

Luca Belli
Breno Pauli Medeiros
Natália Couto
Erica Bakonyi
Walter Britto Gaspar
Daniel Dore Lage



Governança e regulação da cibersegurança no Brasil

Proteção da infraestrutura crítica, segurança da informação e construção da soberania digital

Prefácio de Marcos Antonio Amaro dos Santos, Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

EDITORA LUMEN JURIS
RIO DE JANEIRO
2026

Sumário

Introdução	1
A estrutura deste trabalho.....	4
A conexão deste trabalho com a nova Estratégia Nacional de Cibersegurança	8
1 Cibersegurança: raízes conceituais, políticas e práticas	11
1.1 O conceito de cibersegurança	14
1.2 O processo de securitização do ciberespaço e a construção da ciberdefesa brasileira.....	20
1.3 A análise do caso das infraestruturas críticas digitais e serviços essenciais digitais: multiplicidade de atores e complexidade no tratamento de cibersegurança.....	26
1.3.1 Multiplicidade de atores responsáveis para a securitização das infraestruturas críticas e serviços essenciais.....	30
1.4 A segurança das infraestruturas críticas democráticas digitais	35
1.5 Uma taxonomia de ataques e ameaças cibernéticas e vulnerabilidades exploradas.....	40
1.6 Direitos fundamentais como base de uma abordagem à cibersegurança centrada nas pessoas	47
1.7 Soberania digital: entender, desenvolver e regular as tecnologias digitais de maneira soberana e cibersegura	51
2 Elementos constitutivos da cibersegurança.....	55
2.1 Governança	57
2.1.1 Funções inerentes à governança em cibersegurança.....	58
2.1.2 Qual tipo de estrutura administrativa deve ser criada para a governança de cibersegurança?	61
2.1.3 A Agência Nacional de Cibersegurança como coordenadora de um Sistema Nacional de Cibersegurança	65

2.1.4 O papel e a estrutura dos Grupos de Resposta a Incidentes de Segurança de Computadores - “CSIRTs”	67
2.1.5 O papel e a estrutura dos Centros de Análise e Compartilhamento de Informações “ISACs”	71
2.2 Regulação setorial existente em cibersegurança.....	73
2.3 Segurança da informação.....	86
2.3.1 Segurança de dados pessoais no Brasil	89
2.3.2 Proteção de informações não pessoais.....	92
2.3.3 Demais referenciais de orientação	96
2.4 Combate ao cibercrime.....	102
2.4.1 Normas penais vigentes no ordenamento brasileiro para o enfrentamento do cibercrime	105
2.4.2 A importância da Convenção de Budapeste	109
2.4.3 Contribuições que a Política Nacional de Cibersegurança (PNCiber) pode fornecer para o enfrentamento do cibercrime	116
2.5 Literacia digital: alicerce da cibersegurança e da soberania digital.....	118
2.5.1 A educação como força motriz para a construção da soberania digital.....	122
2.5.2 Ciber-higiene e educação multigeracional em cibersegurança.....	127
2.5.2.1 Crianças e adolescentes.....	129
2.5.2.2. Pais e educadores.....	130
2.5.2.3 Idosos	131
2.5.2.4 Profissionais técnicos	132
2.6 O papel e as modalidades da política industrial	133
2.6.1 Tipos de políticas industriais.....	137
2.6.2 Exemplos de sucesso brasileiro em política industrial	140
2.6.3 A governança da cibersegurança como elemento de política industrial	144

2.7 Tecnologias disruptivas e os desafios da inteligência artificial (IA).....	147
3 Os Caminhos Sinérgicos da Soberania Digital e Cibersegurança.....	151
4 Conclusão: Rumo a uma Nova Governança da Cibersegurança no Brasil	157
5 Glossário	161
5.1 Ameaça Persistente Avançada (Advanced Persistent Threat – APT)	161
5.2 Análise de Risco e Risco Cibernético	162
5.3 Ativo/Ciberativo	163
5.4 Atribuição	164
5.5 Autenticação Multifator (Multi-Factor Authentication – MFA).....	166
5.6 Backdoors	167
5.7 Centro de dados (Data center)	167
5.8 Ciberameaça.....	168
5.9 Ciberdefesa	170
5.10 Ciberespaço.....	171
5.11 Ciber-Guerra	172
5.12 Cibersegurança	174
5.13 Computação em Nuvem (Cloud Computing)	175
5.14 Cópia de Segurança (Backup)	177
5.15 Criptografia.....	178
5.16 Dado anonimizado	179
5.17 Dado pessoal/sensível.....	180
5.18 Desterritorialidade.....	181
5.19 Difusão de Poder.....	183
5.20 Diplomacia Cibernética	184
5.21 Diretor de Segurança de Informação (Chief Information Security Officer - CISO)	185
5.22 Encarregado pelo tratamento de dados.....	186

5.23 Endpoint (Ponto Final) e Endpoint Security (Segurança de Ponto Final)	188
5.24 Engenharia Social.....	189
5.25 Phishing	190
5.26 Gestão de Identidade e Acesso (Identity Access Management - IAM)	190
5.27 Governança	191
5.28 Hacking Ético (Ethical hacking).....	193
5.29 Incerteza cibernética	193
5.30 Incidente de segurança	195
5.31 Malware, Vírus e Ransomware.....	196
5.32 Medidas defensivas (Defensive Measures)	197
5.33 Negação de Serviço Distribuída (Distributed Denial of Service - DDoS)	199
5.34 Organismos de compartilhamento de informação: CERT, CSIRT, ETIR e ISACs.....	199
5.35 Poder cibernético.....	201
5.36 Privacidade desde a concepção (Privacy by design) e Privacidade por Padrão (Privacy by default)	202
5.37 Proteção de dados.....	204
5.38 Protocolo de Transferência de Arquivos Seguro (Secure File Transfer Protocol - SFTP)	205
5.39 Regulação.....	206
5.40 Resposta a Incidentes de Segurança, ou (Security Incident Response - SIR).....	208
5.41 Segurança desde a concepção (Security by design) e Segurança por padrão (Security by default).....	209
5.42 Segurança em Nuvem (Cloud security).....	211
5.43 Servidor de Nuvem (Servidor de Cloud).....	213
5.44 Soberania Digital.....	214
5.45 Superfície de Ataque (Attack Surface)	214

5.46 Teste de Penetração (Pentest).....	216
5.47 Triade da CIA: Confidencialidade, Integridade, Disponibilidade (CIA triad: Confidentiality, Integrity, Availability)	217
5.48 Vulnerabilidade e ataque de Dia Zero	221
5.49 Zero Trust.....	222
5.50 Zona Cinzenta (Gray Zone)	224
Anexo A – Uma proposta de Protocolo de Comunicação Intersectorial	227
Anexo B – Regulação ANTT – Obrigações em cibersegurança e segurança da informação para regulados	231
Referências bibliográficas	233
Normas que formam o <i>corpus</i> documental estudado	275