Una triple amenaza en las Américas: 2022 KPMG Fraud Outlook

Lo más destacado del sector: manufactura industrial

Cinco hechos que el liderazgo en las empresas de manufactura industrial debe conocer

Una triple amenaza en las Américas. 2022 KPMG Fraud Outlook destaca los desafíos de fraude, incumplimiento y ataques cibernéticos que actualmente enfrentan las empresas de todos los sectores. Este artículo de seguimiento analiza las amenazas que se presentan, en específico, para las organizaciones de manufactura industrial, y describe cinco aspectos que la Alta Dirección del sector debe conocer:

01 La mayoría de las empresas de manufactura industrial experimentaron fraude en el último año. Además, sus defensas son las más débiles de cualquier sector

En los últimos 12 meses, 60% de las empresas sufrieron algún tipo de fraude. Dado este nivel de riesgo, los esfuerzos actuales parecen insuficientes, ya que aproximadamente uno de cada nueve ejecutivos del sector (11%) informa que su organización no cuenta con ningún programa antifraude (3% de la encuesta general). Por el contrario, los programas integrales, los cuales incluyen la prevención, detección y respuesta, existen solo en 18% de las organizaciones de manufactura industrial (en comparación con un 32% de la encuesta general). Esto probablemente sea lo más alarmante, debido a que muestra una falta de atención ante el peligro; al respecto, 60% de las personas encuestadas señalan que sus planes de respuesta al fraude son efectivos o muy efectivos, pero solo 46% informa que sus esfuerzos se están concentrado en procedimientos específicos.

02 Es posible que las organizaciones del sector no aprecien el riesgo sustancial de fraude que enfrentan, especialmente por parte de personas internas

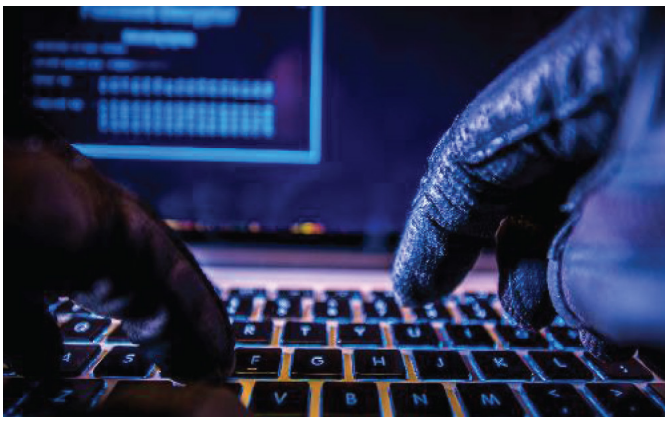
Como grupo, las compañías de manufactura industrial (MI) enfrentan un problema particular con el fraude interno: 36% reporta que, en el último año, alguien dentro de la empresa (un alto directivo, un mando medio o un empleado operativo) había cometido dicho delito. Esta es la cifra más alta para cualquier sector de la encuesta.

No obstante, los resultados no son casuales. Por un lado, las empresas de MI informaron hacer un menor énfasis en los controles internos que aquellas industrias más fuertemente reguladas. Asimismo, la naturaleza de la manufactura industrial brinda oportunidades importantes para la confabulación entre agentes internos y externos. Por ejemplo, si un proveedor cobra de más por las materias primas a cambio de sobornos, ocultar dichas cifras dentro del costo de fabricación en el sistema contable puede ser más fácil. Por lo tanto, la naturaleza del proceso de contabilidad de la MI indica que sería prudente una vigilancia adicional.

Buscando atender este tipo de amenazas, el sector ha luchado más que la mayoría para hacer frente a los desafíos que supone trabajar desde casa. Al respecto, 65% de las empresas encuestadas señalaron que, a raíz del trabajo a distancia, la reducida capacidad para monitorear a los colaboradores aumentaba significativamente el riesgo de experimentar fraude interno y, en ese mismo sentido, 63% estuvo de acuerdo en que este esquema laboral ha afectado de manera negativa su capacidad para responder adecuadamente al fraude. En ambos casos, estos son los resultados más altos de la encuesta.

De cara al futuro, los hallazgos sugieren que las compañías de MI pueden tener una falta de conciencia sobre el alcance de la amenaza interna: solo 28% espera que el riesgo de fraude interno aumente en el próximo año, mientras que 48% prevé una disminución. Por otro lado, demasiados parecen sentir un exceso de confianza en una defensa eficaz, ya que 64% asegura que los controles antifraude existentes antes de la pandemia no se han actualizado para reflejar la nueva realidad laboral (esta es la segunda cifra más alta en cualquiera de los sectores encuestados).

03 La protección de activos intelectuales y de los sistemas de tecnología de la información son las prioridades antifraude más apremiantes



Los ciberataques son el problema más común para las organizaciones de MI, así lo señalan 38% de los encuestados, quienes sufrieron fraude en el último año. Esto se suma a las preocupaciones de ciberseguridad develadas y discutidas a continuación.

De las empresas de manufactura industrial que sufrieron fraude por parte de un perpetrador externo en el último año, 26% expresa que se trató de falsificación o privacidad y 24% señala haber experimentado robo de propiedad intelectual o espionaje industrial (la primera fue la tasa de respuesta más alta, mientras que la segunda ocupó el segundo lugar en los resultados generales). Muchas entidades del sector están mal preparadas para afrontar tales amenazas.

04 Las compañías de manufactura industrial están menos preparadas para el cumplimiento

Este tipo de organizaciones consideran que el riesgo de cumplimiento crecerá en el futuro, ya que nueve de cada diez prevén una expansión en el alcance de una o más de las regulaciones ambientales, de privacidad de datos y laborales en los próximos cinco años. Durante ese mismo período, 51% espera que la aplicación de las normas existentes en estos campos se vuelva más estricta (la cifra más alta para cualquier sector).

Sin embargo, solo 52% de las empresas alcanzan niveles internacionales o nacionales de mejores prácticas en el cumplimiento ambiental y menos de la mitad expresa lo mismo sobre sus esfuerzos de cumplimiento anticorrupción (46%) y antilavado de dinero (45%). En cada caso, estas son las peores o segundas peores cifras de la encuesta. Los Alta Dirección del sector también es la menos propensa a comunicar que sus actividades de gestión de investigación y prevención del incumplimiento sean efectivas o muy efectivas.

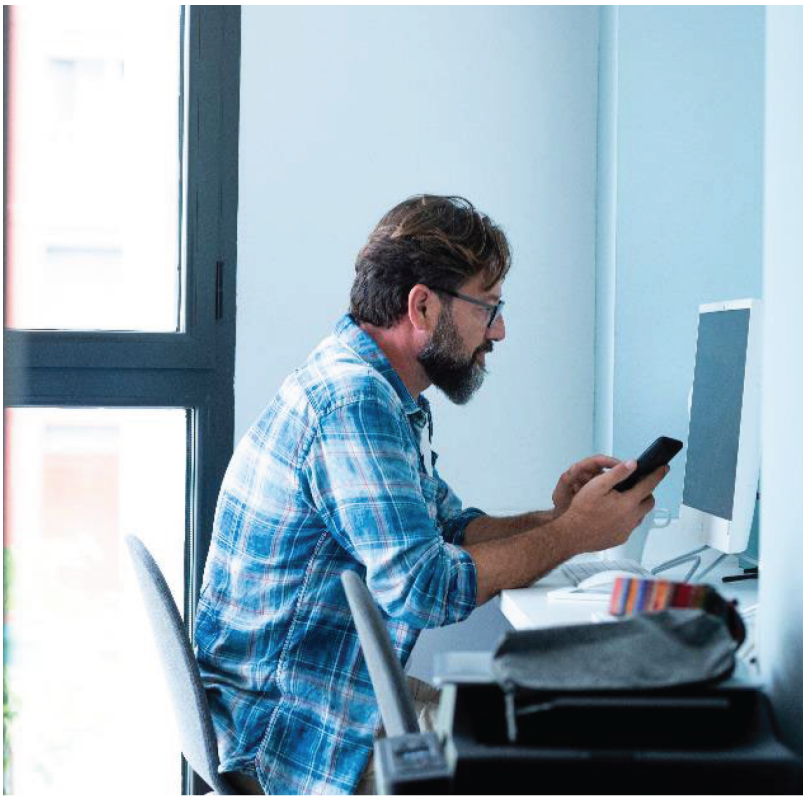
Finalmente, cabe destacar que la mayoría de las entidades no parecen estar preparadas para reforzar sus defensas: solo 41% espera aumentar el gasto en esfuerzos mejorados de cumplimiento normativo, la segunda cifra más baja de todos los sectores encuestados, después de ciencias de la vida (37%).

05 El trabajo a distancia ha presentado mayores desafíos a causa de una ciberseguridad relativamente débil

Poco más de la mitad de las empresas de manufactura industrial (51%) sufrieron pérdidas económicas a causa de un ciberataque en el último año (esta es la cifra más alta en cualquier sector). Asimismo, 75% señala que no le sorprendería presentar una filtración de datos de los clientes durante el próximo año (nuevamente la cifra más alta en la encuesta, cuyo promedio fue 63%). De cualquier forma, las defensas existentes brindan pocas garantías: solo 11% de las organizaciones pueden contener un ataque cibernético o una infracción dentro de la semana posterior a su identificación, muy por debajo del promedio de la encuesta (19%).

Así pues, la ciberseguridad es otra de las áreas en las que el sector está lidiando con las implicaciones del trabajo a distancia: 74% está de acuerdo en que este esquema laboral ha sido un desafío importante, mientras que 59% asegura que las estrategias de protección previas a la pandemia no son suficientes para abordar los riesgos creados por el nuevo entorno en el que actualmente operan (la cifra más alta y segunda más alta en la encuesta general respectivamente).

En medio de todos estos riesgos, sorprende que la proporción de empresas de MI que planean invertir más en ciberseguridad en el próximo año (64%) esté ligeramente por debajo del promedio de la encuesta (65%).



Perspectiva de KPMG: haga que sus defensas se ajusten a su propósito

El mundo siempre está cambiando, pero de vez en cuando experimenta un punto de inflexión dramático. La pandemia de COVID-19 nos llevó a repensar la manera en que vivimos y trabajamos. Ahora, los eventos geopolíticos están exponiendo las fragilidades de nuestras suposiciones sobre el entorno internacional.

El panorama de riesgos al que se enfrentan las empresas se ha reconfigurado de manera similar. La necesidad de mantener el acceso a los suministros ha llevado a muchas organizaciones a depender de socios que no han sido investigados, lo que podría generar nuevos riesgos de fraude. En cuanto al cumplimiento, el impulso del *net zero* creará una mayor regulación ambiental y las nuevas sanciones globales pueden conducir a una supervisión más estricta de la actividad financiera y comercial. Finalmente, los ataques cibernéticos, que ya habían aumentado durante la pandemia, están permitiendo a los ciberatacantes perseguir una nueva variedad de objetivos.

En resumen, si su empresa no ha realizado recientemente una revisión completa de sus riesgos de fraude, cumplimiento y ciberseguridad, debe realizarla cuanto antes. De lo contrario, sus defensas no estarán diseñadas para combatir las amenazas actuales ni podrá reaccionar a medida que esos riesgos evolucionen.

Desafortunadamente, muchas organizaciones de MI aún necesitan desarrollar fundamentos clave para fortalecer sus defensas mientras se preparan para los cambios constantes. Específicamente y como señalan los datos obtenidos, el sector presenta un importante problema de fraude interno, lo que puede reflejar controles internos débiles en relación con los de sectores más regulados. Del mismo modo, a pesar de una gran amenaza de robo de propiedad intelectual, varias empresas del sector carecen de controles sofisticados para protegerla y, con demasiada frecuencia, no saben dónde se encuentran dichas propiedades. Finalmente, la baja inversión planificada para prepararse ante el cumplimiento de la esperada intensificación de las regulaciones que se observa en los datos de nuestra encuesta se ajusta al patrón histórico del sector. Los presupuestos inadecuados en este campo con frecuencia impiden que las compañías se protejan a sí mismas con medidas efectivas, como como el uso proactivo de análisis para identificar riesgos elevados en regiones o funciones específicas.

Para aquellos que estén listos para hacerlo, el marco básico de prevención, detección y respuesta sigue siendo la base más sólida para gestionar el fraude, el incumplimiento y los ciberataques, pero el entorno donde se implementan estas defensas significa que deben conservar los elementos más efectivos y aprovecharlos para vencer las amenazas en evolución.

Prevención

Desde nuestra perspectiva, ciertos elementos permanecerán prácticamente iguales, tales como la implementación o mejora de los controles internos, la debida diligencia basada en riesgos de integridad sobre empleados y terceros, las evaluaciones de seguridad de sistemas de información críticos, y los ataques cibernéticos simulados para exponer vulnerabilidades.

Otros aspectos tomarán una nueva forma. Por ejemplo, puede ser necesario implementar reglas sobre excepciones a las políticas de debida diligencia en la contratación de proveedores en medio de la escasez de la cadena de suministro, pero las empresas deben equilibrar la necesidad estratégica con el imperativo de evitar ser víctima de fraude y mantenerse en el lado correcto de la regulación.

Detección

En KPMG pensamos que herramientas como el análisis de datos, las auditorías internas y los protocolos para la detección de delitos cibernéticos seguirán siendo fundamentales, aunque los comportamientos que estos buscan pueden ser diferentes. Además, incluso cuando hay más empleados y empleadas trabajando en casa, sus ojos y oídos son los que percibirán las fallas de cumplimiento o los riesgos de fraude.

Las medidas que las empresas deben tomar incluyen capacitación actualizada sobre los riesgos, así como sobre la importancia de informar comportamientos inusuales utilizando los mecanismos existentes de informe de incidentes.

Respuesta

Deben existir protocolos eficaces para responder a situaciones de fraude, así como instancias para atender el incumplimiento regulatorio y los incidentes cibernéticos. Las compañías deben prepararse para atender los desafíos emergentes dentro del triángulo de riesgo actual. Esto podría incluir, por ejemplo, decidir con anticipación si están dispuestas a pagar en caso de un ataque vía *ransomware* o definir de antemano quién se hará responsable.

Para obtener más información sobre cómo KPMG puede ayudarle, contáctenos:

Marc Miller
Socio de Asesoría para las Américas* y Líder de Forensic de KPMG en Estados Unidos

Iván Vélez-León
Director Ejecutivo de Asesoría Forense de KPMG en Estados Unidos

Ana López Espinar
Socia de Asesoría y Colíder de la Práctica de Forensic en Sudamérica* y de KPMG en Argentina

Emerson Melo
Socio de Asesoría y Colíder de la Práctica de Forensic en Sudamérica* y de KPMG en Brasil

Luis Preciado
Socio Líder de Risk Advisory Solutions para KPMG en México y Centroamérica

Mario Hernández
Socio Líder del segmento IMMEX para KPMG en México y Centroamérica

kpmg.com.mx KPMG MÉXICO @KPMGMEXICO KPMG MÉXICO KPMGMX

* Todos los servicios profesionales son proporcionados por las firmas miembro de KPMG registradas y autorizadas por KPMG International.