KPMG

¿Está su organización preparada para la triple amenaza?

Fraude, brechas de cumplimiento y ciberataques en las Américas

Por **Ana López Espinar,**
Socia líder de Forensic Services de KPMG
en Argentina y Co-líder en América del Sur

Forensic

Febrero de 2022

La encuesta de fraude 2022 elaborada por KPMG: "Una triple amenaza en las Américas", muestra el fuerte impacto de los riesgos de fraude, incumplimiento y ciberataques en la región, la erosión que han generado en las ganancias de las compañías, y la evolución preocupante que tendrán en el futuro. Además, el acceso más abierto a los sistemas, forzado por el trabajo remoto, dificulta la prevención, el monitoreo y el control.

¿Qué pueden hacer las organizaciones frente a este escenario, y cuáles son los desafíos adicionales que imponen, que pueden incluir desde la mayor presión regulatoria local e internacional hasta los criterios de sustentabilidad de ESG?

Según la referida encuesta recientemente publicada por KPMG, 83% de las compañías de las Américas sufrió al menos un ciberataque en los últimos 12 meses, un 71% fue víctima de fraude y más de la mitad pagó multas por cuestiones regulatorias o tuvo una pérdida económica a raíz de riesgos de incumplimiento no mitigados. El efecto combinado de los casos de fraude e incumplimiento costó a las compañías un 1% de sus ganancias netas, según reportaron los encuestados. Y el 58% indicó haber sufrido una pérdida económica directa como consecuencia de un ciberataque.

De la encuesta surgen, además, otras conclusiones de relevancia. Por ejemplo, que en América Latina los fraudes internos (cometidos por colaboradores) son mucho más frecuentes que en Norteamérica, donde el fraude externo (realizado por clientes, proveedores u otros terceros) prima; que los defraudadores buscan primordialmente atacar los objetivos más jugosos, evidenciando que las pérdidas por fraude e incumplimiento en compañías grandes son mayores que en las de menor tamaño; y que el 77% de los entrevistados considera que el riesgo de ciberseguridad aumentará en los próximos 12 meses.

A la tensión que genera esta instantánea se le agregan factores externos que conllevan desafíos adicionales, tales como:

- **Elevados niveles de corrupción en los países de la región**, tal como indica el Índice de Percepción de la Corrupción (IPC) 2021 que divulgó en estos días Transparencia Internacional ("TI"). Según Delia Ferreira Rubio, presidenta de TI, "Los países de América están totalmente estancados en la lucha contra la corrupción.[1]

- **Mayor aplicación de la FCPA** (ley anticorrupción de EEUU) que podría impactar en países de Latinoamérica. Anunciada en junio de 2021 por el presidente Biden[2] y reforzada posteriormente en diciembre de 2021, al definir el marco estratégico para combatir la corrupción[3] , del cual se desprenden: (1) la importancia de la lucha contra el lavado de activos como medio para reducir la corrupción; (2) una mayor responsabilidad individual por las conductas corruptas; (3) la necesidad de hacer foco en el lado de la demanda del soborno; y (4) un compromiso con la cooperación internacional.[4] En línea con esto, el anuncio del Departamento de Justicia de EEUU[5] indicando que revisará en mayor profundidad las acciones indebidas pasadas de las compañías, requerirá información más detallada a los individuos vinculados a los hechos bajo revisión y permitirá un uso más amplio del *monitorship*.[6]

- Expectativa por los **requerimientos adicionales de la SEC vinculados a la provisión de información de gestión de riesgos de ciberseguridad.** En este sentido, la SEC ha indicado como áreas de relevancia las tendientes a reforzar la "higiene cibernética" de las compañías registradas (prácticas para mantener la seguridad de los dispositivos, redes e información) y mejorar el plazo y contenido de las notificaciones sobre ciberataques ocurridos y su información a clientes, inversores y la misma SEC.[7]

- **Requerimientos multidimensionales vinculados a ESG** (environment, social & governance), que establecen para las compañías criterios de sustentabilidad en áreas tan diversas como el manejo de la ciberseguridad como condición para obtener financiamiento o emitir obligaciones negociables, la gestión del riesgo de terceros, la realización de investigaciones de brechas regulatorias (por ejemplo, en energía), el due diligence ambiental o la necesidad de contar con una línea ética para cuestiones no éticas.

1 https://www.transparency.org/es/press/2021-corruption-perceptions-index-americas-regional

2 Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest | The White House

3 https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf

4 https://www.corporatecomplianceinsights.com/biden-administration-attack-corruption/

5 https://www.corporatecomplianceinsights.com/doj-enforcement-2022-monaco-memo-anti-corruption/

6 Definido de manera amplia tanto por el DOJ como la SEC como "un tercero independiente que evalúa y monitorea la adherencia de la compañía a requerimientos de cumplimiento de un acuerdo que fue diseñado para reducir el riesgo de ocurrencia de comportamientos indebidos por parte de la compañía".

7 SEC.gov | Cybersecurity and Securities Laws

Estos elementos generan una tormenta perfecta para las compañías que enfrentan altos niveles de fraude, brechas de incumplimiento y ciberataques, a la vez que mayores demandas, debiendo decidir qué priorizar con recursos muchas veces limitados o escasos.

Será imposible para las compañías responder adecuadamente a estos flagelos si no efectúan primeramente una evaluación en dos dimensiones. En primer lugar, de los riesgos más sensibles que atentan contra el negocio (de fraude, de cumplimiento y de ciberseguridad), medidos en cuanto a su probabilidad de ocurrencia e impacto, y considerando su nivel de riesgo inherente, efectividad de los controles asociados y nivel de riesgo residual. Y así contar con un mapa de calor de los riesgos más críticos para el negocio, para las tres categorías.

Y, en segundo lugar, de los recursos con que cuenta la organización para hacerles frente, en términos de personal -incluyendo la existencia de un responsable de la gestión de estos riesgos y el posicionamiento de esta función en la organización-, sistemas, normas, procedimientos, protocolos, estilo de liderazgo de la alta dirección, comunicación y capacitación, entre otros. Y así definir su suficiencia y potencial efectividad, identificando oportunidades de mejora.

Luego, identificando qué sets de información existentes en las bases de datos / sistemas de la compañía se vinculan con el comportamiento de los riesgos definidos como sensibles, y estableciendo qué patrones indicarían potenciales irregularidades. Después, estableciendo rutinas de monitoreo y detección temprana que alerten sobre posibles desvíos en su comportamiento, y contando con protocolos de respuesta efectivos. De forma que, ante situaciones de alerta, la compañía sepa cómo responder, y tenga la información necesaria para investigar que podría haber sucedido o estar sucediendo, y así poder informar -de ser necesario- a la Justicia, reguladores, inversores y/u otros terceros relevantes qué, cómo y desde cuándo ocurrió, quiénes están involucrados y el costo implicado.

Entre la información que podría requerirse se encuentra: información de archivos maestros y transaccionales, correos electrónicos que se encuentren en servidores de la compañía, o computadoras, celulares u otros dispositivos asignados por la organización a las personas bajo análisis, y logs de distintos sistemas que deberán conservarse por períodos extensos de forma que permitan reconstruir lo sucedido, por ejemplo, en caso de un ciberataque.

Esta información debe ser obtenida y procesada aplicando procedimientos de tecnología forense, a fin de conservar la cadena de custodia, que permita poder utilizarla como evidencia válida. Por ese motivo, se recomienda la intervención de especialistas, el uso de herramientas forenses que garanticen la integridad de la información adquirida, y la participación de un escribano en el proceso, que dé fe que la información obtenida no fue alterada.

Será entonces importante que como parte del Código de Conducta de la compañía que deba ser firmado idealmente en forma anual por los empleados luego de una capacitación sobre el mismo, se incluya la aseveración de que los recursos informáticos son propiedad de la entidad y, por tanto, podrán ser monitoreados.

También, tener activas funcionalidades que permitan preservar la información almacenada electrónicamente impidiendo que la misma pueda perderse. Fundamental en procesos judiciales o de investigación interna.

En América Latina, sólo 20% de los encuestados por KPMG indicó que su empresa cumple con mejores prácticas de la industria para mitigar los riesgos de ciberseguridad, 11% en lo referente a controles de fraude, y 9 % en cuanto a cumplimiento. Mientras, estos riesgos están en aumento… ¿Está preparada su organización para hacerles frente?

Contacto

Ana López Espinar
Socia líder de Forensic Services de KPMG
en Argentina y Co-líder en América del Sur
T: +54 911 3580-5074
E: ablopez@kpmg.com.ar

kpmg.com/socialmedia

Disponible en App Store

DISPONIBLEE N Google Play