BANCO DE PORTUGAL
EUROSISTEMA

Ciber-resiliência no setor bancário

A perspetiva do Banco de Portugal

Luís Costa Ferreira | Diretor

Departamento de Supervisão Prudencial

3 de junho de 2019

Agenda

Enquadramento

Abordagem das autoridades

Obrigações de reporte

Próximos passos

1 Enquadramento

Enquadramento

Aumento significativo de incidentes de cibersegurança no setor financeiro

25,7%

As instituições do setor financeiro concentraram mais de 25% de todos os ciberataques maliciosos em 2018

↑212%

Aumento situações de roubo de dados de cartões de crédito no primeiro trimestre de 2019

↑129%

Aumento de credenciais de clientes comprometidas em 2018

↑102%

Aumento de aplicações maliciosas, incluindo apps bancárias fraudulentas para dispositivos móveis em 2018

Fonte: IntSights, Cyber Threat Landscape Report, April 2019

Enquadramento

Ranking dos principais riscos operacionais para 2019

#01	Data compromise
#02	IT disruption
#03	IT failure
#04	Organisational change
#05	Theft and fraud
#06	Third-party risk
#07	Regulatory risk
#08	Data management
#09	Brexit
#10	Mis-selling

Os **3 principais riscos** operacionais identificados pela indústria para 2019 estão associados ao **risco cibernético.**

Fonte: https://www.risk.net/risk-management/6470126/top-10-op-risks-2019

Enquadramento

Global banking outlook 2018

90%

dos gestores de topo de 226 bancos a nível internacional considera como principal prioridade de negócio reforçar **a cibersegurança e a proteção de dados.**

Fonte: EY, https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf

Enquadramento

Risk in Focus 2019: Hot Topics for Internal Auditors, Chartered Institute of Internal Auditors

#1	**Cibersegurança**
#2	Compliance
#3	Inovação digital
#4	Alteração regulatória
#5	Incerteza política

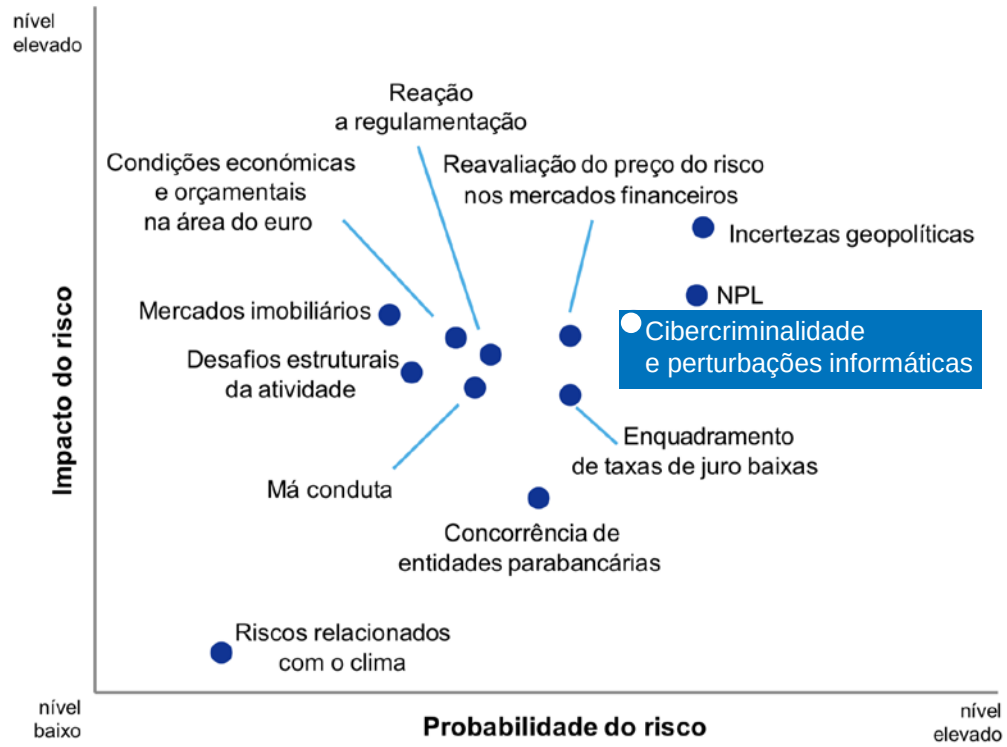
Num inquérito a mais de 300 executivos de auditoria, **a cibersegurança foi considerada como o maior risco** para suas organizações.

Fonte: www.iia.org.uk/media/1689824/risk-in-focus-2019.pdf

Enquadramento

Mapa dos riscos no âmbito do MUS em 2019

Risco de **cibercriminalidade e perturbações informáticas** entre os 3 principais riscos de supervisão do MUS



Fonte: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ra/ssm.ra2019.en.pdf

Enquadramento

Principais riscos associados a incidentes de cibersegurança

Risco financeiro

- Expropriação de fundos e/ou ativos;
- Perdas de receita futura;
- Custos com segurança dos sistemas e remediação;
- Custos judiciais e/ou de resolução;
- Taxas por incumprimento de obrigações contratuais e/ou possíveis sanções.

Risco reputacional

- Perda de confiança devido à recorrência e/ou exposição mediática dos incidentes;
- Impacto em áreas de negócio críticas para a confiança no setor;
- Degradação da imagem devido ao incumprimento de requisitos regulamentares e/ou possíveis sanções;
- Divulgação de dados sensíveis (i.e. pessoais).

Risco operacional

- Disrupção de funções críticas e/ou serviços essenciais para o público;
- Incidentes em sistemas, aplicações e redes e/ou violações de segurança da informação;
- Falhas na integração de sistemas e redes em outsourcing (incl. CSPs e FinTechs);
- Ativação de planos de continuidade de negócio e recuperação de desastre.

Risco legal

- Incumprimento de prazos regulatórios (incluindo reportes financeiros);
- Incapacidade de responder a obrigações legais com clientes/consumidores;
- Incumprimento de regulação AML/CFT;
- Perdas de confidencialidade e integridade de dados sensíveis (i.e. pessoais).
- Possibilidade de ocorrência de litígios.

Enquadramento

Principais riscos associados a incidentes de cibersegurança

Enquadramento

Exemplos recentes de incidentes no setor bancário

REUTERS

INTEL MARCH 13, 2016 / 2:07 PM / 3 YEARS AGO

Bangladesh bank says hackers tried to steal $951 million

Serajul Quadir 3 MIN READ

DHAKA (Reuters) - Bangladesh's central bank confirmed on Sunday that cyber criminals tried to withdraw $951 million from its U.S. bank account, as the country's finance minister said he first got to know of one of the biggest bank heists in history through the media.

BANGLADESH BANK
Central Bank of Bangladesh

Origem: End-points SWIFT

Impacto: $81M + reputação

Enquadramento

Exemplos recentes de incidentes no setor bancário

REUTERS

HOT STOCKS SEPTEMBER 8, 2017 / 1:42 PM / 2 YEARS AGO

Equifax shares slump after data breach likely hits 143 mln consumers

2 MIN READ

Sept 8 (Reuters) - Shares of Equifax Inc tumbled 12 percent on Friday after the provider of consumer credit scores revealed that personal details of as many as 143 million U.S. consumers were likely accessed in one of the largest data breaches in the United States.

EQUIFAX

Origem: vulnerabilidade website

Impacto: reputação

Enquadramento

Exemplos recentes de incidentes no setor bancário

REUTERS

BANKING AND FINANCIAL NEWS FEBRUARY 13, 2019 / 1:09 PM / 4 MONTHS AGO

Major Malta bank suspends operations after cyber attack alert

1 MIN READ

VALLETTA, Feb 13 (Reuters) - Bank of Valletta, which accounts for almost half of Malta's banking transactions, shut down all of its operations on Wednesday after detecting a cyber attack, the company said.

BOV Bank of Valletta

Origem: Phishing e-mail

Impacto: Disrupção de funções críticas (por >24h) + reputação

2 Abordagem das autoridades

Abordagem das autoridades

Crescente preocupação com o nível de segurança das redes e sistemas

2016

Comissão Europeia
Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção de dados pessoais

Comissão Europeia
Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, que define medidas destinadas a garantir um elevado nível de segurança das redes e das informação

BIS
Guidance on cyber resilience for financial market infrastructures

G7
Fundamental elements of cybersecurity for the financial sector

2017

EBA
Orientações relativas à avaliação do risco das TIC no âmbito SREP

EBA
Orientações relativas a medidas de segurança para riscos operacionais e de segurança sob a DSP2

EBA
Orientações relativas a reporte de incidentes significativos sob a DSP2

BIS
Regulatory approaches to enhance banks' cyber security frameworks

2018

AR
Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148

ECB
Cyber resilience oversight expectations for financial market infrastrutures

TIBER-EU
European framework for Threat Intelligence-based Ethical Red Teaming

2019

Joint Committee
Opinião conjunta à CE sobre medidas legislativas para a supervisão do risco TIC e criação de quadro legislativo de ciber-resiliência

EBA
Orientações sobre gestão de riscos TIC e riscos de segurança (a aguardar publicação)

Banco de Portugal
Recomendações relativas à subcontratação externa a prestadores de serviços de computação em nuvem

Abordagem das autoridades

A abordagem do Banco de Portugal assenta em 3 pilares fundamentais

Regulação

- Orientações EBA relativas à avaliação do risco TIC no âmbito SREP;
- Orientações EBA sobre gestão de riscos TIC e riscos de segurança (previstas 2019);
- Recomendações EBA e Carta-Circular do Banco de Portugal sobre a subcontratação externa a prestadores de serviços de computação em nuvem.

Supervisão

- Realização de inspeções com incidência no risco TIC;
- Avaliação da maturidade dos processos de gestão de risco TIC através de questionário para efeito do SREP;
- Definição de reporte de incidentes de cibersegurança;
- Testes de intrusão TLPT (futuramente).

Cooperação

- Protocolo de cooperação com o CNCS;
- Membro da Rede CSIRT;
- Promoção de fóruns de Indústria (e.g. APB);
- Formação interna e promoção de iniciativas sobre cibersegurança.

3 Obrigações de reporte

Obrigações de reporte

Nova Instrução com o objetivo de otimizar as obrigações existentes

Deveres de reporte atuais

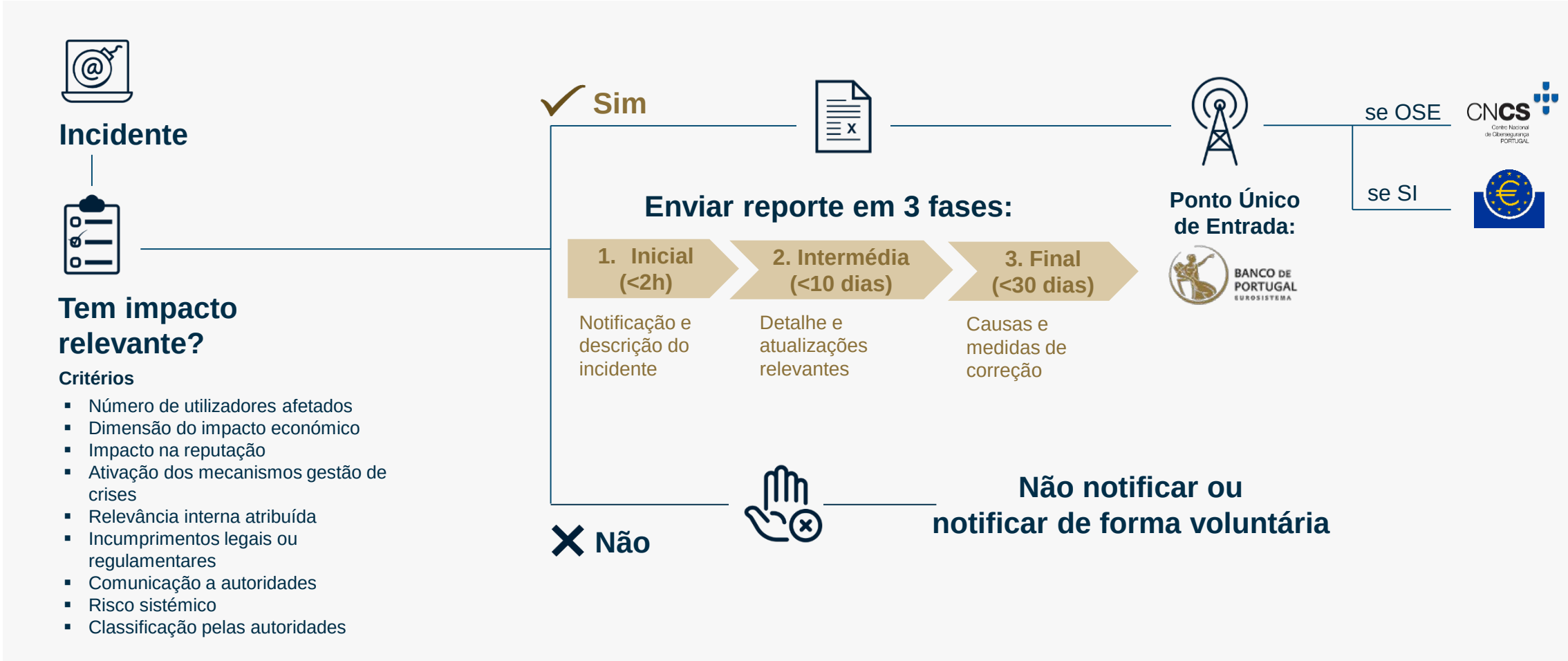
Deveres de reporte previstos

1 único modelo de reporte

- Elimina multiplicidade de reportes
- Promove taxonomia comum
- Estabelece ponto único de entrada

Obrigações de reporte

Descrição geral do projeto de Instrução (a submeter em breve a consulta pública)



Obrigações de reporte

MUS: Principais conclusões de 2 anos de reporte de incidentes de cibersegurança

"A recent ECB analysis of the first two years of data found a **fairly low number of significant cyber incidents in the euro area banking system**. In most cases, the incidents reported were detected – belatedly – by the banks themselves or by a third party. **Most of them led to a short disruption of services with limited financial loss**. The **most frequently reported incidents were distributed denial of service attacks** (in which massive amounts of fake web requests are used to flood the bank's internet-facing servers and prevent access by legitimate users such as bank customers), unauthorised access requests, data leakage and phishing attacks.

The diverse nature of cyber incidents indicates that there is a range of vulnerabilities that banks need to address: from gaps in their IT security infrastructure to insufficient staff awareness. As shown by the ECB analysis, it is important for banks to improve their cyber resilience on the technical and human levels and to install efficient crisis management procedures to ensure they are prepared for the worst-case scenario."

Fonte: SSM Supervision Newsletter – May 2019

4 Próximos passos

Próximos passos

Implementação das orientações da EBA

ICT governance and strategy	ICT risk management framework	Information security	ICT Operations management	ICT Project and Change management	Business continuity management
The management body should ensure that financial institutions have an adequate internal governance and internal control framework in place for their ICT risks.	Financial institutions should identify and manage their ICT risks according to the three lines of defence model.	Financial institutions should develop and document an information security policy which should define the high-level principles and rules to protect the confidentiality, integrity and availability of information.	Financial institutions should manage their ICT operations based on processes and procedures that are documented, implemented and approved by the management body.	Financial institutions should implement a governance process with an adequate project implementation leadership to effectively support the implementation of the ICT strategy through ICT projects.	Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an on-going basis and to limit losses in the event of severe business disruption.

Working together, (…), private and public entities and public authorities can help bolster the overall cybersecurity and resiliency of the international financial system.

G7 Fundamental Elements of Cybersecurity for the Financial Sector