

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



Jorge Monge Alonso - jorge.monge.alonso@managementsolutions.com
Felipe Valer - felipe.valer@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	Liquidez	Contabilidade	Provisões	Mercados	Restante
<ul style="list-style-type: none"> • COREP • LE* • AQR • STE • Pilar III* • Fase I FSB • SBP • ICAAP • Stress Test • FRTB* 	<ul style="list-style-type: none"> • LQs • AE • Funding Plan • AMM • LCR • NSFR* • Fase II FSB • ILAAP 	<ul style="list-style-type: none"> • FINREP • EEFF • Circular 5/2014 • SEC 	<ul style="list-style-type: none"> ! IFRS9* 	<ul style="list-style-type: none"> • Prudent Valuation • EMIR 	<ul style="list-style-type: none"> ! TLAC* ! Anacredit* • Remunerac. • Concentrac. soberanos • QIS e Datahub Basilea • QIS GSIB's • Encostas Derivados BIS

1. Reporting Financeiro

11. Outros

- Volcker Rule
- EDTF
- FATCA – USA

10. Outros Padrões/Tendências

- ! BIG DATA
- COBIT
- ITIL
- CMMI
- Tier IV /CPDs
- DORA

9. Outsourcing !

- EBA & FED Guidelines on outsourcing

8. Continuidade de Negócio !

- High-level principles for business continuity
- ISO 22301 e ISO 22313

7. Risco de Modelo

- Supervisory Guidance on MRM (OCC/Fed)

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 !

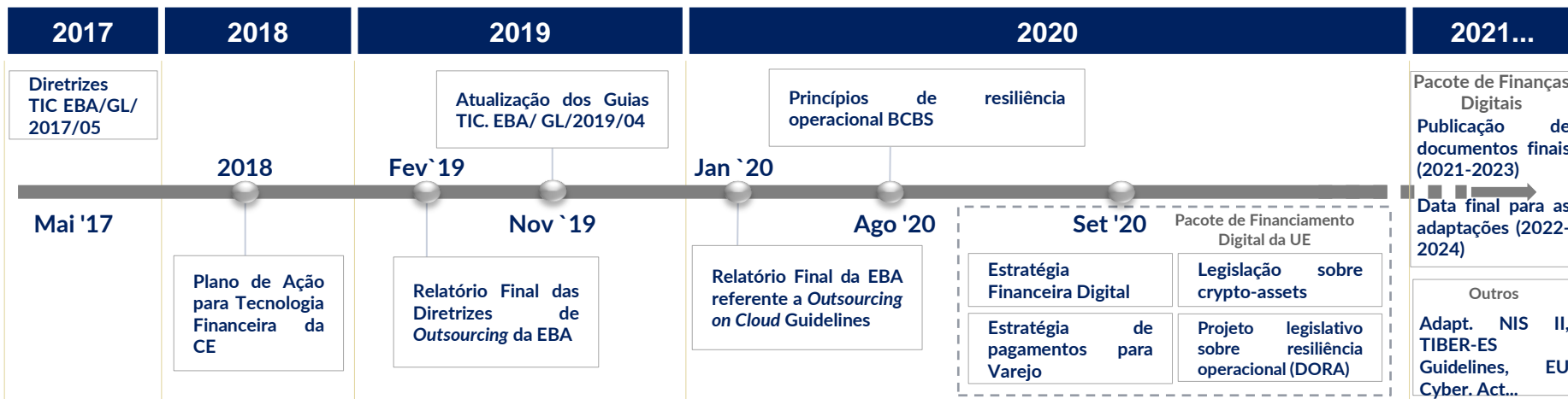
- SOX
- COSO
- COSO II
- Best Practices Controle Interno EBA
- Best Practices on Corporate Governance

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*

Evolução Histórica – Normativo Internacional

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



Guias de Outsourcing EBA

Fornecer 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:**

1. 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:



03

Status Indústria



Status da Gestão de Riscos Tecnológicos e Segurança

Req. Risco ICT

Status Indústria

Blocos	Conteúdo	2018	2019	2020	Nível Risco/Grau de Implementação (%)
I. Nível de risco	Risco de segurança em TI	30 ↑	63 ↑	70	
	Disponibilidade e Risco de Continuidade de TI	27 ↑	63 ↑	67	
	Risco de mudança de TI	33 ↑	60	60	
	Risco de terceirização de TI	27 ↑	63 ↑	67	
	Risco de integridade dos dados de TI	30 ↑	47 ↑	50	

Principais riscos e recomendações para melhorias

- **Novo contexto:** impacto na tecnologia devido ao **trabalho remoto massivo**, adaptação da cibersegurança ao novo ambiente, intensificação das tentativas de fraude e adaptação de medidas para sua prevenção, **relevância na disponibilidade e continuidade dos negócios** (planejamento, desenvolvimento e monitoramento de métricas).
- **Aumento da taxa de terceirização** que aumenta o risco inerente devido à maior dependência de terceiros para processos críticos.
- Ainda há necessidade de empreender uma **profunda e rápida transformação tecnológica** (Digitalização, *Cloud Computing*, *Grandes Dados*, *Robótica*, *Ciência de Dados*, *Blockchain*, etc.). Transformação vs. *compromisso de controle*

II. Nível de controle de risco

Governança de TI	76 ↓	66 ↓	63	
Organização de TI e Terceirização de TI	73 ↓	61 ↓	58	
Auditoria interna de TI	83 ↓	70	70	
Gerenciamento de risco de TI	67 ↓	53 ↑	55	
Gerenciamento de Segurança de TI	73 ↓	60 ↓	59	
Operação de TI Mgmt.	71 ↓	59	59	
SW Acquisition, SW Dev. & Projeto Mgmt.	68 ↓	58	58	
Mgmt. de continuidade de TI.	78 ↓	64	64	
Relatórios de TI	70 ↓	60	60	
Qualidade dos dados mgt.	55 ↓	43 ↑	48	

- **Falta de alinhamento entre TI e estratégia global** e evidência de sua contribuição para a mesma.
- **Falta de definição do apetite de risco** com uma visão integrada de Riscos Tecnológicos e Segurança Cibernética, bem como seu monitoramento pela Alta Administração.
- **Dificuldade na tomada de decisões da alta administração em relação ao investimento em segurança cibernética.**
- **Envolvimento crescente e conscientização da gerência sênior**, mas necessidade de aumentar a *especialização*
- **Maior supervisão da Auditoria Interna e acompanhamento da implementação da estratégia e revisão da estrutura**
- **Dificuldades na segregação de funções (1LoD e 2LoD)**, posição da *CISO* e integração de equipes especializadas.
- **Medindo a eficácia dos planos de treinamento e conscientização**

- **Lacunas metodológicas** nos processos de gerenciamento de risco (*ingestão, medição e quantificação, mitigação e verificação*).
- **Metodologias ruins** para identificar e classificar informações e ativos (*TI sombra*) e gerenciamento de *obsolescência*.

- **Falta de compreensão dos impactos das partes interessadas**
- **Adaptação do modelo de controle à transformação tecnológica**
- **Desenvolvimento/reforço do órgão regulador para a gestão integrada de RT** (necessidade de adaptação às novas *CL* e regulamentações - *ICT 2019*, Pacote Financeiro Digital...).

- **Gestão ineficaz da identidade e do acesso** e processo de recertificação (novas formas de trabalho)
- Expandindo o escopo dos testes de vulnerabilidade

- **Operação de segurança ineficiente**, falta de automação, *ajuste e/ou redundância* de ferramentas e processos.
- **A gestão de incidentes não formalizada e a *perícia forense* insuficiente**

- **Backtests grau de implementação, satisfação e realização de projetos**
- **Logs não implementados em todos os sistemas e inconsistências** em sua manutenção e revisão.

- **Reduzindo os níveis de obsolescência** em sistemas de atividade crítica
- **Continuidade das auditorias/teste de fornecedores**

- **Modelos de relatórios** insuficientes para monitoramento e rastreamento, e não integrados

- **Existência de um censo de aplicações** desenvolvidas pelo usuário final

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.