Q&A – Webinar: Fraude, Cibersegurança e Proteção de Dados – Desafios da Inteligência Artificial

1. *Existe algum estudo para criar um "algoritmo" para identificar um acesso, rastreá-lo e bloquear uma ordem ou comando recebido por IA ao menos para filtrar o que for possível?*

R: Existem iniciativas para desenvolver algoritmos capazes de monitorar acessos e filtrar comandos suspeitos, especialmente usando detecção comportamental e análise preditiva. No entanto, ainda não existe uma solução única e infalível. O caminho é combinar camadas de segurança, IA, monitoramento humano, e controles automatizados para mitigar riscos de forma mais efetiva.

2. *Como o uso de IA no mercado financeiro pode ser compatibilizado com os princípios da LGPD, especialmente no que diz respeito à transparência e à finalidade do uso de dados pessoais?*

R: Para estar alinhado à LGPD, o uso de IA deve observar a finalidade e a transparência no tratamento de dados pessoais. Isso significa informar aos titulares quais dados serão utilizados, para quais objetivos e como a IA contribui para esses fins, evitando usos incompatíveis com o propósito declarado. É essencial aplicar minimização de dados, adotar mecanismos de governança e segurança da informação, permitir que o titular exerça seus direitos e documentar decisões automatizadas.

3. *As criptomoedas facilitam as fraudes para o sistema financeiro?*

R: As criptomoedas por suas características, rapidez e irreversibilidade das transações, podem ser exploradas para a prática de fraudes no sistema financeiro, especialmente quando movimentadas por plataformas não reguladas. Contudo, o uso de mecanismos de *Know Your Client* ("KYC") ou *Anti-Money Laundering* ("AML"), monitoramento de blockchain e a cooperação entre reguladores têm se mostrado essenciais para mitigar esses riscos, permitindo que o ecossistema opere de forma mais segura e transparente.

4. *Como a IA é usada por "criminosos" para aplicar golpes financeiros, e o que nós, como investidores e profissionais, podemos fazer para nos proteger?*

R: Os fraudadores utilizam inteligência artificial para criar *deepfakes* de voz e vídeo, enviar mensagens de *phishing* personalizadas e simular canais de atendimento,

tornando golpes mais convincentes e difíceis de identificar. Para se proteger é essencial confirmar solicitações por canais oficiais, adotar autenticação em dois fatores e senhas fortes, monitorar regularmente contas e investimentos, manter-se informado sobre novas ameaças e reportar rapidamente qualquer suspeita à instituição e às autoridades.

5. *Quais são os sinais de alerta que um investidor deve observar para identificar uma tentativa de fraude sofisticada, como phishing com uso de IA ou deepfakes?*

R: Investidores devem se atentar a sinais como vídeos ou áudios com movimentos faciais suspeitos, mensagens vindas de canais não oficiais, links ou domínios duvidosos, promessas de ganhos elevados e sem risco, pressão para agir rapidamente e solicitações de dados sensíveis. Sempre confirme a informação por outro canal confiável e desconfie de conteúdos alarmantes ou fora de contexto.

6. *Os sistemas das corretoras passam por algum "pentest" para saber se os "HBs" estão seguros?*

R: As corretoras realizam testes de intrusão ("*pentests*") e auditorias de segurança periódicas para avaliar vulnerabilidades e reforçar a proteção de seus sistemas. Esses testes simulam ataques reais para verificar a robustez das defesas, garantindo conformidade com exigências regulatórias e mitigando riscos de acesso não autorizado ou comprometimento de dados sensíveis dos investidores.

7. *A IA de alguma forma poderia ter sido usada para prevenir ou mitigar o problema ocorrido recentemente na invasão das contas no Bacen aparentemente por conta de falha humana?*

R: A inteligência artificial pode contribuir para prevenir ou mitigar incidentes por meio de sistemas de detecção de anomalias, autenticação adaptativa e monitoramento comportamental em tempo real. Algoritmos de IA são capazes de identificar padrões atípicos de acesso ou transações incompatíveis com o perfil do usuário, acionar verificações adicionais e bloquear atividades suspeitas antes de sua conclusão. Além disso, modelos preditivos poderiam reforçar o treinamento de segurança dos colaboradores, reduzindo a probabilidade de erros humanos que expõem vulnerabilidades críticas.

8. *Existe hoje no mercado um excesso de fornecimento de "trades de sucesso" usando soluções de IA. Quais os riscos para os investidores no uso indiscriminado dessas soluções?*

R: O uso indiscriminado de soluções de IA que prometem “trades de sucesso” expõe investidores a riscos como decisões baseadas em dados possivelmente enviesados, ausência de transparência nos critérios de operação e dependência excessiva de algoritmos sem validação adequada. Mesmo algoritmos sofisticados não conseguem prever com precisão todos os movimentos do mercado. A bolsa de valores é influenciada por múltiplos fatores econômicos, políticos e psicológicos, que não podem ser totalmente modelados por IA. Portanto, promessas de retorno garantido são sempre suspeitas.

9. *Existe alguma recomendação prática para organizações que estão começando a estruturar suas políticas internas de prevenção a fraudes digitais?*

R: A prevenção a fraudes digitais começa com mapeamento de riscos, identificação de vulnerabilidades, canais expostos e perfil de clientes. É essencial definir políticas e procedimentos formais, treinar continuamente as equipes e adotar múltiplas camadas de segurança, como monitoramento transacional comportamental, autenticação multifator e testes de intrusão. Planos de contingência atualizados e atuação integrada entre segurança da informação, tecnologia, compliance e atendimento garantem resposta rápida e eficaz.

10. *Considerando a velocidade das ameaças, quais os maiores desafios técnicos para manter os modelos de IA de segurança atualizados e eficazes contra-ataques sofisticados impulsionados por “IA maliciosa”?*

R: O principal desafio técnico é acompanhar a velocidade com que ameaças impulsionadas por IA maliciosa evoluem. Isso exige atualização contínua dos modelos, proteção contra dados enviesados ou corrompidos, e equilíbrio entre automação e supervisão humana para evitar falhas. Sem essa adaptação constante, a IA defensiva rapidamente se torna obsoleta frente a ataques sofisticados.

11. *De que forma a inteligência artificial pode apoiar os participantes do mercado na adequação à LGPD e demais regramentos de proteção de dados, considerando os desafios de conformidade regulatória?*

R: A inteligência artificial pode automatizar a identificação e classificação de dados pessoais, monitorar acessos e atividades em tempo real, detectar incidentes, gerenciar consentimentos e gerar relatórios exigidos por reguladores. Essas

funções, aliadas a políticas internas e treinamentos, fortalecem a governança e facilitam a conformidade com a LGPD e outras normas de proteção de dados.

12. *Os "hackers" podem tentar obter senhas? Até que ponto o sistema é 100% confiável?*

R: Nenhum sistema é 100% confiável, pois agentes mal-intencionados podem tentar obter senhas ou credenciais por meio de ataques direcionados, engenharia social ou exploração de vulnerabilidades. Apesar disso, instituições financeiras aplicam protocolos robustos de criptografia, autenticação multifator e monitoramento constante para dificultar o acesso não autorizado e reduzir o risco de comprometimento. A segurança depende não apenas da tecnologia, mas também de práticas adequadas por parte dos usuários.

13. *Recentemente tomamos conhecimento sobre uma invasão nos dados do cadastro do PIX, incluindo nome, CPF etc. Não houve nenhum tipo de penalidade. Como fica a LGPD nesse contexto?*

R: A LGPD prevê que incidentes de segurança envolvendo dados pessoais devem ser comunicados à ANPD e aos titulares afetados, adotando-se medidas para mitigar eventuais danos. A ausência de penalidade imediata pode estar relacionada à fase de apuração ou ao entendimento da autoridade quanto à responsabilidade do agente de tratamento. No entanto, a lei estabelece que, comprovada a falha na proteção ou o descumprimento das obrigações, podem ser aplicadas sanções que vão de advertências a multas e restrições ao tratamento de dados.

14. *A troca de senha numérica pela senha via impressão digital garante 100% de segurança?*

R: A autenticação por impressão digital aumenta a segurança, mas não garante proteção absoluta. Biometria pode ser falsificada, capturada por *malware* ou comprometida em vazamentos de dados biométricos. Por isso, recomenda-se combiná-la com outros fatores de autenticação, como senhas fortes ou *tokens*, adotando a lógica de autenticação multifator ("MFA") para reduzir riscos de acesso indevido.

15. *Quais são os principais desafios de implementar IA em soluções de cibersegurança em corretoras de investimentos, considerando a proteção de dados sensíveis de clientes e a prevenção de fraudes?*

R: Os principais desafios incluem garantir dados de qualidade para treinar os modelos, proteger informações sensíveis, integrar a IA com segurança aos sistemas existentes, manter os algoritmos atualizados frente a novas ameaças e assegurar conformidade com a LGPD, equilibrando automação e supervisão humana.

16. *Quais as melhores práticas para mitigar ataques de força bruta?*

R: As principais práticas incluem implementar autenticação em dois fatores, exigir senhas fortes e únicas, limitar tentativas de *login* com bloqueio temporário ou *captcha*, monitorar e registrar tentativas de acesso suspeitas e utilizar ferramentas de detecção e bloqueio automático de endereços IP maliciosos.

17. *O face ID é seguro?*

R: O *face ID* é considerado seguro pois utiliza sensores avançados, criptografia robusta e processamento local. Muitos bancos e corretoras já adotam essa tecnologia em seus aplicativos para oferecer autenticidade e agilidade ao usuário. Ainda assim, nenhum método é totalmente infalível e existem casos em que imitações sofisticadas ou vulnerabilidades físicas podem comprometer sua eficácia. Por esse motivo é recomendável combiná-lo com outras camadas de segurança como senhas, *tokens* ou autenticação multifator para garantir uma proteção mais robusta.

18. *Com essa IA avançada, a assinatura por reconhecimento facial hoje em dia é um risco? Os bancos podem deixar de utilizar o meio facial?*

R: A assinatura por reconhecimento facial é considerada uma tecnologia segura pois utiliza algoritmos avançados, criptografia e validação em tempo real. No entanto, a evolução da inteligência artificial também amplia o potencial de ataques sofisticados, como *deepfakes* capazes de imitar rostos com alto grau de precisão. Esse cenário exige que bancos e demais instituições financeiras reforcem os mecanismos de verificação com camadas adicionais de segurança. A tendência não é abandonar o uso do meio facial e sim aprimorá-lo para manter a confiabilidade do processo.

19. *Como identificar se a instituição possui preocupações relacionadas à segurança da informação e de dados?*

R: As instituições devem publicar suas políticas de segurança e privacidade, manter certificações reconhecidas como ISO 27001 e aderir a padrões regulatórios do Banco Central, CVM e LGPD. Outro ponto importante é a postura diante de incidentes, comunicando rapidamente, oferecendo canais seguros de atendimento e demonstrando que existe um time dedicado à segurança da informação.

20. *Apenas treinamentos on-line são suficientes para mitigar as fraudes provenientes de engenharia social?*

R: Treinamentos on-line são importantes, mas sozinhos não bastam para mitigar fraudes de engenharia social. É essencial complementar com simulações práticas de ataques, campanhas recorrentes de conscientização, e reforço constante de protocolos de segurança no dia a dia. A combinação de teoria, prática e cultura organizacional forte é o que realmente reduz o risco.

21. *Com o avanço da IA, acreditam que as instituições precisarão elaborar políticas específicas sobre o tema?*

R: É fundamental que as instituições tenham políticas específicas para seu uso. Essas políticas devem tratar de governança, segurança da informação, proteção de dados conforme a LGPD, uso ético e critérios de validação das ferramentas. Isso ajuda a garantir transparência, mitigar riscos e alinhar a tecnologia às exigências regulatórias.

22. *Os "criminosos" que conhecem os procedimentos de validação de check-in podem driblar essas medidas preventivas?*

R: Fraudadores podem tentar explorar falhas nos procedimentos de validação, especialmente quando esses processos são previsíveis ou padronizados. No entanto, instituições financeiras utilizam camadas múltiplas de segurança, atualizam constantemente seus protocolos e adotam soluções dinâmicas baseadas em análise de risco para dificultar a antecipação e a fraude. A combinação de monitoramento em tempo real, autenticação multifator e inteligência artificial reduz significativamente a possibilidade de que essas medidas preventivas sejam contornadas.