Como os requisitos de segurança cibernética estão auxiliando na mitigação dos ataques cibernéticos?

Jorge Monge Alonso - jorge.monge.alonso@managementsolutions.com
Felipe Valor – felipe.valor@msbrazil.com

01

Contexto Geral

WannaCry

Cyber-attack: Europol says it was unprecedented in scale

13 May 2017

More Evidence Points to North Korea in Ransomware Attack

Ransomware WannaCry já infectou 200 mil computadores em 150 países

Ataque com ransomware está sequestrando arquivos de empresas ao redor do mundo

Ataque do WannaCry foi equivalente a roubo de mísseis Tomahawk dos EUA

O presidente da Microsoft, Brad Smith, reconhece "a necessidade de atuar de forma conjunta e urgente para proteger as pessoas online"

Visão Geral Regulações & Padrões Internacionais

Requerimentos regulatórios
Best Practices Reguladores
Padrões de mercado
! Impactos relevantes Engineering
* Próxima aplicabilidade

Como é um tema de extrema relevância, os diferentes reguladores se preocuparam em gerar publicações à respeito, fato que foi chamado de Tsunami regulatório

Solvência
- COREP
- LE*
- AQR
- STE
- Pilar III*
- Fase I FSB
- SBP
- ICAAP
- Stress Test
- FRTB*

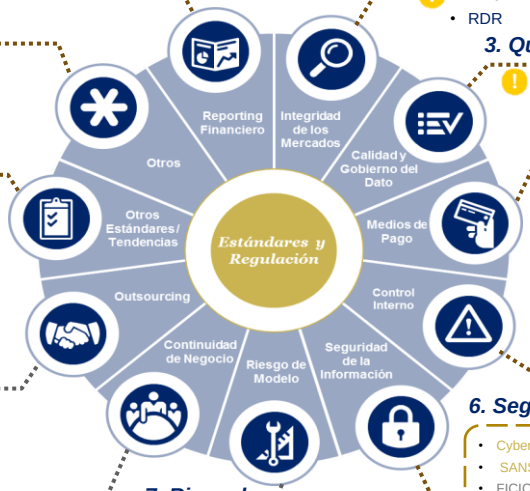
Liquidez
- LQs
- AE
- Funding Plan
- AMM
- LCR
- NSFR*
- Fase II FSB
- ILAAP

Contabilidade
- FINREP
- EEFF
- Circular 5/2014
- SEC

Provisões
- ! IFRS9*

Mercados
- Prudent Valuation
- EMIR

Restante
- TLAC*
- ! Anacredit*
- STE-IRRBB
- Remunerac.
- Concentrac. soberanos
- QIS e Datahub Basilea
- QIS GSIB´s
- Encostas Derivados BIS



1. Reporting Financeiro

2. Integridade dos Mercados
- ! Mifid II*
- RDR
- PRIIPS
- Conduct Risk

3. Qualidade e Governo do Dado
- ! RDA

4. Meios de Pagamento
- ! AML*
- PSD
- ! PSD2*
- Regulamento de taxas de comissão nas transações de cartões
- Pagamento em tempo real
- ENISA – Segurança S.P.
- SEPA
- ! Bitcoin / novas moedas*
- Pagamentos pela internet e celular – EBA
- EMV
- PCI DSS

5. Controle Interno e Gov. Corporativo !
- SOX
- COSO
- COSO II
- Best Practices Controle Interno EBA
- Best Practices on Corporate Governance

6. Segurança da Informação !
- Cybercrime review
- SANS
- FICIC
- NIST
- FFIEC
- Fed/OCC/FDIC – Melhorados
- NIS
- CBEST
- SRI
- Padrões
- NCCP
- GRC
- LOPD
- ISO 27K
- FISMA
- GDPR*

7. Risco de Modelo
- Supervisory Guidance on MRM (OCC/Fed)

8. Continuidade de Negócio !
- *High-level principles for business continuity*
- *ISO 22301 e ISO 22313*

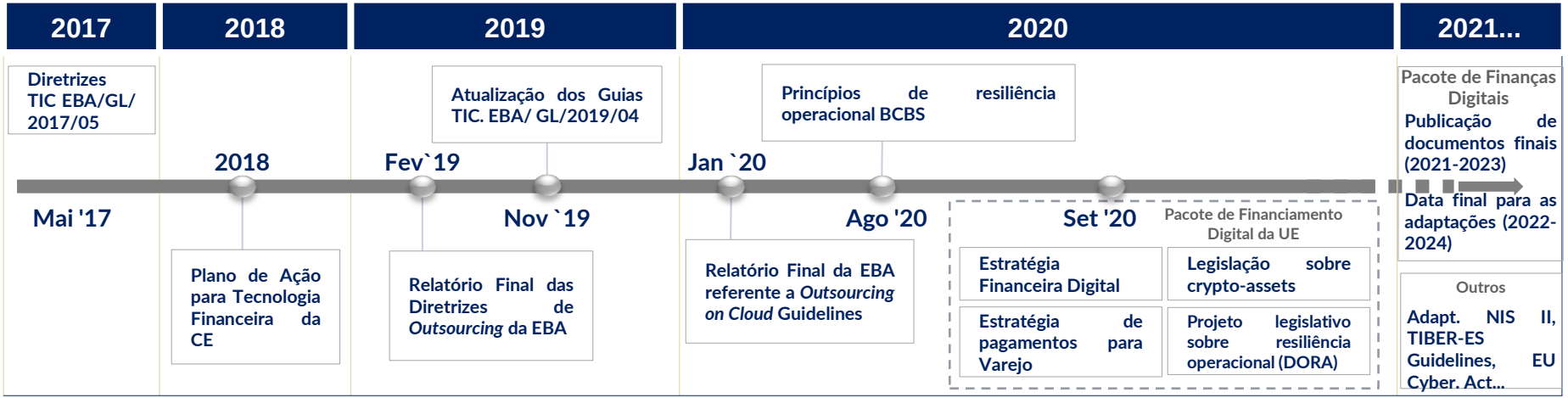
9. Outsourcing !
- EBA & FED Guidelines on outsourcing

10. Outros Padrões/Tendências
- ! BIG DATA
- COBIT
- ITIL
- CMMI
- Tier IV /CPDs
- DORA

11. Outros
- Volcker Rule
- EDTF
- FATCA – USA

Evolução Histórica – Normativo Internacional

O Tsunami regulatório foi evoluindo desde 2017 através das publicações do diferentes reguladores internacionais



Guias de Outsourcing EBA

Fornece uma **definição clara de *outsourcing*** e especifica os critérios para avaliar se uma atividade, serviço, processo ou função externalizada (ou parte dela) é **ou não crítica ou importante.**

Guias TIC EBA

Define requisitos de alto nível para permitir às instituições financeiras **adaptar a sua gestão de risco TIC aos novos desafios e desenvolvimentos**, bem como para melhorar a sua compreensão.

Princípios da resiliência operacional BCBS

Procuram **aumentar a resiliência dos bancos para absorver os impactos do risco operacional** (pandemias, incidentes de cibersegurança ou tecnológicos, catástrofes naturais, etc.).

Pacote de Finanças Digitais da Comissão Europeia

Um pacote de medidas para **estimular a competitividade e inovação da Europa no setor financeiro**, oferecendo aos consumidores mais oportunidades e métodos de pagamento modernos. **Objetivos do plano:**

- **Acabar com a fragmentação do mercado único digital.**
- **2. Adaptar o quadro regulamentar da UE para impulsionar a inovação digital**
- **3. Promover a inovação orientada pelos dados e a criação de um espaço comum**
- **4. Enfrentar os desafios e riscos associados à transformação digital**

02

Circular SUSEP N°638

Circular SUSEP N°638

A Circular determina as práticas relacionadas a Segurança Cibernética que Seguradoras devem adotar subdivididas em três principais categorias:

Política de Segurança Cibernética

Políticas que contemplem os objetivos, os parâmetros e diretrizes relacionados à segurança cibernética perante a temas internos.

Prevenção e Tratamento de Incidentes

Processos, procedimentos e controles visando identificar, prever, reduzir e recuperar-se de incidente e falhas cibernéticas.

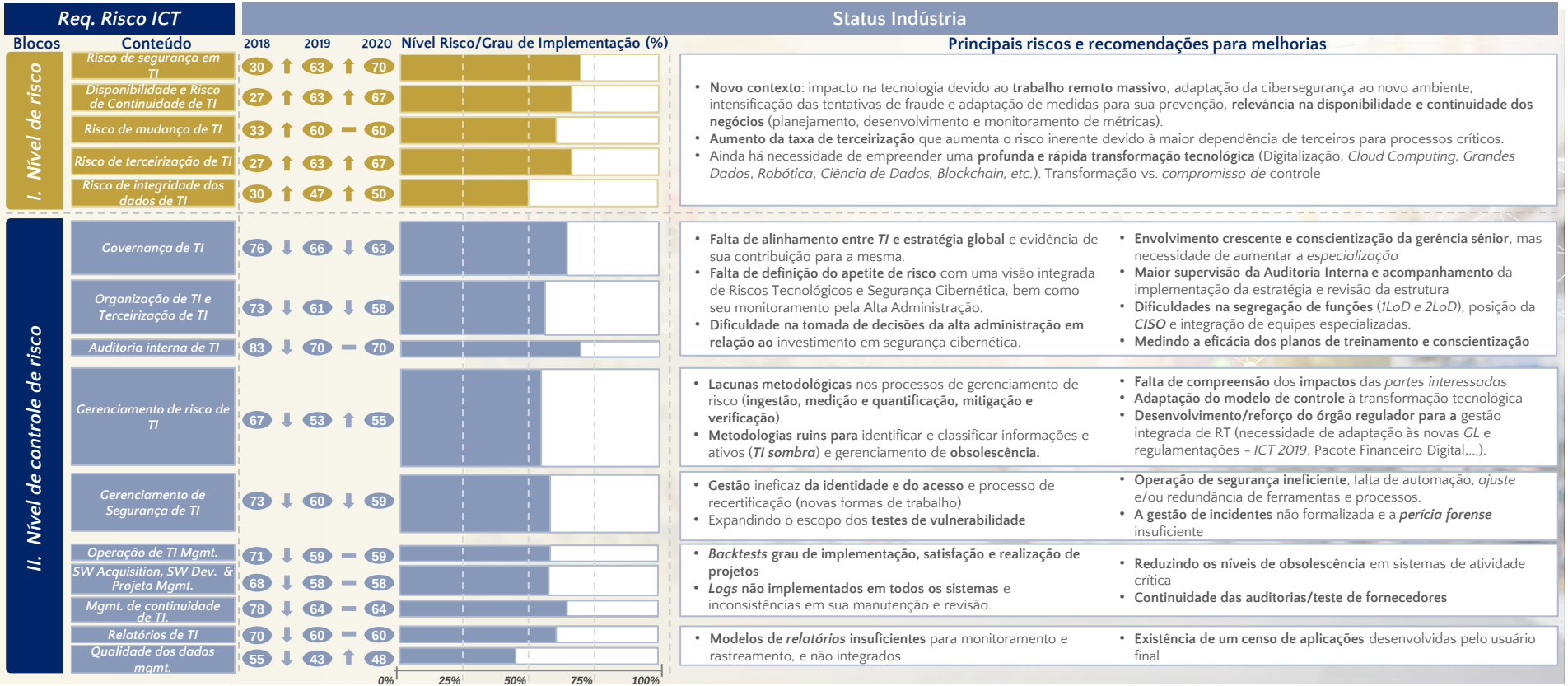
Terceirização de Serviços

Procedimentos para a contratação de serviços de processamento e armazenamento de dados.

03

Status Indústria

Status da Gestão de Riscos Tecnológicos e Segurança



[1] Fontes: *Feedback do BCE* e experiência em projetos de EM. Para facilitar a interpretação, o eixo e as pontuações foram alterados para porcentagem.

Obrigado.