KPMG

Sua empresa está preparada para a tripla ameaça?

Fraudes, violações de compliance e ataques cibernéticos nas Américas

Por **Ana López Espinar,**
Sócia-líder de Forensic Services da KPMG
na Argentina e Colíder na América do Sul

Forensic

Febrero de 2022

A pesquisa de fraudes de 2022 elaborada pela KPMG intitulada: "Uma tripla ameaça nas Américas", mostra o forte impacto dos riscos de fraude, não conformidades e ataques cibernéticos na região, a erosão que eles geraram nos lucros das empresas e a evolução preocupante que terão no futuro. Além disso, um acesso mais aberto aos sistemas, forçado pelo trabalho remoto, dificulta a prevenção, o monitoramento e o controle.

O que as organizações podem faze nesse cenário e quais são os desafios adicionais que ele impõe, que pode incluir o aumento da pressão regulatória local e internacional no que tange aos critérios de sustentabilidade de ESG?

De acordo com a já mencionada pesquisa publicada recentemente pela KPMG, 83% das empresas nas Américas sofreram pelo menos um ataque cibernético nos últimos 12 meses, 71% foram vítimas de fraudes e mais da metade pagou multas por questões regulatórias ou sofreu um prejuízo econômico em função de riscos de descumprimento não mitigados. O efeito combinado de casos de fraude e não conformidade custa às empresas 1% dos seus lucros líquidos, relataram os entrevistados. Além disso, 58% indicaram ter sofrido uma perda econômica direta como resultado de um ataque cibernético.

Outras conclusões relevantes também surgem da pesquisa. Por exemplo, que na América Latina as fraudes internas (cometidas por funcionários) são muito mais frequentes do que na América do Norte, onde as fraudes externas prevalecem (realizadas por clientes, fornecedores ou outros terceiros); que os fraudadores buscam principalmente atacar os alvos mais robustos, mostrando que as perdas por fraudes e descumprimentos nas grandes empresas são maiores do que nas menores; e que 77% dos entrevistados consideram que o risco de segurança cibernética aumentará nos próximos 12 meses.

À tensão gerada por este cenário somam-se fatores externos que trazem desafios adicionais, tais como:

- **Altos níveis de corrupção nos países da região**, conforme apontado pelo Índice de Percepção da Corrupção 2021 (IPC) divulgado recentemente pela Transparência Internacional ("TI"). Segundo Delia Ferreira Rubio, Presidente da TI, "Os países da América Latina estão completamente travados no combate à corrupção.[1]

- **Aumento da aplicação da FCPA** (Lei Anticorrupção dos EUA) que pode afetar os países da América Latina. Anunciada em junho de 2021 pelo presidente Biden[2] e posteriormente reforçada em dezembro de 2021, ao definir o marco estratégico de combate à corrupção[3], do qual surgem: (1) a importância do combate à lavagem de dinheiro como meio da redução da corrupção; (2) uma maior responsabilidade individual pelas condutas corruptas; (3) a necessidade de focar o lado da demanda do suborno; e (4) um compromisso com a cooperação internacional.[4] Em consonância com isso, o anúncio do Departamento de Justiça dos EUA[5], indicando que analisará as ações indevidas passadas das empresas com maior profundidade, exigirá informações mais detalhadas das pessoas ligadas aos fatos sob análise e permitirá um uso mais amplo do *monitorship*.[6]

- Expectativa sobre os **requisitos adicionais da SEC relacionados ao fornecimento de informações de gerenciamento de risco de segurança cibernética.** Nesse sentido, a SEC indicou como áreas de relevância, aquelas que tendem a reforçar a "higiene cibernética" das empresas registradas (práticas para manter a segurança dos dispositivos, redes e informações) e melhorar o prazo e o conteúdo das notificações sobre ataques cibernéticos ocorridos e suas informações para clientes, investidores e a própria SEC.[7]

- **Requisitos multidimensionais vinculados a questões de ESG** (ambientais, sociais e de governança), que estabelecem critérios de sustentabilidade para empresas em áreas tão distintas como a gestão da segurança cibernética como condição para obter financiamentos ou emitir títulos negociáveis, gestão de risco de terceiros, realização de investigações de violações regulatórias (por exemplo, no setor de energia), due diligence ambiental ou a necessidade de ter uma linha direta de ética para questões antiéticas.

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 Amplamente definido tanto pelo DOJ quanto pela SEC como "um terceiro independente que avalia e monitora o cumprimento por uma empresa dos requisitos de compliance de um acordo com o que foi projetado para reduzir o risco de conduta imprópria da empresa".

7 SEC.gov | Cybersecurity and Securities Laws

Esses elementos criam uma tempestade perfeita para empresas que enfrentam altos níveis de fraudes, violações de compliance e ataques cibernéticos, além de demandas crescentes, tendo que decidir o que priorizar com recursos muitas vezes limitados ou escassos.

Será impossível para as empresas responderem adequadamente a esses flagelos se elas não fizerem primeiramente uma avaliação bidimensional. Em primeiro lugar, dos riscos mais sensíveis que ameaçam o negócio (de fraude, compliance e segurança cibernética), mensurados no que tange à sua probabilidade de ocorrência e impacto, e considerando seu nível de risco inerente, efetividade dos controles associados e nível de risco residual. E, dessa forma, ter um mapa de calor dos riscos mais críticos para o negócio, para as três categorias.

Além disso, em segundo lugar, dos recursos que a organização dispõe para enfrentar esses riscos, em termos de pessoal - incluindo a existência de um responsável pela gestão desses riscos e o posicionamento desta função na organização - sistemas, normas, procedimentos, protocolos, estilo de liderança da alta administração, comunicação e treinamento, entre outros. E assim definir sua suficiência e efetividade potencial, identificando oportunidades de melhoria.

Em seguida, identificando quais conjuntos de informações existentes nos bancos de dados/sistemas da empresa estão vinculados ao comportamento dos riscos definidos como sensíveis, e estabelecendo quais padrões indicariam irregularidades potenciais.

Posteriormente, estabelecendo rotinas de monitoramento e detecção precoce que alertem sobre possíveis desvios no seu comportamento, e contando com protocolos de resposta efetivos. Tudo isso de maneira que, em situações de alerta, a empresa saiba responder e tenha as informações necessárias para investigar o que poderia ter ocorrido ou o está acontecendo e, dessa forma, poder informar - caso necessário - a justiça, os órgãos reguladores, investidores e/ou outros terceiros relevantes sobre o que, como e desde quando aconteceu, quem está envolvido e o impacto financeiro.

As informações que podem ser necessárias incluem: informações de arquivos mestre e transacionais, e-mails que estão nos servidores da empresa, ou computadores, celulares ou outros dispositivos atribuídos pela organização às pessoas sob análise, e logs de diferentes sistemas que deverão ser mantidos por longos períodos, de forma que permitam reconstruir o que ocorreu, por exemplo, no caso de um ataque cibernético.

Essas informações devem ser obtidas e processadas mediante a aplicação de procedimentos de tecnologia forense, visando preservar a cadeia de custódia, permitindo poder utilizá-la como uma prova válida. Por isso, recomenda-se a intervenção de especialistas, o uso de ferramentas forenses que garantam a integridade das informações adquiridas e a participação de um tabelião no processo, que atesta que as informações obtidas não foram alteradas.

Portanto, será importante que, como parte do Código de Conduta da empresa, que idealmente deve ser assinado anualmente pelos funcionários após treinamento sobre ele, seja incluída a declaração de que os recursos de informática são de propriedade da entidade e, portanto, podem ser monitorados.

Além disso, contar com funcionalidades ativas que permitam preservar as informações armazenadas eletronicamente, evitando que elas sejam perdidas. Isso é fundamental em processos judiciais ou de investigações internas.

Na América Latina, apenas 20% dos entrevistados pela KPMG indicaram que sua empresa cumpre as melhores práticas para mitigar os riscos de segurança cibernética, 11% em termos de controles de fraudes e 9% em termos de compliance. Entretanto, estes riscos estão aumentando… A sua empresa está preparada para enfrentá-los?

Contato

Ana López Espinar
Sócia-líder de Forensic Services da KPMG na Argentina e Colíder na América do Sul
T: +54 911 3580-5074
E: ablopez@kpmg.com.ar

kpmg.com/socialmedia

Rua Arquiteto Olavo Redig de Campos, 105, Torre A, 6th - 12th floor - ZIP CODE: 04583-110 - São Paulo, SP / Brazil.