FICRO

RELATÓRIO DE ATIVIDADES 2022

FICRO
RELATÓRIO DE ATIVIDADES 2022

ABR. 2023

BANCO DE PORTUGAL
EUROSISTEMA

Lisboa, 2023 • www.bportugal.pt

Índice

1 Editorial

A cibersegurança e a resiliência operacional das entidades que atuam no setor bancário são essenciais para assegurar a prestação de serviços financeiros e promover o bom funcionamento das funções económicas chave.

Tal revela-se ainda mais importante no contexto atual de forte transformação digital do setor financeiro, assente na crescente utilização pelas instituições financeiras de tecnologias de informação e comunicação, adoção de soluções inovadoras e tratamento de grandes volumes de dados.

A estreita cooperação e diálogo entre os diversos intervenientes no sistema financeiro é fundamental, na medida em que estes estão cada vez mais interligados entre si, enfrentam as mesmas ou semelhantes ameaças externas e têm um objetivo comum que serve o interesse público.

Foi neste contexto que o Conselho de Administração do Banco de Portugal deliberou, no final de 2020, constituir o Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO).

Neste que é o seu segundo ano de atividade, o FICRO aprofundou as bases de cooperação, partilha e proteção comum lançadas no passado, que reforçam a capacidade do sistema bancário nacional para enfrentar as ameaças e desafios no âmbito da cibersegurança e da resiliência operacional.

O relatório que agora se publica sistematiza os resultados entretanto alcançados, destacando-se a criação de um grupo de trabalho para a implementação do centro de partilha e análise de informação "CIISI-PT" e a implementação com sucesso do quadro de testes de intrusão baseados em inteligência de ameaças "TIBER-PT".

O Banco de Portugal agradece a todos os membros do FICRO e outros intervenientes que, direta ou indiretamente, têm contribuído para os trabalhos do Fórum, pelo empenho revelado e resultados alcançados, sobretudo no desafiante contexto económico e geopolítico atual.

O Banco de Portugal continua a acreditar que a atividade do FICRO contribuirá para alcançar a Visão 2025 do seu Plano Estratégico para 2021-2025, promovendo a proximidade e reforçando a confiança no sistema financeiro, e considera como uma prioridade estratégica para este período o acompanhamento da evolução e a sustentabilidade dos modelos de negócio das instituições, incluindo nas dimensões de transformação digital e resiliência operacional, nomeadamente através das atividades desenvolvidas por este Fórum.

Rui Pinto

Presidente do FICRO

2 Enquadramento

O risco operacional constitui um risco significativo para as instituições financeiras, que requer uma cobertura adequada através de fundos próprios[1], na medida em que pode originar perdas financeiras materiais que afetem a solvabilidade das instituições. Este risco resulta da probabilidade de ocorrência de perdas resultantes da inadequação ou deficiência de procedimentos, do pessoal ou dos sistemas internos ou de eventos externos, incluindo os acontecimentos com reduzida probabilidade de ocorrência, mas de grande impacto.

A necessidade de incremento da resiliência operacional implica, ainda, para além da gestão do risco operacional na ótica da exposição ao risco para efeito de requisitos de fundos próprios, o estabelecimento pelas instituições financeiras de planos de contingência e de continuidade de negócio, a fim de assegurar a sua capacidade para operarem numa base contínua e conterem perdas na eventualidade de uma perturbação grave da sua atividade de negócio[2].

No contexto atual, de crescente digitalização da economia e, em particular, do setor financeiro, as ameaças de cibersegurança e os impactos operacionais resultantes de incidentes de cibersegurança são cada vez mais frequentes, sofisticados e transversais, tornando este risco premente e de caráter sistémico[3].

Conclui-se, assim, que a resiliência operacional das instituições é essencial para a estabilidade financeira.

Para garantir a resiliência operacional das instituições financeiras e das infraestruturas do mercado financeiro (IMF), as Autoridades competentes podem atuar através de três vertentes, nomeadamente: i) regulação e supervisão (ou superintendência, no caso das IMF); ii) promoção da realização de testes de cibersegurança; e iii) partilha de informação (ou inteligência de ameaças)[4].

2.1 Atuação das Autoridades

Neste sentido, as Autoridades europeias e internacionais estão a promover a introdução de alterações profundas ao enquadramento legal e regulatório do risco operacional, nas suas diversas componentes, com destaque para: i) o pacote legislativo da Comissão Europeia sobre o

[1] Regulamento (UE) n. ° 575/2013 do Parlamento Europeu e do Conselho de 26 de junho de 2013 – prólogo n.º 52 e artigo 4.º-52

[2] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho de 26 de junho de 2013 – artigo 85.º

[3] Systemic Cyber Risk, ESRB (2017)

[4] Keeping cyber risk at bay - our individual and joint responsibility, ECRB (2020)

Financiamento Digital[5] e a nova Estratégia para a Cibersegurança da União Europeia (UE)[6]; ii) várias Orientações da Autoridade Bancária Europeia (EBA), nomeadamente as relativas à subcontratação[7], à avaliação do risco das Tecnologias da Informação e Comunicação (TIC) no âmbito do processo de revisão e avaliação pelo supervisor (SREP)[8] e ao risco associado às TIC e à segurança[9]; e iii) a revisão dos Princípios sobre gestão do Risco Operacional[10] e os novos Princípios para a Resiliência Operacional[11], do Comité de Supervisão Bancária de Basileia (BCBS).

Por outro lado, o Banco Central Europeu (BCE) publicou, em 2018, o quadro de referência *Threat Intelligence Based Ethical Red Teaming* ("TIBER-EU"[12]), o primeiro quadro europeu para a realização de testes de intrusão baseados em ameaças inteligentes, o qual teve como referência o quadro implementado nos Países Baixos. Esta metodologia está a ser implementada por vários Estados-Membros da área do euro e pelo próprio BCE na sua condição de superintendente das infraestruturas críticas de pagamentos[13]. Outras Autoridades têm adotado uma abordagem similar, como por exemplo o Reino-Unido (CBEST[14]), Singapura (AASE[15]), entre outros.

Adicionalmente, existem várias certificações e padrões de indústria aplicáveis a este tipo de testes, alguns dos quais formalmente reconhecidos pela Autoridade correspondente (por exemplo, as certificações da CREST[16]). Existe também uma prática generalizada de realizar testes de intrusão, em geral, e *Threat-Led Penetration Testing* ("TLPT"), em específico, pelas instituições, de forma adequada à sua natureza, dimensão e complexidade. Cabe notar que este requisito consta das Orientações da EBA em vigor relativas ao risco associado às TIC e à segurança e do Regulamento (EU) 2022/2554 do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro (Regulamento DORA) que integra o pacote sobre "Financiamento Digital".

Finalmente, no âmbito da cooperação e partilha de informação, existem atualmente vários órgãos e mecanismos internacionais relacionados com a cibersegurança. A nível europeu, destacam-se, a Agência Europeia para a Cibersegurança (ENISA) [17], o European Financial Institutes – Information Sharing and Analysis Centre (FISAC)[18] e, no BCE, a Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)[19], assim como a CERT-EU, composta por especialistas de TIC das

[5] Pacote «Financiamento Digital» (europa.eu)

[6] Nova Estratégia da UE para a Cibersegurança (europa.eu)

[7] Guidelines on outsourcing arrangements | European Banking Authority (europa.eu)

[8] Guidelines on ICT Risk Assessment under the SREP | European Banking Authority (europa.eu)

[9] Guidelines on ICT and security risk management | European Banking Authority (europa.eu)

[10] Revisions to the principles for the sound management of operational risk (bis.org)

[11] Principles for operational resilience (bis.org)

[12] TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu)

[13] TIBER-EU (europa.eu)

[14] CBEST Implementation guide (bankofengland.co.uk)

[15] AASE Final new 2 (abs.org.sg)

[16] CREST (crest-approved.org)

[17] Information Sharing and Analysis Centres (ISACs) – ENISA (europa.eu)

[18] European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership (europa.eu)

[19] Euro Cyber Resilience Board for pan-European Financial Infrastructures (europa.eu)

principais instituições da UE[20], e a Cyber Information and Intelligence Sharing Initiative (CIISI-EU) do ECRB[21]. Fora do âmbito europeu, merecem destaque o G7[22], e a NATO[23]. Por outro lado, também entre as instituições financeiras existem iniciativas que visam promover a partilha de informação e inteligência sobre ameaças de cibersegurança, contribuindo, assim, para uma maior resiliência coletiva de forma eficiente. Neste âmbito, a ENISA incentiva o estabelecimento de centros de partilha e análise de informação (ISAC)[24] entre instituições, e em particular entre instituições do mesmo setor, atendendo às semelhanças do cenário de ameaças que estas enfrentam. Neste âmbito, cabe destacar a criação do Financial Services Information Sharing and Analysis Center (FS-ISAC[25]) que reúne as maiores instituições do setor financeiro a nível global, e outras iniciativas mais localizadas, como por exemplo na Polónia, o Banking Cybersecurity Centre (BCC) [26].

Neste contexto, o Banco de Portugal entendeu existir a necessidade de coordenação com e entre as instituições financeiras e criou o Fórum com a Indústria para Cibersegurança e Resiliência Operacional ("FICRO" ou o "Fórum").

2.2 O Fórum

O Fórum é uma estrutura consultiva, constituída por iniciativa do Banco de Portugal no final de 2020, que visa contribuir para o reforço da resiliência de cibersegurança e operacional do sistema financeiro português, através da sensibilização das instituições financeiras nacionais para a importância da cibersegurança e da partilha das melhores práticas neste domínio.

Em concreto, o Fórum visa atingir os seguintes objetivos:

- Sensibilizar os membros dos órgãos de administração e de fiscalização das instituições participantes para a importância de atuar na prevenção de eventos operacionais e de cibersegurança, minimizando, assim, os potenciais impactos negativos e o nível de exposição a estes riscos;
- Fomentar a compreensão sobre os requisitos legais de cibersegurança e notificação de incidentes de cibersegurança;
- Aprofundar a cooperação entre o Banco de Portugal e as instituições supervisionadas, e restantes Membros do Fórum, fomentando o diálogo e a partilha de informação entre os participantes sobre cibersegurança;

[20] CERT-EU (europa.eu)

[21] CIISI-EU (europa.eu)

[22] Focus: the G7 Cyber Expert Group | Banque de France (banque-france.fr)

[23] Cyber defence (nato.int)

[24] Information Sharing and Analysis Centres (ISACs) – ENISA (europa.eu)

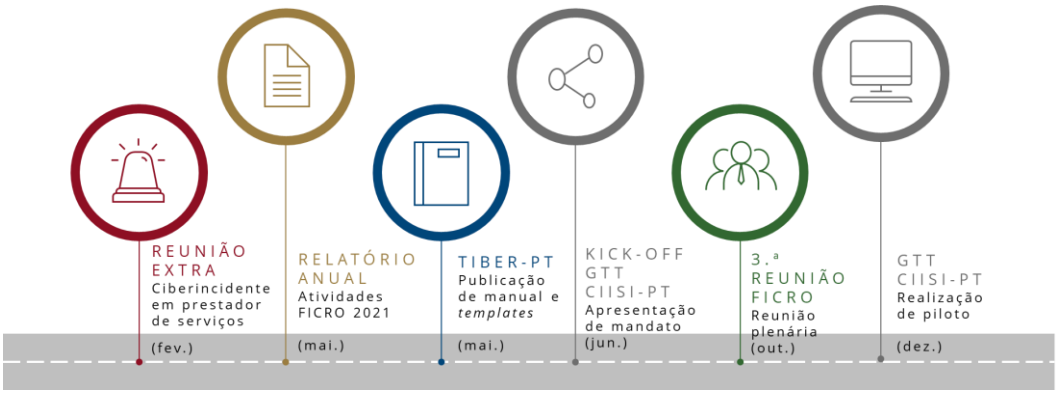
[25] Financial Services Information Sharing and Analysis Center (fsisac.com)

[26] ZBP - Cyberbezpieczeństwo banków i ich klientów

- Debater as diferentes abordagens à prevenção de incidentes de cibersegurança, nomeadamente através da implementação de metodologias de testes de cibersegurança;
- Desenvolver e coordenar a implementação de iniciativas concretas com vista à gestão destes riscos em Portugal, nomeadamente do TIBER-EU;
- Identificar as principais dificuldades encontradas pelas instituições no desenvolvimento e aplicação de novas medidas de cibersegurança.

Neste segundo ano de atividade, o Fórum teve como temas prioritários os relacionados com a resposta a incidentes de cibersegurança, a prevenção de eventuais impactos do clima de tensões geopolíticas na cibersegurança e resiliência operacional das instituições, a evolução do quadro regulatório em matéria de resiliência operacional digital (Regulamento DORA) e as duas iniciativas transversais, já iniciadas em 2021, para a implementação do TIBER-PT e do CIISI-PT.

Figura 2.1 • Plano de atividades de alto nível do FICRO



O Fórum é composto por:

- Um membro do Conselho de Administração do Banco de Portugal, que preside ao Fórum;
- Membros da Direção e equipas relevantes do Departamento de Supervisão Prudencial (DSP), Departamento de Sistemas de Pagamentos (DPG) e Departamento de Sistemas e Tecnologias de Informação (DSI) do Banco de Portugal;
- Membros do órgão de administração com os Pelouros de Sistemas de Informação, Segurança, Digitalização e/ou funções de controlo das instituições designadas como operadores de serviços essenciais do setor bancário ao abrigo da Lei n.º 46/2018, de 13 de agosto;
- Um representante da Associação Portuguesa de Bancos (APB);
- Um representante do Centro Nacional de Cibersegurança (CNCS);
- Um representante da entidade que opera, em nome do Banco de Portugal, o Sistema de Compensação Interbancária - SICOI (atualmente, a SIBS FPS).

Sob a égide do Fórum funcionam ainda dois grupos de trabalho técnicos (GTT) específicos: GTT TIBER-PT e GTT CIISI-PT. Estes GTT têm como objetivo desenvolver os respetivos projetos transversais e são compostos por elementos técnicos nomeados pelos membros do FICRO numa base voluntária.

O GTT TIBER-PT tem como mandato:

- Coordenar a implementação do *framework* TIBER-PT entre o Banco de Portugal e os representantes dos membros do FICRO nomeados para o efeito;
- Assegurar o desenvolvimento de todas as atividades necessárias à preparação do projeto de implementação, transposição e adoção do *framework* e realização do primeiro teste piloto segundo o *framework*;
- Comunicar ao FICRO as decisões relevantes a tomar e recolher a opinião dos membros deste Fórum;
- Promover, com transparência, a articulação entre todos os envolvidos no projeto de implementação que permita tirar o maior partido da experiência partilhada, reduzir custos numa lógica de partilha e minimizar os riscos inerentes à realização de exercícios desta natureza, sobretudo na fase inicial da sua implementação;
- Reunir sempre que necessário, mediante convocatória.

O GTT CIISI-PT tem como mandato:

- Coordenar a implementação da iniciativa CIISI-PT no setor bancário entre o Banco de Portugal, o CNCS e os representantes dos Membros do FICRO nomeados para o efeito;
- Assegurar o desenvolvimento de todas as atividades necessárias à definição, implementação e manutenção da CIISI-PT;
- Comunicar ao FICRO as decisões relevantes a tomar e recolher a opinião dos Membros deste Fórum;
- Promover, com transparência, a articulação entre todos os envolvidos no GTT que permita tirar o maior partido da experiência partilhada, reduzir custos numa lógica de partilha e minimizar os riscos inerentes à realização de exercícios desta natureza, sobretudo na fase inicial da sua implementação.

3 Atividades desenvolvidas

3.1 Temas prioritários

A realização de reuniões semestrais plenárias do Fórum sobre os temas mais relevantes para o setor, em cada momento e neste âmbito, com vista à partilha de informação entre o Banco de Portugal e os participantes é um dos principais objetivos e constitui, em si, a atividade do Fórum.

Com vista à prossecução das atividades descritas neste plano, o Fórum teve duas reuniões em 2022. A primeira reunião, de cariz extraordinário, teve lugar no dia 21 de fevereiro de 2022, e a segunda no dia 3 de outubro de 2022[27].

Relativamente aos temas mais relevantes que foram abordados, destaca-se, de forma não exaustiva:

- Risco para a cibersegurança e resiliência operacional no contexto geopolítico atual;
- Resposta a incidentes de cibersegurança em prestadores de serviços críticos;
- Impacto para o setor bancário do Regulamento (UE) 2022/2554 relativo à resiliência operacional digital do setor financeiro (Regulamento DORA);
- Obrigações em matéria de certificação de cibersegurança de acordo com o disposto no Decreto-Lei n.º 65/2021, de 30 de julho;
- Obrigações para os operadores de infraestruturas críticas nacionais e para as entidades setoriais de acordo com o Decreto-Lei n.º 20/2022, de 28 de janeiro.

3.2 Iniciativas transversais

O acompanhamento pelo Banco de Portugal de testes de intrusão baseados em ameaças inteligentes segundo o *framework* europeu TIBER-EU, a realizar por algumas instituições, terá como objetivo principal assegurar que as instituições compreendem o exercício e a sua importância, analisam a possibilidade de realizar testes desta natureza e, em articulação com o supervisor, iniciam o processo de realização de testes.

Cabe notar que este é um exercício voluntário e que cabe às instituições avaliar as suas prioridades e recursos disponíveis e decidir sobre a participação nesta atividade, bem como o calendário da sua participação, sujeito à capacidade e disponibilidade do Banco de Portugal para acompanhar os testes que as instituições se proponham a realizar. Cabe ainda notar que as instituições devem, com independência do acompanhamento dos exercícios pelo Banco de Portugal, promover a implementação de planos abrangentes de teste da resiliência das suas tecnologias de informação e comunicação, incluindo sobre as principais ameaças.

Durante este período, o GTT TIBER-PT foi responsável pela implementação do quadro nacional de referência para testes avançados, TIBER-PT[28], e pela sua operacionalização através de um primeiro teste piloto.

[27] Banco de Portugal apresentou à indústria financeira proposta de cooperação para a cibersegurança | Banco de Portugal (bportugal.pt)

[28] Banco de Portugal publica quadro de referência TIBER-PT, para realização de testes de cibersegurança avançados por bancos portugueses | Banco de Portugal (bportugal.pt)

Destaca-se a publicação dos manuais e documentos de base para a realização de testes TIBER-PT, em maio de 2022, a observação de um teste TIBER realizado por uma autoridade competente TIBER de outro país, entre o primeiro e o terceiro trimestre de 2022, e a realização de um teste piloto do TIBER-PT, iniciado no terceiro trimestre de 2022 e a concluir no primeiro trimestre de 2023.

Relativamente à CIISI-PT, o FICRO discutiu uma proposta inicial de modelo, objetivos e cronograma de atividades, tendo a primeira reunião do grupo de trabalho afeto a este tema sido realizada em 30 de junho de 2022. As funções de secretariado desta iniciativa serão asseguradas pelo Banco de Portugal, que irá estabelecer a ligação com os membros da Comunidade. No mês de dezembro foi realizado e concluído com sucesso um teste piloto com uma entidade pertencente ao Fórum, permitindo assim validar o funcionamento e testar o acesso da entidade à aplicação ISAC-BPT, a aplicação que irá permitir partilhar *intelligence* sobre cibersegurança no sector financeiro. Foram também iniciados os trabalhos para o desenvolvimento de outra plataforma, neste caso mais operacional e denominada por MISP, cujo objetivo passa por partilhar IoCs (*Indicators of Compromise*), possibilitando às entidades atuar numa fase mais precoce às ameaças reais externas ao sector financeiro.

4 Plano de atividades a desenvolver

Durante o ano de 2023, o FICRO propõe-se a realizar duas reuniões plenárias, previsivelmente no segundo e quarto trimestres do ano. Estas reuniões plenárias deverão servir para acompanhar a evolução das atividades do Fórum, os novos desenvolvimentos regulatórios, como as normas técnicas regulamentares do Regulamento DORA, e desenvolvimentos relevantes no setor bancário.

No que respeita ao GTT TIBER-PT, prevê-se a conclusão de um teste piloto, a concretização do plano de testes TIBER-PT para 2023 (integrado num plano plurianual) e a primeira revisão periódica do quadro de referência.

Relativamente ao GTT CIISI-PT, após a conclusão do piloto realizado em 2022, prevê-se o alargamento da utilização da aplicação ISAC-BPT e a implementação de uma plataforma operacional MISP (*Malware Information Sharing Platform*) para partilha de informação sobre cibersegurança. Após a operacionalização das ferramentas atrás identificadas, o Banco de Portugal atuará como secretariado da iniciativa, dinamizando a mesma ao longo do ano.

Por fim, é expectável que seja lançada uma nova atividade transversal, em cooperação com os membros do Fórum, e no contexto do trabalho desenvolvido pelo BCE (tanto na perspetiva de supervisão como de risco sistémico), que visa implementar um quadro de referência e desenvolver exercícios de análise de impactos de um cenário adverso mas plausível de perturbação da resiliência operacional das instituições, de forma a avaliar o seu nível de cumprimento com os níveis de tolerância de impacto desejáveis face às funções críticas que desempenham.

5 Anexos

Anexo • Composição do FICRO no final de 2022

Presidente: Rui Pinto (ou, na sua ausência, Hélder Rosalino), Administrador do Banco de Portugal

Entidade
Associação Portuguesa de Bancos
Banco Santander Totta
Banco BPI
Bankinter – Sucursal em Portugal
Caixa Central de Crédito Agrícola Mútuo
Caixa Económica Montepio Geral
Caixa Geral de Depósitos
Centro Nacional de Cibersegurança
Banco BIC Português
Banco Comercial Português
Novo Banco
SIBS - Forward Payment Solutions

Anexo • Organização do FICRO