tenga alguna otra señal de alerta, que, hoy en día, incluso puede estar relacionada con violencia motivada ideológicamente, como la UIF de Canadá lo ha comenzado a implementar en pro de los principios ASG, generando una alerta que las organizaciones deben analizar e investigar, previo a ser reportada a la propia unidad.

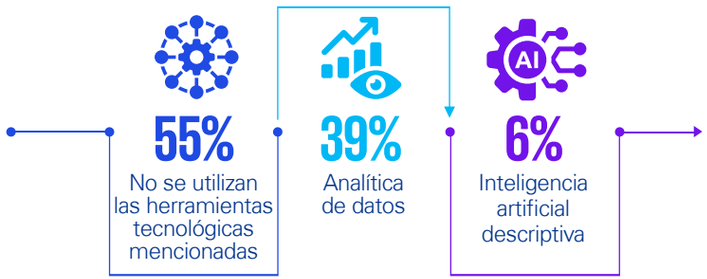
La UIF recopila estos reportes, analiza patrones y tiene la facultad de solicitar información adicional a través de las respectivas comisiones supervisoras y colaborar con autoridades de otros países para generar inteligencia financiera que coadyuve en la identificación de ilícitos.

Una vez que la UIF cuenta con evidencia suficiente sobre una posible actividad ilícita, presenta una denuncia ante el Ministerio Público de la Federación, lo que permite que la Fiscalía General de la República (FGR) asuma una investigación de tipo penal. Cabe destacar que este proceso abarca tanto casos de PLD como de FT, y no se limita a reportes del sistema financiero, sino que puede iniciarse a partir de información obtenida de otras entidades o colaboraciones con autoridades internacionales.

Soluciones tecnológicas

En cuanto a las herramientas para analizar las posibles operaciones inusuales, 39% de la muestra menciona que hace uso de la analítica de datos, y 6%, de la IA descriptiva; sin embargo, 55% afirma no utilizar ninguna de las opciones mencionadas.

¿El área encargada de vigilar los temas de PLD y FT se apoya en alguna de las siguientes herramientas tecnológicas para analizar las posibles operaciones inusuales?



De acuerdo con estas cifras, el uso de herramientas tecnológicas para analizar operaciones inusuales es limitado. Este es un dato revelador, dado que las diversas disposiciones de carácter general aplicables al sistema financiero requieren de herramientas tecnológicas como los sistemas automatizados para monitorear la transaccionalidad y apoyar en la detección de posibles operaciones inusuales.

Si bien lo anterior representa un número alto, potencialmente podría sugerir que algunas organizaciones no asociaron el término "analítica de datos" con los sistemas de monitoreo que ya utilizan y que podrían tener dicha tecnología de manera intrínseca; sin embargo, la tendencia en México y otros países muestra un uso creciente de las denominadas "nuevas tecnologías" como la IA, *machine learning* y analítica avanzada para analizar mayores cantidades de datos relacionados con la transaccionalidad y otros factores conductuales (*behavioral intelligence*) para generar mayor inteligencia financiera.

En definitiva, carecer de estas tecnologías puede aumentar el riesgo de no identificar actividades atípicas y, consecuentemente, generar potenciales incumplimientos de las regulaciones, lo que puede traducirse en multas y sanciones, así como en la materialización del lavado de dinero o del FT sin una detección oportuna o incluso nula.

La importancia de los programas de PLD/FT con una perspectiva ASG

Es imperante que los programas de PLD/FT comiencen a incorporar una perspectiva ASG con la finalidad de contribuir a las metas planteadas por el ODS 16, respecto a la promoción de los derechos humanos en sociedades libres de flujos financieros ilícitos y corrupción. La capacitación y sensibilización en esta materia resulta una actividad sumamente valiosa para las organizaciones.

Al respecto, 27% señala que sus programas de capacitación sí abordan asuntos ASG con énfasis en la debida diligencia en cuanto a derechos humanos; 24%, sobre la prevención de flujos ilícitos por tráfico de personas y esclavitud moderna, mientras que en 64% de los programas no se incluyen estos temas.

En los programas de capacitación y difusión, ¿se aborda cómo los programas ASG pueden ayudar a la PLD y a combatir el FT?

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

Es importante tener en cuenta que los denominados "delitos emergentes" como el tráfico de personas y los delitos ambientales y culturales, han prosperado gracias a las corrientes de flujos ilícitos que logran pasar los controles tradicionales establecidos en el sistema financiero, por lo que integrar temas ASG que permitan a los equipos de monitoreo y las personas involucradas en el sistema financiero desarrollar nuevas estrategias y ajustar modelos de riesgo para identificar y prevenir actividades ilícitas, podría resultar la manera más eficaz de combatirlos.

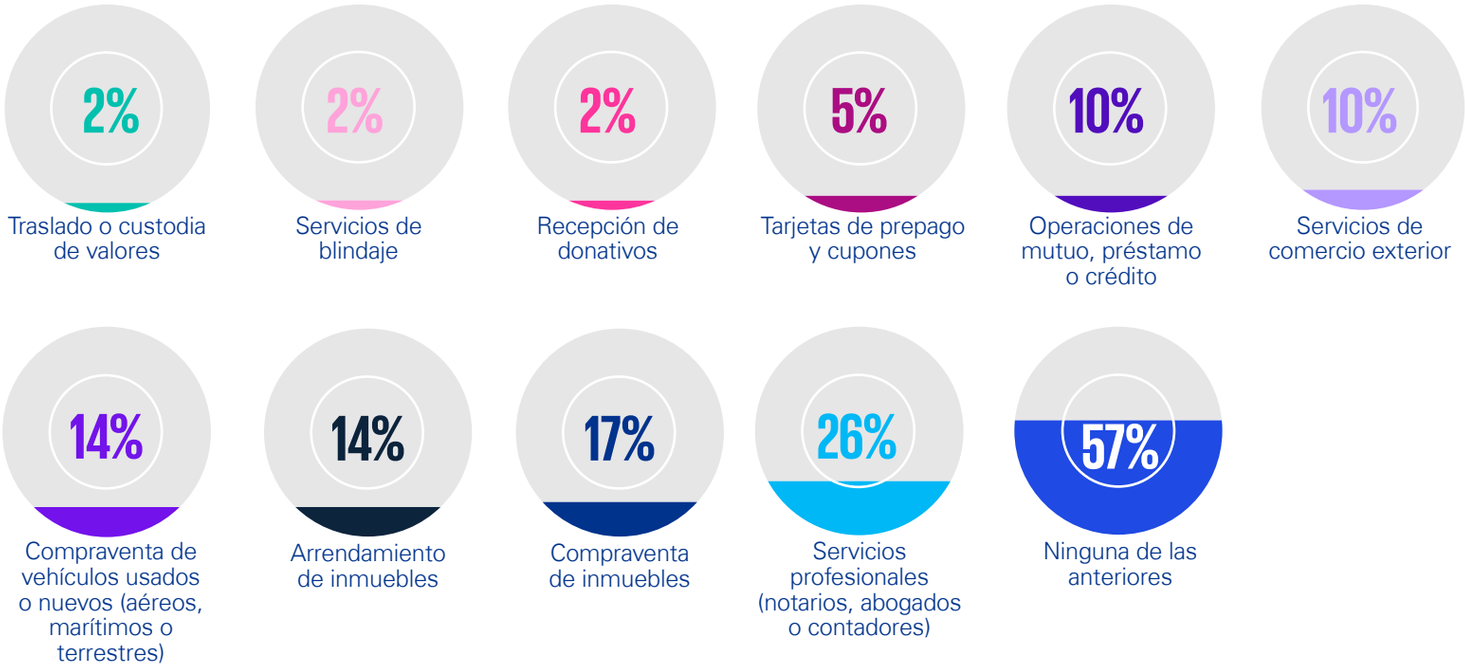
En este sentido, que el sistema financiero se capacite en estos temas facilita la identificación de riesgos emergentes y la adaptación de los modelos de monitoreo, mejorando así la capacidad para prevenir, detectar y mitigar estos delitos.

Sectores no financieros

Como se mencionó en la sección anterior, la normatividad aplicable en materia de PLD/FT no solo se ubica en las organizaciones del sistema financiero, sino también a distintos sectores de la economía real, que para el caso de México se denominan actividades vulnerables y son reguladas bajo la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI), comúnmente conocida como "Ley Antilavado".

En términos de dicha ley, respecto a la realización de las actividades consideradas como vulnerables, 26% de las organizaciones afirman que llevan a cabo servicios profesionales; 17%, compraventa de inmuebles, y 14%, arrendamiento, así como compraventa de vehículos usados o nuevos.

En términos de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, ¿su empresa realiza alguna actividad considerada como vulnerable?



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

Confirmaciones de criterio en la realización de actividades vulnerables

Por otro lado, que la mayoría de las organizaciones (57%) contestaran que no realizan ninguna de las actividades vulnerables de la lista se vuelve relevante considerando que puede indicar un desconocimiento de las regulaciones aplicables o una falta de interés por identificar y cumplir con ellas. Un ejemplo es que 40% menciona que no cuenta con estudios o reportes que confirmen que realizan actividades vulnerables o que no incurren en ningún supuesto para dar cumplimiento a la Ley Antilavado; 35% comenta que lo realizaron a través de un área interna; 20%, mediante un tercero especializado, y 5%, con un criterio de confirmación de la UIF.

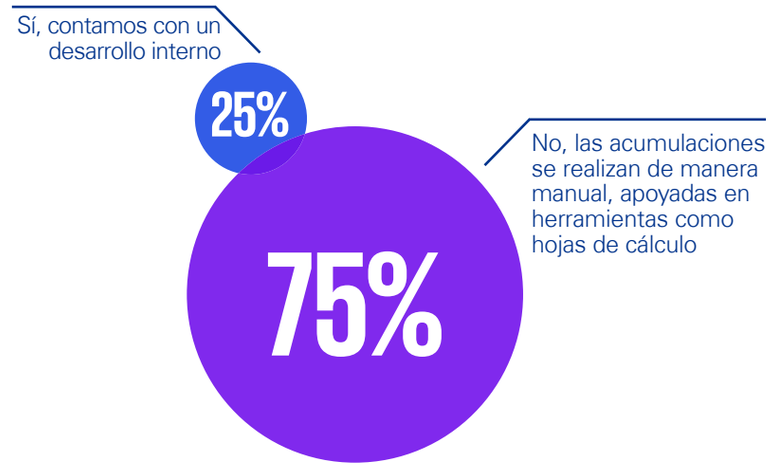
¿Su empresa cuenta con un estudio o reporte que confirme que realiza actividades vulnerables identificadas, o bien que no incurre en ningún supuesto para dar cumplimiento a la Ley Antilavado?

A pesar de que este estudio no es requerido por la Ley Antilavado, es fundamental para demostrar el cumplimiento de la normativa, ya que permite a las organizaciones evitar el riesgo de incumplimiento, facilitando la correcta identificación de actividades que podrían estar sujetas a la regulación. Esto subraya la necesidad de fortalecer los mecanismos de control y la educación sobre las obligaciones en materia de PLD en organizaciones de distintos giros.

Automatización de procesos

Respecto a los sistemas automatizados para la acumulación de operaciones y presentación de avisos, 25% de las organizaciones cuentan con uno de manera interna, mientras que 75% no, y realiza el proceso manualmente con base en hojas de cálculo.

¿Cuenta con un sistema automatizado para la acumulación de operaciones y presentación de avisos?



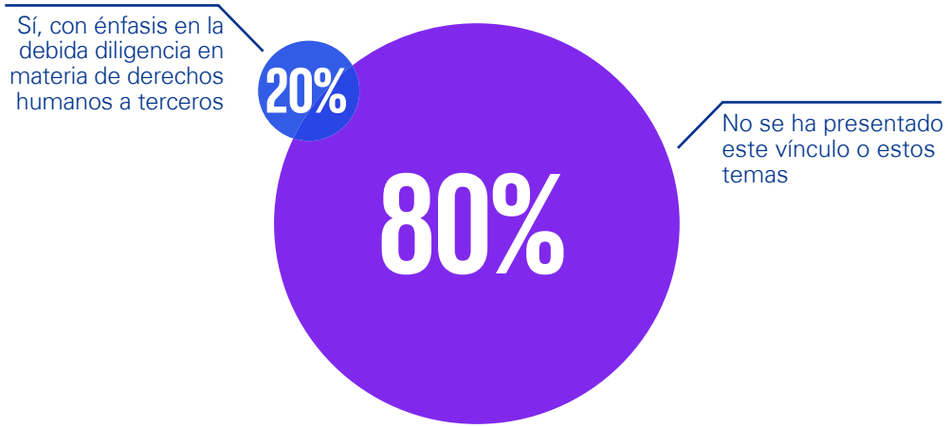
El hecho de que la mayoría de las organizaciones de la muestra utilice procesos manuales para la acumulación de operaciones y presentación de avisos conlleva riesgos significativos. Actualmente, el uso de tecnología automatizada puede ayudar a mitigarlos, particularmente para evitar errores humanos, los cuales son muy comunes en procesos manuales.

En este sentido, aunque la Ley Antilavado no obliga a contar con un sistema automatizado, su implementación es muy recomendable, porque también ayuda a garantizar que la información se maneje eficientemente, y que los procesos que abonan al programa integral de PLD, como la identificación y el conocimiento de cliente, el monitoreo transaccional y, en casos de compraventa de activos virtuales, la trazabilidad de dichos activos, puedan realizarse de manera precisa.

Impacto ASG en las actividades vulnerables

Así como el sistema financiero ha comenzado a incorporar diversos asuntos ASG en los programas de PLD/FT, también en las actividades vulnerables se ha comenzado a tratar la manera de que los programas ASG contribuyan con el ODS 16, particularmente en la reducción de flujos ilícitos relacionados con delitos como el tráfico de personas y ambientales; no obstante, 80% de las organizaciones aún no han integrado este enfoque en sus capacitaciones y programas de difusión. Por otro lado, 20% señala que sí lo ha hecho, destacando la importancia de la debida diligencia en materia de derechos humanos al trabajar con terceros, lo que refuerza la necesidad de vincular más estrechamente los programas ASG con la mitigación de estos riesgos.

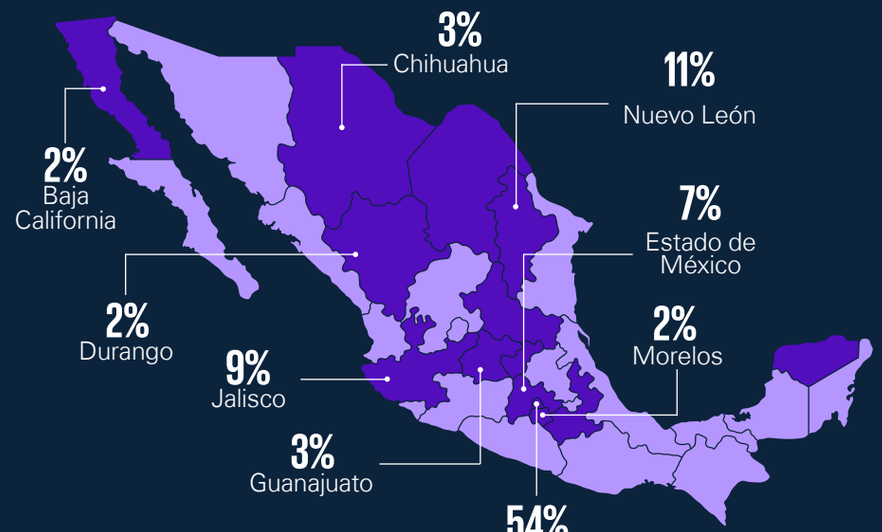
Como parte de la capacitación y difusión, ¿se aborda cómo los programas ASG pueden ayudar a la PLD y a combatir el FT?



Si bien la cifra aún es baja, la concientización en asuntos ASG comienza a tomar importancia en las denominadas actividades vulnerables, que, por su vínculo directo con la economía real, presentan una gran oportunidad para fortalecer la detección de flujos ilícitos relacionados con el tráfico de personas y los delitos culturales y ambientales, con lo cual se pueden fortalecer los marcos de prevención para contribuir a las metas planteadas por el ODS 16 y buscar, hacia 2030, sociedades más justas y equitativas, que prevengan, detecten y respondan adecuadamente ante los flujos financieros ilícitos relacionados con el lavado de dinero y FT.

Metodología

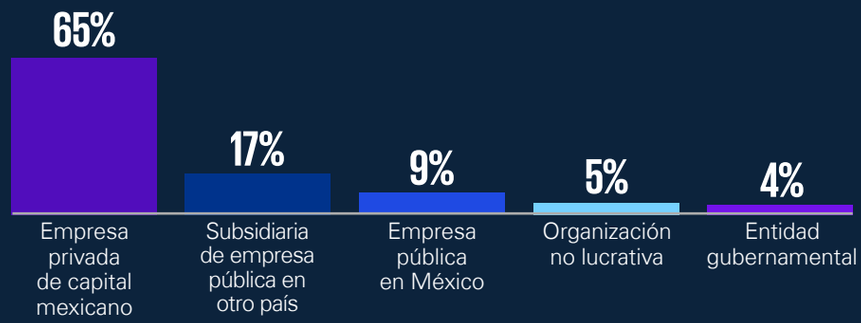
Ubicación de la empresa



Con **1%** cada uno:
- Puebla
- Sonora
- Yucatán
- Aguascalientes
- Coahuila
- Querétaro

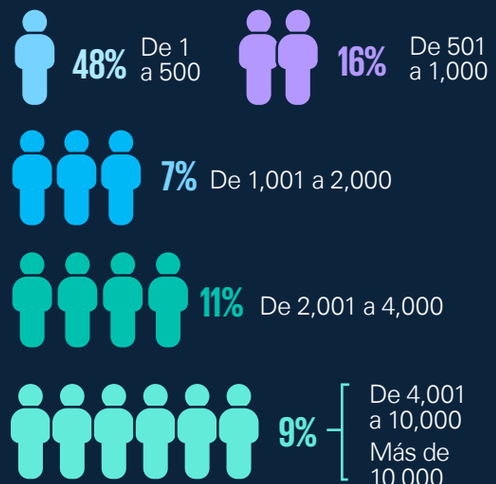
1% se encuentra fuera de la República Mexicana

Tipo de compañía



Nivel del participante

Cantidad de personal



Importe de ventas anuales en millones de pesos

Sector al que pertenece su organización

Conclusiones

El impacto de los delitos financieros en México ha evolucionado significativamente en los últimos años, reflejando un panorama cada vez más complejo, caracterizado por la creciente sofisticación y diversidad de las amenazas, el avance de la tecnología como actor clave y la intensificación y ampliación de las regulaciones.

Como podemos observar en los resultados de este estudio, existen avances y mejoras en las estrategias de prevención; sin embargo, un importante número de organizaciones permanecen expuestas a fraudes, corrupción, lavado de dinero, financiamiento al terrorismo y ciberataques, manifestando una necesidad de contar con enfoques adecuados de identificación y respuesta, lo que resalta la vulnerabilidad del entorno empresarial frente a estos delitos y la urgente necesidad de una respuesta continua y efectiva.

En este contexto, la tecnología se perfila como un habilitador deseable para la detección, respuesta y prevención de actividades ilícitas, derivado de su capacidad para analizar grandes volúmenes de datos y detectar patrones atípicos, contribuyendo al combate contra los delitos. No obstante, ninguna tecnología es una solución infalible, por lo que es fundamental integrarlas a una estrategia más amplia, que incluya la capacitación continua del talento y el fortalecimiento de los controles internos. Además, no se puede soslayar el hecho de que el avance tecnológico crea nuevas posibilidades para la comisión de delitos financieros, por lo que la actualización constante es la mejor forma para hacerles frente.

Por lo anterior, las organizaciones deben invertir en programas de capacitación y entrenamiento en temas de prevención del fraude y corrupción, ciberseguridad y PLD/FT, ahora también con una perspectiva ASG, que parta desde el conocimiento básico sobre estos principios y de una comprensión y sensibilización de los compromisos y circunstancias que impactan o en los que se puede impactar en materia ambiental y de responsabilidad social real, para que, con el paso del tiempo, pueda fortalecerse el compromiso de los negocios con los ODS, especialmente el número 16.

Aunque las organizaciones han adoptado mecanismos de prevención acordes a los requerimientos regulatorios, el estudio muestra que aún hay un largo camino por recorrer, por lo que se deben seguir mejorando los controles y actualizando continuamente las estrategias de prevención, contemplando un enfoque integral, que combine la tecnología de vanguardia, la formación constante y una cultura de prevención proactiva para enfrentar los riesgos emergentes de manera efectiva, que les permita protegerse en un entorno cada vez más complejo y dinámico, con una constante perspectiva de derechos humanos.

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

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

Contactos

Luis Preciado
Socio Líder de Risk Advisory Solutions
KPMG México

Cesar Pérez
Socio de Forensic
KPMG México

Jefferson Gutiérrez
Socio Líder de Asesoría en Tecnología Forense
KPMG México

Dalia Sierra
Socia de Forensic y Asesoría en Cumplimiento Anticorrupción
KPMG México

Daniel Ortiz de Montellano
Director de Forensic
KPMG México