FICRO

RELATÓRIO DE ATIVIDADES 2021

FICRO
RELATÓRIO DE ATIVIDADES 2021

MAR. 2022

BANCO DE PORTUGAL
EUROSISTEMA

Lisboa, 2022 • www.bportugal.pt

Índice

1 Editorial

A cibersegurança e a resiliência operacional das entidades que atuam no setor bancário são essenciais para assegurar a estabilidade financeira e o bom funcionamento da economia.

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).

No seu primeiro ano de atividade, o FICRO contribuiu para a partilha de informação relevante entre os seus membros e permitiu lançar as bases para o desenvolvimento de iniciativas estruturais, que reforçam a capacidade do sistema bancário 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 adoção do quadro de referência "TIBER-PT", um enquadramento para a realização de testes de intrusão baseados em inteligência de ameaças.

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 contexto desafiante da pandemia de COVID-19.

O Banco de Portugal acredita 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 pelo FICRO.

Ana Paula Serra

Presidente do FICRO

2 Enquadramento

O risco operacional constitui um risco significativo para as instituições financeiras, que necessita de 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 para capital, 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 erros operacionais que estes incidentes podem provocar 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 linhas de defesa, nomeadamente: regulação e supervisão (ou superintendência no caso das IMF), promoção da realização de testes de cibersegurança e partilha de informação (ou inteligência de ameaças)[4].

[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)

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 deste risco, nas suas diversas componentes, com destaque para: o pacote legislativo da Comissão Europeia para o Financiamento Digital[5] e a nova Estratégia para a Cibersegurança da UE[6]; 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 SREP[8] e ao risco associado às TIC e à segurança[9]; a proposta de 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, baseado no quadro de referência implementado nos Países Baixos. Esta metodologia foi ou 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 ou haviam já adotado antes 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 da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro que integra o pacote "Financiamento Digital".

[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)

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, na European Union Agency for Cybersecurity (ENISA), o European Financial Institutes – Information Sharing and Analysis Centre (FISAC)[17] e, no BCE, a Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)[18], assim como a CERT-EU, composta por especialistas de TIC das principais instituições da UE[19], e a Cyber Information and Intelligence Sharing Initiative (CIISI-EU) do ECRB[20]. Fora do âmbito europeu, merecem destaque o G7[21], e a NATO[22]. 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) 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[23]) 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)[24].

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;

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

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

[19] CERT-EU (europa.eu)

[20] CIISI-EU (europa.eu)

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

[22] Cyber defence (nato.int)

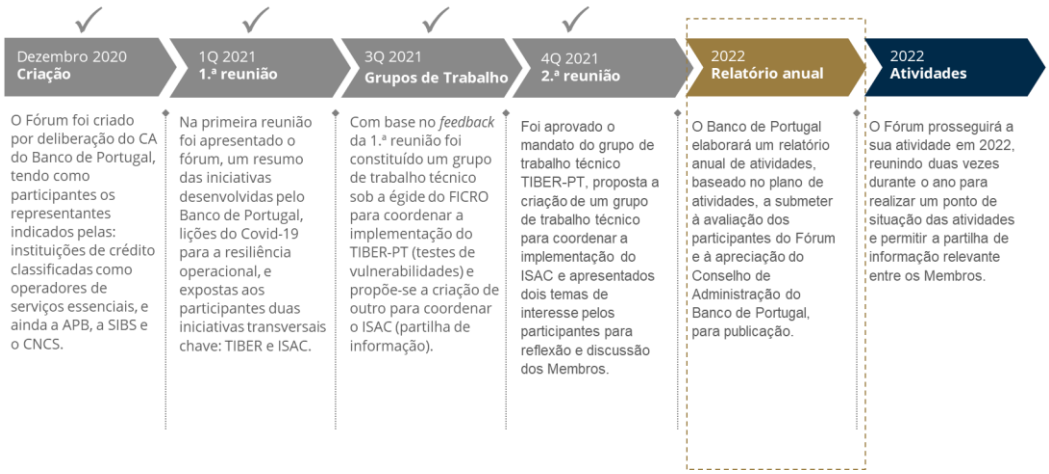
[23] Financial Services Information Sharing and Analysis Center (fsisac.com)

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

- 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, fomentando o diálogo e a partilha de informação entre os participantes sobre cibersegurança;
- 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 primeiro ano de atividade, o Fórum teve como temas prioritários os relacionados com o reporte de incidentes, segurança dos sistemas de pagamentos, risco associado à subcontratação, riscos específicos associados à pandemia de COVID-19 do ponto de vista operacional e o lançamento de duas iniciativas transversais da maior relevância: a implementação do TIBER-EU em Portugal e de um ISAC.

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 (SIBS FPS).

Sob a égide do Fórum funcionam ainda dois grupos de trabalho técnicos (GTT) específicos: GTT TIBER-PT e GTT ISAC. 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 ISAC tem como mandato:

- Definir e desenvolver uma plataforma de colaboração eficaz e fácil de usar que, reconhecidamente, sirva o propósito de partilha e consulta de informação relevante de cibersegurança;
- Mobilizar as equipas das instituições participantes, como membros ativos e interessados do ISAC;
- Promover a confiança entre todas as instituições, e entre estas e o Banco de Portugal, e a livre partilha de informações relevantes, sem reservas ou receios;
- Evoluir e incrementar os serviços disponibilizados e a qualidade dos mesmos, indo ao encontro das necessidades identificadas para o setor.

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 2021. A primeira reunião teve lugar no dia 8 de abril de 2021[25], e a segunda no dia 15 de dezembro de 2021[26].

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

- Incidentes severos e significativos – Deveres de comunicação ao abrigo da Diretiva (UE) 2015/2366 – Diretiva de Serviços de Pagamento revista (DSP2), da Diretiva (UE) 2016/1148 — Cibersegurança das redes e dos sistemas de informação (DSRI), do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF) e do Mecanismo Único de Supervisão; e iniciativas legislativas em curso;
- Subcontratação TIC – Apresentação das novas Orientações da EBA e do trabalho do Banco de Portugal;
- Gestão da Continuidade de Negócio – Apresentação das novas recomendações do CNSF sobre gestão de continuidade de negócio;
- Segurança dos sistemas de pagamentos – O programa de controlos de segurança CSP da SWIFT, e o questionário de autoavaliação do BCE/Banco de Portugal;
- Segurança dos sistemas de pagamentos II – Novo reporte de riscos operacionais e de segurança e outras obrigações da Instrução n.º 4/2021;
- Controlo interno do risco TIC – A importância das linhas de defesa e em especial da 2.ª linha de defesa correspondente à gestão de risco TIC;
- Obrigações em matéria de certificação de cibersegurança de acordo com o Decreto-Lei n.º 65/2021, de 30 de julho;
- Lições de gestão de risco de cibersegurança aprendidas no contexto da pandemia de COVID-19.

[25] Banco de Portugal reforça cooperação para a resiliência operacional do sistema financeiro | Banco de Portugal (bportugal.pt)

[26] O Banco de Portugal apresentou à indústria financeira o plano de implementação do TIBER-EU, o quadro de referência para a realização de testes de cibersegurança avançados na União Europeia | Banco de Portugal (bportugal.pt)

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, portanto, 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.

Durante este período, foi estabelecido o GTT TIBER-PT, que definiu um cronograma de atividades a realizar até ao final do primeiro semestre de 2023 (com o acordo do FICRO), e que inclui a implementação do *framework* TIBER-EU em Portugal, a sua operacionalização através de um primeiro teste piloto, e a sua revisão com base nas lições aprendidas durante esse teste piloto.

Destaca-se o início dos trabalhos da elaboração do guia de transposição do TIBER-EU, sob a sigla proposta "TIBER-PT" ainda no decorrer de 2021, incorporando o contributo dos membros do FICRO relativamente à informação que consideraram relevante e questões relevantes a dirimir neste guia. Prevê-se a publicação do guia do TIBER-PT no final do primeiro trimestre de 2022, a observação de um teste TIBER a realizar por uma autoridade competente TIBER de outro país durante o primeiro semestre de 2022, e a realização de um teste piloto do TIBER-PT no segundo trimestre de 2022 e a concluir no primeiro trimestre de 2023.

Relativamente ao ISAC do setor bancário, o FICRO discutiu uma proposta inicial de modelo, objetivos e cronograma de atividades, estando previsto o estabelecimento do grupo de trabalho afeto a este tema no primeiro trimestre de 2022. As funções de secretariado do ISAC serão asseguradas num formato de parceria entre o Banco de Portugal e o CNCS, assumindo assim o CNCS um papel idêntico ao que já tem em ISAC noutros setores. O CNCS ainda disponibilizou, no âmbito desta iniciativa, uma plataforma de partilha segura de informação, a qual é também utilizada por ISAC doutros setores.

Esta iniciativa deverá conhecer desenvolvimentos relevantes ao longo de 2022.

4 Plano de atividades a desenvolver

Durante o ano de 2022, o FICRO propõe-se a realizar dois plenários, previsivelmente no segundo e quarto trimestres do ano. Estas reuniões plenárias deverão servir para acompanhar a evolução das atividades iniciadas em 2021, os novos desenvolvimentos regulatórios, como a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro (DORA, na sigla inglesa)[27] e a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos (MiCA, na sigla inglesa)[28], e desenvolvimentos relevantes no setor bancário.

No que respeita ao GTT TIBER-PT, prevê-se a observação pelo Banco de Portugal de um teste TIBER a realizar por uma autoridade competente TIBER de outro Estado-membro da UE, a publicação da *framework* TIBER-PT no final do primeiro trimestre de 2022 e a realização de um teste piloto do TIBER-PT.

Relativamente ao GTT ISAC, prevê-se que o grupo reúna durante o primeiro trimestre de 2022, com vista à discussão e aprovação do modelo de governo para o ISAC, definição da plataforma tecnológica de suporte à partilha de informações e definição dos procedimentos de acesso à plataforma. No segundo trimestre deverá iniciar-se um piloto com um número limitado de instituições, com vista a testar a plataforma e ajustar os processos e configurações que lhe estão associadas, em conformidade.

Por fim, no terceiro trimestre é espectável que a implementação do ISAC entre na sua fase final com o convite às instituições do setor bancário para participarem do mesmo, a atribuição de acessos à plataforma e o início da partilha de informações.

[27] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (europa.eu)

[28] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937

5 Anexos

Anexo • Composição do FICRO no final de 2021

Presidente: Ana Paula Serra/Hélder Rosalino, Administradores do Banco de Portugal

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

Anexo • Organização do FICRO