Aliados da produtividade e do aumento de eficiência nas EFPC, os recursos de Inteligência Artificial (IA) também devem ser avaliados do ponto de vista da gestão de riscos, pois integram o grupo de risco cibernético. Antônio Carlos Bastos d'Almeida, Gerente de Riscos, ARGR e DPO da Forluz e coordenador da Comissão Regional Leste de Governança e Riscos da Abrapp, avalia que há uma combinação de fatores na acelerada e complexa dinâmica da IA que torna a identificação, a análise, a medição, o tratamento e o monitoramento de riscos a ela inerentes tarefas desafiadoras, mas possíveis.

Por Rejane Rejo Tamoto

Aliados da produtividade e do aumento de eficiência nas EFPC, os recursos de Inteligência Artificial (IA) também devem ser avaliados do ponto de vista da gestão de riscos, pois integram o grupo de risco cibernético. Antônio Carlos Bastos d'Almeida, Gerente de Riscos, ARGR e DPO da Forluz e coordenador da Comissão Regional Leste de Governança e Riscos da Abrapp, avalia que há uma combinação de fatores na acelerada e complexa dinâmica da IA que torna a identificação, a análise, a medição, o tratamento e o monitoramento de riscos a ela inerentes tarefas desafiadoras, mas possíveis.

Ao adotar essa tecnologia, as entidades devem estabelecer processos de identificação de eventuais riscos inerentes ao desenvolvimento, produção, implantação e/ou uso de produtos, sistemas e/ou serviços que aplicam IA em suas operações. O coordenador sugere que o primeiro passo seja a realização de uma sondagem de processos organizacionais na EFPC que estejam, de fato, utilizando recursos de IA em suas execuções. Exemplos são os assistentes de voz, algoritmos de redes sociais, reconhecimento facial, aplicações para criação de textos, imagens, vídeos, áudios, aplicações de localização, sistemas conversacionais para interação com clientes (chatbots), algoritmos de organização de dados, reconhecimento de padrões e auto aprendizagem (Machine Learning) e equipamentos autônomos (veículos, drones etc).

"Uma vez que a utilização de Inteligência Artificial é constatada, é recomendável avaliar potenciais fontes de riscos", explica. Segundo ele, um risco está associado ao envolvimento das partes relacionadas, para o qual éessencial que as entidades busquem o diálogo com todos os públicos envolvidos, internos e externos, para incorporar feedback e promover conscientização sobre o uso de ferramentas de IA. "A negligência nesse envolvimento pode resultar em riscos de imagem e legais", destaca.

Outro é a necessidade de supervisão humana assegurando a conformidade, com enfoque na validação dos sistemas de IA, antes de levá-los a público, por meio de testes nas bases de dados, revisão de comandos, monitoramento de respostas e atuação com base em feedbacks para evitar respostas inconsistentes ou com vieses indesejáveis. A falta de supervisão pode acarretar em riscos operacionais, de imagem e legais.

O terceiro diz respeito à responsabilização, já que com aadoção de IA, as práticas de responsabilização podem ser alteradas, pois os processos passam a ser operados por sistemas de IA. “Os sistemas devem garantir a rastreabilidade de todas as ações e decisões tomadas, desde a concepção até a manutenção, para evitar riscos operacionais e legais.”

D’Almeida reforça também o aprendizado contínuo, já que os usuários de sistemas de IA devem ter compreensão suficiente do seu funcionamento para detectar e corrigir saídas errôneas ou com vieses indesejáveis. A negligência nesse processo pode resultar em sérios riscos operacionais, de imagem e legais.

Governança cibernética

Patrícia Linhares, sócia do escritório Linhares Advogados Associados e consultora jurídica da Abrapp, lembra que os sistemas das entidades fornecem informações estratégicas e financeiras de importância e volume, além de conter dados pessoais. “Há uma quantidade significativa de dados ligados aos participantes nos ambientes de interação das entidades com o ciberespaço e a internet. Isso acarreta em um maior risco jurídico, onde se destacam três principais preocupações”, afirma.

Primeiramente, segundo Patrícia, há o risco de ressarcimento civil para os participantes em caso de prejuízo. Em segundo lugar, existe o risco administrativo, que envolve penalidades impostas por órgãos reguladores, como a ANPD (Agência Nacional de Proteção de Dados), podendo variar de advertências a multas financeiras. Por fim, há o risco reputacional, que impacta a imagem da entidade e, consequentemente, a confiança dos indivíduos no longo prazo, podendo exigir a divulgação pública de incidentes.

“O risco cibernético já ocupa o top five do Relatório de Riscos da Abrapp. A interface das entidades na internet, incluindo sistemas web, armazenamento em nuvem e aplicativos móveis, representam pontos de vulnerabilidade significativos. Agora, a crescente adoção de inteligência artificial (IA) pelas entidades traz novos desafios. Embora a IA possa acelerar processos internos, sua arquitetura pode representar riscos”, afirma.

Patrícia destaca que quando a entidade utiliza sistemas de IA de arquitetura fechada, na qual trafegam dados da própria entidade, os riscos tendem a ser menores, pois ela está familiarizada com o histórico da organização. No entanto, ao depender de fontes externas ou gerar informações artificialmente, a IA pode produzir resultados imprecisos ou até mesmo criar realidades fictícias.

“Isso pode levar a decisões equivocadas e expor a entidade a responsabilidades legais e danos à reputação. Para mitigar esses riscos, é fundamental implementar uma governança cibernética robusta sobre as ferramentas de IA, garantindo a origem e a qualidade dos dados utilizados e limitando seu uso a ambientes controlados. A falta de governança pode aumentar os riscos de fraude e comprometer a confiança dos stakeholders”, alerta.

Ela conclui que é essencial que as entidades adotem uma abordagem proativa na gestão de riscos cibernéticos, integrando considerações de privacidade, segurança e governança cibernética em todas as etapas do processo de tomada de decisão. Além de proteger os interesses da entidade, também fortalecerá a reputação e o relacionamento com os participantes e demais partes interessadas.

Fonte: Abrapp em Foco , em 15.04.2024.