

# FICRO

## RELATÓRIO DE ATIVIDADES 2023



BANCO DE  
PORTUGAL  
EUROSISTEMA



# FICRO

## RELATÓRIO DE ATIVIDADES 2023

MAI. 2024



**BANCO DE PORTUGAL**  
EUROSISTEMA

Lisboa, 2024 • [www.bportugal.pt](http://www.bportugal.pt)



# Índice

- 1** Editorial 5
- 2** Enquadramento 6
  - 2.1** Atuação das Autoridades 6
  - 2.2** O Fórum 8
- 3** Atividades desenvolvidas 10
  - 3.1** Temas prioritários 10
  - 3.2** Iniciativas transversais 11
- 4** Plano de atividades a desenvolver 12
- 5** Anexos 13



# 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, em paralelo com a 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 seu terceiro ano de atividade, o FICRO aprofundou as bases de cooperação, partilha e proteção comum, com o objetivo de reforçar 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 as atividades do último ano, destacando-se a constituição da Comunidade “CIISI-PT” para a cooperação e partilha de informação, com e entre as entidades financeiras, utilizando para o efeito a plataforma MISP, e a atualização do quadro de testes de intrusão baseados em inteligência de ameaças “TIBER-PT”, após conclusão do teste piloto. Foram ainda lançados os alicerces para a realização de um exercício setorial de avaliação da capacidade de resposta a crises no âmbito da cibersegurança e resiliência operacional (CyRST-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.

**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<sup>1</sup>, 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 dos 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<sup>2</sup>.

No contexto atual, de crescente digitalização da economia e, em particular, do setor financeiro, as ameaças de cibersegurança são cada vez mais frequentes, sofisticadas e transversais, tornando este risco premente e de caráter sistémico<sup>3</sup>.

A resiliência operacional das instituições é, assim, essencial para a estabilidade financeira.

Para garantir a resiliência operacional das instituições financeiras e das infraestruturas do mercado financeiro (IMF), as Autoridades competentes atuam em 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 sobre ameaças)<sup>4</sup>.

### 2.1 Atuação das Autoridades

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 Financiamento Digital<sup>5</sup> e a nova Estratégia para a Cibersegurança da União Europeia (UE)<sup>6</sup>; ii) várias Orientações da Autoridade Bancária Europeia (EBA), nomeadamente as relativas à

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

<sup>2</sup> Diretiva 2013/36/UE do Parlamento Europeu e do Conselho de 26 de junho de 2013 – artigo 85.º

<sup>3</sup> Systemic Cyber Risk, ESRB (2017)

<sup>4</sup> Keeping cyber risk at bay - our individual and joint responsibility, ECRB (2020)

<sup>5</sup> Pacote «Financiamento Digital» (europa.eu)

<sup>6</sup> Nova Estratégia da UE para a Cibersegurança (europa.eu)



subcontratação<sup>7</sup>, à avaliação do risco das Tecnologias da Informação e Comunicação (TIC) no âmbito do processo de revisão e avaliação pelo supervisor (SREP)<sup>8</sup> e ao risco associado às TIC e à segurança<sup>9</sup>; e iii) a revisão dos Princípios sobre gestão do Risco Operacional<sup>10</sup> e os novos Princípios para a Resiliência Operacional<sup>11</sup>, 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”<sup>12</sup>), 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<sup>13</sup>. Outras Autoridades têm adotado uma abordagem similar, como por exemplo o Reino Unido (CBEST<sup>14</sup>), Singapura (AASE<sup>15</sup>), entre outros.

A realização de exercícios TIBER com vista à deteção e reparação de vulnerabilidades de cibersegurança tem vindo a tornar-se uma exigência transversal a nível internacional, tendo Portugal sido um dos países pioneiros neste domínio. 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<sup>16</sup>). 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 agora 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)<sup>17</sup>, o *European Financial Institutes – Information Sharing and Analysis Centre* (FISAC)<sup>18</sup> e, no BCE, o *Euro Cyber Resilience Board for pan-European Financial Infrastructures* (ECRB)<sup>19</sup>, assim como a CERT-EU, composta por especialistas de TIC das principais instituições da UE<sup>20</sup>, e a *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU) do

<sup>7</sup> Guidelines on outsourcing arrangements | European Banking Authority (europa.eu)

<sup>8</sup> Guidelines on ICT Risk Assessment under the SREP | European Banking Authority (europa.eu)

<sup>9</sup> Guidelines on ICT and security risk management | European Banking Authority (europa.eu)

<sup>10</sup> Revisions to the principles for the sound management of operational risk (bis.org)

<sup>11</sup> Principles for operational resilience (bis.org)

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

<sup>13</sup> TIBER-EU (europa.eu)

<sup>14</sup> CBEST Implementation guide (bankofengland.co.uk)

<sup>15</sup> AASE Final new 2 (abs.org.sg)

<sup>16</sup> CREST (crest-approved.org)

<sup>17</sup> Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)

<sup>18</sup> European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership (europa.eu)

<sup>19</sup> Euro Cyber Resilience Board for pan-European Financial Infrastructures (europa.eu)

<sup>20</sup> CERT-EU (europa.eu)

ECRB<sup>21</sup>. Fora do âmbito europeu, merecem destaque o G7<sup>22</sup> e a NATO<sup>23</sup>. 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)<sup>24</sup> 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<sup>25</sup>) que reúne as maiores instituições do setor financeiro a nível global e outras iniciativas mais localizadas, como por exemplo o Fórum com a Indústria para Cibersegurança e Resiliência Operacional (“FICRO” ou o “Fórum”), em Portugal, e o *Banking Cybersecurity Centre* (BCC)<sup>26</sup>, na Polónia.

## 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. 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;
- 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 terceiro ano de atividade, o Fórum teve como temas prioritários os relacionados com a resposta a incidentes de cibersegurança, eventos de burla, fraude e engenharia social, bem como

<sup>21</sup> CIISI-EU (europa.eu)

<sup>22</sup> Cyber resilience and financial market infrastructures (europa.eu)

<sup>23</sup> Cyber defence (nato.int)

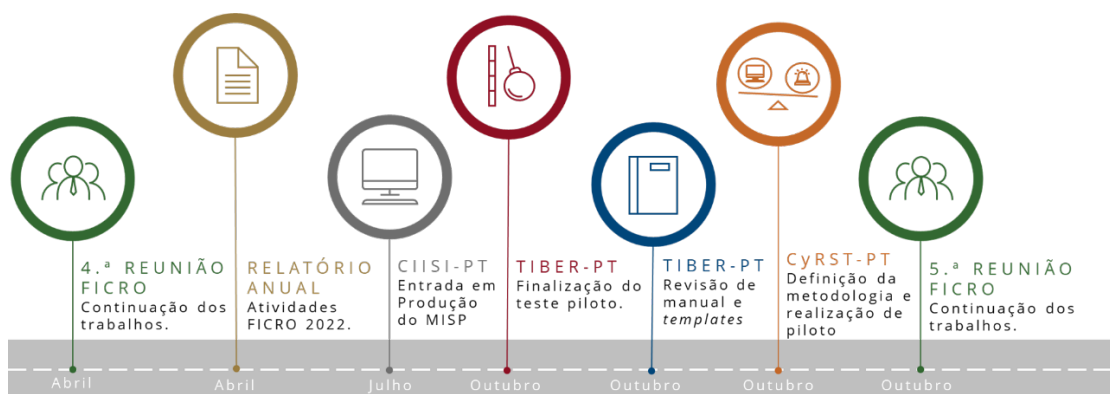
<sup>24</sup> Information Sharing and Analysis Centres (ISACs) – ENISA (europa.eu)

<sup>25</sup> Financial Services Information Sharing and Analysis Center (fsisac.com)

<sup>26</sup> ZBP - Cyberbezpieczeństwo banków i ich klientów

a evolução do quadro regulatório em matéria de resiliência operacional digital, e o desenvolvimento das iniciativas transversais TIBER-PT e CIISI-PT, com ações já implementadas e em curso, e ainda o CyRST-PT, com implementação planeada para 2024.

**Figura 2.1 • Plano de atividades de alto nível do FICRO em 2023**



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 CII-PT tem como mandato:

- Prevenir, detetar, responder e sensibilizar os membros que participam na CII-PT para as ameaças de cibersegurança, assumindo assim uma responsabilidade de interesse público;
- Permitir a partilha de informação e *intelligence* relevante e útil dentro da comunidade CII-PT e com as autoridades responsáveis, com vista a uma melhor proteção das instituições financeiras nacionais contra as ameaças de cibersegurança;
- Incentivar o contributo ativo e a participação ativa em termos de partilha de informação sobre ameaças de cibersegurança;
- Sintetizar e difundir ativamente a partilha de *intelligence* estratégica, para além de TTPs (*Tactics, Techniques and Procedures*) operacionais e de IOCs (*Indicators of Compromise*);
- Aprender e evoluir continuamente, enquanto coletivo, no que respeita ao processo de análise, desenvolvimento e partilha de informação e *intelligence* sobre cibersegurança.

## 3 Atividades desenvolvidas

### 3.1 Temas prioritários

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

Com vista à prossecução das atividades descritas neste plano, o Fórum teve duas reuniões em 2023, realizadas a 28 de abril de 2023 e a 13 de outubro.

Nestas reuniões foram discutidos vários temas, com destaque para os seguintes:

- Impacto de campanhas de burla, fraude e engenharia social;
- Resposta a incidentes de cibersegurança;

- Impacto para o setor bancário do Regulamento (UE) 2022/2554 relativo à resiliência operacional digital do setor financeiro (Regulamento DORA).

## 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, tem 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.

Sendo de aplicação obrigatória a partir de 2025 com a entrada em vigor do DORA, este é atualmente 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. Em todo o caso, o Banco de Portugal tem incentivado a sua realização, não só para garantir uma adequada preparação das instituições para as exigências decorrentes do DORA, mas sobretudo porque esta é uma ferramenta de elevado valor acrescentado para teste da resiliência das tecnologias de informação e comunicação, incluindo sobre as principais ameaças.

Durante este período, o GTT TIBER-PT foi responsável pela operacionalização do quadro nacional de referência para testes avançados **TIBER-PT**, implementado no ano anterior<sup>27</sup>, através de um primeiro teste piloto, concluído no último trimestre de 2023. Da experiência retirada deste exercício destaca-se a atualização dos manuais e documentos de base para a realização de testes TIBER-PT, iniciada em 2023, os quais deverão ser publicados no primeiro trimestre de 2024. Foram ainda iniciados dois testes TIBER-PT, no primeiro e segundo semestre de 2023, a concluir no segundo e terceiro trimestre de 2024, respetivamente.

Relativamente à **CIISI-PT**, foi implementada a plataforma MISP (*Malware Information Sharing Platform*) para a partilha de informação e *intelligence* sobre ameaças de cibersegurança entre os membros, alargado o teste piloto do portal de partilha de informação, realizado um primeiro teste piloto do MISP e, finalmente, realizado o *onboarding* às demais instituições que participam na iniciativa. Desde setembro de 2023 foram realizadas reuniões mensais de partilha de informação entre os membros, e a plataforma apresenta indicadores positivos de crescimento e interação.

Destaca-se ainda o início dos trabalhos de elaboração dos moldes do exercício **CyRST-PT**. Este teste de esforço de supervisão temático sobre resiliência operacional cibernética será realizado em moldes semelhantes ao desenvolvido pelo BCE. Uma vez que apenas as instituições mais significativas são abrangidas pelo exercício europeu, o Banco de Portugal irá realizar o teste a

<sup>27</sup> Banco de Portugal publica quadro de referência TIBER-PT, para realização de testes de cibersegurança avançados por bancos portugueses | Banco de Portugal (bportugal.pt)

outra amostra de instituições, com as necessárias adaptações ao calendário, ajustado à realidade local e objetivos específicos do exercício nacional. O Banco de Portugal neste período esteve envolvido na definição do teste a nível europeu, que será semelhante ao exercício nacional, a realizar no ano de 2024.

## 4 Plano de atividades a desenvolver

Durante o ano de 2024, o FICRO propõe-se realizar duas reuniões plenárias, previsivelmente no segundo e quarto trimestres do ano. Estas reuniões plenárias visarão 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 dos dois testes em curso, tal como o início de outros dois testes, dando cumprimento à concretização do plano de testes TIBER-PT para 2024 (integrado num plano plurianual), e a publicação da revisão periódica do quadro de referência. Devido à implementação do Regulamento DORA, prevê-se ainda a articulação do TIBER-PT com os novos Regulatory Technical Standards (RTS) do Regulamento DORA.

Relativamente ao GTT CIISI-PT, prevê-se a continuação da dinamização da iniciativa, com a realização de reuniões mensais, e um estudo relativo ao alargamento dos membros do grupo a instituições à data ainda não integrantes.

Prevê-se iniciar o exercício CyRST-PT no primeiro semestre, através da comunicação com as instituições abrangidas pelo exercício nacional e respetiva resposta.

Por fim, prevê-se que seja gradualmente incorporada nas prioridades e planeamento do Fórum em 2024 a preocupação com o combate à prevalência de esquemas de fraude, burla e engenharia social, prevendo-se uma partilha regular entre as instituições participantes.

# 5 Anexos

## Anexo • Composição do FICRO no final de 2023

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 Económica Montepio Geral

Caixa Geral de Depósitos

Centro Nacional de Cibersegurança

Banco BIC Português

Grupo Crédito Agrícola

Banco Comercial Português

Novo Banco

SIBS Forward Payment Solutions

---

## Anexo • Organização do FICRO

