1ª Conferência do Jornal PT50: "Cibersegurança no Sector Financeiro"

7 de outubro de 2025 | 8h30-12h30

INTERVENÇÃO DE ENCERRAMENTO

Minhas Senhoras e meus Senhores,

Começo por felicitar o Jornal PT50 pela organização desta conferência dedicada à Cibersegurança no Sector Financeiro, e agradecer, em nome da Associação Portuguesa de Bancos, o convite para efetuar esta intervenção de encerramento.

É um gosto poder partilhar convosco algumas reflexões sobre um tema que se tornou absolutamente central para a estabilidade do setor financeiro e para a confiança da sociedade: a cibersegurança. E que, do lado dos bancos, tem envolvido consideráveis investimentos e alocação de recursos, que permitem afirmar que o sector bancário é, reconhecidamente, um dos sectores nacionais com grau de maturidade mais elevado nos temas da Cibersegurança.

Quero também felicitar a organização pelo formato escolhido: um encontro restrito, mas qualificado, reunindo representantes dos principais bancos, o regulador, empresas tecnológicas globais como a Amazon e a Microsoft, e especialistas nesta área. Essa dimensão restrita não limita a relevância da iniciativa — pelo contrário, favorece a qualidade do debate e a franqueza na troca de experiências.

Hoje falamos de cibersegurança num contexto em que o setor financeiro vive uma transformação digital acelerada. As interações com os clientes, os pagamentos, o acesso ao crédito, os modelos de investimento, tudo está cada vez mais dependente de infraestruturas digitais. Essa digitalização traz benefícios enormes em termos de eficiência, comodidade e inovação. Mas traz também vulnerabilidades novas, complexas e globais.

E aqui chegamos a um ponto essencial: **a confiança é o maior ativo do setor financeiro.** E essa confiança depende hoje, em grande medida, da capacidade de proteger dados, sistemas e transações. Em suma, a cibersegurança tornou-se numa nova linha da frente da confiança bancária.

Lições desta manhã

As intervenções que ouvimos ao longo da manhã deixaram mensagens muito ricas. Permitam-me sintetizar três ideias que me parecem fundamentais.

Primeira ideia: a inteligência artificial é, ao mesmo tempo, oportunidade e risco.

Os oradores sublinharam o seu potencial para reforçar a defesa contra ataques, automatizar tarefas rotineiras, detetar padrões anómalos em tempo real. Mas também nos alertaram para o facto de a mesma tecnologia estar disponível para quem ataca. Os agentes maliciosos também identificaram benefícios de utilização da inteligência artificial para as suas atividades criminosas e tentam cada vez mais explorar essas possibilidades, criando mensagens fraudulentas cada vez mais sofisticadas, gerando *deepfakes* que iludem utilizadores e automatizando campanhas de *phishing* em larga escala. É o que se pode chamar a dupla face da inovação: o escudo e a espada.

Segunda ideia: incidentes e crises não são uma possibilidade remota, são uma certeza.

Incidentes e crises já não são uma hipótese distante, são uma realidade para a qual devemos estar preparados. A experiência internacional mostra-nos que, em vários setores e geografias, a ocorrência de interrupções digitais e falhas temporárias deixou claro que a questão já não é "se", mas "quando". E é precisamente por isso que a preparação, os planos de contingência, a cooperação institucional e a comunicação transparente são tão determinantes. Em momentos críticos, a serenidade e a coordenação são, muitas vezes, a diferença entre um incidente controlado e um impacto prolongado. Nesses contextos, a diferença entre o colapso e a recuperação reside, repito, na preparação, na capacidade de resposta coordenada e na comunicação transparente com clientes e autoridades.

Terceira ideia: inovação e c*ompliance* não são alternativas, são imperativos complementares.

Sem inovação, as instituições financeiras perdem competitividade. Mas sem conformidade regulatória, perdem legitimidade e expõem-se a riscos sistémicos. Conciliar estas duas exigências não é fácil.

O quadro regulatório é cada vez mais denso – com diretivas e regulamentos europeus como o NIS2 (*Network and Information Systems Directive 2*), o CRA (*Cyber Resilience Act*), o CRE

(*Critical Infrastructure Resilience Directive*) ou o DORA (*Digital Operational Resilience Act*) – e complexo – com múltiplas camadas e diversos supervisores, nos níveis europeu e nacional.

Mas as instituições financeiras têm de adotar as tecnologias de ponta para se manterem competitivas, modernizarem as operações e reforçar a segurança. O que requer um exercício de equilibrismo numa corda muito fina, que nem sempre é fácil de conseguir.

Os grandes desafios globais

Quero agora referir algumas tendências globais que reforçam a importância deste debate.

1. O tsunami regulatório.

A Europa decidiu colocar a cibersegurança no centro da sua agenda estratégica. O DORA é um marco, porque procura garantir resiliência operacional digital no setor financeiro. Mas a sua aplicação nacional exige cuidado. É crucial evitar duplicações, incoerências ou requisitos que dispersem recursos. Se a regulação se tornar um labirinto, perde-se eficácia e as instituições ficam sobrecarregadas.

Entretanto, recordo que: (i) o Regulamento DORA, está em vigor desde 17 de janeiro, mas só no passado dia 19 de setembro deu entrada, na Assembleia da República, a proposta de lei do Governo que assegurará a sua implementação no ordenamento nacional; (ii) o diploma para transposição da Diretiva NIS2, que deveria ter ocorrido até outubro do ano passado, só recentemente foi aprovado na Assembleia da República.

Sobre estes dois instrumentos regulatórios, permitam-me partilhar duas preocupações. Em relação à NIS2, a sua transposição para o enquadramento legal nacional deverá, de forma clara e inequívoca, salvaguardar a não aplicabilidade de certas disposições da diretiva às entidades já obrigadas ao Regulamento DORA – nomeadamente no que respeita a obrigações de gestão de riscos de cibersegurança, de notificação de incidentes e de supervisão e *enforcement*. E deverá evitar a duplicação de requisitos de notificação e a coexistência de metodologias diferenciadas de reporte, geradores de ineficiências e consumo de recursos das Instituições, sem acrescentar qualquer valor.

O objetivo deve ser claro: um quadro regulatório que seja completo, coerente e eficaz, focado em reforçar a segurança e não em criar burocracia adicional.

2. A inteligência artificial como fronteira da cibersegurança.

A IA já não é promessa de futuro, é realidade presente, como ficou claro. A sua integração na defesa cibernética pode permitir avanços extraordinários: deteção preditiva, resposta automatizada, triagem em segundos de volumes massivos de dados. Mas não é solução mágica, nem pode ser vista como um processo apenas tecnológico. É, de facto, um processo contínuo de adaptação, mas que também é humano e organizacional. A sua eficácia depende de equipas multidisciplinares, que articulem engenharia, ética, regulação e gestão de risco. E exige vigilância, porque os mesmos instrumentos estão acessíveis a atacantes. A grande batalha do futuro pode não ser apenas entre sistemas financeiros e criminosos humanos, mas entre algoritmos defensivos e ofensivos.

Em última análise, inovação e risco caminham juntos. Cabe às instituições financeiras, aos reguladores e às empresas de tecnologia encontrar o equilíbrio certo para garantir resiliência e confiança, transformando a inteligência artificial numa aliada para a proteção do sistema financeiro.

3. A evolução da fraude digital.

O crime acompanha sempre a inovação. O *phishing*, o *smishing* e o *spoofing* já fazem parte do nosso vocabulário e constituem importantes vetores de ataque fraudulento. Visam a obtenção de dados da vítima através de meios digitais, combinada com a usurpação de identidade de empresas, instituições ou autoridades, para manipular a vítima de forma a obter um proveito ilegítimo. Mas hoje enfrentamos também *deepfakes* de voz e vídeo, utilizados para enganar colaboradores ou clientes. Casos recentes mostram gestores a autorizar transferências depois de ouvirem o que acreditavam ser a voz de um superior hierárquico – quando era apenas uma imitação gerada por IA.

Para o combater, é necessária uma colaboração por parte de entidades com grande relevo no ecossistema digital, como as operadoras de comunicações eletrónicas e das plataformas digitais.

É necessário que os operadores nacionais de telecomunicações estejam habilitados para adotar medidas mitigadoras já implementadas noutros países, como a validação da autenticidade de chamadas telefónicas e mensagens SMS antes do encaminhamento, o bloqueio de remetentes fraudulentos e a criação de um registo de remetentes SMS para impedir usos indevidos.

Assim como, ao nível das plataformas digitais, é fundamental combater a proliferação de sites maliciosos, dotando os motores de pesquisa de instrumentos para não exibirem esses conteúdos e prevenindo que redes sociais difundam anúncios fraudulentos, que conduzam as vítimas às mãos dos atacantes.

4. A interdependência sistémica.

As redes digitais são globais, e os efeitos de um ataque já não ficam confinados a fronteiras ou setores. Um ataque a uma instituição pode propagar-se por todo o sistema financeiro, afetando pagamentos, crédito e até confiança nos mercados. E não falamos apenas de incidentes cibernéticos: recordo o apagão energético de abril passado, que deixou claro que o funcionamento do setor financeiro depende de infraestruturas críticas como energia e telecomunicações. Hoje, cibersegurança e segurança operacional são duas faces da mesma moeda.

5. A dimensão geopolítica.

Não podemos esquecer que alguns ataques são patrocinados por Estados ou grupos com objetivos políticos e estratégicos. A cibersegurança é também um campo da chamada guerra híbrida. Isso coloca a questão da autonomia estratégica: até que ponto a Europa consegue proteger os seus sistemas financeiros sem depender excessivamente de soluções tecnológicas externas? Aqui, a cibersegurança cruza-se com a soberania digital e com a própria resiliência democrática.

6. A resiliência social.

Por fim, mas não menos importante, está a literacia digital e financeira. Um sistema pode ter barreiras robustas, mas se o elo humano for frágil, a vulnerabilidade mantém-se. Muitos ataques exploram não falhas técnicas, mas falhas de atenção, confiança ou informação. A manipulação psicológica, a chamada engenharia social, continua a ser uma das armas mais eficazes dos criminosos. A resposta passa por educar e sensibilizar.

A recente campanha de sensibilização nacional para prevenção da fraude, promovida pela APB – *"Não passes cartão à fraude"* – é um bom exemplo de como se pode mobilizar a sociedade para práticas digitais mais seguras. Mas precisamos de mais: programas contínuos de literacia que envolvam escolas, empresas e comunidade em geral.

O caminho a seguir

Face a estes desafios, o que devemos fazer? Permitam-me destacar três prioridades estratégicas.

Primeira prioridade: reforçar a cooperação.

Nenhuma instituição está isolada. A cibersegurança só é eficaz quando existe partilha de informação e coordenação de respostas. Isso implica colaboração estreita entre bancos, reguladores, autoridades nacionais, mas também com empresas tecnológicas e fornecedores críticos.

Internamente, a APB dinamiza diversos grupos de trabalho dedicados à segurança física, à cibersegurança e à resiliência operacional. Destaco o papel importante do Fórum Interbancário de Segurança Online, focado na análise e partilha de experiências sobre incidentes relacionados com a banca digital, e o Grupo de Trabalho dos CISOs, que promove uma reflexão mais alargada sobre segurança de redes e da informação.

Ao nível da cooperação sectorial, o Banco de Portugal criou em 2021 o Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO), onde participam, além da APB e instituições de crédito consideradas operadores de infraestruturas críticas, a SIBS, o Centro Nacional de Cibersegurança e o Conselho Nacional de Planeamento Civil de Emergência. Neste fórum têm sido lançadas iniciativas muito relevantes, como a *Cyber Information and Intelligence Sharing Initiative* (CIISI-PT) e um novo Mecanismo de Comunicação e Cooperação Cibernética Operacional (M3CO-PT), além das discussões em torno da fraude, da burla e da engenharia social, que têm permitido desenhar ações concretas ao nível da partilha de informação, da literacia e da capacitação da sociedade.

Não obstante estas iniciativas, importa recordar algumas recomendações do sector para casos de incidentes com impacto sistémico: é fundamental que existam protocolos claros de atuação e comunicação, sob a coordenação do Banco de Portugal, que incluam contacto direto e célere com as instituições afetadas, monitorização próxima da situação operacional e definição precisa dos elementos de reporte, respeitando as exigências do DORA. A existência de um quadro claro contribuirá para que as equipas técnicas possam atuar com a serenidade necessária, na resolução dos incidentes que surjam.

Segunda prioridade: fortalecer a confiança dos cidadãos.

A segurança deve estar presente desde a conceção de cada produto digital — *security by design*. Mas isso não chega. É preciso também transparência: quando há um incidente, comunicar de forma clara e célere. A confiança não se constrói apenas com ausência de falhas; constrói-se também com a forma como se responde quando as falhas ocorrem.

Terceira prioridade: adotar uma visão estratégica e global.

A cibersegurança não é apenas uma questão técnica. É também uma questão de governação e de soberania. A capacidade de proteger o setor financeiro é um fator de credibilidade das democracias e de autonomia da Europa.

Conclusão

Minhas Senhoras e meus Senhores,

O setor financeiro português é hoje reconhecido como um dos mais maduros em matéria de cibersegurança. Mas isso não nos deve levar a complacência. Os desafios não param. Adaptam-se, reinventam-se e globalizam-se.

O que fizemos aqui hoje foi dar mais um passo nesse caminho coletivo. Partilhámos experiências, identificámos riscos e explorámos soluções. A cibersegurança não é um destino a atingir, mas um processo contínuo de adaptação. E esse processo só terá sucesso se for construído em conjunto: instituições, reguladores, tecnológicas, autoridades e cidadãos.

Permitam-me terminar com um apelo: **que possamos transformar a complexidade das ciberameaças numa oportunidade para reforçar a cooperação, para estimular a inovação responsável e, sobretudo, para consolidar a confiança no sistema financeiro.**

É essa confiança que sustenta a economia, que garante estabilidade social e que, em última análise, protege as democracias em que vivemos.

Muito obrigado.