

DOMINGO MONTANARO  
GIULIANO GIOVA  
RENATO OPICE BLUM  
COORDENADORES

# CYBER RISK

Estratégias Nacionais e  
Corporativas sobre Riscos  
e Segurança Cibernética

## AUTORES

Alexandre Quinze ■ Armando Lima Amaral ■ Caio César  
Carvalho Lima ■ Camilla do Vale Jimene ■ Cristiano  
Petroni ■ Domingo Montanaro ■ Fernanda Kac ■ Giuliano  
Giova ■ Guilherme Hernandez Siculo ■ Gustavo  
Batistuzzo ■ Marcelo Buz ■ Marcelo Caiado ■ Maria Augusta  
Peres Catelli ■ Maurício Antonio Tamer ■ Paula Marques  
Rodrigues ■ Renata Yumi Idie ■ Roberto Gallo ■ Rodrigo  
Moura Fernandes ■ Rony Vainzof ■ Taciana Eugênia Duarte

## ORGANIZADORES

Renato Opice Blum e Shirly Wajsbrot

THOMSON REUTERS

**REVISTA DOS  
TRIBUNAIS™**

*Diretora de Conteúdo e Operações Editoriais*

**JULIANA MAYUMI ONO**

*Gerente de Conteúdo*

**MILISA CRISTINE ROMERA**

*Editorial:* Aline Marchesi da Silva, Diego Garcia Mendonça, Karolina de Albuquerque Araújo e Quenia Becker

*Gerente de Conteúdo Tax:* Vanessa Miranda de M. Pereira

*Direitos Autorais:* Viviane M. C. Carmezim

*Assistente de Conteúdo Editorial:* Juliana Menezes Drumond

*Analista de Projetos:* Camilla Dantara Ventura

*Estagiários:* Alan H. S. Moreira, Ana Amalia Strojnowski, Bárbara Baraldi e Bruna Mestriner

*Produção Editorial*

*Coordenação*

**ANDRÉIA R. SCHNEIDER NUNES CARVALHAES**

*Especialistas Editoriais:* Gabriele Lais Sant'Anna dos Santos e Maria Angélica Leite

*Analista de Projetos:* Larissa Gonçalves de Moura

*Analistas de Operações Editoriais:* Alana Fagundes Valério, Caroline Vieira, Damares Regina Felício, Danielle Castro de Morais, Mariana Plastino Andrade, Mayara Macioni Pinto e Patricia Melhado Navarra

*Analistas de Qualidade Editorial:* Ana Paula Cavalcanti, Fernanda Lessa, Thais Pereira e Victória Menezes Pereira

*Designer Editorial:* Lucas Kfoury

*Estagiárias:* Maria Carolina Ferreira, Sofia Mattos e Tainá Luz Carvalho

*Capa:* Linotec

*Lider de Inovações de Conteúdo para Print*

**CAMILLA FUREGATO DA SILVA**

*Equipe de Conteúdo Digital*

*Coordenação*

**MARCELLO ANTONIO MASTROROSA PEDRO**

*Analistas:* Gabriel George Martins, Jonathan Souza, Maria Cristina Lopes Araujo e Rodrigo Araujo

*Gerente de Operações e Produção Gráfica*

**MAURICIO ALVES MONTE**

*Analistas de Produção Gráfica:* Aline Ferrarezi Regis e Jéssica Maria Ferreira Bueno

*Estagiária de Produção Gráfica:* Ana Paula Evangelista

**Dados Internacionais de Catalogação na Publicação (CIP)**  
**(Câmara Brasileira do Livro, SP, Brasil)**

---

Cyber Risk : Estratégias nacionais e corporativas sobre riscos e segurança cibernética / Renato Opice Blum e Shirly Wajsbrot, organizadores ; Domingo Montanaro, Giuliano Giova e Renato Opice Blum, coordenação. -- 1. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

Bibliografia

ISBN 978-65-5614-337-8

1. Cibernética 2. Cibernética - Medidas de segurança 3. Direito digital 4. Internet - Medidas de segurança 5. Proteção de dados - Direito - Brasil 6. Segurança (Direito) I. Blum, Renato Opice. II. Wajsbrot, Shirly. III. Montanaro, Domingo. IV. Giova, Giuliano.

20-46358

CDU-34:004

---

**Índices para catálogo sistemático:**

1. Segurança cibernética : Direito digital 34:004  
Maria Alice Ferreira - Bibliotecária - CRB-8/7964

# Sumário

<b>1. Prevenir para mitigar: a importância do desenvolvimento de cultura de segurança cibernética nas organizações.....</b>	<b>13</b>
<i>Maria Augusta Peres Catelli e Renata Yumi Idie</i>	
1. Panorama dos recentes incidentes de segurança da informação e seus reflexos .....	14
2. Da responsabilidade e sanções decorrentes dos incidentes de segurança da informação .....	18
3. Das estratégias para a mitigação de riscos: a adoção de boas práticas e o desenvolvimento de cultura de segurança cibernética .....	24
3.1. A (i)maturidade da sociedade e das organizações brasileiras no campo da segurança cibernética.....	24
3.2. A segurança cibernética no ambiente interno das organizações: adoção de medidas para assegurar a proteção dos ativos informacionais.....	26
3.2.1. Atendimento aos padrões internacionais de gestão de segurança da informação (Normas ISO/IEC).....	28
3.2.2. Implementação de política de segurança da informação e elaboração de termos de compromisso e responsabilidade.....	30
3.2.3. Investimentos na educação e no treinamento de colaboradores.....	33
4. Considerações finais .....	35
Referências bibliográficas.....	37
<b>2. Segurança da informação sob a perspectiva da legislação brasileira: aspectos convergentes.....</b>	<b>41</b>
<i>Camilla do Vale Jimene e Guilherme Hernandez Siculo</i>	
1. Introdução .....	42

2.	Aspectos convergentes: segurança da informação e legislação brasileira .....	43
	Constituição Federal.....	44
	Código Penal.....	46
	Código de Processo Civil .....	47
	Consolidação das Leis do Trabalho.....	49
	Lei da Propriedade Industrial.....	49
	Lei do Sigilo Bancário .....	50
	Lei da Interceptação Telefônica.....	50
	Medida provisória sobre certificação digital.....	51
	Lei de Acesso à Informação e seu decreto regulamentador .....	52
	Lei de Identificação Criminal.....	54
	Marco Civil da Internet e seu decreto regulamentador .....	54
	Lei Geral de Proteção de Dados Pessoais .....	56
	Outras iniciativas legislativas relevantes.....	58
3.	Conclusão.....	59
<b>3. A importância da identificação digital segura: confiança ....</b>		<b>61</b>
<i>Marcelo Buz</i>		
1.	Um país, várias identidades .....	62
2.	Estratégia de governo digital.....	63
	2.1. Governança cibernética.....	66
	2.2. Riscos cibernéticos .....	67
	2.3. Aperfeiçoamento da infraestrutura cibernética .....	70
3.	Oportunidades para o documento de identificação digital .....	71
	3.1. Segurança na identificação de pessoas, instituições e objetos .....	72
	3.2. Passar nosso sistema de registro civil a limpo .....	73
4.	Mundo virtual e suas peculiaridades.....	76
	4.1. Autenticidade, integridade e autoria .....	80
	4.2. Proteção da privacidade.....	83
	4.3. Recursos criptográficos .....	84
	Referências bibliográficas .....	85
<b>4. Tratamento de dados brutos e informações pessoais .....</b>		<b>89</b>
<i>Gustavo Batistuzzo</i>		
	Referências bibliográficas.....	106

<b>5. O desafio de <i>cyber security</i> em grandes e heterogêneas infraestruturas</b> .....	109
<i>Armando Lima Amaral</i>	
1. Evolução da segurança da informação nos últimos 20 anos .....	110
2. A importância da governança e dos processos .....	111
3. O time é o habilitador da transformação .....	112
4. Autonomia e suporte da alta gestão .....	113
5. Segurança como parceiro do negócio .....	113
6. Criando uma visão centrada no cliente .....	114
7. Lidando com crise de segurança .....	115
8. A organização de um time de segurança dentro de uma grande empresa .....	117
9. O papel do CISO em uma grande corporação .....	118
Conclusão .....	118
<b>6. Desafios e oportunidades na perícia digital</b> .....	119
<i>Marcelo Caiado</i>	
1. Introdução .....	120
1.1. Um breve histórico da perícia forense .....	121
2. Perícias de TIC .....	123
2.1. Desafios .....	125
2.2. Oportunidades .....	128
2.3. Peritos em TIC .....	130
2.4. Crimes de informática .....	132
2.5. A atividade pericial .....	135
2.6. Evidências digitais .....	140
2.7. Perícias corporativas .....	143
3. Conclusões .....	146
Referências bibliográficas .....	148
<b>7. Criptografia: não salva, mas pode matar</b> .....	151
<i>Roberto Gallo</i>	
1. Breve história .....	152
2. Objetivos, serviços e mecanismos criptográficos .....	154
3. Quão segura pode ser a criptografia? .....	156
4. Recursos criptográficos .....	157
4.1. Perguntas que precisam ser respondidas .....	157
4.2. Soluções criptográficas-padrão .....	159

## 8 | CYBER RISK

4.3.	Criptografia por design .....	161
4.3.1.	Controle, conveniência e risco.....	164
4.3.2.	Suporte correto para a criptografia nas plataformas computacionais: hardware <i>versus</i> software .....	166
4.4.	Algoritmos criptográficos .....	169
4.4.1.	Criptografia e desempenho.....	169
4.4.2.	Nível de segurança criptográfico.....	169
4.4.3.	Envelhecimento de algoritmos .....	171
4.4.4.	Computação quântica, algoritmos pós-quânticos...	173
5.	Fatores exógenos .....	174
6.	Referências bibliográficas .....	176

## **8. Resposta a incidentes de segurança da informação: da identificação do incidente à notificação à autoridade e aos titulares de dados.....**

*Caio César Carvalho Lima e Rony Vainzof*

Introdução.....	180
1. Entendendo o conceito de incidente de segurança da informação .....	182
2. Padrões de segurança da informação envolvendo dados pessoais ...	184
3. Identificando e reagindo a incidentes de segurança.....	186
3.1. Preservação das evidências .....	186
3.2. Comunicar a seguradora, quando pertinente .....	187
3.3. Formação de “comitê de crise” .....	187
3.4. Identificação da causa-raiz do incidente.....	188
3.5. Contenção da vulnerabilidade.....	188
3.6. Identificação da exposição de dados.....	188
3.7. Varredura da web: monitoramento da <i>surface</i> e <i>deep web</i> ....	189
3.8. Elaboração de <i>score</i> de gravidade do incidente.....	189
3.9. Definição sobre a comunicação aos titulares/às autoridades ...	190
3.10. Elaboração de <i>script</i> para resposta a questionamentos dos consumidores .....	190
3.11. Elaboração de Fato Relevante, se cabível.....	190
3.12. Elaboração de notas reativas à imprensa .....	191
3.13. Relatório forense do incidente .....	191
3.14. Estratégia jurídica para contenção .....	192
3.15. Medidas jurídicas para identificar o ofensor.....	192
4. Comunicando incidentes de segurança da informação .....	192
4.1. Conteúdo da comunicação .....	194

Considerações finais.....	196
Referências bibliográficas.....	196
<b>9. Pelo amor ou pela dor – lições aprendidas pelas instituições brasileiras depois de milhares de incidentes cibernéticos .....</b>	<b>199</b>
<i>Domingo Montanaro</i>	
Introdução.....	200
<i>Brace for impact: o incidente vai acontecer.....</i>	200
Tenha uma prática reativa, pronta .....	205
Entenda o conflito de interesses.....	207
Categorize os incidentes.....	213
<b>10. Aplicação das tecnologias <i>blockchain</i> e <i>smart contracts</i> na proteção de infraestruturas sistêmicas em consonância com a estratégia nacional de segurança cibernética .....</b>	<b>217</b>
<i>Cristiano Petroni</i>	
Introdução.....	218
Revisão da literatura.....	220
<i>Blockchain</i> .....	220
<i>Smart Contracts</i> .....	222
Ataques cibernéticos .....	223
Arquitetura proposta .....	229
Estrutura dos <i>Smart Contracts</i> .....	233
Considerações finais.....	234
Referências bibliográficas.....	235
<b>11. Segurança cibernética e telemedicina .....</b>	<b>241</b>
<i>Taciana Eugênia Duarte</i>	
Considerações iniciais.....	241
A tecnologia como ferramenta de apoio à saúde .....	242
A segurança cibernética como proteção aos dados médicos.....	246
Quais são as ameaças? .....	246
● que desejamos proteger? .....	248
Quais medidas serão implementadas?.....	250
Como agir diante de ocorrências indesejadas?.....	251
Considerações finais.....	252
Referências bibliográficas.....	252

<b>12. Resiliência e Governança Digital</b> .....	257
<i>Rodrigo Moura Fernandes</i>	
1. Introdução .....	258
2. Um pouco de história: de Alan Turing ao surgimento da internet ...	259
3. A inevitabilidade de um ataque cibernético .....	261
4. Métodos de instalação de malware.....	263
4.1. <i>Download drive-by</i> .....	263
4.2. <i>Trojans</i> .....	263
4.3. Engenharia social .....	263
4.4. <i>Phishing</i> e <i>spear phishing</i> .....	264
5. Tipos de ataques.....	264
5.1. Engenharia social .....	265
5.2. Ataques de <i>phishing</i> e <i>spear phishing</i> .....	265
5.3. Ataques de <i>spear phishing</i> (ou <i>whale phishing</i> ) .....	266
5.4. Ataques de contrapartida.....	266
5.5. Utilização não autorizada .....	267
5.6. Ataques distribuídos de negação de serviço .....	267
5.7. Ameaças persistentes avançadas.....	267
5.8. Ataques de força bruta.....	268
6. Identificando ativos críticos.....	268
6.1. Introdução.....	268
6.2. Os pilares da segurança digital .....	269
6.3. Confidencialidade .....	269
6.4. Integridade .....	270
6.5. Disponibilidade .....	270
6.6. Identificação de sistemas, redes e dados críticos .....	271
7. Análise de impacto.....	271
8. Os benefícios de um efetivo programa de governança .....	273
9. Ciber-resiliência.....	273
9.1. Política corporativa de segurança da informação .....	274
9.2. A cultura da segurança cibernética.....	274
10. A cultura da ciber-resiliência .....	274
10.1. Transparência .....	275
10.2. Responsabilidade.....	276
10.3. Conhecimento adequado do sistema.....	276
10.4. Cumprimento das políticas e procedimentos .....	276



10.5. Criação de canais de comunicação formais.....	277
10.6. Orçamento e alocação de recursos .....	277
10.7. Retorno sobre o investimento na mitigação do impacto de um ataque.....	278
10.8. Estabelecimento de métricas e eficácia mensuráveis.....	278
11. Conclusão .....	278
Referências .....	279
<b>13. E-Ciber e o paradoxo da produtividade .....</b>	<b>281</b>
<i>Giuliano Giova</i>	
1. As leis e o ciberespaço.....	281
2. Normas jurídicas ou técnicas.....	284
3. Gênese .....	293
4. Paradoxo da produtividade.....	300
5. Conclusão .....	305
Abreviaturas e siglas.....	305
6. Referências bibliográficas .....	305
<b>14. Compliance digital: o que é e a compreensão da tarefa de conformidade para a mitigação de riscos cibernéticos.....</b>	<b>309</b>
<i>Maurício Antonio Tamer</i>	
Introdução.....	310
1. O que parece ser o <i>compliance</i> .....	311
2. E o <i>compliance</i> digital? O que é? .....	314
3. Fundamentos do <i>compliance</i> digital.....	318
3.1. Autorregulação regulada .....	318
3.2. Governança corporativa ou <i>corporate governance</i> .....	321
3.3. Responsabilidade social e ética empresarial .....	330
4. A mitigação de riscos cibernéticos.....	331
Referências bibliográficas.....	333
<b>15. Pelo mercado, pela lei ou pelo inimigo. Entenda por que não podemos ficar parados.....</b>	<b>337</b>
<i>Alexandre Quinze</i>	
Referências bibliográficas.....	356

<b>16. Inteligência artificial e estratégia nacional de segurança cibernética: perspectivas acerca da prevenção a riscos cibernéticos</b> .....	357
<i>Fernanda Kac e Paula Marques Rodrigues</i>	
Introdução.....	358
1. Os desafios da segurança cibernética diante do panorama dos riscos cibernéticos na sociedade da informação.....	360
1.1. Segurança cibernética em pauta .....	360
1.2. Panorama dos riscos cibernéticos.....	362
2. A Inteligência Artificial (IA) e seu contexto no mundo interconectado .....	367
2.1. Entendendo a IA.....	367
2.2. Os desafios ético-jurídicos quanto à implementação de sistemas de IA.....	369
3. Da aplicação de soluções de IA perante os riscos cibernéticos na atualidade .....	372
Conclusão .....	375
Referências bibliográficas.....	377