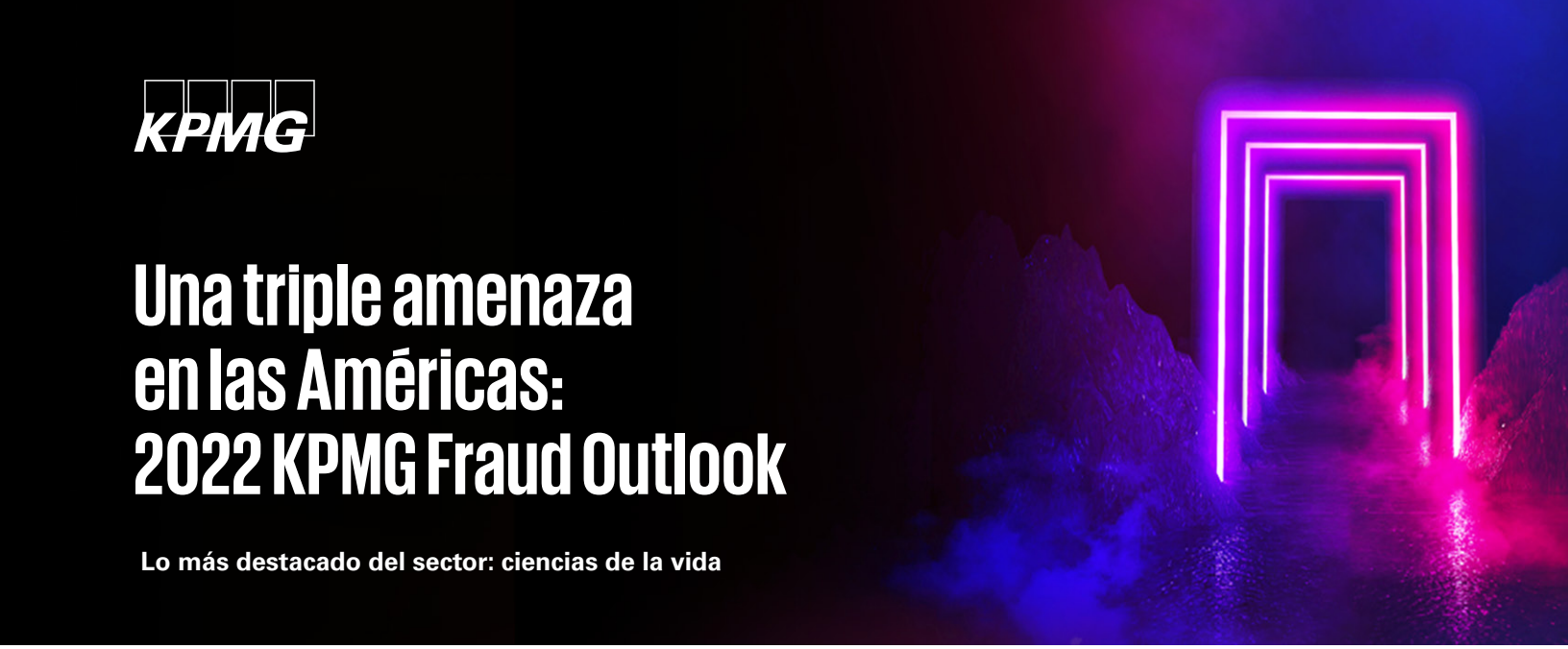


Una triple amenaza en las Américas: 2022 KPMG Fraud Outlook

Lo más destacado del sector: ciencias de la vida

Cinco hechos que el liderazgo de las empresas de ciencias de la vida 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 a las que están expuestas las compañías de ciencias de la vida y describe cinco aspectos que el liderazgo de la industria debe conocer:

01 Las organizaciones de ciencias de la vida viven el mayor desafío de cumplimiento que cualquier otro sector cubierto por nuestra encuesta; pero solo una minoría está invirtiendo los recursos necesarios para gestionarlo

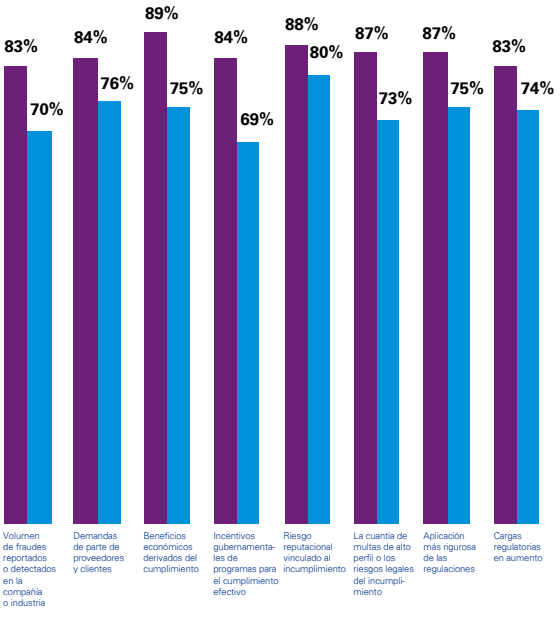
Esta industria fue, con mucho, la más afectada por las multas de incumplimiento en los últimos 12 meses, el equivalente a 0.76% de las ganancias durante ese periodo. Esto hace palidecer el promedio del estudio, de 0.46%. Los encuestados también son más propensos que los de otras industrias a decir que cada factor citado está impulsando a los líderes a prestar más atención a los problemas de cumplimiento, como se ve en la gráfica.

Finalmente, otros elementos de la triple amenaza están exacerbando los problemas de cumplimiento para las entidades de ciencias de la vida. Como se comenta a continuación, las compañías del sector se enfrentan a importantes retos relacionados con la ciberseguridad y los tipos de fraude que utilizan como vector los ciberataques. Ambos tipos de problema, a su vez, plantean dificultades de cumplimiento: 36% de todos los encuestados de este sector informan que un ataque cibernético en el último año ha llevado a una revisión legal o de cumplimiento, o a una investigación en sus empresas.

La Alta Dirección de la industria tampoco espera que estos problemas disminuyan: 73% de quienes respondieron la encuesta esperan que el riesgo de cumplimiento aumente el próximo año, nuevamente la cifra más alta que la de cualquier otro sector.

Parece preocupante, por lo tanto, que solo 37% de los encuestados de ciencias de la vida esperen ver un mayor gasto en esfuerzos de cumplimiento en el próximo año; el número más bajo para cualquiera de los sectores cubiertos en estos reportes.

¿Hasta qué punto los siguientes factores están incrementando el tiempo y atención que el liderazgo de su empresa dedica a temas de cumplimiento? (Porcentaje de quienes respondieron "significativamente" o "mucho")

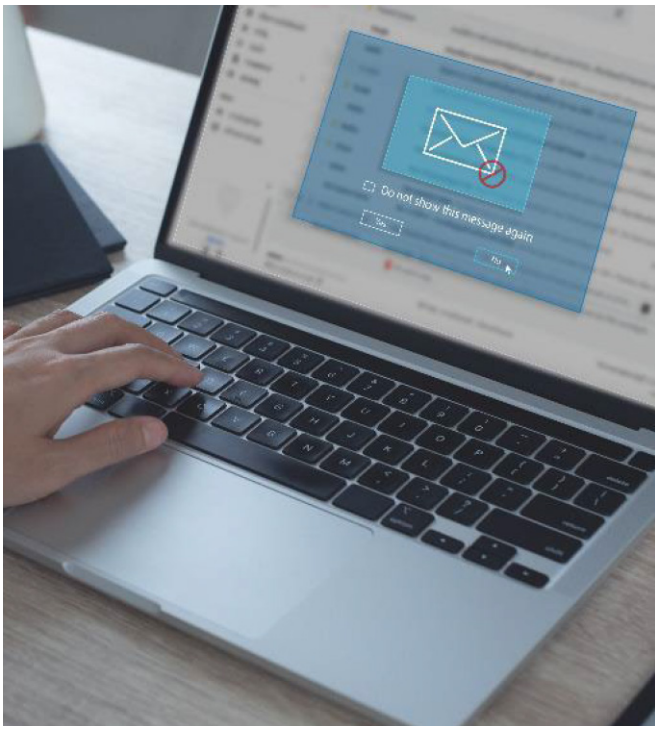


02 Las compañías de ciencias de la vida muestran una gran confianza en sus defensas contra el fraude, a pesar de tener los mayores cargos por fraude que cualquier sector

Las compañías de ciencias de la vida sufrieron las mayores pérdidas por fraude que cualquier industria en nuestra encuesta en los últimos 12 meses, alcanzando 0.54% de las ganancias durante ese periodo. La proporción afectada por al menos un caso de fraude (76%) también fue más alta que el promedio de la encuesta (71%). De cara al futuro, 76% del liderazgo de ciencias de la vida prevé un aumento del riesgo de intento de fraude por parte de actores externos a la empresa (72%).

Una vez más, hay signos preocupantes de exceso de confianza. Estos encuestados son los más propensos a informar que las políticas antifraude (85%) y la prevención del fraude (79%) en sus negocios son algo o extremadamente efectivas, pero solo 40% de la Alta Dirección espera aumentar el gasto en medidas antifraude en el próximo año. Esta es la cifra más baja para cualquier sector y muy por debajo del promedio, de 53%. Esto puede reflejar un exceso de confianza: en el último año, 23% de las empresas de ciencias de la vida se enteraron de un caso de fraude, incumplimiento o violación cibernética gracias a un regulador gubernamental o un informe policial, también la cifra más alta de la investigación. En todas las demás organizaciones, el promedio fue 15%.

03 Los ataques cibernéticos, en particular el *ransomware* y el robo de propiedad intelectual son los desafíos de fraude dominantes en el sector de ciencias de la vida



Tal vez, como era de esperarse para un campo tan basado en el conocimiento, los encuestados del sector fueron los más propensos a haber experimentado recientemente un robo de propiedad intelectual o espionaje industrial. Una cuarta parte de las empresas de esta industria sufrió un ataque de este tipo el año pasado, en comparación con solo 9% de las organizaciones en general. Durante el mismo periodo, el fraude cometido a través de los canales cibernéticos fue común, observado en 27% de las empresas de ciencias de la vida.

El sector también fue un objetivo particular para el *ransomware*: un tercio de las compañías de ciencias de la vida dicen que los intentos de defraudarlas de esta manera aumentaron durante el año pasado. Esta es también la cifra más alta para cualquier sector, sustancialmente por encima del promedio general de 20%.

Aquí, también, el exceso de confianza puede ser un problema. Muchos más encuestados de ciencias de la vida (84%) creen que sus empresas son algo o muy buenas en la prevención de ataques de *ransomware*, que en cualquier otro sector (el promedio general es 65%).

04 Los principales tipos de perpetradores que han afectado a compañías de ciencias de la vida reflejan los tipos dominantes de fraude que enfrenta la industria

Quienes cometen fraude contra este sector se diferencian de la norma por aspectos importantes. Se sabe que los empleados que trabajan con vendedores, proveedores y empresas asociadas participaron en dicha actividad en 43% de las compañías del sector en el último año, el nivel más alto que cualquier industria. De manera similar, 40% sufrió a manos del crimen organizado y los piratas informáticos (*hackers*), también el número sectorial más grande y muy superior al promedio general de la encuesta, de 26%.

Este tipo de delitos reflejan las luchas del sector para proporcionar vacunas que salvan vidas y, eventualmente, medicamentos para controlar el COVID-19. Las compañías de ciencias de la vida suelen tener cadenas de suministro globales. La necesidad de adquirir materiales en medio de la interrupción inducida por la pandemia y, a menudo, de encontrar acuerdos alternativos de logística y almacenamiento, han hecho que sea más difícil seguir los controles más estrictos sobre la incorporación de proveedores externos y otros socios. Es una prioridad encontrar mejores formas de abordar estos riesgos en medio de una interrupción continua y potencialmente a largo plazo de la cadena de suministro.

05 La seguridad cibernética es otra área para esta industria donde coexisten un riesgo extenso y un exceso de confianza

Los encuestados de ciencias de la vida fueron los más propensos de todos los sectores a informar un aumento de *phishing* en el último año (53% en comparación con 40% en general), estafas (44% vs. 25%) y, como se discutió anteriormente, ataques de *ransomware* (33% vs. 20%). Por lo tanto, no sorprende que el liderazgo de esta industria tenga una creencia casi universal de que el riesgo cibernético seguirá aumentando el próximo año (92%).

La incapacidad de muchos sistemas de Tecnologías de la Información (TI) para responder a estos peligros genera preocupación. Solo 21% de los encuestados del sector de ciencias de la vida afirman que sus organizaciones pueden identificar un ataque cibernético en el lapso de una semana o menos desde que comienza, y únicamente 8% cree poder contener uno dentro de una semana a partir de que se descubre. En la última métrica, es el más lento de todos los sectores. Más preocupante aún es la actitud del liderazgo de ciencias de la vida ante estas respuestas: 91% tiene cierta o mucha confianza en la rapidez con que sus compañías pueden reconocer los ataques y 81% en la agilidad con la que responden.

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 cuestionarnos las suposiciones que teníamos sobre cómo la gente vive y trabaja. 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 antes no habían sido investigados, lo que podría generar nuevos riesgos de fraude. En cuanto al cumplimiento, el impulso por lograr la meta *net zero* crea 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, ya en aumento durante la pandemia, están permitiendo a los actores de dichas amenazas perseguir una gama de objetivos.

En resumen, si su compañía no ha realizado recientemente una revisión completa de sus riesgos de fraude, cumplimiento y ciberseguridad, debe hacerlo lo antes posible. De lo contrario, sus defensas no estarán diseñadas para combatir las amenazas actuales, ni podrán reaccionar a medida que los riesgos evolucionen rápidamente.

En términos más generales, muchos negocios del sector de ciencias de la vida deben reenfocarse en la triple amenaza. El exceso de confianza es un problema generalizado. Para citar un ejemplo evidente, la Alta Dirección del sector evalúa muy bien la calidad de las defensas de sus empresas contra los ataques de *ransomware*, pero parte de este aparente éxito puede deberse simplemente a que algunos ciberdelincuentes evitan el sector salud. Por lo tanto, los sistemas de seguridad de la industria pueden ser no tan buenos, sino que no han sido probados.

Para aquellos que estén listos para lidiar seriamente con el nuevo entorno de la triple amenaza, el marco básico de prevención, detección y respuesta sigue siendo la base más sólida para abordar el fraude, el incumplimiento y los ataques cibernéticos. Sin embargo, el ambiente en el que se implementan estas defensas exige que deban conservarse 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 explotables. Otros se espera que tomen 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 compañías deben equilibrar la necesidad estratégica con el imperativo de evitar ser víctima de fraude y mantenerse en el lado correcto de la regulación.

Detección

Consideramos que herramientas como el análisis de datos, las auditorías internas y los protocolos para la detección de delitos cibernéticos seguirán siendo fundamentales, pero los malos 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 fraudes. Las medidas que las organizaciones deben tomar incluyen capacitación actualizada sobre los riesgos de fraude e incumplimiento, así como sobre la importancia de reportar 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 que 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

Fausto Ávila
Socio de Auditoría especialista en el Sector Salud para KPMG en México y Centroamérica

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