SUMÁRIO

1. INTRODUÇÃO 1

1.1 Breve histórico, conceito e intersecção com o direito digital 1
Larissa Lotufo

1.2 O que diferencia os crimes digitais dos crimes comuns? 4
Larissa Lotufo

1.3 Transformação digital e a mudança organizacional 6
Cristina Sleiman

2. DIREITO DIGITAL E O CIBERESPAÇO 11
Larissa Lotufo

2.1 Legislações e o aspecto internacional (sem fronteiras) 11

3. ATAQUES E CRIMES CIBERNÉTICOS 15
Marcos Tupinambá

3.1 Ataques e crimes objetivando funcionários e a alta direção da empresa 16
3.1.1 *Phishing* 16
3.1.1.1 *Spear phishing* 16
3.1.2 *Malware* 17
3.1.2.1 *Ransomware* 18
3.1.3 Ataques em comunicadores instantâneos 19
3.1.4 Golpe do falso boleto 21
3.1.5 Furto de dados por funcionários e terceirizados 22
3.1.5.1 Furto de dados e extorsão na vigência da LGPD 22
3.1.6 *Botnets* 23
3.1.7 DDoS 23
3.1.8 Armazenamento indevido de dados ilícitos 24

3.1.9 Fraudes em meios de pagamento e formulários web 24
3.1.10 Acessos diretos e indevidos a base de dados 26
3.1.11 Espionagem industrial e comercial 26
3.2 Simulação empresarial e aproveitamento parasitário 27
3.2.1 Vulnerabilidades em sistemas 28
3.2.2 Ataques ao DNS 28
3.2.3 Ataques por vetores físicos 29
Conclusão 30

4. PROTEÇÃO DE DADOS PESSOAIS 31
Patricia Peck Pinheiro e Larissa Lotufo

4.1 Proteção de dados no ciberespaço 31
4.2 Legislação brasileira: LGPD 32
4.3 Melhores práticas em proteção de dados 33
4.3.1 Adotar uma política de segurança da informação sólida 33
4.3.2 Definir bem os atores responsáveis pela proteção de dados na organização 34
4.3.3 Assegurar a execução dos direitos dos titulares de dados 35
4.3.4 Adotar a anonimização ou pseudoanonimização dos dados se possível 35
4.3.5 Emitir o Relatório de Impacto de Proteção de Dados (RIPD) como uma prática 36
4.3.6 Construir um Comitê de Proteção de Dados e enfocar a figura do DPO 37
4.3.7 Atentar às particularidades da transferência internacional de dados 38

5. COMO IMPLEMENTAR UMA CIBERSEGURANÇA CORPORATIVA? 41
Larissa Lotufo, Leandro Bissoli e Rafael Siqueira

5.1 Sistema de Gestão de Segurança da Informação (SGSI) 41
5.2 Normas gerais de segurança da informação 44
5.2.1 ISO 27000 46
5.2.2 *NIST Cybersecurity Framework* – componentes 48

5.3 Normas específicas de segurança da informação 51
5.4 Código de ética 51
5.5 Código de conduta do colaborador 53
5.6 Termos de uso 54
5.7 Política de redes sociais 56
5.8 Regras sobre perfil de acesso dos usuários 59
5.9 Monitoramento e inspeção 61
5.10 BYOD 62
5.11 Comunicadores instantâneos 63
5.11.1 Análise de comunicadores instantâneos – particularidades do WhatsApp 66
5.11.2 Uso de ferramentas com sincronização entre celular e computador: WhatsApp Web e WhatsApp Desktop 66
5.11.3 *Backup* de informações – uso de diretórios em nuvem de terceiros 68
5.11.4 Análise de políticas de privacidade – dados coletados 69
5.12 Melhores práticas para acompanhamento de controles de segurança 73

6. VAZAMENTO DE INFORMAÇÕES 75
Marcos Sêmola

6.1 Gestão de riscos e vazamento de informações 75
6.1.1 Conceitos estruturantes e plano de resposta a uma crise real 75
6.2 Estratégia de gestão de riscos de segurança da informação 77
6.3 Vazamento de informações 79
6.3.1 Caso *Snowden* 80
6.3.2 *Ransomware* 81
6.4 Respostas a incidentes 82
6.4.1 Equipe 90

7. ENGENHARIA SOCIAL 95
Larissa Lotufo

7.1 Pessoas: o elo fraco da corrente (ainda) 95

8. ESTRATÉGIAS DE LEGÍTIMA DEFESA DIGITAL: QUAL O LIMITE? ... 103
Henrique Rocha

8.1 Da legítima defesa digital e suas limitações ... 103
8.1.1 Considerações sobre a legítima defesa ... 104
8.1.2 Breves considerações acerca do *ethical hacking* e da legítima defesa digital ... 108
8.2 As possíveis implicações quando do manejo de medidas de legítima defesa digital ... 113
Conclusão ... 115

9. ANÁLISE DE VULNERABILIDADES ... 117
Leandro Bissoli e Rafael Siqueira

9.1 Cuidados ao realizar/contratar análise de vulnerabilidades ... 117
9.2 Considerações quanto à contratação de testes de vulnerabilidades executados por parceiros de negócio ... 118
9.2.1 Autorização ... 119
9.2.2 Escopo e dever de aviso ... 119
9.2.3 Acesso a conteúdos ... 120
9.2.4 Danos, controle de danos e indenização ... 120
9.2.5 Equipe técnica ... 121
9.2.6 Território dos testes ... 122
9.2.7 Regulação setorial ... 122
9.2.8 Regulação por tipo de serviço ... 124
9.2.9 Proteção à privacidade e proteção de dados pessoais ... 125
9.2.10 Propriedade das informações ... 127
9.2.11 Engenharia social ... 127
9.2.12 Produtos finais e cronograma do projeto ... 129
9.3 Áreas envolvidas ... 130
Conclusão ... 131

10. TERCEIRIZADOS: COMO LIDAR? ... 133
Cristina Sleiman e Larissa Lotufo

10.1 Vulnerabilidade empresarial ... 133
10.2 Contextualização legal e mercadológica ... 136

10.2.1 Reputação vale "ouro" 140
10.2.2 Segurança da informação 141
10.3 Supervisão e fiscalização 142
10.3.1 NDA (*Non-Disclosure Agreement*) – "Acordo de Confidencialidade" 142
10.3.2 Proteção de dados pessoais e a terceirização 142

11. IOT, INTELIGÊNCIA ARTIFICIAL E *SMART CITIES* 149
Cristina Sleiman, Larissa Lotufo e Marcos Tupinambá

11.1 Para onde vamos (ou já estamos)? 149
11.2 Entendendo cada tecnologia e suas especificidades 153
11.2.1 IoT – *Internet of Things* (internet das coisas) 153
11.2.1.1 IoT – Segurança 155
11.2.2 Inteligência artificial 156
11.2.3 *Smart cities* 157
11.2.3.1 *Smart cities* – segurança da informação, privacidade e continuidade dos negócios 157
11.2.3.2 Riscos da IoT, *smart cities* e inteligência artificial 159
11.2.4 *Machine learning* – reprodução de preconceitos e injustiças sociais 159
11.2.4.1 *Machine learning* – perda de controle 159
11.3 Aspectos e considerações jurídicas acerca das novas tecnologias 160
11.3.1 Proteção de dados pessoais 165
11.4 Cuidados em segurança gerais em IOT, IA e *smart cities* 170

12. *SECURITY BY INFORMATION*, UM ENSAIO SOBRE O FUTURO ... 175
Marcos Sêmola

12.1 Segurança digital na sociedade da informação líquida 175
12.2 *Security by information for information* 180

CONSIDERAÇÕES FINAIS 181
Patricia Peck Pinheiro

REFERÊNCIAS BIBLIOGRÁFICAS 183

ANEXOS 195
ANEXO 1 – Modelos de Documentos 195
ANEXO 2 – "Patente: US4405829A" 239
ANEXO 3 243