



UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FABIANA FIGUEIRA SANCHES FLORES

DESENVOLVIMENTO ÉTICO DE *SOFTWARE*:

A impossibilidade de desconsideração da Segurança Computacional na produção de *software* e a premência de mudança na conduta da Indústria, da Academia e dos desenvolvedores

Recife
2019

FABIANA FIGUEIRA SANCHES FLORES

DESENVOLVIMENTO ÉTICO DE *SOFTWARE*:

A impossibilidade de desconsideração da Segurança Computacional na produção de *software* e a premência de mudança na conduta da Indústria, da Academia e dos desenvolvedores

Este trabalho foi apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Doutor em Ciência da Computação.

Área de concentração: Engenharia de *Software*

Orientador(a): Silvio Romero de Lemos Meira

Recife

2019

Catálogo na fonte
Bibliotecária Mariana de Souza Alves CRB4-2105

F634d Flores, Fabiana Figueira Sanches

Desenvolvimento Ético de Software: a impossibilidade de
desconsideração da Segurança Computacional na produção de software
e a premência de mudança na conduta da Indústria, da Academia e dos
desenvolvedores/ Fabiana Figueira Sanches Flores – 2019.

353 f., fig., tab.

Orientador: Silvio Romero de Lemos Meira.

Tese (Doutorado) – Universidade Federal de Pernambuco. CIn,
Ciência da Computação. Recife, 2019.

Inclui referências, apêndices e anexos.

1. Engenharia de Software. 2. Ética. 3. Segurança. 4.
Responsabilidade. I. Meira, Silvio Romero de Lemos (orientador). II.
Título.

005.1

CDD (22. ed.)

UFPE-MEI 2019-168

Fabiana Figueira Sanches Flores

“DESENVOLVIMENTO ÉTICO DE SOFTWARE: A impossibilidade de desconsideração da Segurança Computacional na produção de software e a premência de mudança na conduta da Indústria, da Academia e dos desenvolvedores”

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Doutor em Ciência da Computação.

Aprovado em: 13/09/2019.

Orientador: Prof. Dr. Silvio Romero de Lemos Meira

BANCA EXAMINADORA

Profª. Dra. Ana Carolina Brandão Salgado
Centro de Informática/UFPE

Prof. Dr. Vinicius Cardoso Garcia
Centro de Informática/UFPE

Prof. Dr. Sergio Castelo Branco Soares
Centro de Informática/UFPE

Prof. Dr. Leandro Marques do Nascimento
Departamento de Computação/UFRPE

Prof. Dr. Felipe Silva Ferraz
CESAR School

Prof. Dr. Marcus Vinícius Dantas Linhares
Pós-Graduação em Gestão Estratégica de Mercado/IFPI

***In memoriam* do eterno incentivador de projetos,
o Dr. Paulo Nunes Meireles**

AGRADECIMENTOS

Para a realização deste estudo, diversas pessoas concorreram direta e indiretamente, razão pela qual agradeço a todos os que, de alguma forma, fomentaram minha busca por conhecimento, registrando, em particular minha especial gratidão:

a Evandro Curvelo Hora, por sua solicitude, disponibilidade, diligência, paciência e inúmeras recomendações quando da realização deste estudo;

à Tempest Security Intelligence, pela gratuita cessão de amostra de dados reais de análises de segurança, insumo essencial à produção deste trabalho;

a Marco Carnut (Kiko), por sugestões iniciais relativas à temática da pesquisa;

ao Des. Federal Paulo Machado Cordeiro, por seu incentivo à participação em determinadas atividades do Doutorado;

aos voluntários que, anonimamente, cederam parte de seu tempo respondendo questionários em *survey* utilizado na investigação;

ao solícito e diligente orientador desta pesquisa, o Professor Dr. Silvio Romero de Lemos Meira, por sua contínua atenção, acessibilidade, disponibilidade e gentileza durante toda a minha experiência no Doutorado e na produção deste trabalho.

“Where there is great Power there is great Responsibility”

Winston Churchill (GREAT BRITAIN, 1906)

RESUMO

Devido ao advento da Internet e à massiva produção de sistemas embarcados no presente, há, literalmente, *software* em todos os lugares. Na sociedade atual, esta irreversível onipresença do *software* impacta na vida das pessoas e empreendimentos em uma forma inédita, tendo feito com que o desenvolvimento de *software* e a Indústria de *Software* atingissem um nível de importância sem precedentes. Embora a Indústria de *Software* tenha crescido em relevância e evoluído muito nas últimas décadas, dados empíricos sugerem que algumas de suas práticas podem apresentar uma faceta preocupante, especialmente quando considerados a Segurança, a forma com que este atributo é considerado ao longo do desenvolvimento do *software* e um procedimento usual adotado para evasão de responsabilidade pelo que se produz: a definição de *End User License Agreements* e de *Terms of Services*, documentos nos quais são feitas exclusões e limitações de responsabilidade, bem como a difusão da ideia de que o *software* é oferecido no “estado em que se encontra”. Pretendendo-se examinar estas condutas, foi realizada a investigação ora relatada nesta Tese com foco na obtenção de respostas às seguintes perguntas de pesquisa: Qual é, atualmente, a expressividade das vulnerabilidades de segurança em *software*? Existem fatores que contribuem para a insegurança no *software*? É possível se associar preterição dos Requisitos de Segurança em favor dos Requisitos Funcionais ao longo dos processos de desenvolvimento de *software*? Os desenvolvedores em geral têm um conhecimento formal mínimo sobre Segurança Computacional e sobre Segurança no *software*? O que a Indústria de *Software* tem feito relativamente à Segurança? Está a Indústria de *Software* tentando se evadir à responsabilidade por falhas de Segurança no *software* que produz, condicionando o uso dos seus produtos/serviços à irrestrita aceitação de cláusulas unilaterais de exclusão/limitação de responsabilidade em *End User License Agreements* e *Terms of Services*? Se a Indústria de *Software* estiver se furtando à responsabilidade pelo que produz, é possível a sua responsabilização no Direito Civil? Se as cláusulas em *End User License Agreements* e *Terms of Services* puderem ser tidas como legais, é possível as considerar antiéticas? A Indústria de *Software* e os desenvolvedores de *software* agem eticamente quando lidam com os Requisitos de Segurança? Que consequências podem resultar, para o público em geral e para a própria Indústria de *Software*, da consolidação de um estado de insegurança relativamente ao *software*? Há algo que possa ser feito para se evitar a consolidação referida? Para se responder a estas perguntas de pesquisa, foi delineado um pragmático estudo quantiquantitativo. Formado um referencial teórico, realizaram-se coletas primárias e secundárias de dados. Partindo-se de uma amostra de dados reais de *pentesting* obtida junto a uma empresa de Segurança Computacional, de entrevistas, de *surveys* e de análise documental, construiu-se um panorama geral sobre a segurança atual no *software*, apresentando-se reflexões sobre a significância dos números obtidos para a Engenharia de *Software*, para a Academia, para a Indústria de *Software* e para a sociedade civil. Após a exposição referida, fez-se uma proposta para a superação das potenciais nocivas consequências da Crise de Segurança no *Software*, apresentando-se comentários finais.

PALAVRAS-CHAVE: *Software*. Engenharia. Segurança. Responsabilidade. Ética.

ABSTRACT

Due to the advent of the Internet and to the massive production of embedded systems at present, there is, literally, software everywhere. In nowadays society, this irreversible omnipresence of software impacts people's lives and enterprises in an *inedita* way, making the software development and the Software Industry to reach an unprecedented level of importance. Although the Software Industry has grown in relevance and evolved a lot in the last decades, empirical data suggest that some of its practices may have a very worrisome aspect, specially when considered Security, the way in which this attribute is dealt during software development and an usual procedure adopted for evading the responsibility/liability by what it is produced: the definition of End User License Agreements and Terms of Services, documents in which there are liability exclusions and limitations, as well as the diffusion of the idea that the software is provided as it is. Intending to examine these conducts, it was done the inquiry exposed in this thesis with the purpose of obtaining answers to the following research questions: What is the expressiveness of security vulnerabilities in software nowadays? Are there factors that contribute to insecurity in software? Is it possible to associate a preterition in Security Requirements in favor of Functional Requirements during software development processes? Do developers in general have a minimal formal knowledge about Computational Security and about Security in software? What does the Software Industry have done about Security? Is the Software Industry trying to evade its liability by Security fails in the software it produces, conditioning the use of its products/services to the unrestricted acceptance of liability exclusion/limitation clauses that it creates unilaterally in End User License Agreements and Terms of Services? If the Software Industry is evading the liability for what it produces, is it possible its responsabilization by Civil Law? If the clauses in the End User License Agreements and Terms of Services can be reputed legal, is it possible to consider them antiethical? Do Software Industry and software developers act ethically when they deal with Security Requirements? Which consequences can result, for the general public and for the Software Industry itself, from the consolidation of a state of insecurity in software? Is there anything that can be done for avoiding the referred consolidation? For answering these research questions, it was designed a pragmatic quantitative and qualitative study. Built a theoretical background, primary and secondary data gathering were done. Starting with a pentesting sample obtained from real data of a Security Intelligence Company, interviews, surveys and documental analysis, it was constructed an overview about software security nowadays, presenting reflexions about the significance of the number obtained in the mentioned overview to the Software Engineering, to the Academy, to the Software Industry and to the general society. After the exposition referred, it was made a proposal for overcoming the potential nocive consequences of the Crisis of Security in Software, presenting final comments.

KEYWORDS: Software. Engineering. Security. Liability. Ethics.

LISTA DE FIGURAS

Figura 1 - Etapas da investigação relatada	32
Figura 2 - Detalhamento do fluxo de atividades da investigação	33
Figura 3 - Classificação dos <i>softwares</i> quanto à espécie de destinatários-alvos	37
Figura 4 - Categorias de atividades voltadas à produção de <i>software</i> ..	39
Figura 5 - Modelos de processos de desenvolvimento de <i>software</i>	41
Figura 6 - Atributos em <i>softwares</i>	44
Figura 7 - Espécies de riscos	61
Figura 8 - Categorias de atividades de gestão de riscos.....	65
Figura 9 - Ciclo de ações para a gestão de riscos.....	66
Figura 10 - Diagrama de atividades representativo de ações diante de riscos.....	67
Figura 11 - Classificação dos planos de resposta a riscos.....	68
Figura 12 - Foco da Segurança Computacional	73
Figura 13 - Objetos da Segurança Computacional.....	75
Figura 14 - Objetos da Segurança Computacional.....	76
Figura 15 - Classificação das vulnerabilidades quanto ao objeto sobre o qual recaem	77
Figura 16 - Classificação das vulnerabilidades de segurança quanto ao nível de seus impactos potenciais para uma organização	79
Figura 17 - Classificação das ameaças quanto à intencionalidade em sua manifestação	81
Figura 18 - Categorias de atacantes a sistemas computacionais	83
Figura 19 - Motivação dos atacantes de sistemas computacionais.....	85
Figura 20 - Critérios de classificação de ataques à segurança	86
Figura 21 - Agrupamento adicional dos ataques ativos e passivos	90
Figura 22 - Variações de ataques superficiais.....	91
Figura 23 - Categorias de ameaças e ataques respectivos.....	93
Figura 24 - Etapas gerais dos ataques à Segurança Computacional.....	94
Figura 25 - Estratégias e técnicas de coleta de informações	95
Figura 26 - Gerenciamento atual da Segurança em sistemas computacionais	101
Figura 27 - Processos do gerenciamento de Segurança em sistemas computacionais	101
Figura 28 - Abordagens de Segurança.....	102
Figura 29 - Delineamento de estratégias de Segurança Computacional.	104
Figura 30 - Princípios norteadores do delineamento e da implantação de estruturas de Segurança Computacional	106
Figura 31 - Estruturação da Segurança Computacional.....	109
Figura 32 - Aspectos relevantes às políticas de segurança	111
Figura 33 - Pilares de sustentação das políticas de segurança	112
Figura 34 - Agentes atuantes na construção das políticas de segurança	113
Figura 35 - Triangulação em ambientes cooperativos.....	118
Figura 36 - Recursos para divulgação de políticas de segurança	119
Figura 37 - Elementos usuais dos documentos refletivos das políticas de segurança	122

Figura 38 - Elementos empregados na implementação da Segurança Computacional.....	123
Figura 39 - Categorias macroscópicas de condutas causadoras de danos e geradoras de responsabilidade.....	128
Figura 40 - Condutas e volitividade.....	129
Figura 41 - Classificação da responsabilidade	131
Figura 42 - Transmutação de obrigações na responsabilidade civil	134
Figura 43 - Pressupostos principais da responsabilidade civil.....	134
Figura 44 - Conjunto ampliado de pressupostos da responsabilidade civil.....	135
Figura 45 - Eventos configuradores de fato antijurídico.....	136
Figura 46 - Objetos de incidência do dano	137
Figura 47 - Classificação dos danos quanto à natureza do objeto afetado.....	138
Figura 48 - Espécies de dano moral	138
Figura 49 - Classificação dos danos quanto ao cabimento de indenização	140
Figura 50 - Atributos do dano indenizável.....	141
Figura 51 - Teorias embasadoras do nexo causal.....	142
Figura 52 - Teorias embasadoras da responsabilidade civil	144
Figura 53 - Atributos de conduta reveladores da culpa do agente causador do dano.....	149
Figura 54 - Elementos da culpa	150
Figura 55 - Classificação da culpa em função da origem do dever violado	151
Figura 56 - Classificação da responsabilidade civil fundada nas teorias de base.....	153
Figura 57 - Fenômenos de exclusão e mitigação da responsabilidade civil.....	155
Figura 58 - Descumprimento de dever jurídico e sanção.....	160
Figura 59 - Funções da sanção	161
Figura 60 - Espécies de sanção.....	161
Figura 61 - Classificação geral das sanções civis.....	162
Figura 62 - Categorias de princípios no Código de Ética IEEE/ACM para Engenharia de <i>Software</i>	171
Figura 63 - Categorias dos <i>softwares/serviços</i> em <i>software</i> considerados na pesquisa	199

LISTA DE GRÁFICOS

Gráfico 1 - Segmentos econômicos & Pontos de vulnerabilidades de segurança em <i>software</i>	178
Gráfico 2 - Segmentos & Severidade dos pontos de vulnerabilidades de segurança em <i>software</i>	179
Gráfico 3 - Pontos de vulnerabilidades & Segmentos econômicos (Dados normalizados).....	180
Gráfico 4 - Vulnerabilidades de alta severidade & Segmento econômico (Dados normalizados)	181
Gráfico 5 - Distribuição dos pontos de vulnerabilidade de segurança na camada de aplicação <i>web</i>	182
Gráfico 6 - Pontos de vulnerabilidade na camada de aplicações <i>web</i>	183
Gráfico 7 - Metodologias de desenvolvimento de <i>software</i> empregadas pelos participantes do <i>survey</i>	193
Gráfico 8 - Requisitos prevalentes nos projetos de <i>software</i>	194
Gráfico 9 - Razão de cursos de graduação sem disciplina obrigatória relacionada à Segurança	196
Gráfico 10 - Origem geográfica das empresas produtores/fornecedoras de <i>software</i>	198
Gráfico 11 - Responsabilidade nos <i>EULAs</i> e <i>ToSs</i>	203
Gráfico 12 - Responsabilidade nos <i>EULAs</i> e <i>ToSs</i>	203
Gráfico 13 - Exclusão/limitação de responsabilidade x segmento do produto/serviço	205
Gráfico 14 - Contato prévio dos desenvolvedores de <i>software</i> com algum Código de Ética.....	223
Gráfico 15 - Razão de cursos de graduação examinados com disciplinas obrigatórias relacionadas à Ética	226

LISTA DE QUADROS

Quadro 1 - Delineamento geral da pesquisa	31
Quadro 2 - Classificação dos <i>softwares</i> quanto à espécie de destinatários-alvos	38
Quadro 3 - Categorias de atividades voltadas à produção de <i>software</i> .	40
Quadro 4 - Modelos de processos de desenvolvimento de <i>software</i>	42
Quadro 5 - Atributos em <i>softwares</i>	45
Quadro 6- Explorações de falhas de segurança em <i>software</i> destacadas pela mídia ao longo da última década em razão de suas expressividades (vulto de usuários/empreendimentos afetados e repercussões financeiras diretas)	48
Quadro 7 - Espécies de riscos	62
Quadro 8 - Critérios de classificação dos riscos.....	63
Quadro 9 - Planos de reposta a riscos	69
Quadro 10 - Focos e objetivos da proteção almejada com a Segurança Computacional	74
Quadro 11 - Vulnerabilidades associadas à confidencialidade, integridade e disponibilidade	77
Quadro 12 - Vulnerabilidades, seus objetos e potenciais repercussões exemplificativas	78
Quadro 13 - Classificação das vulnerabilidades de segurança quanto ao nível de seus impactos potenciais para uma organização ...	79
Quadro 14 - Categorias de ameaças em função de suas potenciais consequências	81
Quadro 15 - Categorias de atacantes a sistemas computacionais.....	83
Quadro 16 - Classificação dos ataques de segurança	87
Quadro 17 - Categorias de ataques ativos e passivos	90
Quadro 18 - Variações de ataques superficiais.....	92
Quadro 19 - Estratégias e técnicas de coleta de informações	96
Quadro 20 - Falhas de segurança identificadas com <i>scanners</i> de vulnerabilidades	99
Quadro 21 - Abordagens de Segurança.....	103
Quadro 22 - Delineamento de estratégias de Segurança Computacional	104
Quadro 23 - Princípios norteadores do delineamento e da implantação de estruturas de Segurança Computacional	107
Quadro 24 - Estruturação da Segurança Computacional	109
Quadro 25 - Pilares de sustentação das políticas de segurança.....	112
Quadro 26 - Contribuições dos partícipes na construção de políticas de segurança.....	114
Quadro 27 - Níveis de compreensão e detalhamento das políticas de segurança.....	116
Quadro 28 - Políticas de segurança	117
Quadro 29 - Elementos empregados na implementação da Segurança Computacional	124
Quadro 30 - Categorias macroscópicas de condutas causadoras de danos e geradoras de responsabilidade.....	129
Quadro 31 - Condutas e volitividade	130

Quadro 32 - Classificação da responsabilidade.....	131
Quadro 33 - Espécies de dano moral	139
Quadro 34 - Teorias embasadoras do nexo causal	143
Quadro 35 - Teorias embasadoras da responsabilidade civil	146
Quadro 36 - Classificação da culpa em função da gradação da falta cometida	150
Quadro 37 - Culpa & ônus da prova	151
Quadro 38 - Classificação da culpa quanto à conduta do agente causador do dano	152
Quadro 39 - Classificação da responsabilidade civil fundada nas teorias de base	153
Quadro 40 - Fenômenos interferentes na responsabilidade civil	157
Quadro 41 - Espécies de sanção.....	162
Quadro 42 - Ramos da Ética	168
Quadro 43- Vulnerabilidades de Segurança mais frequentes na camada de aplicações de acordo com o <i>OWASP</i>	185
Quadro 44- Plano de ação mínimo para o tratamento do problema da insegurança no <i>software</i>	233
Quadro 45- Repercussões da manutenção da postura atual da Indústria de <i>Software</i> e de seus agentes em relação à Segurança Computacional.....	256
Quadro 46- Extrato das respostas às perguntas de pesquisa da investigação relatada	262

LISTA DE TABELAS

Tabela 1 -	Pontos de vulnerabilidade na camada de aplicação <i>web</i>	182
Tabela 2 -	Origem geográfica das empresas produtoras/fornecedoras de <i>software</i>	197
Tabela 3 -	Distribuição dos <i>softwares</i> /serviços em <i>software</i> considerados no estudo em função da livre taxonomia adotada	199
Tabela 4 -	Domínios dos aplicativos/utilitários considerados cujos <i>EULAs/ToSs</i> foram considerados na pesquisa	200
Tabela 5 -	Domínios dos serviços <i>web</i> cujos <i>EULAs/ToSs</i> foram considerados no estudo	202
Tabela 6 -	Responsabilidade nos <i>EULAs/ToSs</i>	202
Tabela 7 -	Exclusão/limitação de responsabilidade x segmento do produto/serviço.....	204
Tabela 8 -	Disciplinas obrigatórias com conteúdo relativo à Ética em cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação	225

LISTA DE ABREVIATURAS E SIGLAS

ABET	Accreditation Board for Engineering and Technology
ABNT	Associação Brasileira de Normas Técnicas
ACLs	Access Control Lists
ACSE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
AICHE	American Institute of Chemical Engineers
APIs	Application Programming Interfaces
BSI Group	British Standard Group
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CBSE	Component-Based Software Engineering
CIn/UFPE	Centro de Informática da Universidade Federal de Pernambuco
CVSS	Common Vulnerability Scoring System
DNS	Domain Name System
EULA	End User License Agreement
EULAs	End User License Agreements
FTP	File Transfer Protocol
HIDS	Host-Based Intrusion Detection System/Host-Based Prevention System
Hybrid IDS	Hybrid Intrusion Detection System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineering
IEC	International Electrotechnical Commission
IIS	Internet Information Services
IP	Internet Protocol
ISO	International Organization for Standardization
KIS	Keep it Simple
LAN	Local Area Network
LGPD	Lei Geral de Proteção de Dados Pessoais
LM	LAN Manager

LPD	Line Printer Daemon
MDAC	Microsoft Data Access Components
MVP	Minimum Viable Product
NetBIOS	Network Basic Input/Output System
NIDS	Network-Based Intrusion Detection System/Network-Based Prevention System
NSPE	National Society of Professional Engineers
OPM	Office of Personal Management
OWASP	Open Web Application Security Project
PDF	Portable Document Format
RPC	Remote Procedure Calls
SAT	Seguro contra Acidentes do Trabalho
SBC	Sociedade Brasileira de Computação
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
ToS	Terms of Service
ToSs	Terms of Services
UDP	User Datagram Protocol
UFPE	Universidade Federal de Pernambuco
UML	Unified Modeling Language
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-Site Scripting

SUMÁRIO

1	INTRODUÇÃO	29
2	SOFTWARE	37
2.1	DEFINIÇÃO	37
2.2	CLASSIFICAÇÃO	37
2.3	PRODUÇÃO	38
2.3.1	Atividades	38
2.3.2	Processo	40
2.4	ATRIBUTOS ALMEJADOS	43
3	RISCOS	61
3.1	NOTAS GERAIS	61
3.2	RISCOS NA PRODUÇÃO/FORNECIMENTO DE <i>SOFTWARE</i>	70
4	SEGURANÇA	73
4.1	DEFINIÇÃO E OBJETOS	73
4.2	VULNERABILIDADES	76
4.2.1	Definição	76
4.2.2	Espécies	76
4.3	AMEAÇAS	80
4.3.1	Definição	80
4.3.2	Espécies	80
4.4	ATAQUES	82
4.4.1	Definição	82
4.4.2	Agentes	82
4.4.3	Classificação	85
4.4.4	Planejamento e execução de ataques	93
4.4.4.1	Coleta de informações	94
4.4.4.2	Planejamento	99
4.4.4.3	Execução	99
4.4.5	Resultados potenciais dos ataques	100
4.5	GERENCIAMENTO DA SEGURANÇA EM SISTEMAS COMPUTACIONAIS	100
4.5.1	Abordagens de Segurança	102
4.5.2	Delineamento da estratégia de Segurança	103
4.5.3	Princípios fundamentais de Segurança	105
4.5.4	Objetos da Segurança Computacional	108
4.5.4.1	Políticas de Segurança	110
4.5.4.2	Técnicas, procedimentos e recursos	123
5	RESPONSABILIDADE POR DANOS	127
5.1	CONSIDERAÇÕES PRELIMINARES	127
5.2	RESPONSABILIDADE CIVIL	133
5.2.1	Definição e justificativa	133
5.2.2	Pressupostos	134
5.2.2.1	Antijuridicidade do fato	135
5.2.2.2	Dano	137
5.2.2.3	Nexo de causalidade	142
5.2.2.4	Fator de imputação	144
5.2.3	Teorias	144
5.2.3.1	Notas adicionais sobre a culpa na Teoria da Responsabilidade	

	Subjetiva.....	149
5.2.4	Espécies.....	152
5.2.5	Exclusão e mitigação da responsabilidade civil.....	155
5.2.6	Sanções.....	160
5.2.6.1	Breves comentários sobre indenizações	163
5.2.7	Regresso	164
5.2.8	Transferência da responsabilidade civil	164
5.3	RESPONSABILIDADE CIVIL POR DANOS DECORRENTES DA EXPLORAÇÃO DE VULNERABILIDADE DE SEGURANÇA EM <i>SOFTWARE</i>	165
6	ÉTICA PROFISSIONAL.....	167
6.1	CONSIDERAÇÕES PRELIMINARES	167
6.2	CÓDIGOS DE ÉTICA PROFISSIONAL.....	168
6.3	CÓDIGO DE ÉTICA IEEE/ACM PARA ENGENHARIA DE <i>SOFTWARE</i>	170
7	PANORAMA ATUAL DA SEGURANÇA EM <i>SOFTWARE</i>	175
7.1	ENGENHARIA OU NÃO ENGENHARIA? EIS AINDA A QUESTÃO	177
7.2	ALGO DE PODRE NO REINO DA INDÚSTRIA DE <i>SOFTWARE</i>	191
7.3	MUITO BARULHO POR NADA	210
8	SEGURANÇA & DESENVOLVIMENTO ÉTICO DE <i>SOFTWARE</i>	221
8.1	HOUSTON, NÓS PODEMOS TER UM PROBLEMA.....	221
8.2	PROPOSIÇÃO PARA O DESENVOLVIMENTO ÉTICO DE <i>SOFTWARE</i> NO TOCANTE À SEGURANÇA COMPUTACIONAL	228
9	CONCLUSÕES E CONSIDERAÇÕES FINAIS.....	249
	REFERÊNCIAS.....	267
	APÊNDICE A - DIRETRIZES PARA O MAPEAMENTO SISTEMÁTICO.....	293
	APÊNDICE B - DIRETRIZES PARA O LEVANTAMENTO E A ANÁLISE DE <i>EULAS/TOSS</i>.....	295
	APÊNDICE C - MODELO DE QUESTIONÁRIO DE SONDAGEM DE PERCEPÇÕES QUANTO AOS REQUISITOS DE SEGURANÇA EM <i>SOFTWARE</i> E À RESPONSABILIDADE GERAL PELO <i>SOFTWARE</i>.....	297
	APÊNDICE D - MODELO DE QUESTIONÁRIO DE AVALIAÇÃO DO PRÉVIO CONTATO DE DESENVOLVEDORES DE <i>SOFTWARE</i> COM CÓDIGOS DE ÉTICA.....	315
	APÊNDICE E – PLANO DA PRIMEIRA ENTREVISTA INFORMAL COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO.....	317
	APÊNDICE F – PLANO DA SEGUNDA ENTREVISTA INFORMAL COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO.....	319
	APÊNDICE G - PLANO DE ENTREVISTA TELEFÔNICA INFORMAL COM PESSOA DESENVOLVEDORA DE SOLUÇÕES EM <i>BUSINESS INTELLIGENCE</i>.....	321
	APÊNDICE H - DIRETRIZES PARA O LEVANTAMENTO E A	

ANÁLISE DA DOCUMENTAÇÃO RELATIVA ÀS GRADES CURRICULARES DOS CURSOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO DE INSTITUIÇÕES BRASILEIRAS DE ENSINO	323
APÊNDICE I - DIRETRIZES PARA A ANÁLISE DA AMOSTRA DE DADOS DE <i>PENTESTS</i> OBTIDA JUNTO A EMPRESA DE SEGURANÇA COMPUTACIONAL	325
APÊNDICE J - RELAÇÃO ALFABÉTICA DAS INSTITUIÇÕES DE ENSINO CUJOS CURSOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO FORAM CONSIDERADOS NO ESTUDO	327
APÊNDICE K - RELAÇÃO ALFABÉTICA DOS <i>SOFTWARES/SERVIÇOS</i> EM <i>SOFTWARE</i> CUJOS <i>EULAS/TOSS</i> FORAM EXAMINADOS NA PESQUISA	329
APÊNDICE L - RELAÇÃO ALFABÉTICA DAS EMPRESAS PRODUTORAS/FORNECEDORAS DE <i>SOFTWARE/SERVIÇOS</i> EM <i>SOFTWARE</i> CUJOS <i>EULAS/TOSS</i> FORAM EXAMINADOS NA PESQUISA	335
APÊNDICE M - RELAÇÃO ALFABÉTICA DAS EMPRESAS PRODUTORAS/FORNECEDORAS DE <i>SOFTWARE/SERVIÇOS</i> EM <i>SOFTWARE</i> E DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS <i>EULAS/TOSS</i> FORAM CONSIDERADOS NA INVESTIGAÇÃO..	337
ANEXO A - REPRODUÇÃO DE DISCUSSÃO ATINENTE A <i>EULAS</i> E <i>TOSS</i> EM <i>FORUM WEB</i> DE USO CORRENTE POR DESENVOLVEDORES DE JOGOS	341
ANEXO B - CÓDIGO DE ÉTICA IEEE/ACM PARA ENGENHARIA DE <i>SOFTWARE</i>	345

1 INTRODUÇÃO

O advento da Internet e a difusão de sistemas embarcados mudaram as vidas das pessoas e os modos com que indivíduos e companhias se conectam e se relacionam (BORGIA, 2014) (BAJARIN, 2014).

Com efeito, tem-se, hoje, um momento único na história humana, em que a global interconexão de *software* ubíquo constitui-se uma realidade inédita, não se vislumbrando, por ora, a possibilidade de retrocesso na difusão e no emprego de sistemas computacionais globais, de modo que, em paráfrase a um conhecido brocardo jurídico (*Ubi homo ibi societas; ubi societas, ibi jus*), poderia ser dito, sem pleonismo ou hipérbole, algo como: *Ubi homo ibi societas; ubi societas, ibi software*.

Muitas facilidades e vantagens adviram desta nova era de interconexão e ubiquidade, mas riscos e ameaças também emergiram, especialmente nos domínios da Segurança. De fato, se o *software* é ubíquo e se “tudo é *software*” (MEIRA, 2008), há riscos e ameaças em todos os lugares. Embora esta onipresença leve, por lógica, à conclusão de que é relevante o tratamento dos Requisitos de Segurança nos processos de desenvolvimento que resultem em algum tipo de *software*, dados empíricos indicam que a Indústria caminha em direção diversa.

Violações de segurança, roubos de dados e outros crimes cibernéticos estão constantemente na imprensa. Ao mesmo tempo, a Indústria de Segurança cresce e a Indústria Geral de *Software* parece tentar se ver livre de quaisquer responsabilidades por danos resultantes de erros e falhas de Segurança, condicionando o uso do que produz/fornece à irrestrita prévia aceitação de questionáveis disposições de documentos que elabora unilateralmente, conhecidos como *End User License Agreements (EULAs)* e *Terms of Service (ToSs)*.

Para se examinar a (im)propriedade da conduta referida, realizou-se a investigação condensada na presente Tese. Os seguintes questionamentos foram eleitos como perguntas de pesquisa:

Que proporções assumem as vulnerabilidades de Segurança em softwares atualmente?

Que fatores concorrem para a insegurança do software?

É possível se associar a existência de vulnerabilidades de Segurança a uma preterição dos Requisitos de Segurança em favor dos Requisitos Funcionais durante o processo de desenvolvimento de software?

Os desenvolvedores de software têm, no geral, um conhecimento formal mínimo sobre Segurança Computacional e sobre Segurança em software?

O que a Indústria de Software tem feito no tocante à questão da Segurança?

Está a Indústria de Software tentando se furtar à responsabilidade pela Segurança do que produz, valendo-se, para isso, do condicionamento do uso de seus produtos/serviços à irrestrita aceitação das condições unilaterais de isenção/limitação de responsabilidade constantes, usualmente, de EULAs e ToSs?

Caso a Indústria de Software esteja se furtando à responsabilidade pelo que produz, é possível sua responsabilização na esfera civil¹?

Caso se considerem legalmente válidas as disposições excludentes e limitantes de responsabilidade dos EULAs e ToSs, pode-se cogitar da persistência de um viés antiético?

Agem eticamente a Indústria e os desenvolvedores de software, ao lidar com os requisitos de Segurança?

Que repercussões nocivas podem decorrer da consolidação de um estado de insegurança de software para a sociedade em geral e para a própria Indústria de Software?

Há algo a ser feito para se evitar a consolidação citada?

Em outras palavras, com a pesquisa ora relatada, almejou-se conceber:

- panorama atual da Segurança Computacional relativamente ao *software*;
- *status* presente do tratamento dispensado à segurança em *software*;
- avaliação da (in)admissibilidade do tratamento mencionado, considerados o Direito Civil e a Ética;
- proposição inicial para reforma da postura atual quanto à questão da segurança em *software*.

¹ Optou-se, no estudo ora relatado, por analisar o problema apenas sob a ótica da Ética e do Direito Civil, a despeito de ser possível e viável sua apreciação sob outras perspectivas, como a do Direito Penal. A opção em debate foi feita em função da anuência do pesquisador com o reconhecimento, na Doutrina brasileira, de que o Direito Penal apresenta, no ordenamento pátrio, um caráter fragmentário, residual e excepcional, devendo ser acionado apenas em casos extremos, quando a resposta a ser dada por outro ramo do Direito não se mostre suficiente à defesa do bem jurídico ameaçado/violado. Em caso de interesse a respeito deste caráter e desta natureza do Direito Penal, recomenda-se a leitura de Bitencourt (2018) e Sanches Cunha (2019).

Com foco nas perguntas de pesquisa mencionadas e na obtenção dos resultados esperados, delineou-se a investigação como exposto no Quadro 1:

Quadro 1 – Delineamento geral da pesquisa.

DELINEAMENTO GERAL DA PESQUISA	
ELEMENTO METODOLÓGICO	ELEIÇÃO FEITA PARA A PESQUISA
ASSUNÇÃO FILOSÓFICA	• Pragmatismo
PARADIGMA DE INVESTIGAÇÃO	• Quantitativo
BASES LÓGICAS PARA PRODUÇÃO DE INFERÊNCIAS	• Análise • Síntese • Dedução • Indução
ESPÉCIES DE COLETAS DE DADOS	• Primária • Secundária
INSTRUMENTOS DE COLETA DE DADOS	• Levantamento bibliográfico não sistemático • Mapeamento sistemático • Aplicação de questionários • Realização de entrevistas informais • Observação • <i>Pentesting</i>² • Levantamento não sistemático de <i>EULAs</i> e <i>ToS</i> • Levantamento sistemático de documentação relativa a cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação • Estudo retrospectivo do desenvolvimento de uma solução de <i>Business Intelligence</i>
INSTRUMENTOS DE PROCESSAMENTO E ANÁLISE DE DADOS	• Codificações • Classificações • Tabulações • Cálculos estatísticos (médias e razões percentuais, especialmente) • Lógica formal • Triangulação

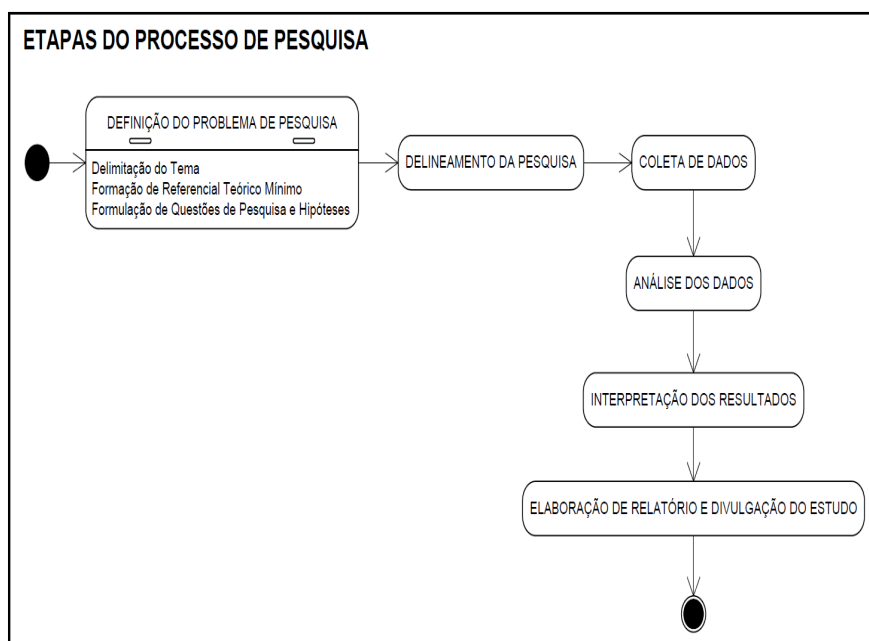
Fonte: Autor (2019) ^{3 4}.

² Em termos simplistas, pode-se dizer que os *pentests*, ou *penetration tests*, consistem em testes de avaliação e exploração de vulnerabilidades de segurança em *software* (ALLEN, 2012). Em outras palavras, os *pentests* são simulações cujo foco é a descoberta de vulnerabilidades de segurança e a sua exploração, com a produção de resultados indevidos, ou a subversão de funcionalidades ordinárias de um sistema computacional (BALOCH, 2015).

³ Quadro elaborado com o emprego das considerações metodológicas tecidas por Singh (2006), Kothari (2004) e Gray e Malins (2004).

Como se infere com o exame do Quadro 1, a investigação consistiu de um estudo pragmático e quantiquantitativo acerca do atual tratamento dispensado à Segurança em *software* e da (in)admissibilidade deste tratamento, considerados o Direito Civil e a Ética, objetivando-se a proposição de mudança de paradigma com foco na melhoria do *software* quanto à Segurança. Na Figura 1, apresenta-se macroscópica representação sintética do fluxo de atividades realizadas ao longo da investigação, sendo detalhamento seu exposto na Figura 2.

Figura 1– Etapas da investigação relatada.



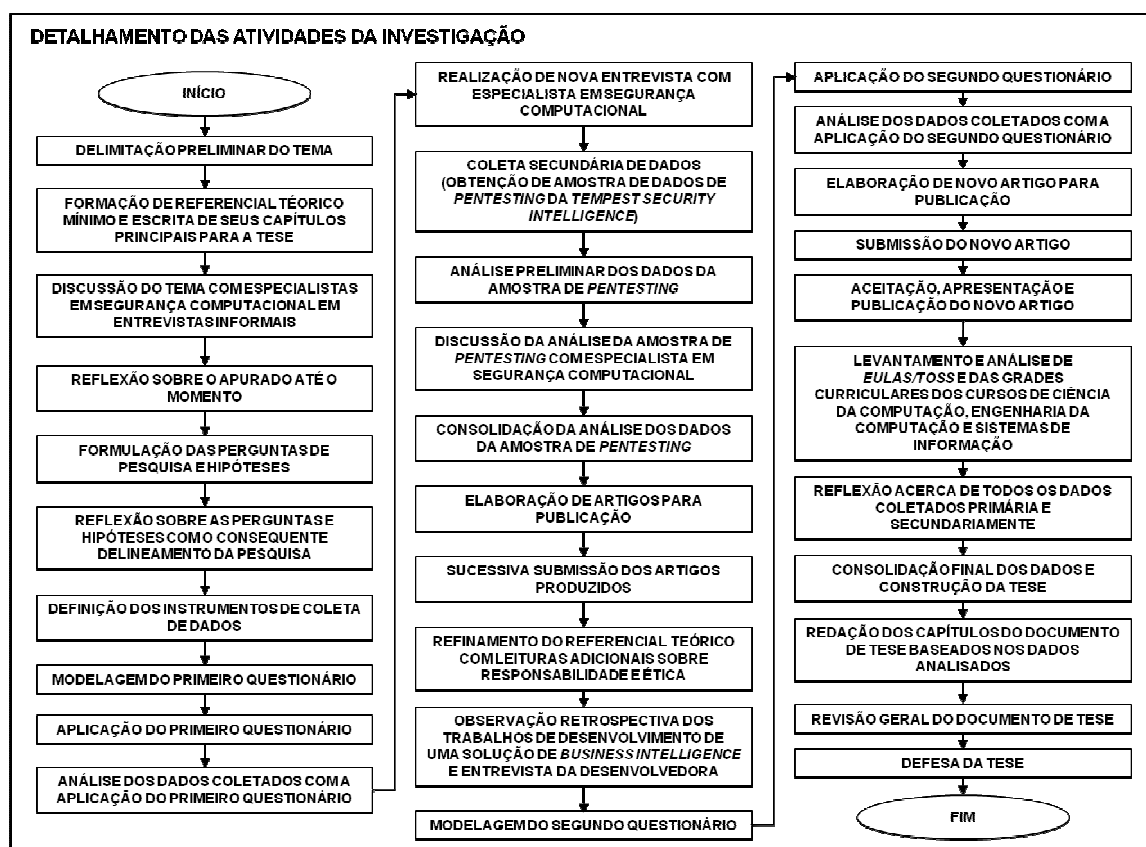
Fonte: Autor (2019) ^{5 6}.

⁴ Vale esclarecer que, a despeito de a pesquisa ter sido delineada da forma apresentada no Quadro 1, o relatório da pesquisa, em verdade, como consignado ulteriormente nesta Introdução, foi elaborado com base em ideias diversas, dada a necessidade de propiciar aos potenciais leitores uma melhor experiência com a investigação.

⁵ Representação elaborada com base nos comentários de Kothari (2004) e Gil (2002) acerca de pesquisa científica e da estratégia efetivamente definida para a condução da investigação ora relatada.

⁶ Esclarece-se, relativamente à representação produzida, que, apesar da linearidade macroscópica indicada, o processo de investigação, em verdade, acabou por ser iterativo, dada, em algumas ocasiões, a constatação da necessidade de ajustes quanto ao planejamento original. Tal se verificou, por exemplo, no tocante à aplicação de questionários, pois, após a aplicação do primeiro deles, observou-se pequena quantidade de respondentes diante do não diminuto número de perguntas feitas. Diante de tal constatação, quando da realização de coleta diversa de dados, redefiniu-se a estratégia e o modelo do segundo questionário, tornando-o uma versão extremamente enxuta com foco em maior adesão por potenciais respondentes.

Figura 2 – Detalhamento do fluxo de atividades da investigação



Fonte: Autor (2019).

Como se pode inferir do exame da Figura 2, na investigação descrita neste documento, foram realizados levantamento bibliográfico não sistemático, mapeamento sistemático (diretrizes no apêndice A), levantamento sistemático de *EULAs/ToSs* (diretrizes no apêndice B). Foram, ainda, aplicados questionários (modelos nos apêndices C e D), realizadas entrevistas informais com dois especialistas em Segurança da Informação (planos nos apêndices E e F) e com uma desenvolvedora de solução em *Business Intelligence* (roteiro de entrevista telefônica no apêndice G), conduzida avaliação retrospectiva do desenvolvimento da solução referida e registradas anotações em observações.

Fez-se, também, análise de diálogos entre desenvolvedores em fóruns *web* (anexo A) e levantamento de documentação, avaliando-se, de forma macroscópica, as grades curriculares dos cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de instituições de ensino brasileiras que também possuísem um programa de pós-graduação com

Mestrado e Doutorado. Esta delimitação da amostra foi feita com o objetivo de se obter um “panorama ideal”, verificando-se, para os cursos cujas grades foram examinadas, quais apresentavam disciplinas voltadas à Segurança Computacional e à Ética (roteiro de levantamento no apêndice H).

Como dados vitais à pesquisa, especial destaque merecem, finalmente, os essenciais dados obtidos junto à *Tempest Security Intelligence*, empresa brasileira com atuação internacional que, gentilmente, cedeu amostra de dados relativos a *Pentests* por ela realizados no período compreendido entre Janeiro/2013 e Junho/2018. A amostra em questão foi examinada a partir das diretrizes descritas no apêndice I, cabendo registrar que ela foi disponibilizada no estado em que se encontrava, já suprimidas informações sensíveis que, para preservação do negócio e dos clientes da própria empresa de Segurança Computacional, não poderiam ser objeto de divulgação.

Seguindo-se, então, a metodologia mencionada, conduziu-se o estudo, estando seu referencial teórico exposto nos Capítulos 2, 3, 4, 5 e 6.

No Capítulo 2, discorre-se sinteticamente sobre *software*, seus atributos e sua produção. Acerca da inclusão deste Capítulo no documento de Tese, importa esclarecer que não se desconhece o fato de que, na percepção de alguns potenciais leitores (especialmente os que atuem ou tenham atuado na Engenharia de *Software*), a apresentação de noções basilares sobre *software* e o seu desenvolvimento poderiam ser tidos como supérfluos. Ocorre, porém, que, no momento atual, em virtude da ubiquidade do *software* já referida neste texto, estes assuntos não são de interesse restrito de tal parcela potencial de leitor. *Software* e desenvolvimento de *software* interessam ou podem interessar a qualquer indivíduo, de maneira que, para viabilizar uma compreensão por indivíduos atuantes em outras áreas e para se oferecer um documento “autocontido”, i.e., um documento compreensível minimamente por si mesmo, fez-se a inserção em discussão, destacando-se, contudo, que o leitor já familiarizado com este domínio pode, tranquilamente, caso não repute pertinente o exame de tal Capítulo, passar diretamente aos subsequentes.

Finda a exposição sobre *software* e desenvolvimento de *software*, trata-se, no Capítulo 3, dos riscos em qualquer atividade produtiva, dando-se especial enfoque aos riscos aos associados aos processos de produção de

software, uma vez que a hercúlea tarefa de produzir/fornecer *software* é sujeita a inúmeras incertezas.

Dada a relevância dos riscos associados à Segurança⁷, trata-se, no Capítulo 4, acerca de tal tema, apresentando-se noções basilares sobre vulnerabilidades, ameaças, ataques e gerenciamento da Segurança em sistemas computacionais.

Dos riscos de Segurança, passa-se, no Capítulo 5, à abordagem da Responsabilidade por Danos, considerado o Direito Civil, uma vez que, não estando os dirigentes da Indústria de *Software* e os desenvolvedores de *software* em uma casta superior imune à consequência de suas ações, podem eles também vir a sofrer responsabilização, inclusive no tocante a falhas em Segurança. Ainda que, por leigos, este Capítulo possa ser considerado excessivamente denso, tal impressão não procede. Em verdade, neste Capítulo, foram apresentadas apenas noções mínimas, tomando-se por base a doutrina, a legislação e a jurisprudência nacionais.

Por fim, finaliza-se, no Capítulo 6, a exposição do referencial teórico com comentários rápidos a respeito de Ética Profissional. A inclusão deste Capítulo se fez necessária porque, a par de certas hipotéticas condutas relacionadas ao fornecimento de *software*/serviços em *software* poderem ser tidas como ilegais, elas também poderiam ser reputadas antiéticas e porque, como registrado nos Capítulos ulteriores ao referencial teórico, estando-se em uma era de globalização, a solução de questões comuns ao desenvolvimento/fornecimento de *software* em âmbito internacional não deveria depender de burocráticos acordos transnacionais de difícil pactuação, sendo muito mais simples e factível, em benefício dos próprios atores envolvidos, com foco na mencionada solução, a adoção de comportamentos éticos.

Concluída a apresentação do aludido referencial, passa-se, finalmente, no Capítulo 7, aos resultados principais da investigação ora relatada: a) traçando-se

⁷ Ainda que a relevância da Segurança Computacional seja objeto de Capítulos ulteriores a este, coloca-se, neste momento, a título de mera provocação antecipada do leitor, questionamento relativo ao hipotético vazamento de seus próprios dados pessoais. Consoante notícia veiculada em mídia eletrônica (ILASCU, 2019), lançou-se, em certos fóruns obscuros de discussão, leilão para a não autorizada venda de dados sensíveis de 92 milhões de brasileiros (dados relativos a nome, endereço, telefone, números de documentos oficiais, filiação, formação familiar, grau de instrução acadêmica, etc.), ou seja, *hacker*/grupo de *hackers* tem a posse de dados sensíveis de vultoso número de cidadãos brasileiros e, sem a autorização destes, tenciona comercializar estes dados, o que, obviamente, pode ensejar prejuízos diversos aos indivíduos que tiverem suas informações pessoais divulgadas. Mesmo que o exemplo envolva um caso isolado, neste contexto de potencial venda não autorizada de informações provavelmente obtidas mediante a exploração de vulnerabilidades de Segurança, é, ou não, relevante o tratamento dos riscos relacionados à Segurança Computacional associados ao *software*? Mesmo para o cidadão comum, a resposta a esta questão é evidente.

um panorama atual da Segurança em *software* a partir de amostra de dados reais obtidos através de *pentests*; b) expondo-se questionamento relativo à significância dos números encontrados no citado panorama para a Engenharia de *Software*, para a Academia, para a Indústria e para a sociedade como um todo; c) examinando-se, rapidamente, potenciais repercussões do quadro de insegurança no *software*.

No Capítulo 8, discorre-se sobre o panorama traçado no referido Capítulo 7, apresentando-se, consideradas as nocivas potenciais repercussões do estado de insegurança, possível saída para a Crise de Segurança no *Software*: uma proposta para o Desenvolvimento Ético de *Software* no tocante à Segurança Computacional.

Conclusões e considerações finais sobre o estudo são expostas no Capítulo 9.

2 SOFTWARE

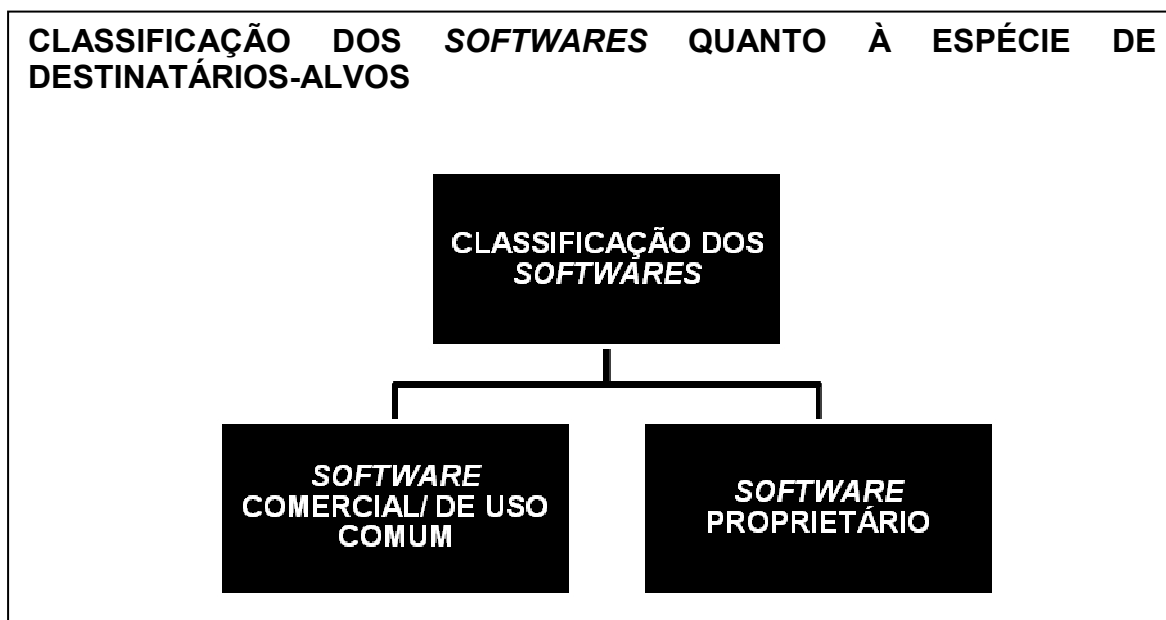
2.1 DEFINIÇÃO

Genericamente, *softwares* podem ser concebidos como programas empregados em computadores/sistemas computacionais, havendo, contudo, concepções segundo as quais os *softwares* compreendem, também, a documentação associada e dados de configuração (SOMMERVILLE, [2007?]).

2.2 CLASSIFICAÇÃO

Como ilustrado na Figura 3, é possível a classificação dos *softwares* em função de seus destinatários-alvos.

Figura 3 - Classificação dos *softwares* quanto à espécie de destinatários-alvos.



Fonte: Autor (2019) ⁸.

⁸ Ilustração construída a partir de exposição de Sommerville ([2007?]).

No Quadro 2, apresentam-se notas distintivas das categorias referidas na Figura 3.

Quadro 2 - Classificação dos *softwares* quanto à espécie de destinatários-alvos.

CLASSIFICAÇÃO DOS SOFTWARES QUANTO À ESPÉCIE DE DESTINATÁRIOS-ALVOS			
CATEGORIA	NOTA DISTINTIVA	DESTINATÁRIOS-ALVOS	EXEMPLOS DE SOFTWARES
SOFTWARE COMERCIAL/DE USO COMUM	Especificação do <i>software</i> definida e controlada pela própria entidade desenvolvedora	Quaisquer interessados em sua aquisição/uso no mercado	• Sistemas de Bases de Dados Relacionais • Processadores de Texto • Pacotes de Desenho • Sistemas de Gerenciamento de Projetos
SOFTWARE PROPRIETÁRIO	Especificação do <i>software</i> definida e controlada pela entidade que o adquirirá/utilizará	Pessoas físicas/jurídicas particularmente interessadas em funcionalidades específicas, que contratam o desenvolvimento de um sistema especialmente destinado a atender suas necessidades	• Sistemas Personalizados de Controle de Dispositivos Eletrônicos • Sistemas de Controle de Tráfego Aéreo • Sistemas de Suporte a Negócios Específicos

Fonte: Autor (2019) ⁹.

2.3 PRODUÇÃO

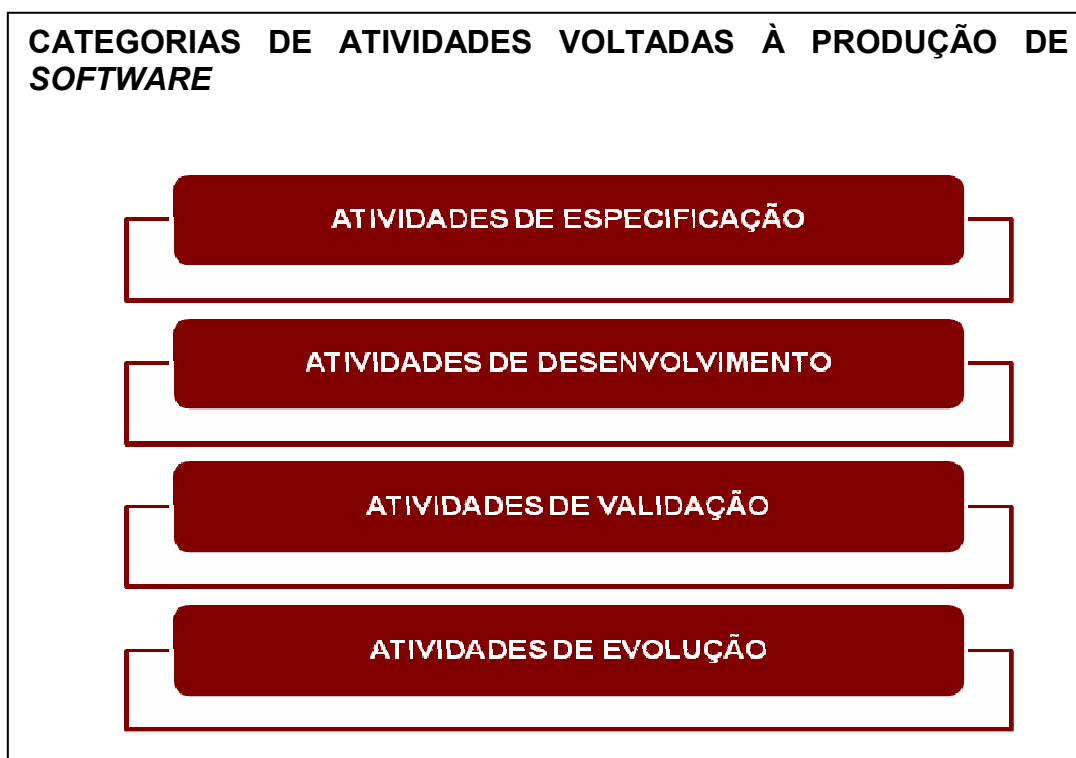
2.3.1 Atividades

Usualmente, para a construção de um *software*, atividades de diversas naturezas são realizadas. Na Figura 4, apresentam-se as principais categorias de

⁹ Quadro produzido a partir de considerações expostas por Sommerville ([2007?]).

atividades realizadas nesta construção.

Figura 4 - Categorias de atividades voltadas à produção de *software*.



Fonte: Autor (2019) ¹⁰.

No Quadro 3, discorre-se, rapidamente, sobre as categorias de atividades referidas na Figura 4.

¹⁰ Ilustração concebida a partir de exposição de Sommerville ([2007?]).

Quadro 3 - Categorias de atividades voltadas à produção de *software*.

CATEGORIAS DE ATIVIDADES VOLTADAS À PRODUÇÃO DE <i>SOFTWARE</i>		
CATEGORIA	IDEIA CENTRAL	EXEMPLOS DE ATIVIDADES
ATIVIDADES DE ESPECIFICAÇÃO	Definição do que o <i>software</i> deve realizar e as condições em que deve operar	Elicitação de requisitos do <i>software</i>¹¹
ATIVIDADES DE DESENVOLVIMENTO PROPRIAMENTE DITO	Delineamento e programação	- Modelagem em <i>Unified Modeling Language (UML)</i> - Codificação
ATIVIDADES DE VALIDAÇÃO	Checagem de que o <i>software</i> atende às pretensões do seu destinatário (cliente/usuários)	- Simulação do uso do <i>software</i> - Teste do <i>software</i>
ATIVIDADES DE EVOLUÇÃO	Modificação e adaptação do <i>software</i> a mudanças de requisitos do cliente e do mercado	- Inserção de nova funcionalidade no <i>software</i> - Modificação de módulos do <i>software</i> para atendimento de legislação superveniente

Fonte: Autor (2019) ¹².

2.3.2 Processo

No desenvolvimento de *software*, as atividades referidas na Seção 2.3.1 sucedem-se em processo, de modo que, ao conjunto de atividades executadas para a construção de um *software* denomina-se processo de desenvolvimento de *software* (SOMMERVILLE, 2005).

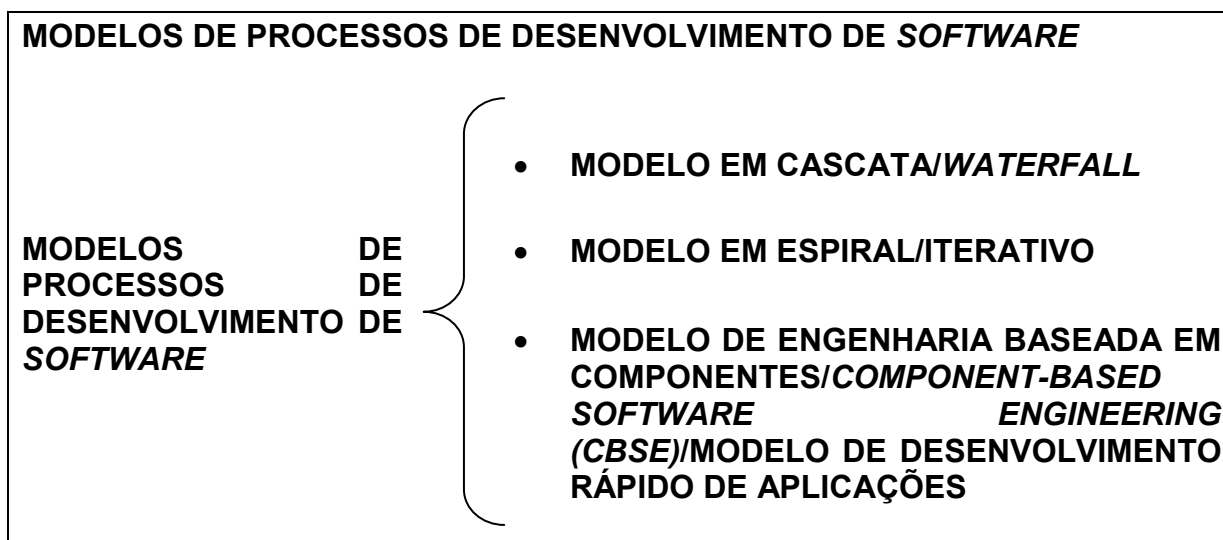
Para a construção de *software*, definiram-se e se definem, com foco

¹¹ Em termos gerais, quando se refere um requisito, fala-se em uma especificação que deveria ser implementada em um produto/serviço de *software* (SOMMERVILLE; SAWYER, 2003). Há uma grande gama de espécies de requisitos que são usualmente implementados em *softwares*, os quais costumam ser objeto de categorização segundo variados critérios (AURUM; WOHLIN, 2005). Embora cada critério apresente suas vantagens e desvantagens e embora seja possível a identificação de ambiguidades e recíprocas influências entre requisitos, o critério relacionado à funcionalidade é frequentemente empregado. De acordo com este critério, dizem-se requisitos funcionais os associados às funcionalidades que o *software* deve apresentar. Os requisitos não funcionais, por seu turno, representam qualidades/atributos do *software*. A Segurança, por exemplo, sob este enfoque, é tida como um requisito não funcional.

¹² Quadro elaborado em função das observações de Sommerville ([2007?]), bem como de Sommerville e Sawyer (2003).

em otimização e racionalização de esforços, modelos de processo de produção/desenvolvimento. Na Figura 5, elencam-se alguns modelos de processos de desenvolvimento de *software*.

Figura 5 - Modelos de processos de desenvolvimento de *software*.



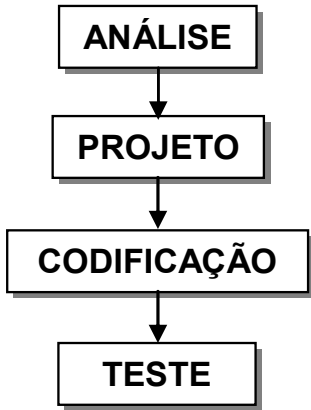
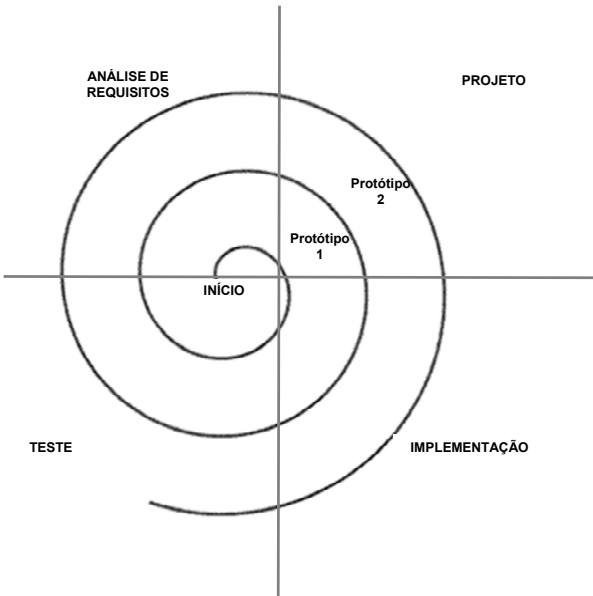
Fonte: Autor (2019) ^{13 14}.

No Quadro 4, apresentam-se considerações gerais acerca dos modelos de processo representados na Figura 5.

¹³ Figura elaborada com base em exposição de Sommerville (2005) e de Pressman (2002).

¹⁴ Vale esclarecer, com a representação feita na Figura 5, que não se desconsidera a existência de outros modelos/estratégias de desenvolvimento correntemente adotadas. Ocorre que tais modelos/estratégias, quando analisados mais detalhadamente, acabam por, em verdade, apresentar, com poucas inovações, ideias dos modelos já elencados, de modo que, por simplicidade, considerado o escopo da investigação ora relatada, tais modelos/estratégias adicionais não são citados neste documento.

Quadro 4 - Modelos de processos de desenvolvimento de *software*.

MODELOS DE PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE		
MODELO	IDEIAS CENTRAIS ASSOCIADAS	ESQUEMA ILUSTRATIVO DE ETAPAS/FASES DE ATIVIDADES
MODELO EM CASCATA/WATERFALL	As atividades de desenvolvimento são tratadas como processos estanques que se sucedem ordenadamente em um fluxo unidirecional	 <pre> graph TD A[ANÁLISE] --> B[PROJETO] B --> C[CODIFICAÇÃO] C --> D[TESTE] </pre>
MODELO EM ESPIRAL/ITERATIVO	As atividades de especificação, desenvolvimento e validação se sucedem de modo intercalado em contínuo refinamento, ou seja, partindo-se de uma versão com especificações abstratas, constrói-se uma versão preliminar do <i>software</i> , que é posteriormente objeto de refinamentos	

MODELOS DE PROCESSOS DE DESENVOLVIMENTO DE SOFTWARE		
MODELO	IDEIAS CENTRAIS ASSOCIADAS	ESQUEMA ILUSTRATIVO DE ETAPAS/FASES DE ATIVIDADES
MODELO DE ENGENHARIA BASEADA EM COMPONENTES/ COMPONENT-BASED SOFTWARE ENGINEERING (CBSE)/MODELO DE DESENVOLVIMENTO RÁPIDO DE APLICAÇÕES	O <i>software</i> é construído a partir da mera junção e rearranjo de componentes previamente existentes	<pre> graph TD A[ESPECIFICAÇÃO DE REQUISITOS] --> B[ANÁLISE DE COMPONENTES] B -- v --> C[MODIFICAÇÃO DE REQUISITOS] C --> D[PROJETO DO SISTEMA COM REUSO] D -- v --> E[DESENVOLVIMENTO E INTEGRAÇÃO] E --> F[VALIDAÇÃO DO SISTEMA] </pre>

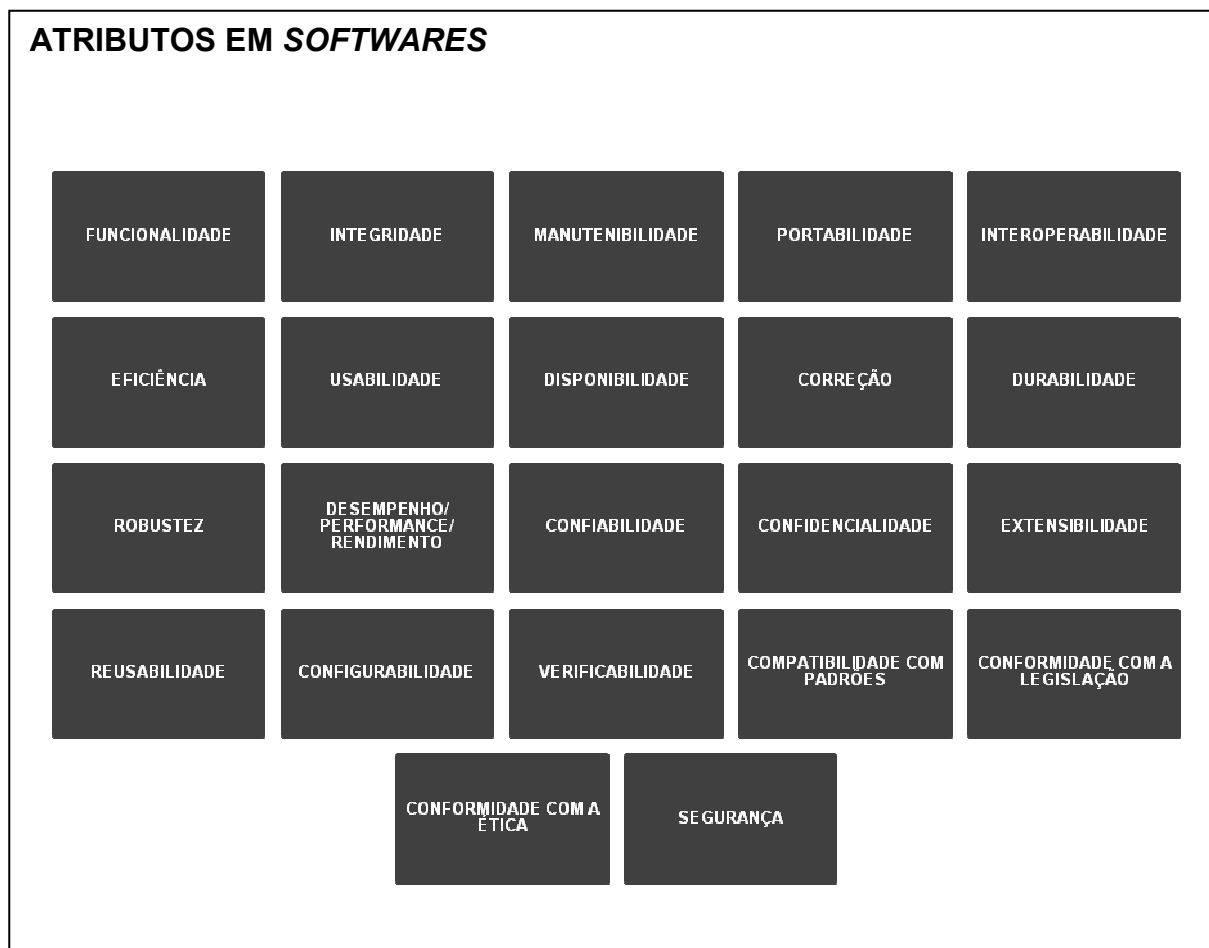
Fonte: Autor (2019) ¹⁵.

A eleição de um dado modelo de processo de desenvolvimento de *software* se dá com a consideração de fatores diversos, como: custos, recursos disponíveis (tempo, inclusive) e natureza do produto final almejado.

2.4 ATRIBUTOS ALMEJADOS

Desenvolvido um *software*, espera-se que o mesmo, considerada sua finalidade, apresente qualidade, ou seja, receba boas avaliações quanto a alguns atributos (SOMMERVILLE, 2005, [2007?]), como os atributos ilustrados na Figura 6.

¹⁵ Quadro concebido a partir das ideias tecidas por Sommerville (2005) e Pressman (2002).

Figura 6 - Atributos em *softwares*.

Fonte: Autor (2019) ¹⁶.

No Quadro 5, discorre-se, brevemente, sobre os atributos representados na Figura 6.

¹⁶ Ilustração construída com o emprego de observações tecidas por Sommerville ([2007?]), Meyer (2006), Berenbach *et al* (2009), Kotonya e Sommerville (2003), Gomes Filho (2005) e Almeida (2015).

Quadro 5 - Atributos em *softwares*.

ATRIBUTOS EM SOFTWARES	
ATRIBUTO	IDEIA BÁSICA ASSOCIADA
FUNCIONALIDADE	Para que um <i>software</i> mostre-se efetivamente útil, ele deve oferecer aos seus usuários as funcionalidades que estes almejam, ou seja, deve realizar operações que os usuários desejem executar
INTEGRIDADE	O <i>software</i> e os dados através dele manipulados devem ser íntegros, i.e., deve haver mecanismos que previnam danos ao seu conteúdo
MANUTENIBILIDADE	Deve ser possível a realização de ajustes/adaptações no <i>software</i> , de modo a se viabilizar sua evolução, em caso de modificações nos requisitos já estabelecidos
PORTABILIDADE	Há portabilidade quando um <i>software</i> pode, sem drásticas medidas, ser transferido para um outro ambiente e nele utilizado
INTEROPERABILIDADE	Espera-se que dados/informações de outros veículos possam ser repassados ao <i>software</i> e, também, no sentido inverso
EFICIÊNCIA	O <i>software</i> não deve desperdiçar recursos do sistema (memória, armazenamento e processamento, e.g.).
USABILIDADE	A utilização do <i>software</i> deve ser simples e direta, não devendo ser necessário que seus usuários despendam esforços para tanto. O <i>software</i> deve, ainda, apresentar interfaces apropriadas para seus usuários e documentação adequada.
DISPONIBILIDADE	Sempre que os usuários dele necessitem, o <i>software</i> deve estar disponível e pronto para uso imediato, ou, subsidiariamente, deve estar minimamente disponível, assegurando-se uma taxa de disponibilidade crítica
CORREÇÃO	O <i>software</i> , nos casos de uso de sua especificação, deve operar de acordo com esta especificação
DURABILIDADE	O <i>software</i> deve apresentar uma boa vida útil estimada e real, considerados os gastos para o seu desenvolvimento e a persistência da demanda
ROBUSTEZ	Em caso de equivocada utilização em desconformidade com sua especificação, o <i>software</i> deve prevenir a ocorrência de danos
DESEMPENHO/ PERFORMANCE/ RENDIMENTO	O <i>software</i> deve operar com garantia de métricas mínimas de performance (número mínimo de transações por minuto, tempo de resposta a solicitações, etc.)
CONFIABILIDADE	Espera-se que se possa confiar no <i>software</i> , contando-se com sua disponibilidade e correção (baixa taxa de erros)
CONFIDENCIALIDADE	Apenas pessoas autorizadas devem ter acesso ao <i>software</i> e aos dados através dele manipulados, obstando-se a divulgação de informação a entes não autorizados
EXTENSIBILIDADE	Deseja-se que, em um futuro incerto, seja possível se incluir novas funcionalidades/recursos no <i>software</i>
REUSABILIDADE	Potencial de aproveitamento do <i>software</i> , ou de seus componentes, para outros fins/usos

ATRIBUTOS EM SOFTWARES	
ATRIBUTO	IDEIA BÁSICA ASSOCIADA
CONFIGURABILIDADE	É interessante que o <i>software</i> seja configurável, ou seja, que determinadas opções suas possam ser personalizadas, em função de preferências/necessidades de seus usuários/destinatários
VERIFICABILIDADE	O <i>software</i> deve ser verificável, i.e., deve ser possível se checar se ele opera corretamente, considerada sua especificação
COMPATIBILIDADE COM PADRÕES	Definidos padrões na Indústria, devem os mesmos serem seguidos nos <i>softwares</i> , para se assegurar sua compatibilidade com outros padrões e sistemas
CONFORMIDADE COM A LEGISLAÇÃO	A legislação, em razão de seu caráter cogente, há de ser observada no <i>software</i> , ou seja, o seu uso não deve implicar máculas às disposições normativas
CONFORMIDADE COM A ÉTICA	Com foco no respeito aos valores sociais, o <i>software</i> deve observar a Ética vigente em seu local de utilização
SEGURANÇA	Danos devem ser evitados, coibindo-se o uso hostil e não autorizado do sistema em desconformidade com sua especificação

Fonte: Autor (2019) ¹⁷.

Atingir-se patamar em que os atributos mencionados se façam presentes não é missão trivial, uma vez que, em variadas ocasiões, alguns dos atributos em debate são, naturalmente, mutuamente excludentes (performance e Segurança, em alguns casos, por exemplo) e que diversas são as incertezas que permeiam o processo de desenvolvimento de *software*.

Considerada, pois, a potencial ocorrência de riscos associados à produção de *software*, discorre-se, no Capítulo 3, acerca de tais incertezas, tratando-se, no Capítulo 4, de especial categoria de incertezas que maculam relevante atributo entre os elencados na Figura 6, a Segurança, já que, como asseverado anteriormente ao longo do presente documento, vive-se, atualmente, uma era de *software* ubíquo e interconectado globalmente e que, como se depreende do mero acompanhamento da mídia, em razão da ubiquidade e da interconexão mencionadas, as repercussões de violações de Segurança assumem proporções expressivas para empreendimentos e indivíduos. Ilustrando-se a expressividade das repercussões citadas, especialmente no tocante ao número de empreendimentos/indivíduos afetados e aos custos financeiros decorrentes de forma

¹⁷ Quadro elaborado com a consideração de ideias expostas por Sommerville ([2007?]), Meyer (2006), Berenbach *et al* (2009), Kotonya e Sommerville (2003), Gomes Filho (2005) e Almeida (2015).

direta do evento, colaciona-se o Quadro 6.

Quadro 6 – Explorações de falhas de segurança em *software* destacadas pela mídia ao longo da última década em razão de suas expressividades (vulto de usuários/empreendimentos afetados e repercussões financeiras diretas).

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)				
CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
ADOBE	2013	• EXTRAÍO DE DADOS SENSÍVEIS DE CLIENTES ATIVOS	• 38 MILHÕES DE CLIENTES ATIVOS	• US\$ 1 MILHÃO EM TAXAS LEGAIS PARA O ESTABELECIMENTO DE UM ACORDO • US\$ 1 MILHÃO EM COMPENSAÇÃO A CLIENTES
ADULT FRIEND FINDER	2016	• ROUBO DE DADOS SENSÍVEIS RELATIVOS A 20 ANOS DE USUÁRIOS	• 412,2 MILHÕES DE USUÁRIOS	-
ANTHEM	2015	• EXTRAÍO DE DADOS SENSÍVEIS DE SEGURADOS ATUAIS E ANTIGOS	• 78,8 MILHÕES DE CLIENTES	• US\$ 100 MILHÕES EM GASTOS NÃO DIVULGADOS DE FORMA INDIVIDUALIZADA
BESSEMER SYSTEM FEDERAL CREDIT UNION	2018	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE CLIENTES BANCÁRIOS • REINICIALIZAÇÃO DE SENHAS BANCÁRIAS POR QUALQUER INDIVÍDUO NÃO AUTORIZADO	-	-

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
BIOSTAR	2019	• VAZAMENTO DE DADOS SENSÍVEIS E DE IMAGENS DE IMPRESSÕES DIGITAIS DE USUÁRIOS	• 1 MILHÃO DE USUÁRIOS	-
BRITISH AIRWAYS	2018	• VAZAMENTO DE DADOS SENSÍVEIS	-	• US\$ 230 MILHÕES EM MULTA IMPOSTA POR ÓRGÃO REGULATÓRIO INGLÊS
CAPITAL ONE	2019	• EXTRAVIO DE INFORMAÇÕES SENSÍVEIS DE CRÉDITO DE CLIENTES AMERICANOS E CANADENSES	• 100 MILHÕES DE CLIENTES AMERICANOS • 60 MILHÕES DE CLIENTES CANADENSES	-
CLICK2MAIL	2019	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE USUÁRIOS	• 200 MIL USUÁRIOS	-
COTTAGE HEALTH	2013 E 2015	• VAZAMENTO DE DADOS SENSÍVEIS DE PACIENTES	• 62,5 MIL INDIVÍDUOS/ PACIENTES	• US\$ 3 MILHÕES EM MULTA IMPOSTA POR ÓRGÃO DE CONTROLE AMERICANO
CREDIT UNION & FISERV	2019	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE CLIENTES BANCÁRIOS	-	-

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
DELTA AIR LINES & [24]7 INC.	2017	• EXPOSIÇÃO DE DADOS SENSÍVEIS PESSOAIS E DE PAGAMENTO RELATIVOS A CLIENTES • OCULTAÇÃO DA EXISTÊNCIA DA VULNERABILIDADE DE SEGURANÇA	• 825 MIL CLIENTES	-
DESJARDIN GROUP	2019	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE CLIENTES	• 2,9 MILHÕES DE CLIENTES DE EMPRÉSTIMOS	• US\$ 53 MILHÕES EM GASTOS DIVERSOS
eBAY	2014	• ROUBO DE DADOS SENSÍVEIS DE USUÁRIOS	• 145 MILHÕES DE USUÁRIOS	-
EQUIFAX	2017	• VAZAMENTO DE DADOS SENSÍVEIS DE CLIENTES	• 148 MILHÕES DE CLIENTES	• US\$ 1,38 BILHÃO EM ACORDO PARA RESOLUÇÃO DAS DEMANDAS OPOSTAS POR CLIENTES • US\$ 175 MILHÕES EM HONORÁRIOS PERICIAIS • US\$ 100 MILHÕES PARA QUE OS DEMANDANTES DESISTISSEM DE

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
				DEMANDAS JUNTO A ÓRGÃOS GOVERNAMENTAIS AMERICANOS • US\$ 664 MIL EM MULTA IMPOSTA PELO ÓRGÃO REGULATÓRIO INGLÊS (INFORMATION COMMISSIONER'S OFFICE) • US\$ 1 BILHÃO PARA MELHORIA DE SUA SEGURANÇA • US\$ 700 MILHÕES EM MULTAS EM FAVOR DE ÓRGÃO REGULATÓRIO AMERICANO • US\$ 559 MILHÕES EM OPERAÇÕES COMERCIAIS PERDIDAS

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
FACEBOOK	2018	• ACESSO NÃO AUTORIZADO A CONTAS DE USUÁRIOS	• 50 MILHÕES DE USUÁRIOS	-
FIAT-CHRYSLER	2015	• ACESSO NÃO AUTORIZADO E SUBVERSÃO DO SISTEMA DE VEÍCULOS JEEP	-	-
FOXIT	2019	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE USUÁRIOS DO <i>SOFTWARE</i> FOXIT PDF READER	• 328 MIL CONTAS DE USUÁRIOS	-
FREEDOM HEALTHCARE	2019	• VAZAMENTO DE DADOS SENSÍVEIS DE FUNCIONÁRIOS	• 957 MIL REGISTROS DE FUNCIONÁRIOS	-
GEARBEST	2019	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE INDIVÍDUOS	• 1,5 MILHÕES DE INDIVÍDUOS	-
HANCOCK HEALTH & RANSOMWARE SAMSAM	2018	• ACESSO NÃO AUTORIZADO A DADOS • OBSTRUÇÃO DO SERVIÇO MEDIANTE SEQUESTRO DOS DADOS E DO CONTROLE DO SISTEMA • INOPERÂNCIA DO SISTEMA	-	• US\$ 55 MIL PAGOS AOS CONTROLADORES DO RANSOMWARE

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
HEARTLAND PAYMENT SYSTEMS	2008	• VAZAMENTO DE DADOS SENSÍVEIS DE CARTÕES DE CRÉDITO E DE DÉBITO DE CLIENTES	• 134 MILHÕES DE CARTÕES DE CLIENTES	• US\$ 145 MILHÕES DE DÓLARES EM COMPENSAÇÃO POR PAGAMENTOS FRAUDULENTOS
HOME DEPOT	2014	• EXTRAVIO DE DADOS DE CRÉDITO/DÉBITO DE CLIENTES	• 56 MILHÕES DE CLIENTES	• US\$ 13 MILHÕES EM ACORDO PARA A CRIAÇÃO DE FUNDO PARA A COMPENSAÇÃO DE CLIENTES • US\$ 6,5 MILHÕES EM ACORDO PARA A CRIAÇÃO DE SERVIÇO DE PROTEÇÃO À IDENTIDADE DOS CLIENTES • US\$ 161 MILHÕES DE DESPESAS PRELIMINARES AO ACORDO
HY-VEE REDE DE SUPERMERCADOS	2019	• EXTRAVIO DE DADOS SENSÍVEIS E SEU COMÉRCIO EM MERCADO	• 5,3 MILHÕES DE CONTAS DE CLIENTES	-

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
		NEGRO DE DADOS (DADOS DE CRÉDITO E DÉBITO DE CONTAS DE CLIENTES)		
JACKSON COUNTY GOVERNMENT & RANSOMWARE RYUK	2019	• OBSTRUÇÃO DO SERVIÇO MEDIANTE SEQUESTRO DOS DADOS E DO CONTROLE DO SISTEMA • INOPERÂNCIA DO SISTEMA	-	• US\$ 400 MIL PAGOS AOS CRIMINOSOS CONTROLADORES DO RANSOMWARE
JP MORGAN CHASE	2014	• VAZAMENTO DE DADOS DE CLIENTES BANCÁRIOS	• 76 BILHÕES DE CONTAS PESSOAIS • 7 MILHÕES DE CONTAS DE PEQUENOS EMPREENHIMENTOS	-
LABCORP & RAMNSOWARE	2018	• ACESSO NÃO AUTORIZADO A DADOS • OBSTRUÇÃO DO SERVIÇO MEDIANTE SEQUESTRO DOS DADOS E DO CONTROLE DO SISTEMA • INOPERÂNCIA DO SISTEMA	-	-

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
LAKE CITY & RANSOMWARE QUERVAR	2019	• OBSTRUÇÃO DO ACESSO A DADOS • ACESSO NÃO AUTORIZADO A DADOS • OBSTRUÇÃO DO SERVIÇO MEDIANTE SEQUESTRO DOS DADOS E DO CONTROLE DO SISTEMA • INOPERÂNCIA DO SISTEMA	-	• US\$500 MIL PAGOS AOS CONTROLADORES DO RANSOMWARE
MARRIOTT INTERNATIONAL	2014 A 2018	• ROUBO DE DADOS SENSÍVEIS DE CLIENTES	• 500 MILHÕES DE USUÁRIOS/CLIENTES	• US\$ 28 MILHÕES EM DESTINAÇÃO INESPECÍFICA • US\$ 124 MILHÕES EM MULTA IMPOSTA PELO ÓRGÃO DE REGULAÇÃO INGLÊS • US\$ 265 MIL EM MULTA IMPOSTA POR ÓRGÃO TURCO DE REGULAÇÃO

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
PITNEY BOWES & RANSOMWARE	2019	• PARCIAL INOPERÂNCIA DOS SISTEMAS EM RAZÃO DO SEQUESTRO DO SISTEMA/DADOS	-	-
RIVIERA BEACH CITY & RAMNSOWARE	2019	• ACESSO NÃO AUTORIZADO A DADOS • OBSTRUÇÃO DO SERVIÇO MEDIANTE SEQUESTRO DOS DADOS E DO CONTROLE DO SISTEMA • INOPERÂNCIA DO SISTEMA	-	• US\$ 600 MIL PAGOS AOS CRIMINOSOS CRONTROLADORES DO RANSOMWARE
RSA SECURITY	2011	• EXTRAVIO DE DADOS SENSÍVEIS DE EMPREGADOS	• 40 MILHÕES DE INDIVÍDUOS	-
SONY'S PLAYSTATION NETWORK	2011	• VAZAMENTO DE DADOS SENSÍVEIS DE USUÁRIOS • INOPERÂNCIA DOS SERVIÇOS DO SITE POR UM MÊS	• 77 MILHÕES DE CONTAS DE USUÁRIOS	• US\$ 15 MILHÕES EM ACORDO INDENIZATÓRIO EM AÇÃO COLETIVA • US\$ 171 MILHÕES DE PREJUÍZOS PELA INOPERÂNCIA DO SITE

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
STUXNET	2005 A 2010	• DANOS EM INSTALAÇÕES NUCLEARES IRANIANAS	-	-
TARGET STORES	2013	• VAZAMENTO DE DADOS SENSÍVEIS DE CARTÕES DE CRÉDITO E DE DÉBITO DE CLIENTES	• 110 MILHÕES DE CLIENTES	• US\$ 18,5 MILHÕES EM ACORDO INESPECÍFICO • US\$ 39 MILHÕES EM ACORDO COM INSTITUIÇÕES FINANCEIRAS LESADAS • US\$ 10 MILHÕES EM ACORDO EM AÇÃO COLETIVA • US\$ 6,75 MILHÕES EM HONORÁRIOS ADVOCATÍCIOS • US\$ 202 MILHÕES EM DESPESAS JUDICIAISE OUTROS CUSTOS
TJX COMPANIES	2006	• VAZAMENTO DE DADOS SENSÍVEIS DE CARTÕES DE CRÉDITO E DE DÉBITO DE CLIENTES	• 96 MILHÕES DE CARTÕES DE CRÉDITO/DÉBITO DE CLIENTES	• US\$ 200 MILHÕES EM GASTOS NÃO DIVULGADOS INDIVIDUALMENTE

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM *SOFTWARE* DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
TOUCHSTONE MEDICAL IMAGING	2014	• VAZAMENTO DE DADOS SENSÍVEIS DE PACIENTES	• 300 MIL INDIVÍDUOS/ PACIENTES	• US\$ 3 MILHÕES EM MULTA IMPOSTA POR ÓRGÃO DE CONTROLE AMERICANO
UBER	2016	• VAZAMENTO DE DADOS SENSÍVEIS DE USUÁRIOS E DE CONDUTORES UBER	• 57 MILHÕES DE USUÁRIOS UBER • 600 MIL CONDUTORES UBER	• US\$ 20 MILHÕES EM PERDA NO VALOR DE MERCADO DA EMPRESA • US\$ 148 MILHÕES EM MULTAS IMPOSTAS POR ÓRGÃO REGULATÓRIO AMERICANO
UNITED STATES OFFICE OF PERSONAL MANAGEMENT (OPM)	2013 A 2015	• EXPOSIÇÃO DE DADOS SENSÍVEIS DE PESSOAL DO GOVERNO AMERICANO	• 22 MILHÕES DE INDIVÍDUOS	-
UNIVERSIDADE DO TEXAS E MD ANDERSON CÂNCER CENTER	2012 A 2013	• PERDA DE INFORMAÇÕES MÉDICAS DE PACIENTES	• 33,5 MIL INDIVÍDUOS/ PACIENTES	• US\$ 4,3 MILHÕES EM MULTAS IMPOSTAS POR ÓRGÃO AMERICANO DE CONTROLE
VERISIGN	2010	• EXTRAVIO DE INFORMAÇÕES SENSÍVEIS	-	-
VOLUSION PAYMENT PLATFORM	2019	• VAZAMENTO DE DADOS SENSÍVEIS	-	-

EXPLORAÇÕES DE FALHAS DE SEGURANÇA EM SOFTWARE DESTACADAS PELA MÍDIA AO LONGO DA ÚLTIMA DÉCADA EM RAZÃO DE SUAS EXPRESSIVIDADES (VULTO DE USUÁRIOS/EMPREENHIMENTOS AFETADOS E REPERCUSSÕES FINANCEIRAS DIRETAS)

CASO	PERÍODO	NATUREZA PRINCIPAL DAS REPERCUSSÕES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA	NÚMERO DE EMPREENHIMENTOS/ INDIVÍDUOS AFETADOS PELA EXPLORAÇÃO DA FALHA DE SEGURANÇA	MONTANTE ESTIMADO DOS CUSTOS DECORRENTES DA EXPLORAÇÃO DA FALHA NA SEGURANÇA
WENDY'S REDE DE LANCHONETES	2015 A 2016	• PERDA DE DADOS DE TRANSAÇÕES DE PAGAMENTOS REALIZADOS COM CARTÕES	• TRANSAÇÕES DE PAGAMENTOS REALIZADOS COM 18 MILHÕES DE CARTÕES	• US\$ 50 MILHÕES EM ACORDO COM 7,5 MIL INSTITUIÇÕES BANCÁRIAS PARCEIRAS DE NEGÓCIOS
WOLTERS KLUWER	2019	• INOPERÂNCIA DO SERVIÇO	-	-
YAHOO	2013 A 2014	• ACESSO NÃO AUTORIZADO A CONTAS DE USUÁRIOS	• 3 BILHÕES DE USUÁRIOS	• US\$ 35 MILHÕES EM MULTA IMPOSTA POR ÓRGÃO DE CONTROLE AMERICANO • US\$ 50 MILHÕES EM COMPENSAÇÃO EM AÇÃO COLETIVA
ZENDESK	2016	• VAZAMENTO DE DADOS SENSÍVEIS E DE CERTIFICAÇÕES DIGITAIS DE CLIENTES	• 100 MIL CLIENTES	-

Fonte: Autor (2019) ¹⁸.

¹⁸ Quando elaborado a partir de informações disponibilizadas em Arghire (2019), Armerding (2019), Baraniuk (2019), Brumfield (2019), Ferguson (mar, 2010; out, 2019), Fruhlinger (2018), Gatlan (2019), Kanell (2019), Krebs (mai.; ago, 2019), Leyden (2019), Matsakis e Lapowsky (2018), McCarthy (2019), Mehrotra (2019), Paganini (mar.; 15 out.; jun., 2019), Pymnts (2019), Rashid (2017), Schwartz (fev.; mar.; 2019), Seals (2019), Spamfighter (2019), Stupp (2019), Swinhoe (jul.; ago., 2019), Townsend (2018) e Whittaker (jun.; jul., 2019).

3 RISCOS

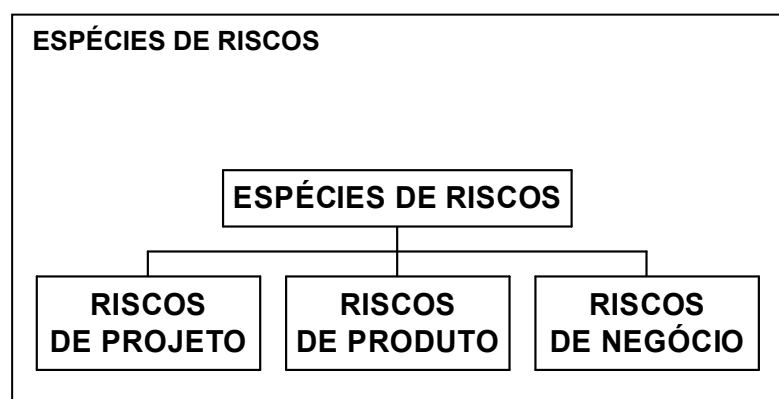
3.1 NOTAS GERAIS

Em face de seus potenciais efeitos, as incertezas associadas a projetos (riscos) constituem-se em importante elemento a ser considerado pelos gestores e tomadores de decisão em entidades de qualquer natureza, pois podem, em aparente contraditória dualidade, representar ameaças ou novas oportunidades (HM TREASURY, 2004).

Genericamente, os riscos podem ser concebidos como incertezas/eventos de ocorrência indeterminada potencialmente causadores de danos ou geradores de janelas/nichos de oportunidades (COLLIER, 2009).

Ainda que existam espécies diversas de riscos, consideradas diferentes óticas de análise, é comum sua categorização em função de seu objeto macroscópico, tal como ilustrado na Figura 7.

Figura 7 - Espécies de riscos.



Fonte: Autor (2019) ^{19 20}.

Expõem-se, no Quadro 7, observações distintivas das categorias

¹⁹ Ilustração concebida a partir de ideias expostas por Sommerville (2005) e, originalmente, apresentada em Flores (2010), p. 21.

²⁰ A exposição das categorias macroscópicas indicadas na Figura 9 teve por finalidade a simples ilustração, cabendo o destaque de que é possível a simultânea classificação de um risco em mais de uma das aludidas categorias, já que não rechaçada a hipótese de sua repercussão em mais de um dos citados domínios (projeto, produto ou negócio), ou seja, uma mesma incerteza pode representar, assim, uma ameaça/oportunidade ao projeto, ao produto e ao negócio.

referidas na Figura 7.

Quadro 7 – Espécies de riscos.

ESPÉCIES DE RISCOS		
ESPÉCIE	DESCRIÇÃO	EXEMPLOS
RISCOS DE PROJETO	Incertezas influentes no cronograma e nos recursos de um projeto	• Redução de verbas; • Diminuição do quadro de funcionários; • Voluntária saída de parceiros; • Equivocado dimensionamento do projeto.
RISCOS DE PRODUTO	Riscos impactantes na qualidade/rendimento/desempenho de um produto	• Insuficiente desempenho de elemento do produto; • Insuficiente desempenho global do produto; • Equivocado funcionamento do produto.
RISCOS DE NEGÓCIO	Incertezas influentes na organização/entidade	• Estabelecimento de entidade concorrente no ramo de atuação da organização; • Lançamento antecipado de novo produto por entidade concorrente.

Fonte: Autor (2019) ²¹.

Exposto o critério de categorização dos riscos quanto ao seu objeto macroscópico, é relevante se observar que outros focos e critérios são usualmente empregados, havendo, pois, outras classificações em que se consideram os interesses e objetivos da entidade classificadora.

No Quadro 8, apresentam-se os critérios e classificações referidos por Pandian (2007).

²¹ Quadro concebido por Flores (2010), p. 21-22, a partir dos resultados de revisão sistemática que conduziu e das ideias expostas por Sommerville (2005).

Quadro 8 – Critérios de classificação dos riscos.

CLASSIFICAÇÃO DOS RISCOS		
CRITÉRIO	CATEGORIAS	DESCRIÇÃO
ORIGEM	Riscos Internos	Riscos oriundos da própria organização
	Riscos Externos	Riscos decorrentes do ambiente externo à organização
NATUREZA	Riscos de Negócio	Riscos associados a fatores organizacionais e de mercado
	Riscos Técnicos	Riscos relativos a questões técnicas
DOMÍNIO	Riscos de Projeto	Riscos inerentes à elaboração e à condução de um projeto
	Riscos de Processo	Riscos de inadequação/ineficiência de processos empreendidos
	Riscos de Produto	Riscos impactantes no produto desenvolvido/fornecido por uma organização
MÁXIMA AMPLITUDE DO IMPACTO	Riscos Catastróficos	Riscos de drásticos impactos
	Riscos Não Catastróficos	Riscos de impactos não drásticos
PROBABILIDADE DE OCORRÊNCIA	Riscos Constantes	Riscos presentes ao longo de todo o projeto
	Riscos Nominais	Riscos com probabilidade de ocorrência variada e distinta de 100% ou baixa
	Riscos Triviais	Riscos com baixa probabilidade de ocorrência

CLASSIFICAÇÃO DOS RISCOS		
CRITÉRIO	CATEGORIAS	DESCRIÇÃO
OBJETO DO PROJETO IMPACTADO	Riscos Orçamentários e de Custos	Riscos de insuficiência de recursos ou de majoração de despesas
	Riscos de Cronograma	Riscos de não atingimento de objetivos
	Riscos de Requisitos	Riscos de equivocado estabelecimento de requisitos ou de modificação dos mesmos
	Riscos de Qualidade	Riscos de inadequação, inutilidade e incorreto funcionamento
	Riscos de Performance	Riscos de insuficiente desempenho
PRAZO PARA CONSUMAÇÃO DO RISCO	Riscos Imediatos	Riscos de consumação imediata a partir de sua identificação
	Riscos a Médio Prazo	Riscos de consumação em prazo médio, relativamente ao momento de sua identificação
	Riscos a Longo Prazo	Riscos de consumação tardia em relação ao período de sua identificação
RAPIDEZ DE PRODUÇÃO DE IMPACTO	Riscos de Impacto Imediato	Riscos de imediata produção de consequências
	Riscos de Impacto Lento	Riscos não produtivos de consequências imediatas
VISIBILIDADE EXTERNA	Riscos Evidentes	Riscos de plano perceptíveis
	Riscos Moderadamente Perceptíveis	Riscos não imediatamente observáveis
	Riscos Imperceptíveis/de Baixa Visibilidade	Riscos não perceptíveis

Fonte: Autor (2019) ²².

Consideradas as potenciais repercussões da consumação de riscos (efeitos nocivos ou oportunidades), é relevante se gerenciar as incertezas, independentemente da natureza da organização em que se apresentem. Deste

²² Quadro concebido em Flores (2010), p. 23 – 24, com o emprego de considerações tecidas por Pandian (2007).

gerenciamento podem resultar benefícios diversos (FLORES, 2010)²³:

- redução das probabilidades de ocorrência de efeitos adversos decorrentes da consumação de riscos;
- diminuição do impacto dos danos originados da consumação de riscos;
- fortalecimento do produto, do projeto e do empreendimento;
- redução da vulnerabilidade do produto, do projeto e do empreendimento a riscos nocivos;
- identificação de oportunidades e nichos de crescimento.

Na gestão de riscos, atividades de naturezas variadas são realizadas. Usualmente, estas atividades são agrupadas em categorias como as indicadas na Figura 8.

Figura 8 – Categorias de atividades de gestão de riscos.



Fonte: Autor (2019) ²⁴.

As atividades insertas nas categorias apontadas na Figura 8 não se sucedem em um processo unidirecional linear, apresentando-se, em realidade, um

²³ Rol de benefícios condensado em Flores (2010), p. 25, a partir dos resultados de revisão sistemática que conduziu, bem como das ideias expostas por Pandian (2007) e por Sommerville (2005).

²⁴ Ilustração produzida por Flores (2010), p. 6, com base nas ideias de Cox e Tait (1998).

contínuo e permanente ciclo de atividades voltadas à gestão do risco (HM TREASURY, 2004), como ilustrado na Figura 9.

Figura 9 – Ciclo de ações para a gestão de riscos.



Fonte: Autor (2019) ²⁵.

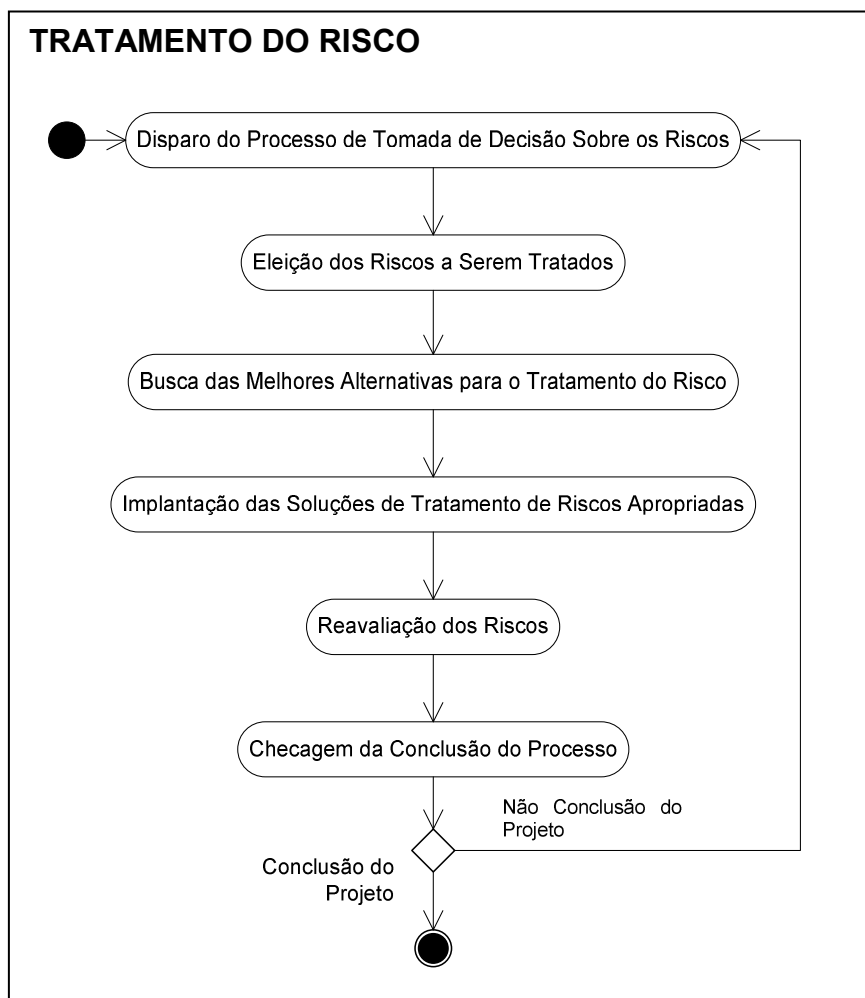
Como se depreende do exame da Figura 9, a gestão dos riscos tem início com a identificação das incertezas associadas. Identificados os riscos, passa-se à sua análise com foco na seleção e tratamento dos riscos relevantes, considerados critérios e recursos da entidade interessada/responsável. Selecionados os riscos relevantes, adotam-se medidas voltadas ao seu tratamento. Tratados os riscos eleitos, realiza-se monitoramento para verificação da eficiência das medidas adotadas. Persistindo o interesse/responsabilidade da entidade, volta-se ao estágio inicial do ciclo, procedendo-se à identificação das incertezas, à sua análise, ao seu tratamento e ao seu contínuo monitoramento.

Acerca do tratamento dos riscos, algumas observações se fazem necessárias. Enquanto persistente o interesse/responsabilidade de uma entidade quanto a um dado conjunto de riscos e seus impactos, há de se eleger a conduta da entidade diante da incerteza, i.e., há de se definir o tratamento a ser dado a este

²⁵ Adaptação de ilustração de Cox e Tait (1998), p. 6, exposta no trabalho de Flores (2010), p. 30.

conjunto de riscos. Esta definição envolve, essencialmente, atividades diversas, como as representadas na Figura 10.

Figura 10 – Diagrama de atividades representativo de ações diante de riscos.



Fonte: Autor (2019) ²⁶.

Como registrado em Flores (2010), atividades variadas são realizadas para efetivação do processo ilustrado na Figura 10, como:

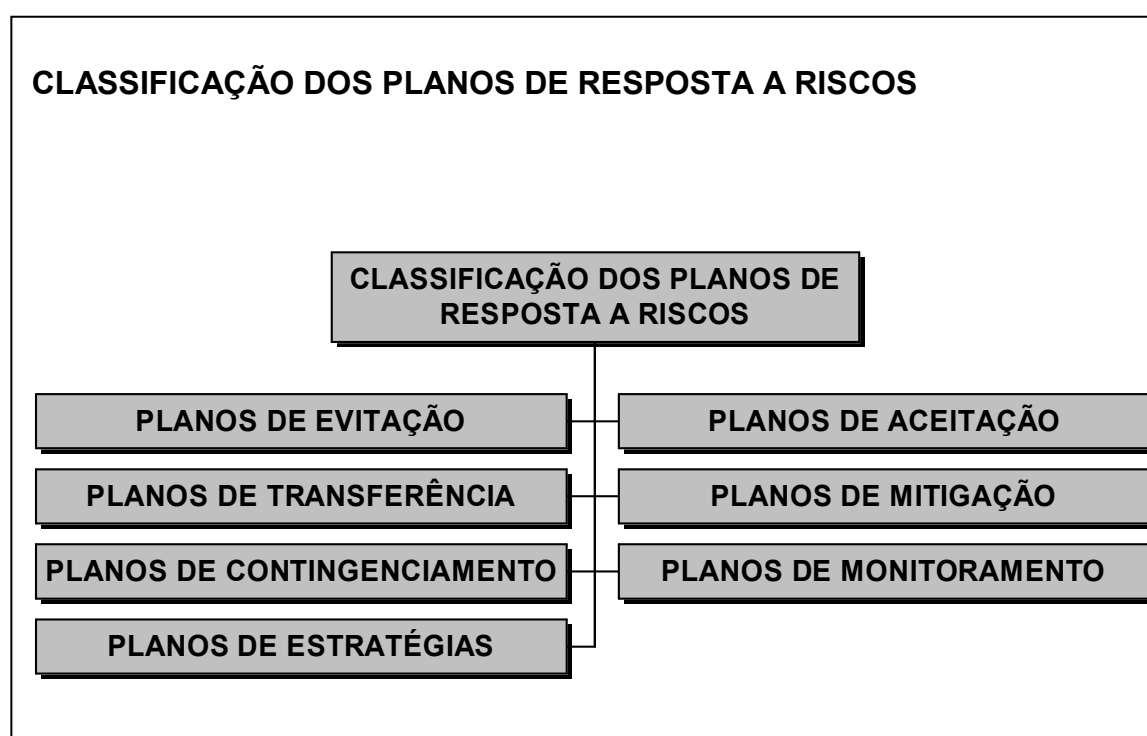
- comunicação do risco, ou seja, divulgação aos setores interessados/envolvidos acerca de sua potencial ocorrência, bem como sua devida inserção nas anotações representativas da Cultura de Risco da entidade;
- resolução sobre a política da entidade diante do risco apontado;

²⁶ Ilustração concebida em Flores (2010), p. 35, com construção fundada em exposição de Pandian (2007).

- busca por soluções/respostas para manipulação/tratamento do risco;
- eleição da melhor solução para o risco apontado e definição de plano próprio de ação (Plano de Resposta);
- implementação da solução eleita para o tratamento do risco;
- reavaliação dos riscos e da situação da entidade diante de sua nova configuração.

Relativamente aos Planos de Resposta, vale salientar, consoante Pandian (2007), a possibilidade de sua classificação quanto ao seu objetivo principal, como ilustrado na Figura 11.

Figura 11 – Classificação dos planos de resposta a riscos.



Fonte: Autor (2019) ²⁷.

Observações distintivas das classes expostas na Figura 11 podem ser visualizadas no Quadro 9.

²⁷ Figura concebida em Flores (2010), p. 36, a partir de observações de Pandian (2007).

Quadro 9 – Planos de resposta a riscos.

PLANOS DE RESPOSTAS A RISCOS		
ESPÉCIE	IDÉIA BÁSICA	EXEMPLOS DE ATIVIDADES
PLANO DE EVITAÇÃO	Evitação/desvio, se possível, de elementos com relevantes riscos associados	• Remoção de funcionalidade experimental não essencial de um sistema • Eleição de metodologia menos ágil de desenvolvimento porém mais formal
PLANO DE ACEITAÇÃO	Aceitação da possibilidade de consumação de riscos de menores impactos sem a adoção de medidas contra sua configuração ou para o seu aproveitamento	• Desconsideração/intencional ignorância do risco no gerenciamento do projeto e nas atividades da entidade
PLANO DE TRANSFERÊNCIA	Transferência do risco (postergação de tratamento e repasse de responsabilidade pelo risco, e.g.)	• Postergação do tratamento do risco • Atribuição de novo responsável pela gerência do risco e de suas consequências (Contratação de seguro, terceirização de atividade etc.)
PLANO DE MITIGAÇÃO	Redução do impacto e/ou da exposição a riscos	• Estabelecimento de reserva de recursos • Fixação de prazos com margens para eventos imprevistos
PLANO DE CONTINGENCIAMENTO	Estabelecimento de extremas medidas alternativas na hipótese de concretização de riscos catastróficos e de grande impacto	• Definição de reserva de recursos • Replicação de bases de conhecimento

PLANOS DE RESPOSTAS A RISCOS		
ESPÉCIE	IDÉIA BÁSICA	EXEMPLOS DE ATIVIDADES
PLANO DE MONITORAMENTO	Simple monitoramento/acompanhamento do estado de riscos potenciais de ocorrência não imediata e de seus elementos de disparo sem a adoção de medidas para sua manipulação (enfrentamento/aproveitamento)	• Contínuo monitoramento dos gatilhos/disparos dos riscos
PLANO DE ESTRATÉGIAS	Gerenciamento global dos riscos a que uma entidade se sujeita (riscos internos e externos)	• Identificação dos riscos internos da organização • Detecção de potenciais pontos de melhoria na estruturação da entidade • Análise do mercado • Avaliação e organizações concorrentes

Fonte: Autor (2019) ²⁸.

3.2 RISCOS NA PRODUÇÃO/FORNECIMENTO DE SOFTWARE

A produção e o fornecimento de *software* apresentam-se como complexas e peculiares áreas em que nem sempre se obtém êxito pleno, ou seja, áreas em que, inúmeras vezes, não são atingidos os resultados almejados, mormente quando considerados a qualidade e os custos envolvidos.

Como consignado em Flores (2010), é possível a identificação de diversos obstáculos ao sucesso no desenvolvimento de *software*:

- alto grau de abstração dos processos de concepção e desenvolvimento;
- complexidade da tarefa de criação de *software*;
- alta dependência do produto (composição e qualidade final) em relação à atuação e experiências da equipe de desenvolvimento;

²⁸ Quadro elaborado por Flores (2010), p. 136 – 137, com base em considerações feitas por Pandian (2007).

- ineditismo de certas aplicações e consequente desconhecimento dos reais requisitos do *software*;
- contínuo aumento dos requisitos do produto (performance e desempenho, e.g.);
- inerentes dificuldades da estimativa de necessidades e recursos;
- imaturidade dos domínios de aplicação;
- imaturidade da tecnologia de desenvolvimento da solução;
- usual desconhecimento, pelos desenvolvedores, das regras de negócio e de noções elementares da área da aplicação/*software*;
- desconhecimento/superficial conhecimento, pelos desenvolvedores, das tecnologias eleitas para a construção do produto;
- constante mutabilidade das necessidades dos clientes e dos ambientes de operação do *software*;
- extrema dependência do produto em relação a tecnologias subjacentes altamente mutantes;
- natural dificuldade à adaptação de novas realidades e susceptibilidade do produto final a influências externas;
- inexistência, em dados domínios, de padronização e uniformidade;
- ineficiência na comunicação;
- desconhecimento ou não emprego de técnicas formais na produção de *software*;
- temerária adoção de soluções imediatistas impactantes no restante do processo de desenvolvimento;
- falhas humanas.

Northover *et al* (2008), bem como Sommerville ([2007?]), analisando o tema, entendem que fatores diversos contribuem para problemas no desenvolvimento de *software*:

- existência de múltiplas possibilidades hermenêuticas na apreensão dos requisitos de um *software*;
- variedade ideográfica;
- alto grau de subjetividade ao longo de todo o processo de desenvolvimento;
- impossibilidade de perfeita repetição de procedimentos de produção;
- existência de múltiplas soluções para um mesmo problema;

- susceptibilidade do processo produtivo a influências socioculturais;
- limitada ou restrita aplicabilidade da Filosofia Clássica de Produção na Engenharia de *Software*;
- exiguidade dos prazos de desenvolvimento;
- constante mutabilidade das necessidades a serem supridas pelo *software*;
- heterogeneidade dos ambientes de operação do *software*;
- natural inafastabilidade de requisitos de Confiabilidade e Segurança.

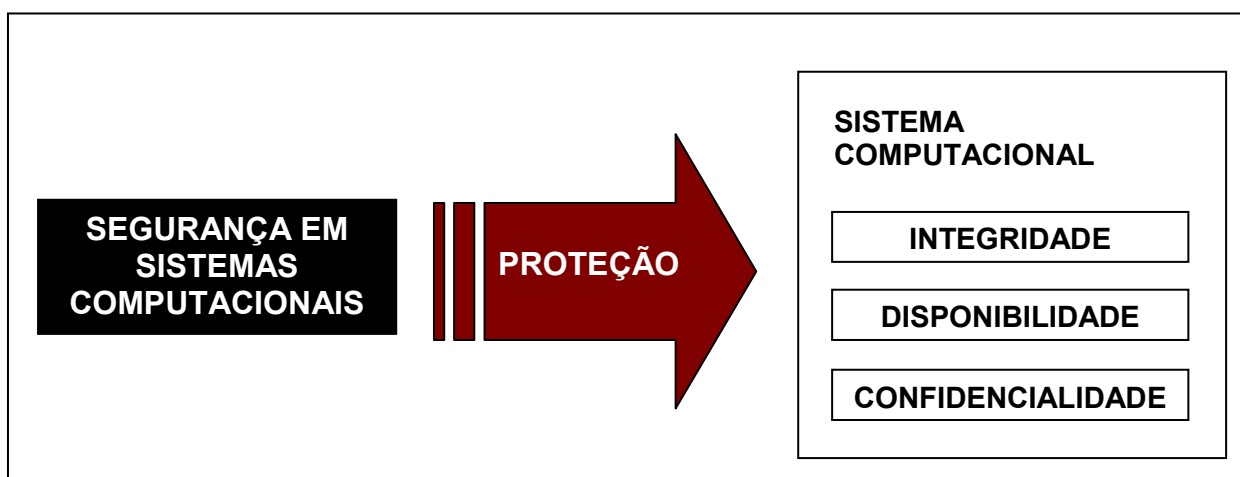
Com o exame dos conjuntos de fatores antes referidos e a consideração de suas possíveis consequências, resulta a percepção de que incertezas de diferentes espécies se apresentam no processo de desenvolvimento de *software*, constatando-se, ademais, dada a já referida relevância da Segurança nos produtos finais deste processo, que especial atenção há de ser conferida a ela e aos riscos de segurança, temas do Capítulo 4.

4 SEGURANÇA

4.1 DEFINIÇÃO E OBJETOS

Em termos gerais, diz-se que há segurança em um sistema computacional quando o mesmo é dotado de proteção para preservação de sua integridade e disponibilidade, bem como para proteção da confidencialidade dos recursos de informação (STALLINGS; BROWN, 2015), como ilustrado na Figura 12.

Figura 12 - Foco da Segurança Computacional.



Fonte: Autor (2019) ²⁹.

Ainda que a tríade Confidencialidade, Integridade e Disponibilidade³⁰ constitua o foco de proteção na Segurança Computacional, há que se observar que outros objetivos também podem ser identificados, tais como a Autenticidade e a Responsabilidade. No Quadro 10, esclarecem-se algumas ideias acerca destes focos e objetivos.

²⁹ Ilustração construída com base nas ideias de Stallings e Brown (2015).

³⁰ A tríade mencionada é usualmente referida por CIA, empregando-se as denominações inglesas *Confidentiality, Integrity and Availability*.

Quadro 10 - Focos e objetivos da proteção almejada com a Segurança Computacional.

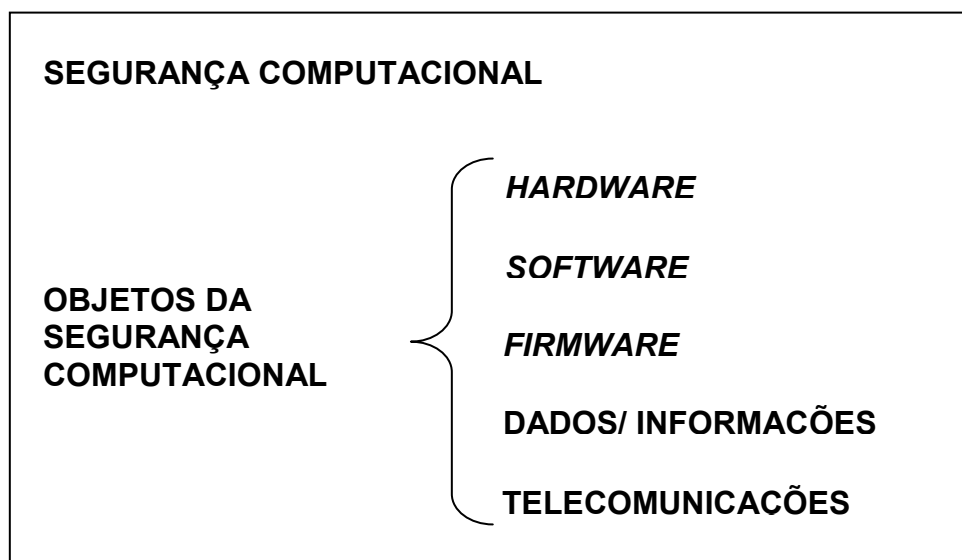
FOCOS E OBJETIVOS DA PROTEÇÃO ALMEJADA NA SEGURANÇA COMPUTACIONAL		
FOCO/OBJETIVO	IDEIAS ESSENCIAIS	CONCEITOS ABARCADOS
INTEGRIDADE	Imutabilidade do sistema por pessoas não autorizadas e perfeição no funcionamento esperado do sistema	• Integridade de Dados • Integridade do Sistema
DISPONIBILIDADE	Operacionalidade e disponibilidade plena do sistema para uso imediato por seus usuários	-
CONFIDENCIALIDADE	Sigilo relativo aos dados e informações, afastando-se o seu vazamento para pessoas não autorizadas	• Confidencialidade dos Dados • Privacidade
AUTENTICIDADE	Originalidade e fidedignidade da transmissão, bem como sua verificabilidade e dos usuários em uma transmissão	-
RESPONSABILIDADE	Necessidade de rastreabilidade de ações para eventual futura responsabilização por falhas de segurança	-
NÃO REPÚDIO	Operacionalidade e funcionalidade do sistema, mesmo quando alvo de ataques, e ulterior inquestionabilidade das operações de acesso e uso pelos indivíduos autorizados	-

Fonte: Autor (2019) ³¹.

Para Stallings e Brown (2015), a proteção referida deve se estender ao *hardware*, ao *software*, ao *firmware*, aos dados/informações e às telecomunicações, como representado na Figura 13.

³¹ Quadro concebido empregando-se as considerações tecidas por Stallings e Brown (2015).

Figura 13 - Objetos da Segurança Computacional.



Fonte: Autor (2019) ³².

Nakamura e Geus (2014), contudo, têm como mais amplo o objeto da segurança computacional, asseverando que outros fatores nela repercutem (usuários, e.g.), como ilustrado na Figura 14, estando, pois, os seus objetos dispostos em níveis.

³² Representação elaborada a partir das observações de Stallings e Brown (2015).

Figura 14 - Objetos da Segurança Computacional.



Fonte: Autor (2019) ³³.

Para Nakamura e Geus (2014), sob pena de se mostrar ineficaz, dada a possibilidade de existência de "brechas" permissivas de exploração, atenção deve ser dada a todos os níveis/objetos que referem.

4.2 VULNERABILIDADES

4.2.1 Definição

Vulnerabilidades de segurança podem ser concebidas como falhas ou fraquezas de projeto, implementação, operação ou gerenciamento de um sistema computacional, que, se exploradas, possibilitam violações de segurança (STALLINGS; BROWN, 2015).

4.2.2 Espécies

Múltiplos são os critérios empregáveis na classificação das vulnerabilidades, sendo usual o concernente à natureza da proteção que deveria ser conferida ao sistema (Confidencialidade, Integridade e Disponibilidade, e.g.)

³³ Adaptação de ilustração produzida por Nakamura e Geus (2014), p. 80.

(STALLINGS; BROWN, 2015). No Quadro 11, apresentam-se, ilustrativamente, exemplos de vulnerabilidades a estas associadas.

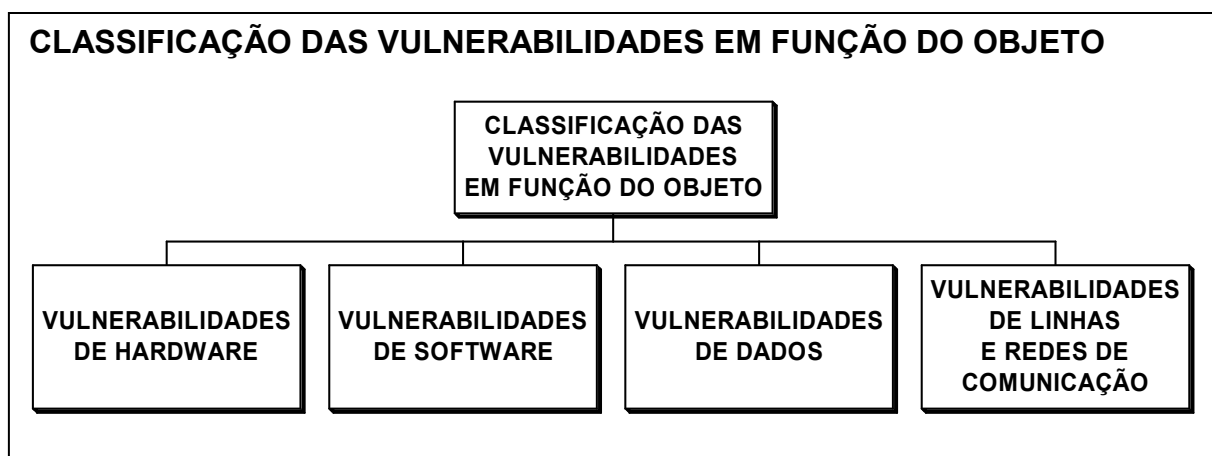
Quadro 11 - Vulnerabilidades associadas à confidencialidade, integridade e disponibilidade.

VULNERABILIDADES ASSOCIADAS À CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE	
VARIANTE DE VULNERABILIDADE	EXEMPLOS
VULNERABILIDADE DE CONFIDENCIALIDADE	• Acesso não autorizado a informações
VULNERABILIDADE DE INTEGRIDADE	• Corrupção ou modificação não autorizada de dados
VULNERABILIDADE DE DISPONIBILIDADE	• Indisponibilidade do sistema • Lentidão do sistema

Fonte: Autor (2019) ³⁴.

Dado o fato de que os sistemas computacionais são formados por *hardware*, *software*, dados e por linhas e redes de comunicação, é possível, também, a classificação das vulnerabilidades quanto ao objeto sobre o qual recaem, como ilustrado na Figura 15.

Figura 15 - Classificação das vulnerabilidades quanto ao objeto sobre o qual recaem.



Fonte: Autor (2019) ³⁵.

³⁴ Representação concebida a partir das ideias de Stallings e Brown (2015).

³⁵ Ilustração produzida com o emprego de exposição feita por Stallings e Brown (2015).

No Quadro 12, apresentam-se informações adicionais sobre as categorias de vulnerabilidades referidas na Figura 15.

Quadro 12 - Vulnerabilidades, seus objetos e potenciais repercussões exemplificativas.

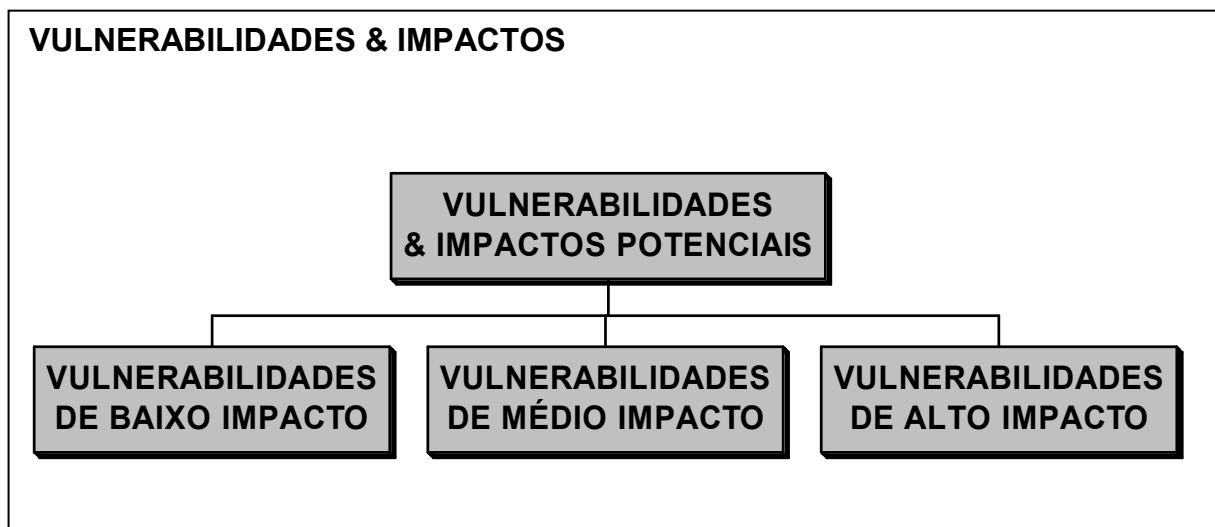
VULNERABILIDADES E SEUS OBJETOS		
CATEGORIA DE VULNERABILIDADE	OBJETO	EXEMPLOS DE REPERCUSSÕES POTENCIAIS
VULNERABILIDADE DE HARDWARE	<i>Hardware</i>	• Dano acidental a equipamento • Dano físico a equipamento • Furto/roubo de equipamento
VULNERABILIDADE DE SOFTWARE	<i>Software</i> (Sistema/ ambiente operacional, aplicativos e utilitários, e.g.)	• Deleção indevida de <i>software</i> impeditiva de acesso ao sistema por usuários autorizados • Alteração não autorizada de <i>software</i> impeditiva de sua execução ou de seu uso apropriado • Cópia não autorizada de <i>software</i> (Pirataria)
VULNERABILIDADE DE DADOS	Dados (Arquivos de dados, v.g.)	• Acesso não autorizado a dados • Análise de dados sigilosos • Alteração não autorizada de dados • Deleção indevida de dados • Destruição de dados • Negativa a usuários autorizados de acesso a dados
VULNERABILIDADE DE LINHAS E DE REDES DE COMUNICAÇÃO	Linhas e Redes de Comunicação	• Deleção de mensagens • Destruição de mensagens • Indisponibilidade de linhas de comunicação • Leitura não autorizada de mensagens • Avaliação do tráfego de mensagens • Modificação de mensagens • Retardamento, reordenação ou duplicação de mensagens • Envio de falsas mensagens

Fonte: Autor (2019) ³⁶.

É importante observar, ainda, a possibilidade de classificação das vulnerabilidades de segurança no tocante ao nível de impacto a elas associado, tal como ilustrado na Figura 16 e esclarecido no Quadro 13 (STALLINGS; BROWN, 2015).

³⁶ Quadro elaborado com a consideração de argumentos apresentados por Stallings e Brown (2015).

Figura 16 - Classificação das vulnerabilidades de segurança quanto ao nível de seus impactos potenciais para uma organização.



Fonte: Autor (2019) ³⁷.

Quadro 13 - Classificação das vulnerabilidades de segurança quanto ao nível de seus impactos potenciais para uma organização.

CLASSIFICAÇÃO DAS VULNERABILIDADES QUANTO AO SEU IMPACTO POTENCIAL		
NÍVEL DE IMPACTO	CARACTERIZAÇÃO	EXEMPLOS
VULNERABILIDADES DE BAIXO IMPACTO	Pequenas repercussões adversas a recursos do sistema e ao patrimônio e às operações de uma organização, bem como a indivíduos e entes	• Momentânea visível degradação de performance do sistema computacional • Danos de pequena monta ao patrimônio material e imaterial da organização em que o sistema vulnerável é utilizado • Prejuízos de pequeno porte a indivíduos/entes
VULNERABILIDADES DE MÉDIO IMPACTO	Efeitos adversos sérios a recursos do sistema e ao patrimônio e às operações da organização vulnerável, bem como a indivíduos e entidades	• Significativa degradação na performance do sistema vulnerável existente em uma organização • Danos de moderado porte ao patrimônio material e imaterial da organização em que utilizado o sistema

³⁷ Ilustração construída com base em exposição feita por Stallings e Brown (2015).

CLASSIFICAÇÃO DAS VULNERABILIDADES QUANTO AO SEU IMPACTO POTENCIAL		
NÍVEL DE IMPACTO	CARACTERIZAÇÃO	EXEMPLOS
		computacional vulnerável Danos significativos não vitais a indivíduos/entes
VULNERABILIDADES DE ALTO IMPACTO	Catastróficas consequências a recursos do sistema e ao patrimônio e às operações da organização em que se utiliza o sistema vulnerável, bem como a outros entes (pessoas e empresas)	- Degradação severa ou inoperância do sistema computacional vulnerável durante um determinado período de tempo (repercussão impeditiva da realização de funções essenciais) - Danos de grande vulto ao patrimônio material e imaterial da organização em que se emprega o sistema vulnerável - Danos significativos ou riscos de danos sérios a indivíduos (vida e integridade física pessoal)

Fonte: Autor (2019) ³⁸.

4.3 AMEAÇAS

4.3.1 Definição

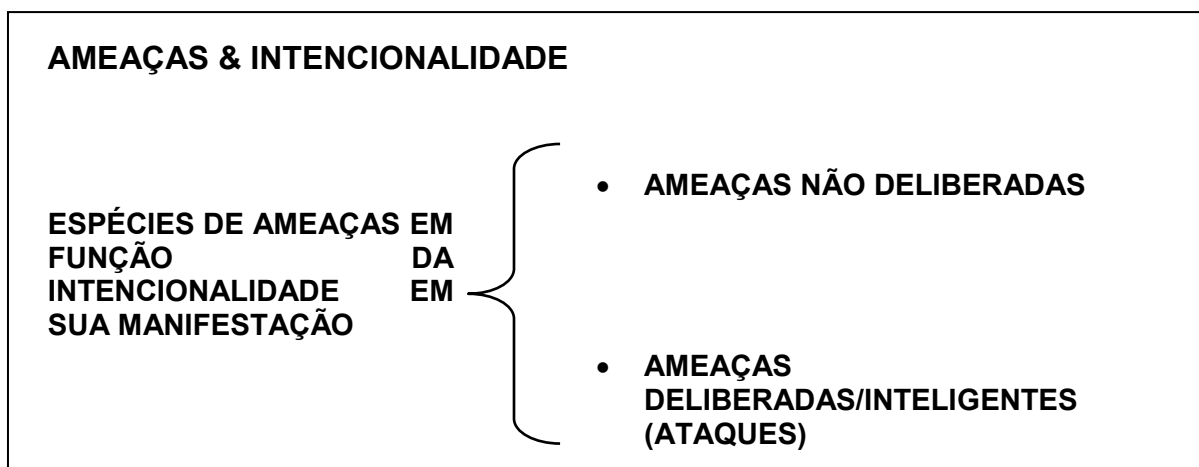
Usualmente, as ameaças são definidas como eventos, ações e circunstâncias que, em razão de vulnerabilidades, podem levar a violações de segurança em sistemas computacionais, ocasionando danos a indivíduos e a organizações (STALLINGS; BROWN, 2015).

4.3.2 Espécies

As ameaças, em termos genéricos, podem ser classificadas quanto à intencionalidade (STALLINGS; BROWN, 2015), como ilustrado na Figura 17.

³⁸ Quadro produzido em função das ideias referidas por Stallings e Brown (2015).

Figura 17 - Classificação das ameaças quanto à intencionalidade em sua manifestação.



Fonte: Autor (2019) ³⁹.

Como pode se depreender da nomenclatura utilizada na Figura 17, há duas variantes de ameaças considerado o aspecto volitivo, a intencionalidade. Nas Ameaças Não Deliberadas, não se evidencia o propósito de se violar segurança, o que, no entanto, se apresenta nas Ameaças Deliberadas/Inteligentes/Ataques.

Há que se observar, ainda, a possibilidade de as ameaças virem a ser categorizadas em função de suas potenciais consequências, como destacado no Quadro 14.

Quadro 14 - Categorias de ameaças em função de suas potenciais consequências.

CATEGORIAS DE AMEAÇAS EM FUNÇÃO DE SUAS POTENCIAIS CONSEQUÊNCIAS			
CATEGORIA DE AMEAÇA	DE	CARACTERIZAÇÃO	OBJETOS DA AMEAÇA
AMEAÇAS DE ACESSO NÃO AUTORIZADO		Circunstâncias ou eventos que possibilitam o acesso não autorizado a dados do sistema	• Confidencialidade
AMEAÇAS DE DECEPÇÃO		Circunstâncias ou eventos que tornam possível o recebimento de dados falsos, que se acredita terem sido remetidos por ente verdadeiro, mas não foram	• Integridade (Sistema e/ou Dados)

³⁹ Ilustração elaborada considerando-se ideias expostas em Stallings e Brown (2015).

CATEGORIAS DE AMEAÇAS EM FUNÇÃO DE SUAS POTENCIAIS CONSEQUÊNCIAS		
CATEGORIA DE AMEAÇA	CARACTERIZAÇÃO	OBJETOS DA AMEAÇA
AMEAÇAS DE RUPTURA	Circunstâncias ou eventos que interrompem o uso regular do sistema, ou impedem que este se dê de forma correta	• Integridade • Disponibilidade
AMEAÇAS DE USURPAÇÃO	Circunstâncias ou eventos que resultam na indevida transferência de controle do sistema a pessoa/entidade não autorizada	• Integridade

Fonte: Autor (2019) ⁴⁰.

Dada a relevância das Ameaças Deliberadas (Ataques), é destinada a Seção 4.4 à sua abordagem.

4.4 ATAQUES

4.4.1 Definição

Ataques constituem ameaças deliberadas voltadas à superação de obstáculos para violação de segurança de sistemas computacionais (STALLINGS; BROWN, 2015).

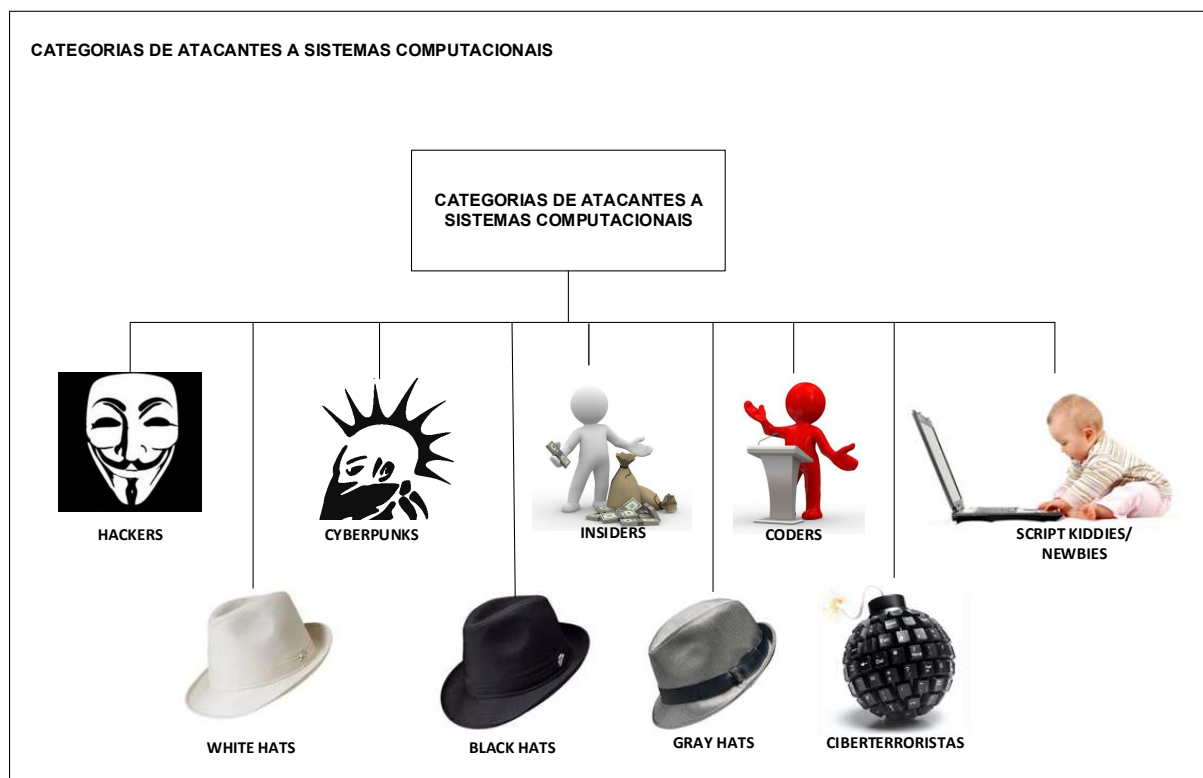
4.4.2 Agentes

O agente responsável pela deliberada e intencional realização de um ataque é, geralmente, denominado de atacante, agente ameaçador ou *hacker*.

É usual, considerados a *expertise* e o propósito do agente, o agrupamento dos atacantes em categorias próprias, como observado por Módulo Security Solutions *apud* Nakamura e Geus (2014) e ilustrado na Figura 18.

⁴⁰ Quadro construído com o emprego das considerações tecidas por Stallings e Brown (2015).

Figura 18 - Categorias de atacantes a sistemas computacionais.



Fonte: Autor (2019) ⁴¹.

No Quadro 15, apresentam-se informações básicas sobre as categorias indicadas na Figura 18.

Quadro 15 - Categorias de atacantes a sistemas computacionais.

CATEGORIAS DE ATACANTES A SISTEMAS COMPUTACIONAIS	
CATEGORIA	DESCRIÇÃO
 Hackers	Indivíduos que se dedicam a identificar vulnerabilidades de segurança sem propósito de causar danos a terceiros, para simples aferição de suas habilidades pessoais
 Script Kiddies/Newbies	<i>Hackers</i> iniciantes e inexperientes que, valendo-se de ferramentas pré-existent e prontas, realizam ataques sem ter o pleno conhecimento do que fazem
	<i>Hackers</i> de conhecimento extremo que se dedicam a identificar vulnerabilidades por prazer e que divulgam estas vulnerabilidades publicamente, contribuindo

⁴¹ Figura elaborada a partir de exposição feita por Nakamura e Geus (2014).

CATEGORIAS DE ATACANTES A SISTEMAS COMPUTACIONAIS	
CATEGORIA	DESCRIÇÃO
Cyberpunks	para pressionar, indiretamente, a indústria de <i>software</i> a corrigir estas falhas. São especialistas que costumam ter cuidado especial com a proteção de suas informações pessoais e são tidos como antissociais
 Insiders	Participantes da rede interna ao sistema de segurança computacional (funcionários, ex-funcionários, empregados terceirizados, etc.) que, por motivações diversas (insatisfação pessoal com chefia, ou intenção de usufruir ganho, e.g.), se aproveitam do conhecimento técnico e pessoal de que dispõem e divulgam/exploram vulnerabilidades
 Coders	<i>Hackers</i> que, atraídos por resultados financeiros, compartilham seus conhecimentos escrevendo livros e proferindo palestras/seminários sobre suas experiências
 White Hats/"Hackers do Bem"/Hackers Éticos/Samurais/Sneakers	<i>Hackers</i> profissionais contratados por organizações para identificar vulnerabilidades e promover as correções necessárias, mediante testes de invasão e análises de segurança
 Black Hats/Crackers/Full Fledged	Atacantes que invadem sistemas com a finalidade de se apropriar de informações ou de causar danos a terceiros ⁴²
 Gray Hats	<i>Black Hackers</i> com formação principal em <i>hacking</i> que atuam como <i>White Hats</i> em operações de segurança computacional
 Ciberterroristas	<i>Hackers</i> que, por convicções religiosas ou políticas, invadem sistemas computacionais para os derrubar, ou para obter informações sigilosas.

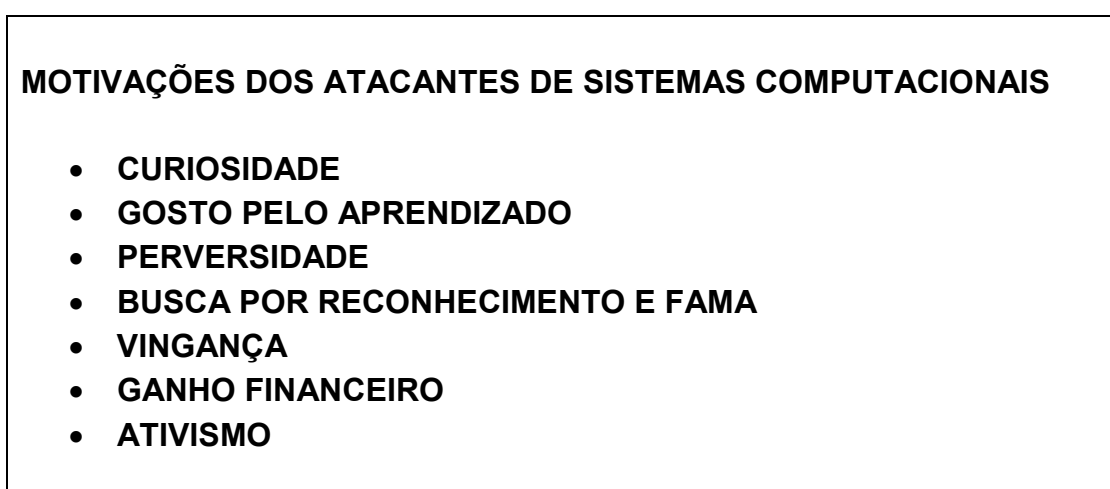
Fonte: Autor (2019) ⁴³.

⁴² Vale salientar, também, que a denominação *Cracker* é ainda utilizada na referência aos indivíduos que decifram códigos e que rompem proteções contra pirataria em *software*.

⁴³ Quadro construído em função das considerações tecidas por Nakamura e Geus (2014).

Do exame do Quadro 15, infere-se, ainda, que diversas são as motivações dos atacantes. Na Figura 19, apresentam-se as principais motivações dos atacantes (NAKAMURA; GEUS, 2014).

Figura 19 - Motivação dos atacantes de sistemas computacionais.



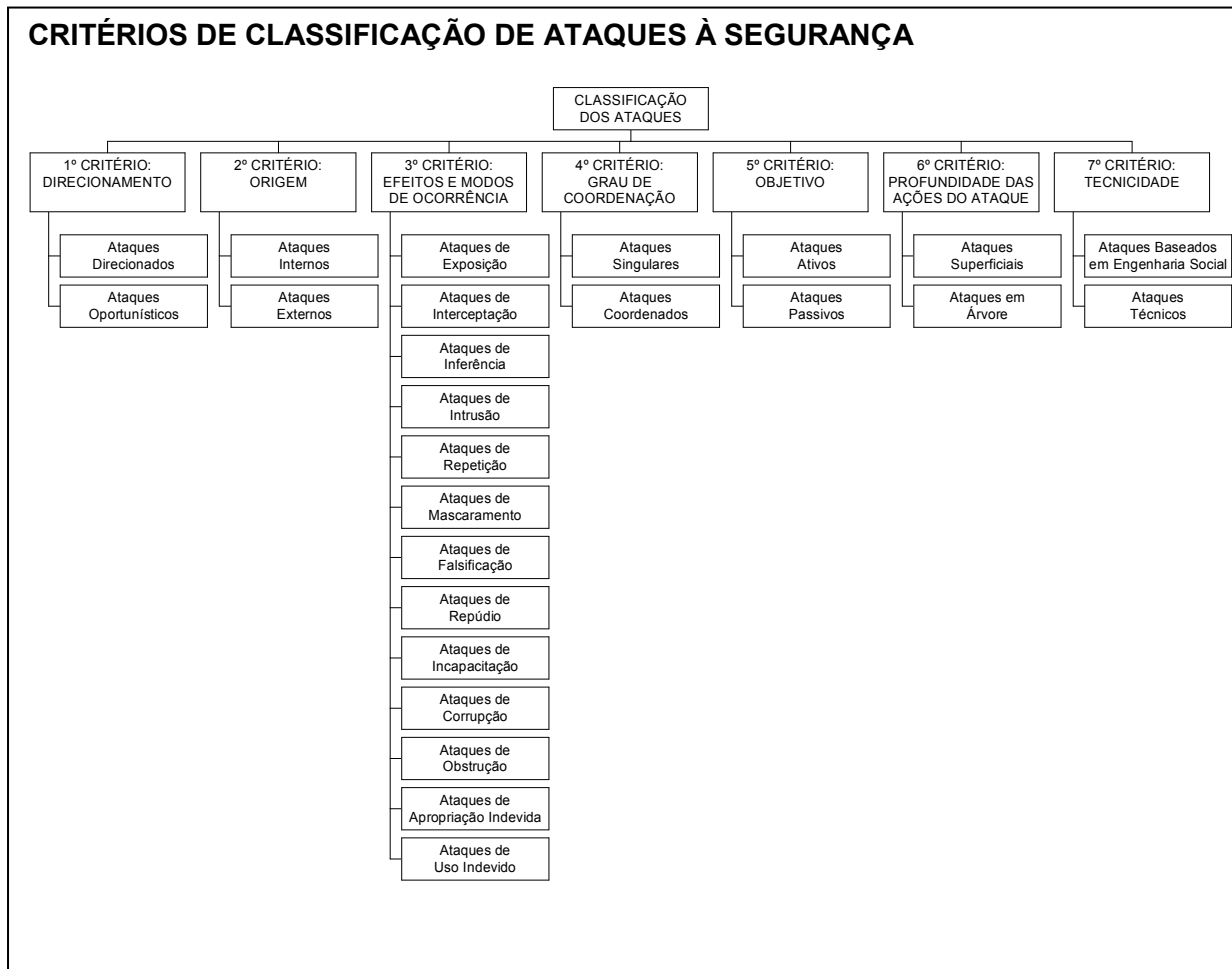
Fonte: Autor (2019) ⁴⁴.

4.4.3 Classificação

Diversos são os critérios empregáveis na classificação dos ataques (STALLINGS; BROWN, 2015; NAKAMURA; GEUS, 2014), como ilustrado na Figura 20.

⁴⁴ Figura elaborada a partir de exposição de Nakamura e Geus (2014).

Figura 20 - Critérios de classificação de ataques à segurança.



Fonte: Autor (2019) ⁴⁵.

No Quadro 16, apresentam-se informações suplementares sobre os critérios referidos na Figura 20.

⁴⁵ Figura construída com o emprego das ideias expostas por Nakamura e Geus (2014), bem como por Stallings e Brown (2015).

Quadro 16 - Classificação dos ataques de segurança.

CLASSIFICAÇÃO DOS ATAQUES DE SEGURANÇA		
CRITÉRIO	CATEGORIAS	DESCRIÇÃO
DIRECIONAMENTO	Ataques Direcionados	Ataques com alvos certos e determinados previamente definidos pelo atacante
	Ataques Oportunísticos	Ataques decorrentes de oportunidades identificadas e não da intencional busca por alvo específico
ORIGEM	Ataques Internos	Ataques iniciados por entes com certo nível de autorização, localizados dentro do perímetro de segurança, que agem como se lhes tivessem sido conferidas prerrogativas maiores de acesso
	Ataques Externos	Ataques iniciados fora do perímetro de segurança por usuários externos não autorizados (" <i>outsiders</i> ")
NATUREZA DOS POTENCIAIS EFEITOS E MODOS DE OCORRÊNCIA	Ataques de Exposição	Ataques em que dados sensíveis/sigilosos são liberados a entes não autorizados por usuário autorizado
	Ataques de Interceptação	Ataques em que entes não autorizados ganham acesso direto a dados em transmissão entre origens e destinos autorizados
	Ataques de Inferência	Ataques e, que um ente não autorizado, mediante observação/análise de características e padrões em blocos de transmissão e em blocos de dados, infere/deduz informações sensíveis
	Ataques de Intrusão	Ataques em que entes não autorizados, rompendo barreiras/proteções de segurança, ganham acesso a dados sensíveis
	Ataques de Repetição	Ataques em que uma unidade de dados é capturada e retransmitida com foco na produção de efeito não autorizado

CLASSIFICAÇÃO DOS ATAQUES DE SEGURANÇA		
CRITÉRIO	CATEGORIAS	DESCRIÇÃO
	Ataques de Mascaramento	Ataques em que um ente não autorizado, passando-se por ente autorizado, ganha acesso a dados sensíveis
	Ataques de Falsificação	Ataques em que dados falsos/dados adulterados são recebidos como verdadeiros por ente autorizado
	Ataques de Repúdio	Ataques em que uma entidade ludibria outra mediante negativa de responsabilidade por atos, ou pela posse de dados
	Ataques de Incapacitação	Ataques em que a operação do sistema é impedida ou interrompida com a desativação/destruição de componente do próprio sistema
	Ataques de Corrupção	Ataques em que dados ou funcionalidades do sistema são alterados indevidamente
	Ataques de Obstrução	Ataques em que o fornecimento de serviços pelo sistema é interrompido através da obstrução dos sistemas mediante, por exemplo, alteração/inativação da comunicação, ou imposição de carga/tráfego excessivo aos recursos de processamento do sistema
	Ataques de Apropriação Indevida	Ataques em que uma entidade não autorizada assume o controle lógico ou físico de recursos de um sistema
	Ataques de Uso Indevido	Ataques em que componentes do sistema realizam funções ou fornecem serviços que são indevidos ou até mesmo nocivos à segurança do próprio sistema
GRAU DE COORDENAÇÃO	Ataques Singulares	Ataques realizados por indivíduos/grupos isolados sem prévio ajuste coletivo organizado

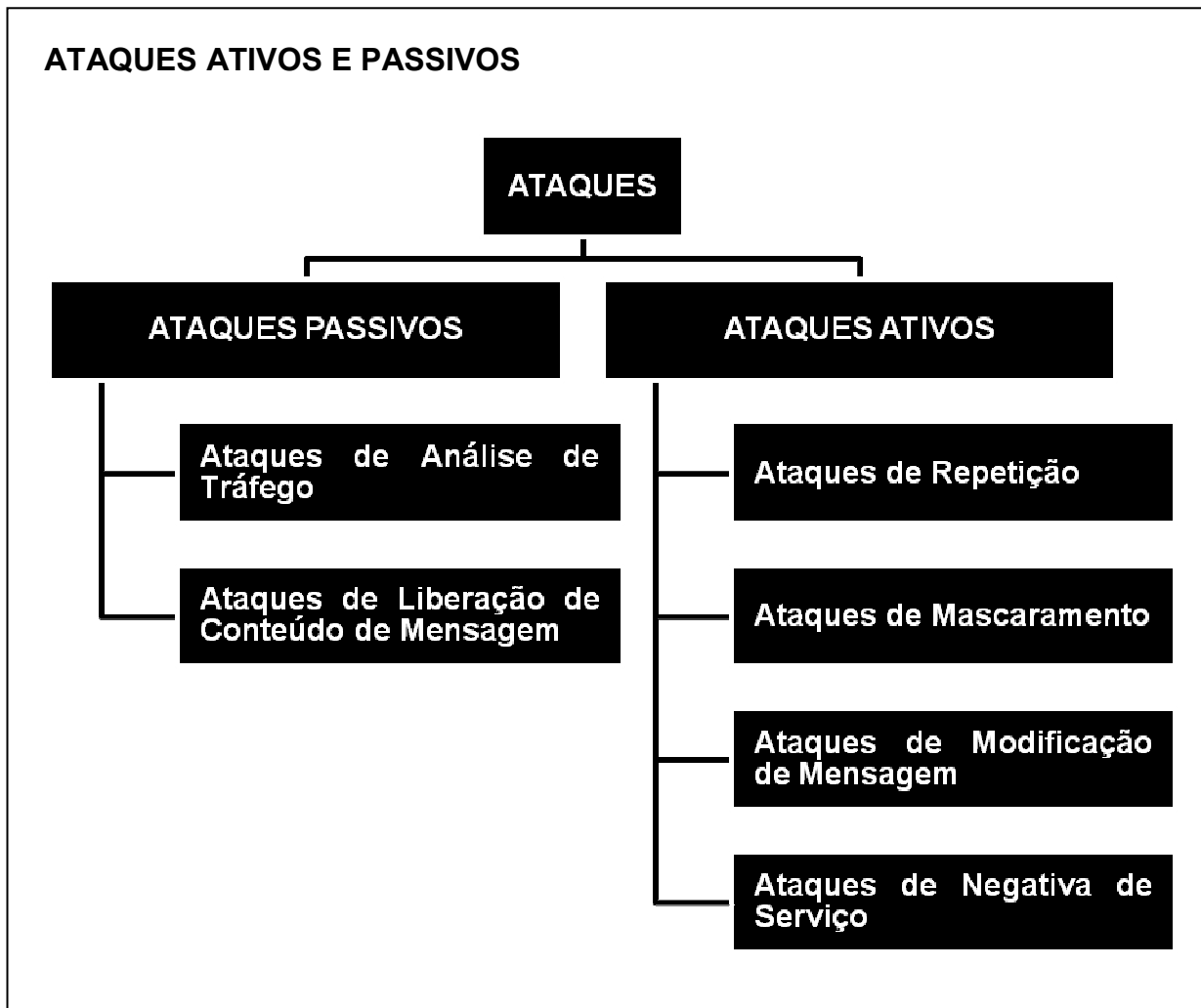
CLASSIFICAÇÃO DOS ATAQUES DE SEGURANÇA		
CRITÉRIO	CATEGORIAS	DESCRIÇÃO
OBJETIVO	Ataques Coordenados	Ataques que para sua realização concorrem indivíduos/grupos diversos de modo organizado e ajustado
	Ataques Ativos	Ataques voltados a alterar recursos do sistema (dados, inclusive), ou a afetar sua operação
	Ataques Passivos	Ataques cujo objetivo é propiciar aprendizado, ou fazer uso de informação do sistema, sem que, contudo, recursos do sistema sejam afetados
PROFUNDIDADE DAS AÇÕES DO ATAQUE	Ataques Superficiais	Ataques em que vulnerabilidades são diretamente acessíveis, não sendo necessário empreender esforços prévios para que as mesmas se tornem expostas
	Ataques em Árvores	Ataques em que, para se acessar uma dada vulnerabilidade em particular, há de se percorrer um caminho, uma "série", de vulnerabilidades prévias
TECNICIDADE	Ataques Baseados em Engenharia Social	Ataques em que estratégias de manipulação/convencimento humano são utilizadas para descoberta/exploração de vulnerabilidade
	Ataques Técnicos	Ataques em que apenas o conhecimento técnico é empregado na exploração de vulnerabilidades

Fonte: Autor (2019) ⁴⁶.

Na Figura 21, apresenta-se agrupamento adicional dos ataques ativos e passivos (STALLINGS; BROWN, 2015), expondo-se, no Quadro 17, informações adicionais sobre as categorias nela referidas.

⁴⁶ Quadro elaborado com o emprego das considerações de Nakamura e Geus (2014), bem como de Stallings e Brown (2015).

Figura 21 - Agrupamento adicional dos ataques ativos e passivos.



Fonte: Autor (2019)⁴⁷.

Quadro 17 - Categorias de ataques ativos e passivos.

CATEGORIAS DE ATAQUES ATIVOS E PASSIVOS		
ESPÉCIE DE ATAQUE	CATEGORIA	DESCRIÇÃO
ATAQUES PASSIVOS	Ataque de Liberação de Conteúdo	Ataque em que, mediante observação, conteúdo de mensagem é aprendido/inferido por ente não autorizado
	Ataque de Análise de Tráfego	Ataque em que, mediante observação, aspectos e padrões de comunicação são aprendidos/inferidos

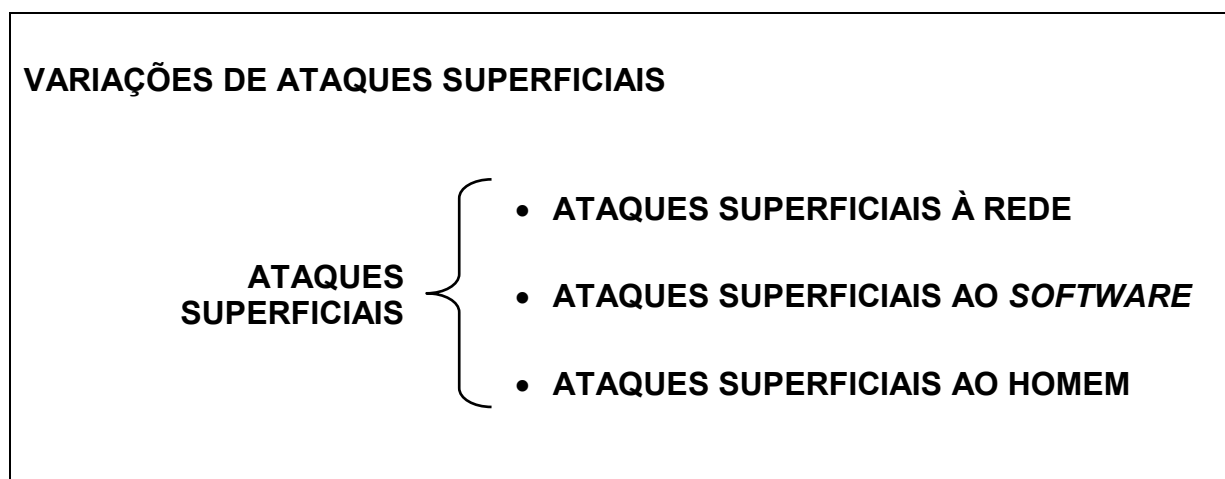
⁴⁷ Figura construída com aproveitamento de ideias expostas por Stallings e Brown (2015).

CATEGORIAS DE ATAQUES ATIVOS E PASSIVOS		
ESPÉCIE DE ATAQUE	CATEGORIA	DESCRIÇÃO
ATAQUES ATIVOS	Ataque de Repetição	Ataque em que unidade de dado interceptada é retransmitida, produzindo resultados não autorizados
	Ataque de Mascaramento	Ataque em que uma entidade se faz passar por outra, obtendo, sem autorização legítima, privilégios de acesso e uso do sistema
	Ataque de Modificação de Mensagem	Ataque em que mensagem retardada/alterada ou reordenada produz resultado não autorizado
	Ataque de Negativa de Serviço	Ataque em que se inibe ou se impede o normal uso/gerenciamento de facilidades de comunicação

Fontr: Autor (2019)⁴⁸.

Há que se observar, ainda, que os ataques superficiais também apresentam variações (STALLINGS; BROWN, 2015), como ilustrado na Figura 22.

Figura 22 - Variações de ataques superficiais.



Fonte: Autor (2019)⁴⁹.

Como se depreende do exame da Figura 22, os ataques superficiais apresentam variações, considerado o seu alvo: rede, *software* ou pessoas (STALLINGS; BROWN, 2015). No Quadro 18, são expostas observações acerca destas variantes de ataques.

⁴⁸ Quadro produzido com base na exposição de Stallings e Brown (2015).

⁴⁹ Ilustração concebida a partir das considerações de Stallings e Brown (2015).

Quadro 18 - Variações de ataques superficiais.

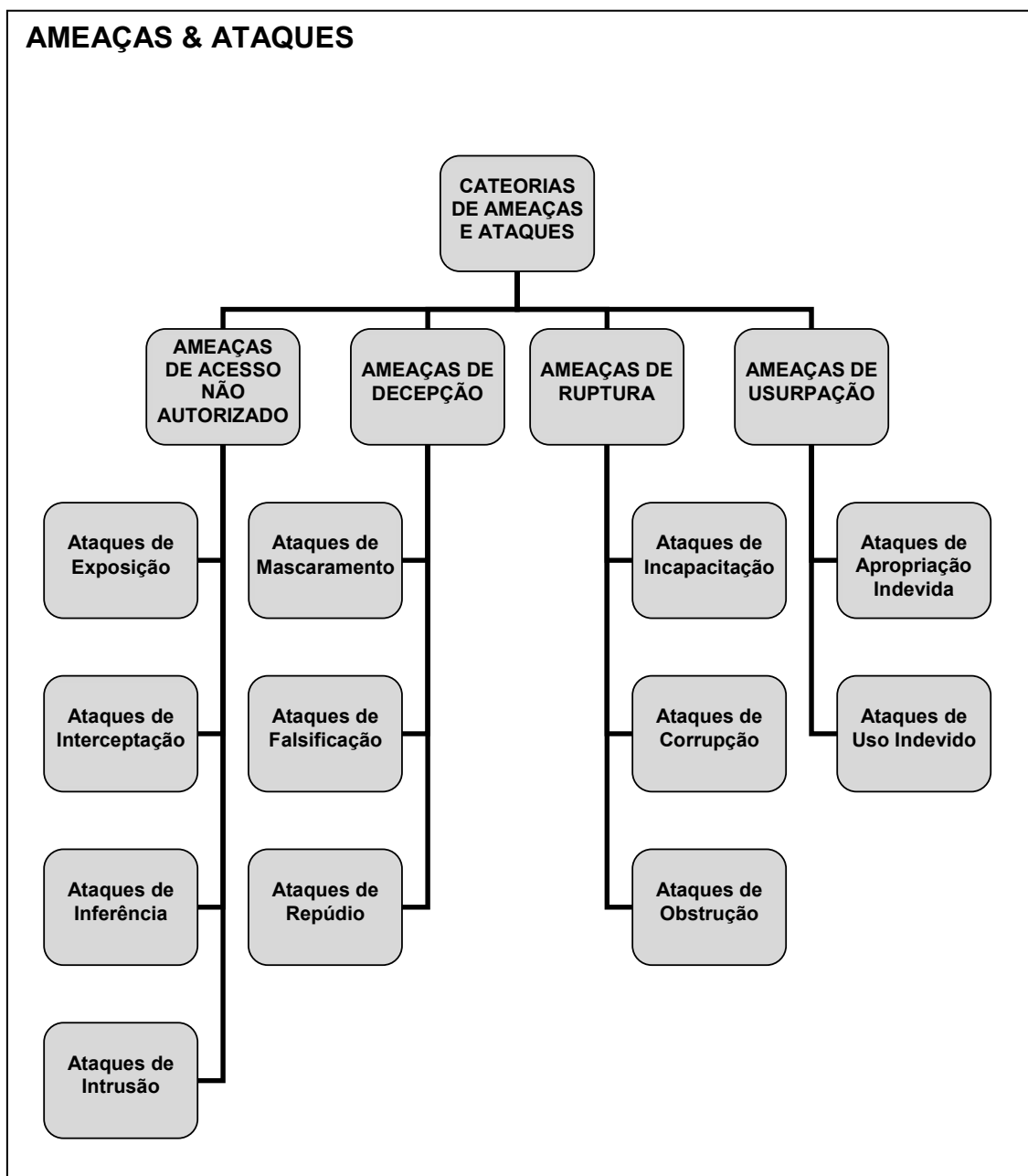
VARIAÇÕES DE ATAQUES SUPERFICIAIS		
VARIAÇÃO	DESCRIÇÃO	EXEMPLOS DE VULNERABILIDADES ASSOCIADAS
ATAQUE SUPERFICIAL À REDE	Ataque em que vulnerabilidades de uma rede são exploradas, sejam estas redes, por exemplo, <i>Local Area Networks (LANs)</i> , <i>Wide Area Networks (WANs)</i> , ou Internet	- Falhas em protocolos de comunicação <i>Links</i> corrompidos - Indevida abertura de portas - Equivocada disponibilização de serviços via <i>firewall</i>
ATAQUE SUPERFICIAL AO SOFTWARE	Ataque em que vulnerabilidades de <i>software</i> são alvos	- Falhas em aplicações e sistemas (Formulários <i>Web</i> com entradas desprotegidas para comandos em <i>Structured Query Language (SQL)</i> e código que processa dados em formatos padronizados de conhecimento público, e.g.) - Brechas de acesso em sistemas/ambientes operacionais
ATAQUE SUPERFICIAL AO HOMEM	Ataque em que vulnerabilidades geradas por pessoas (internas ou externas à organização) são aproveitadas	- Erro humano - Elevado nível de confiança interpessoal com indevido compartilhamento de acessos exclusivos - Susceptibilidade pessoal individual à exposição de informações sensíveis

Fonte: Autor (2019) ⁵⁰.

Por fim, quanto às espécies de ataques, é válido registrar a possibilidade de estabelecimento de relações com as ameaças respectivas, tal como ilustrado na Figura 23.

⁵⁰ Quadro elaborado com o emprego de ideias apresentadas por Stallings e Brown (2015).

Figura 23 - Categorias de ameaças e ataques respectivos.



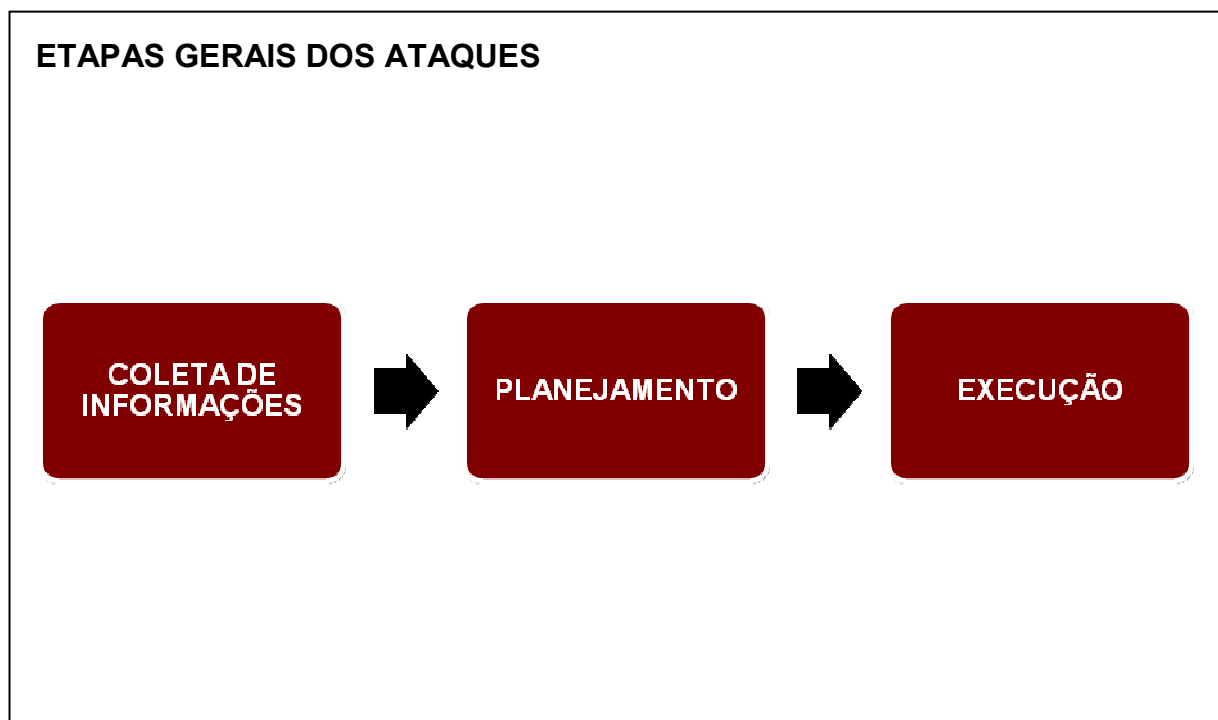
Fonte: Autor (2019) ⁵¹.

4.4.4 Planejamento e execução de ataques

Para a exitosa realização de ataques, é necessário, usualmente, que alguns passos sejam percorridos pelo atacante (NAKAMURA; GEUS, 2014), como se ilustra na Figura 24.

⁵¹ Figura construída considerando-se exposição de Stallings e Brown (2015).

Figura 24 - Etapas gerais dos ataques à Segurança Computacional.



Fonte: Autor (2019) ⁵².

Da leitura da Figura 24, depreende-se que, coletando informações sobre o alvo, o atacante se torna mais apto a definir suas abordagens de ataque, ou seja, é mais provável que o mesmo consiga planejar uma estratégia mais eficaz. Definidas as estratégias de abordagem, passa-se à execução, ocasião em que técnicas diversas são empregadas para consecução do fim almejado.

4.4.4.1 Coleta de informações

Na coleta de informações, diversas estratégias e técnicas são adotadas pelos atacantes (NAKAMURA; GEUS, 2014), como as referidas na Figura 25.

⁵² Ilustração produzida com o emprego das ideias expostas por Nakamura e Geus (2014).

Figura 25 - Estratégias e técnicas de coleta de informações.

Fonte: Autor (2019) ⁵³.

No Quadro 19, são expostas informações básicas sobre as estratégias e técnicas referidas na Figura 25 (NAKAMURA; GEUS, 2014).

⁵³ Ilustração concebida com a adaptação de ideias expostas por Nakamura e Geus (2014).

Quadro 19 - Estratégias e técnicas de coleta de informações.

ESTRATÉGIAS E TÉCNICAS DE COLETA DE INFORMAÇÕES		
ESTRATÉGIA/TÉCNICA	IDEIA BÁSICA	INFORMAÇÕES/MATERIAIS PASSÍVEIS DE OBTENÇÃO
DUMPSTER DIVING/ TRASHING	Inspeciona-se o lixo do alvo a ser atacado ou de seus colaboradores/associados, na busca por informações sobre a organização e/ou seus usuários	• Logins de contas • Senhas de acesso • Informações pessoais sigilosas • Listas telefônicas corporativas • Organogramas • Memorandos internos • Manuais de políticas • Manuais de sistemas de eventos e de férias⁵⁴ • Código-fonte sigiloso • Calendários de reuniões • Inventários de <i>hardware</i>
ENGENHARIA SOCIAL	Explorando-se fraquezas e características humanas e sociais (simpatia, busca por aprovação social, consistência, autoridade e medo, e.g.), manipulam-se pessoas com a assunção de falsa identidade e/ou instalação de <i>backdoors</i> /bombas lógicas em <i>softwares</i> , obtendo-se, indevidamente, informações de acesso restrito	• Logins de contas • Senhas de acesso • Documentos sigilosos

⁵⁴ Ainda que possa parecer improvável a utilidade de informações sobre eventos e férias, tais informações poderiam, sim, vir a ser úteis a *hackers*. Conhecendo a escala de eventos da organização-alvo (organização que ele deseja invadir), um *hacker* poderia vir a saber, por exemplo, de alguma confraternização na aludida organização-alvo, o que, provavelmente, afastaria, de suas funções habituais, significativa parcela dos funcionários desta organização, deixando seus serviços e estrutura mais vulneráveis. O conhecimento no tocante às férias dos colaboradores/funcionários, por seu turno, poderia ser utilizado por um *hacker* em estratégias de Engenharia Social, ou seja, sabendo das férias de um dado colaborador “X” que têm acesso a recursos “Y”, o *hacker* poderia se passar por um colaborador fictício e informar, aos funcionários subordinados a “X”, que ele seria o mais novo contratado e que “X”, antes de entrar em férias, teria lhe incumbido de diversas atividades, para as quais ele precisaria de permissão especial de acesso aos recursos “Y”. Um subordinado incauto poderia dar estas permissões, ou fornecer ao *hacker* noções sobre como obtê-las na estrutura administrativa da organização.

ESTRATÉGIAS E TÉCNICAS DE COLETA DE INFORMAÇÕES		
ESTRATÉGIA/TÉCNICA	IDEIA BÁSICA	INFORMAÇÕES/MATERIAIS PASSÍVEIS DE OBTENÇÃO
ACESSO FÍSICO	Mediante furto/roubo de equipamentos/ <i>software</i> , através de ocorrência extraordinária que altere o meio físico (terremoto, furacão, enchente e incêndio, e.g.), ou via contato direto, obtém-se indevido acesso à organização, ou ao sistema computacional alvo, não sendo necessário empreender medidas para acesso remoto	• <i>Logins</i> de contas • Senhas de acesso • Documentos sigilosos • E-mails de terceiros • Informações privilegiadas sobre o alvo (salários de colaboradores e projetos de lançamento de novos produtos/serviços, e.g.)
BUSCA POR INFORMAÇÕES LIVRES	Através da simples observação e de consultas diversas (análise de cabeçalhos de e-mail, consulta a servidores de sistemas de nomes de domínio – <i>Domain Name System (DNS)</i> , pesquisas em listas de discussão e buscas na própria Internet ⁵⁵ , e.g.), obtém-se informações significativas acerca da organização e seus sistemas computacionais	• Organograma da organização • Listas de <i>e-mails</i> • Identificação e versão dos sistemas operacionais em uso
PACKET SNIFFING/ PASSIVE EAVESDROPPING	Captura, com o uso de <i>software</i> próprio, de informações valiosas diretamente do fluxo de pacotes em rede, através de sua análise	• Senhas de serviços na rede • Conteúdos em transmissão na rede

⁵⁵ Através de pesquisas em fóruns de discussão e de simples buscas na Internet, um agente mal intencionado poderia, por exemplo, saber qual o quadro de funcionários da equipe de Tecnologia de uma organização (organização-alvo) e, de posse desta informação, poderia analisar os *currícua* dos citados funcionários, identificando possíveis falhas em suas formações acadêmicas e profissionais. Cientes das referidas falhas, o hipotético *hacker* em debate poderia elaborar um plano (plano de invasão, por exemplo) com maior probabilidade de sucesso, já que não gastaria recursos com estratégias que envolvessem o ataque de pontos possivelmente fortes da organização, dado que a força/fraqueza/deficiência de uma organização advém da força/fraqueza/deficiência de seus colaboradores.

ESTRATÉGIAS E TÉCNICAS DE COLETA DE INFORMAÇÕES		
ESTRATÉGIA/TÉCNICA	IDEIA BÁSICA	INFORMAÇÕES/MATERIAIS PASSÍVEIS DE OBTENÇÃO
PORT SCANNING	Obtenção, o emprego de <i>software</i> próprio (<i>port scanners</i>), de informações relativas aos serviços acessíveis por portas nos protocolos <i>Transmission Control Protocol (TCP)</i> e <i>User Datagram Protocol (UDP)</i> , evitando-se desperdício de recursos <i>hackers</i> com o ataque de serviços inexistentes ⁵⁶	• Informações dos serviços acessíveis através de portas <i>TCP</i> e <i>UDP</i>
SCANNING DE VULNERABILIDADES	Mapeados os serviços utilizados com o emprego de <i>port scanners</i> , <i>scanners</i> de vulnerabilidades são usados para identificar falhas de segurança em protocolos, serviços, aplicativos ou sistemas operacionais	• Senhas de acesso fáceis de adivinhação (<i>password guessing</i>) • Compartilhamentos desprotegidos por senhas • Configurações de serviços e roteadores • Configurações incorretas • Desatualização de <i>software</i>
FIREWALKING	Obtenção de informações do <i>firewall</i> e da própria rede (topologia), mediante a passagem de pacotes	• Dados de Roteadores • Topologia da rede do sistema computacional alvo
IP SPOOFING	Acesso ao sistema computacional alvo através do mascaramento de endereços no <i>Internet Protocol (IP)</i> : mascaramento falso para autenticação em relações de confiança	• Dados originalmente disponíveis no sistema computacional alvo

Fonte: Autor (2019) ⁵⁷.

Conclusivamente, quanto aos *scanners* de vulnerabilidades, apresenta-

⁵⁶ É importante se observar, ainda, a possibilidade de o ataque em si se efetivar com *port scanners*, já que eles podem apresentar repercussões outras (NAKAMURA; GEUS, 2014).

⁵⁷ Quadro elaborado com a adaptação das ideias apresentadas por Nakamura e Geus (2014).

se o Quadro 20, elencando-se alguns objetos com falhas de segurança através deles identificadas em dois sistemas/ambientes operacionais.

Quadro 20 - Falhas de segurança identificadas com *scanners* de vulnerabilidades.

OBJETOS COM FALHAS DE SEGURANÇA IDENTIFICÁVEIS COM SCANNERS DE VULNERABILIDADES	
WINDOWS	UNIX
• <i>Servidor Web Internet Information Services (IIS)</i> • <i>Microsoft Data Access Components (MDAC)</i> • <i>Microsoft SQL Server</i> • <i>Network Basic Input/Output System (NetBIOS)</i> • <i>LAN Manager (LM)</i> • <i>Internet Explorer (IE)</i> • <i>Windows Scripting Host</i>	• <i>Remote Procedure Calls (RPC)</i> • <i>Servidor Web Apache</i> • <i>Secure Shell (SSH)</i> • <i>Simple Network Management Protocol (SNMP)</i> • <i>File Transfer Protocol (FTP)</i> • <i>Servidor Remoto de Impressão Line Printer Daemon (LPD)</i> • <i>Servidor de E-mail Sendmail</i>

Fonte: Autor (2019) ⁵⁸.

4.4.4.2 Planejamento

Coletadas informações dos possíveis alvos, reflete-se acerca dos objetivos do ataque e dos recursos disponíveis a esta finalidade, definindo-se a estratégia de ataque e seu planejamento de ações.

4.4.4.3 Execução

Coletadas as informações e definida a estratégia, o ataque do sistema computacional se efetiva, geralmente, através de quatro espécies de ações (NAKAMURA; GEUS, 2014):

- monitoramento da rede;
- penetração no sistema;
- inserção de códigos prejudiciais ou de falsas informações no sistema;
- envio de séries de pacotes desnecessários ao sistema, tornando-o inoperante.

⁵⁸ Ilustração produzida a partir de exposição do SANS Institute *apud* Nakamura e Geus (2014).

4.4.5 Resultados potenciais dos ataques

Na visão de Nakamura e Geus (2014), dentre os potenciais resultados dos ataques, sobressaem-se:

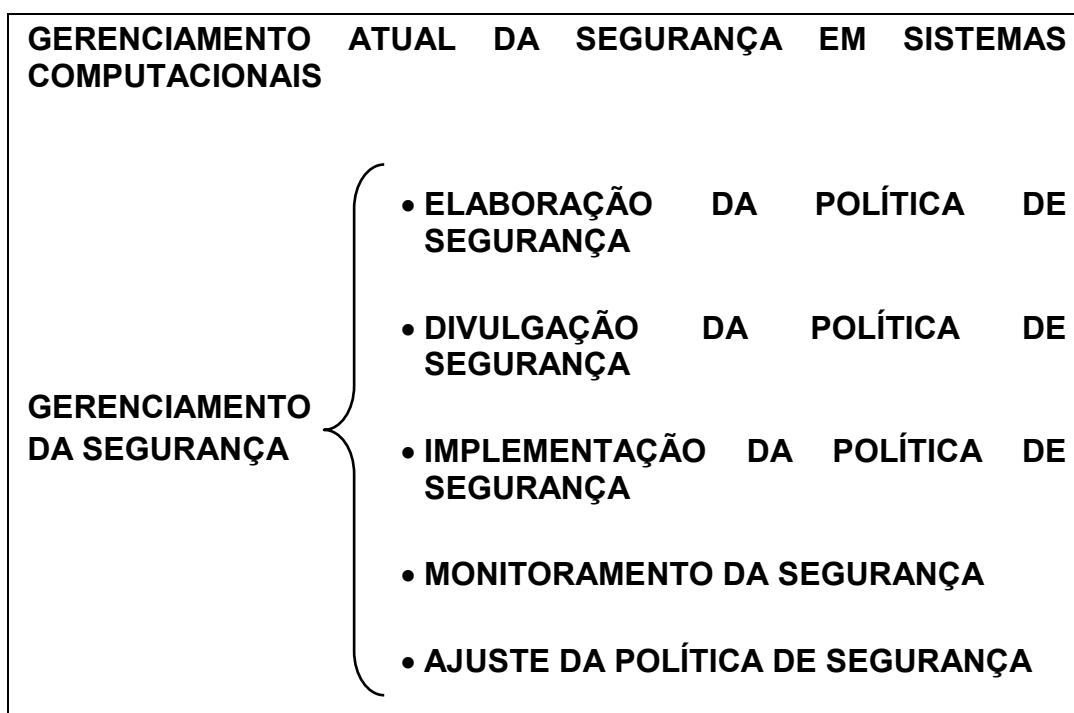
- monitoramento não autorizado do sistema computacional;
- obtenção e divulgação não autorizada de informações sigilosas;
- corrupção ou negação de serviços;
- prejuízos financeiros e fraudes;
- danos à imagem da organização em que se utiliza o sistema computacional atacado;
- perda de clientes, negócios e oportunidades;
- dispêndio de recursos (trabalho humano, inclusive) para recuperação de recursos do sistema computacional atacado.

4.5 GERENCIAMENTO DA SEGURANÇA EM SISTEMAS COMPUTACIONAIS

O gerenciamento da segurança em sistemas computacionais, hoje, envolve, essencialmente, a adoção de contramedidas voltadas à redução do risco potencial de danos em face de vulnerabilidades, ameaças e ataques. Com este desiderato, executam-se ações e se adotam técnicas/procedimentos/ferramentas que, sucessivamente, eliminem, evitem ou minimizem as probabilidades de danos e os seus impactos, observada, entretanto, a possibilidade de as contramedidas adotadas também apresentarem vulnerabilidades, que constituiriam riscos residuais (STALLINGS; BROWN, 2015).

Para Nakamura e Geus (2014), o atual gerenciamento da segurança envolve, em geral, cinco processos básicos, como ilustrado na Figura 26.

Figura 26 - Gerenciamento atual da Segurança em sistemas computacionais.



Fonte: Autor (2019) ⁵⁹.

Vale salientar que quatro dos processos referidos na Figura 26 integram uma espécie de ciclo, como ilustrado na Figura 27, eis que a gestão da segurança há de ser contínua e permanente.

Figura 27 - Processos do gerenciamento de Segurança em sistemas computacionais.



Fonte: Autor (2019) ⁶⁰.

⁵⁹ Ilustração concebida após reflexão sobre as considerações tecidas por Nakamura e Geus (2014).

⁶⁰ Ilustração concebida a partir de ideias expostas por Nakamura e Geus (2014).

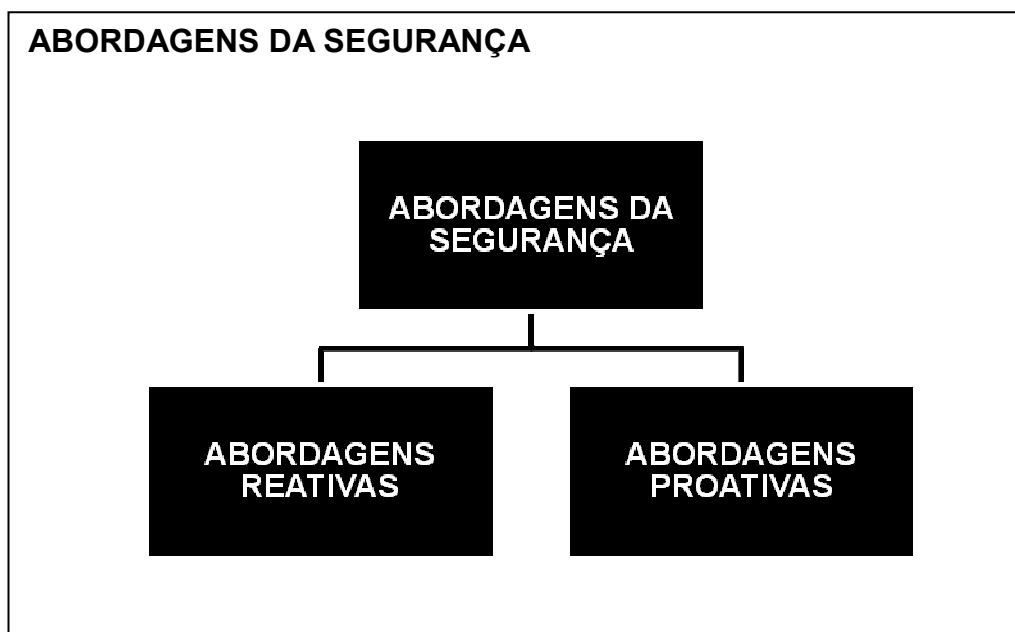
Usualmente, a gestão em debate é, assim, realizada *a posteriori*, isto é, desenvolvido e implantado um sistema, estabelecem-se diretrizes de segurança. Esta estratégia, contudo, tem sido alvo de questionamentos, vez que envolve postergação e transferência dos ônus relativos à segurança.

Apesar dos questionamentos mencionados, é patente a adoção prevalente da estratégia *a posteriori* de gestão da segurança computacional, razão pela qual, nas subseções seguintes, discorre-se sobre formas de abordagem, seu delineamento, princípios associados e objetos (políticas e recursos tecnológicos, em especial).

4.5.1 Abordagens de Segurança

A Segurança pode ser considerada sob dois enfoques (reativo e proativo), havendo, assim, duas abordagens principais de segurança, como ilustrado na Figura 28.

Figura 28 - Abordagens de Segurança.



Fonte: Autor (2019) ⁶¹.

⁶¹ Figura concebida a partir das ideias expostas por Nakamura e Geus (2014).

No Quadro 21, apresentam-se definições distintivas das abordagens referidas na Figura 28.

Quadro 21 - Abordagens de Segurança.

ABORDAGENS DE SEGURANÇA	
ABORDAGEM	DEFINIÇÃO
ABORDAGEM REATIVA DE SEGURANÇA	Abordagem em que a Segurança é considerada como relevante apenas após a ocorrência de ataques, havendo a preocupação apenas com o que já ocorreu em uma entidade/organização
ABORDAGEM PROATIVA DE SEGURANÇA	Abordagem em que a Segurança é pensada em termos de futuro, focando-se em evitar/minimizar a vulnerabilidade da organização a ataques, diminuindo-se as chances de prejuízos e/ou o seu vulto

Fonte: Autor (2019) ⁶².

4.5.2 Delineamento da estratégia de Segurança

O delineamento de estratégias de segurança computacional envolve, essencialmente, a definição de políticas de segurança e a implementação de mecanismos de segurança, bem como a avaliação e a garantia da confiabilidade de ambos (STALLINGS; BROWN, 2015), como ilustrado na Figura 29.

⁶² Quadro elaborado em função de exposição de Nakamura e Geus (2014).

Figura 29 - Delineamento de estratégias de Segurança Computacional.



Fonte: Autor (2019) ⁶³.

No Quadro 22, apresentam-se observações adicionais sobre os estados representados na Figura 29.

Quadro 22 - Delineamento de estratégias de Segurança Computacional.

DELINEAMENTO DE ESTRATÉGIAS DE SEGURANÇA COMPUTACIONAL		
ETAPA	DESCRIÇÃO	PONTOS DE ESPECIAL ATENÇÃO
DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA	Estabelecimento do que se espera do sistema computacional em termos de segurança, i.e., definição de um documento, formal ou informal ⁶⁴ , em	• Valores que se almeja proteger com o esquema de segurança • Vulnerabilidades do sistema computacional • Ameaças potenciais • Probabilidades de ataques • Balanceamento entre facilidade/simplicidade de uso do

⁶³ Ilustração construída com a consideração das ideias defendidas por Stallings e Brown (2015).

⁶⁴ Saliente-se, contudo, que, para alguns autores (Nakamura e Geus, por exemplo), a política de segurança há, necessariamente, de constituir um documento formal, vez que, assim, é mais evidente a obrigatoriedade de seu seguimento, dado o maior comprometimento que da formalização resulta. Estes mesmos autores registram, ainda, que, ausente uma política de segurança formal, eventual responsabilização por violações de segurança não pode ser imputada aos administradores/gestores de segurança, cabendo, pois, à direção da organização que rejeitar proposta de sua definição e implantação.

DELINEAMENTO DE ESTRATÉGIAS DE SEGURANÇA COMPUTACIONAL		
ETAPA	DESCRIÇÃO	PONTOS DE ESPECIAL ATENÇÃO
	que se consigne o que se espera que o esquema de segurança faça, que valores ele deve assegurar (requisitos de segurança, integridade, disponibilidade, etc.)	sistema computacional e segurança • Relação custo & benefício do esquema de segurança, i.e., avaliação do custo da segurança em comparação ao custo da exploração de vulnerabilidades e das medidas de recuperação (custo financeiro, legal e imaterial, e.g.)
IMPLEMENTAÇÃO DE MECANISMOS DE SEGURANÇA	Efetiva instalação dos mecanismos voltados à preservação da segurança computacional	• Prevenção de ataques e ameaças • Detecção de ameaças e ataques (ataques de intrusão e de negação de serviço, especialmente) • Resposta a ataques, interrompendo-se suas ocorrências e se evitando novos danos adicionais • Recuperação/restabelecimento do estado anterior do sistema ao ataque (estado de disponibilidade/funcionalidade do sistema e estado de integridade dos dados)
AVALIAÇÃO E GARANTIA DA CONFIABILIDADE DA ESTRUTURA DE SEGURANÇA (POLÍTICAS E MECANISMOS)	Avaliação e garantia da confiabilidade da estrutura de segurança definida (adequação e correção das políticas e mecanismos de segurança)	• Avaliação, mediante testes e análises matemáticas, do grau de confiabilidade da estrutura de segurança delineada e implantada • Fornecimento de sentimento de segurança técnica e operacional

Fonte: Autor (2019) ⁶⁵.

4.5.3 Princípios fundamentais de Segurança

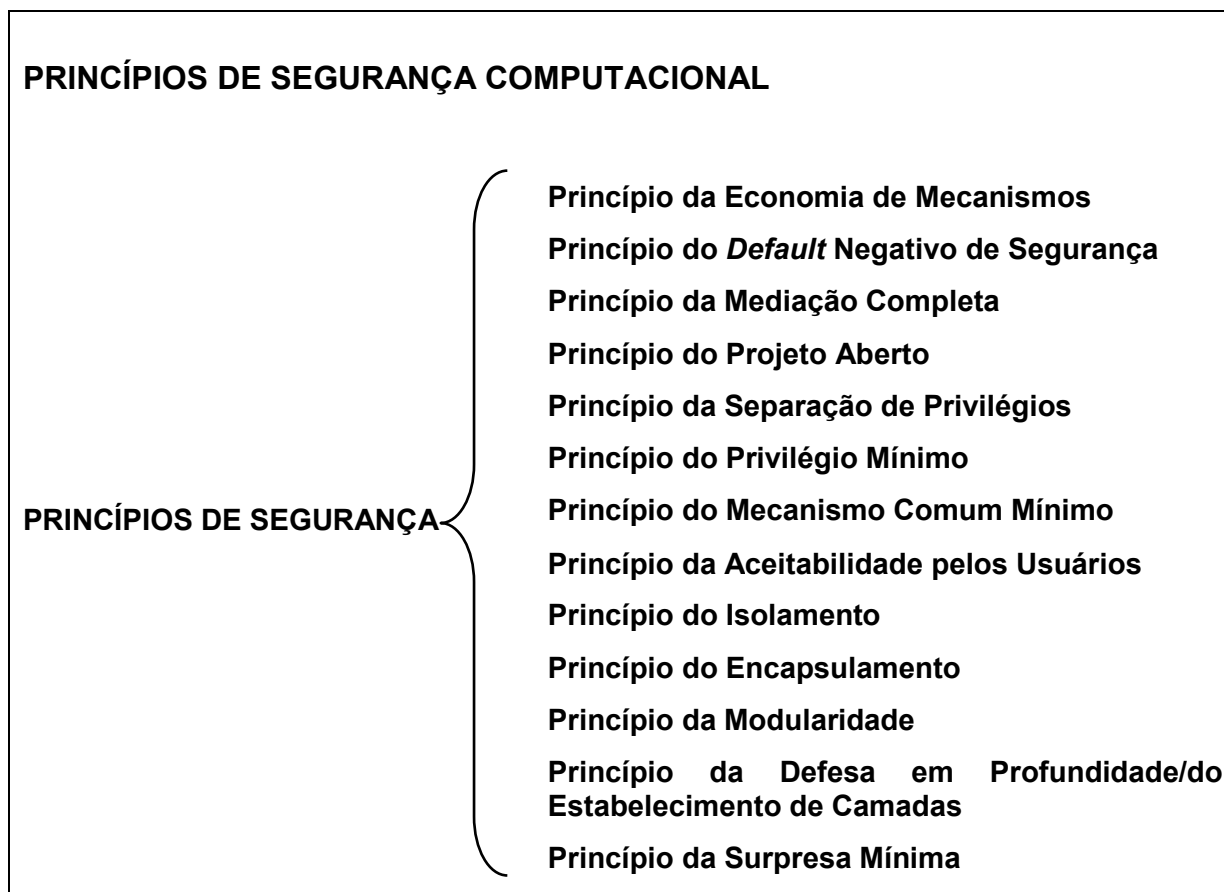
Ainda que não seja possível se assegurar, sistematicamente, a plena eficácia e eficiência de estruturas de segurança computacional, há como se

⁶⁵ Quadro elaborado a partir de exposição de Stallings e Brown (2015).

promover o delineamento e a implantação de estruturas com boa relação custo & benefício, recomendando-se, para tanto, a consideração de princípios fundamentais (STALLINGS; BROWN, 2015).

De acordo com Stallings e Brown (2015), são razoáveis as diretrizes/princípios traçados pelos *National Centers of Academic Excellence in Information Assurance* e pelos *National Centers of Academic Excellence in Cyber Defense*⁶⁶. Na Figura 30, apresentam-se estes princípios norteadores da definição de estruturas de segurança computacional, recorrendo-se brevemente acerca dos mesmos no Quadro 23.

Figura 30 - Princípios norteadores do delineamento e da implantação de estruturas de Segurança Computacional.



Fonte: Autor (2019)⁶⁷.

⁶⁶ Instituições americanas voltadas à promoção da excelência na garantia de informações e à defesa cibernética, com informações adicionais acessíveis em https://www.nsa.gov/ia/academic_outreach/nat_cae/.

⁶⁷ Figura construída com base nas ideias apresentadas por Stallings e Brown (2015).

Quadro 23 - Princípios norteadores do delineamento e da implantação de estruturas de Segurança Computacional.

PRINCÍPIOS NORTEADORES DO DELINEAMENTO E DA IMPLANTAÇÃO DE ESTRUTURAS DE SEGURANÇA COMPUTACIONAL	
PRINCÍPIO	IDEIAS BÁSICAS ASSOCIADAS
Princípio da Economia de Mecanismos	O delineamento da segurança computacional deve ser tão simples quanto possível, utilizando-se, idealmente, o menor número de mecanismos, pois, assim, evita-se desperdício de recursos, simplifica-se a gestão/teste do sistema de segurança e se diminui a quantidade de vulnerabilidades potenciais
Princípio do <i>Default</i> Negativo de Segurança	Por padrão, o acesso ao sistema computacional é definido como proibido, estabelecendo-se, caso a caso, as situações de permissão, vez que, deste modo, evita-se a ocorrência de eventual acesso não autorizado imediato e se pode conferir permissões, quando necessário
Princípio da Mediação Completa	Idealmente, cada acesso ao sistema deve ser feito diretamente através dos mecanismos de controle de acesso, não se admitindo decisões de acesso fundadas em cache. Por questões prático-operacionais, nem sempre este princípio é aplicável
Princípio do Projeto Aberto	Ainda que as chaves e certos objetos sejam secretos, o projeto de sistemas de segurança deve ser aberto e não sigiloso, possibilitando-se a realização de testes e auditorias por terceiros
Princípio da Separação de Privilegios	Para se evitar/minimizar ataques, devem ser conferidos privilégios de acesso individualizados para finalidades específicas
Princípio do Privilégio Mínimo	A cada usuário deve ser conferido o menor conjunto de privilégios possível, i.e., o conjunto mínimo de privilégios necessário e suficiente ao desempenho de suas atividades
Princípio do Mecanismo Comum Mínimo	Para se promover segurança mútua, rastreabilidade e responsabilidade, bem como para se simplificar o sistema e se reduzir a quantidade de fluxos indesejados de comunicação, deve-se evitar/minimizar o compartilhamento de funções entre usuários
Princípio da Aceitabilidade pelos Usuários	Deve-se almejar boa aceitação/receptividade dos usuários à segurança computacional, o que somente se verifica quando o sistema adotado não dificulta ou torna excessivamente custoso o seu uso regular e quando a estrutura do sistema de segurança é transparente para o usuário, ou seja, é compatível com um modelo mental de segurança que o próprio usuário consegue perceber/construir por si mesmo

PRINCÍPIOS NORTEADORES DO DELINEAMENTO E DA IMPLANTAÇÃO DE ESTRUTURAS DE SEGURANÇA COMPUTACIONAL	
PRINCÍPIO	IDEIAS BÁSICAS ASSOCIADAS
Princípio do Isolamento	Com foco na segurança (sigilo e veracidade, v.g.), há de se preservar recursos, obstando-se a interligação, física ou lógica, entre: a) recursos críticos do sistema e o acesso público ao sistema; b) processos e arquivos individuais de distintos usuários; c) mecanismos de segurança diversos
Princípio do Encapsulamento	Consideradas as ideias de isolamento e de orientação a objeto, coleções de procedimentos e objetos de dados são protegidos, fazendo-se com que sua estrutura interna apenas seja visível e acessível a determinados e específicos procedimentos de subsistemas já protegidos
Princípio da Modularidade	Com foco em atualizações, migrações e ajustes em tecnologias, é recomendado que a segurança seja trabalhada através de módulos, pois, assim, simplificam-se estes processos e se evita retrabalho no sistema como um todo
Princípio da Defesa em Profundidade/do Estabelecimento de Camadas	Aconselha-se a definição de defesas profundas, ou seja, o estabelecimento de camadas de segurança endereçadas a aspectos diversos do sistema computacional (pessoas, tecnologias e operações, e.g.), já que, com a adoção de múltiplas camadas, falha em uma única camada não expõe o sistema
Princípio da Surpresa Mínima	Atenção especial deve ser conferida às interfaces com usuários, de modo a evitar que os mesmos sejam indevidamente surpreendidos com <i>feedback</i> inapropriado

Fonte: Autor (2019) ⁶⁸.

4.5.4 Objetos da Segurança Computacional

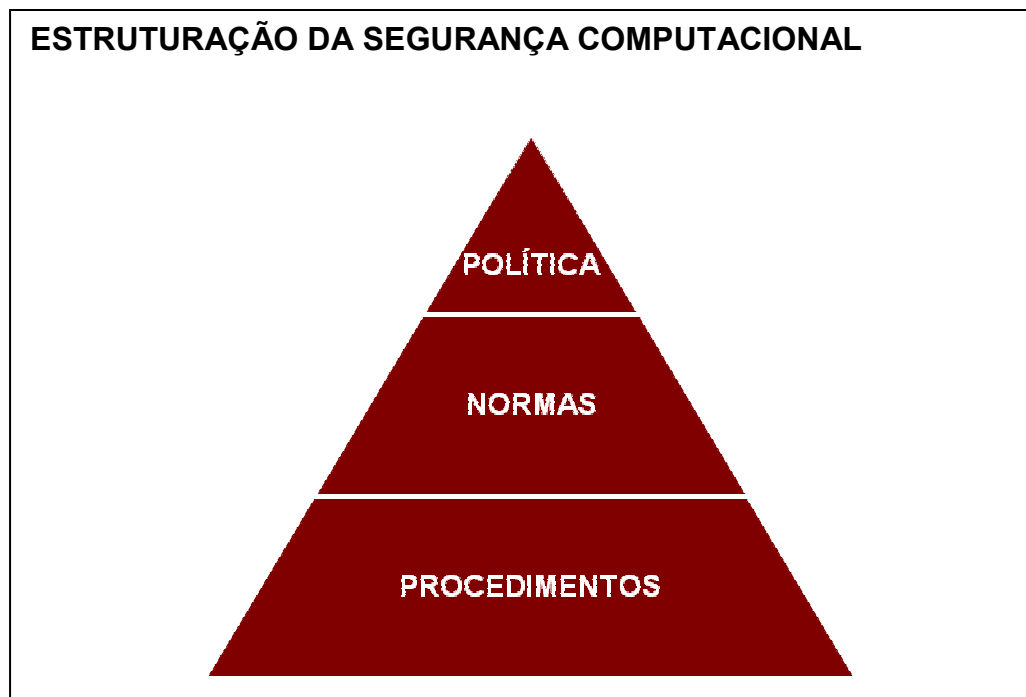
Para o estabelecimento da segurança em sistemas computacionais, há de se definir e implantar, como antes já dito, políticas de segurança, bem como técnicas, procedimentos e recursos de segurança.

A Segurança Computacional instaura-se, deste modo, mediante

⁶⁸ Quadro elaborado a partir de exposição de Stallings e Brown (2015).

políticas, normas e procedimentos, como ilustrado na Figura 31.

Figura 31 - Estruturação da Segurança Computacional.



Fonte: Autor (2019) ⁶⁹.

No Quadro 24, apresentam-se comentários basilares sobre os objetos indicados na Figura 31.

Quadro 24 - Estruturação da Segurança Computacional.

ESTRUTURAÇÃO DA SEGURANÇA COMPUTACIONAL	
OBJETO	FUNÇÃO
POLÍTICA	Orientação global de futuras ações e implementações relativas à Segurança
NORMAS	Detalhamento dos conceitos, projetos, sistemas de controle e implementações de segurança
PROCEDIMENTOS	Direcionamento específico das ações de administradores e usuários do sistema, consideradas as definições de segurança do sistema e as necessidades da organização

Fonte: Autor (2019) ⁷⁰.

⁶⁹ Adaptação de ilustração produzida por Nakamura e Geus (2014).

⁷⁰ Quadro elaborado com a consideração de exposição de Nakamura e Geus (2014).

Através dos objetos indicados na Figura 31 e no Quadro 24, estabelece-se a Segurança, vez que definidos:

- recursos acessíveis;
- permissões de acesso a recursos;
- procedimentos e controles de acesso e uso.

Quanto à estruturação em debate, é importante que se observe, por fim, como registrado por Nakamura e Geus (2014), que padrões podem ser seguidos, como os definidos pelo *British Standard Group (BSI Group)*, pela *International Organization for Standardization (ISO)*, pela *International Electrotechnical Commission (IEC)* e pela Associação Brasileira de Normas Técnicas (ABNT).

4.5.4.1 Políticas de Segurança

- **Definição, Atributos Almejados e Aspectos Relevantes**

Base da Segurança Computacional, a Política de Segurança se constitui no documento formal a respeito do tratamento da Segurança em uma entidade/organização (NAKAMURA; GEUS, 2014). A formalidade referida é, para alguns (NAKAMURA; GEUS, 2014), relevante atributo da Política de Segurança, dado o maior comprometimento que dela surge.

Outros atributos também são almejados nas políticas de segurança, como:

- generalidade;
- flexibilidade;
- criatividade;
- completude;
- enxugamento.

Considerado o propósito e o escopo amplo da Política de Segurança (regramento de todas as questões atinentes à Segurança em uma entidade),

incidem em sua definição aspectos de distintas naturezas, como os representados na Figura 32.

Figura 32 - Aspectos relevantes às políticas de segurança.

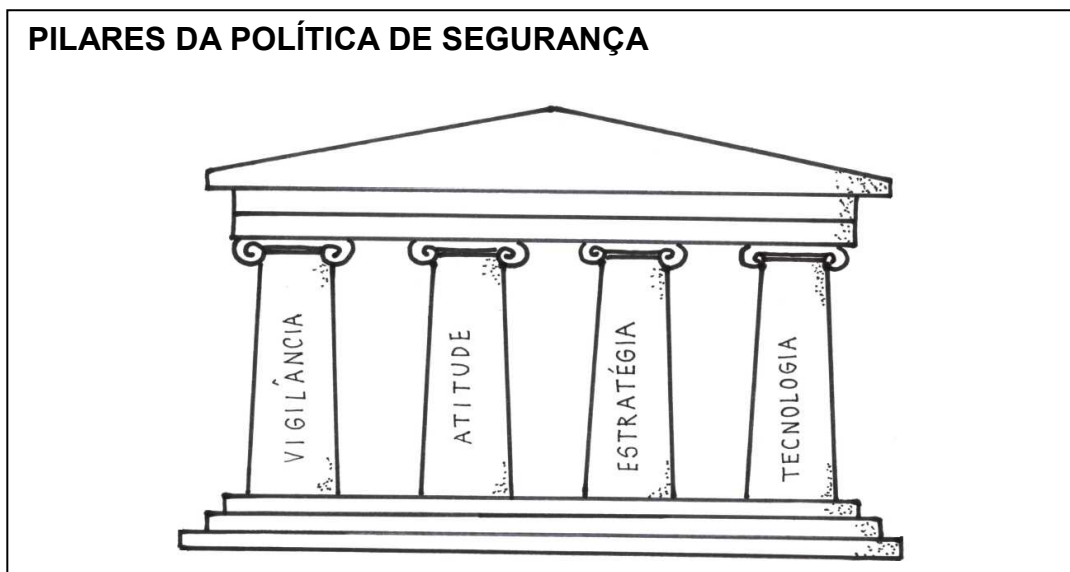


Fonte: Autor (2019) ⁷¹.

Em função das configurações específicas de cada organização/entidade quanto aos aspectos referidos na Figura 32, define-se a política de segurança, estabelecendo-se seus pilares de sustentação, como ilustrado na Figura 33.

⁷¹ Adaptação de ilustração produzida por Nakamura e Geus (2014).

Figura 33 - Pilares de sustentação das políticas de segurança.



Fonte: Autor (2019) ⁷².

No Quadro 25, tecem-se algumas considerações sobre os pilares representados na Figura 33.

Quadro 25 - Pilares de sustentação das políticas de segurança.

PILARES DE SUSTENTAÇÃO DAS POLÍTICAS DE SEGURANÇA	
PILAR	NOTA BÁSICA
ESTRATÉGIA	Foco e metas da segurança organizacional, considerados seus processos de negócio e peculiaridades
ATITUDE	Envolvimento concreto e efetivo dos que integram a organização, para que a segurança se torne uma realidade institucional
TECNOLOGIA	Emprego de tecnologias apropriadas adaptáveis à realidade da entidade/organização
VIGILÂNCIA	Monitoramento de sistemas e redes por administradores de segurança, bem como proatividade dos demais usuários conscientizados de seu papel para a Segurança

Fonte: Autor (2019) ⁷³.

⁷² Ilustração elaborada mediante adaptação de Figura e ideias de Nakamura e Geus (2014).

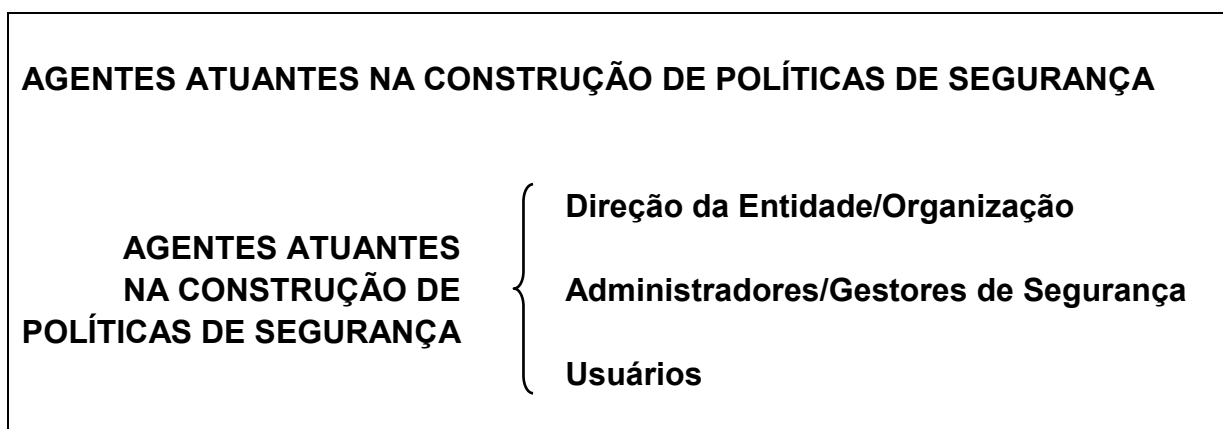
⁷³ Quadro construído mediante reflexão a partir de exposição de Nakamura e Geus (2014).

Por fim, é importante que se registre que, quando da definição dos pilares referidos, ou seja, quando da definição da própria política de segurança, há de se estabelecer, também, as punições e os procedimentos aplicáveis em caso de sua violação, pois, sem sanções, há o risco de ineficácia/inutilidade da política de segurança (NAKAMURA; GEUS, 2014).

- **Agentes atuantes na concepção das políticas de segurança**

Tem-se, em função do propósito das Políticas de Segurança e dos fatores relevantes à sua definição (processos, regras de negócio e pessoal, especialmente), a necessidade de conjunta atuação, em sua produção, de distintos agentes, como representado na Figura 34.

Figura 34 - Agentes atuantes na construção das políticas de segurança.



Fonte: Autor (2019) ⁷⁴.

A participação dos agentes mencionados na Figura 34 se faz relevante, pois cada um deles contribui de forma própria para a construção da política de segurança, como revelam as informações constantes do Quadro 26.

⁷⁴ Representação elaborada a partir da análise de considerações tecidas por Nakamura e Geus (2014).

Quadro 26 - Contribuições dos partícipes na construção de políticas de segurança.

CONTRIBUIÇÕES DOS PARTÍCIPES NA CONSTRUÇÃO DE POLÍTICAS DE SEGURANÇA	
AGENTE	CONTRIBUIÇÃO ESSENCIAL
DIREÇÃO DA ENTIDADE/ORGANIZAÇÃO	Demonstração de comprometimento e apoio à Política de Segurança
ADMINISTRADORES/GESTORES DE SEGURANÇA	Concepção técnica da segurança
USUÁRIOS	Fornecimento de substrato relativo a processos, regras de negócio, procedimentos/rotinas de trabalho e cultura organizacional efetiva

Fonte: Autor (2019) ⁷⁵.

• Planejamento e Espécies de Políticas de Segurança

Como observado por Nakamura e Geus (2014), com o propósito de se estabelecer as diretrizes macroscópicas da segurança de uma entidade/organização, planeja-se a segurança, concebendo-se, de modo genérico, abrangente, sintético e flexível:

- a definição de segurança da informação para a instituição/organização, esclarecendo-se sua relevância para esta (sua importância estratégica para sobrevivência da entidade/organização, para a regularidade de seus negócios/operações e para o compartilhamento de informações);
- a síntese do escopo da segurança na organização, bem como das metas de segurança da entidade;
- a declaração de comprometimento da direção para com a segurança institucional;
- a breve exposição dos princípios, padrões e requisitos de segurança específicos para a organização (conformidade com a legislação, educação e treinamento em segurança e consequências de violações da política de segurança, e.g.);
- o rol de responsabilidades quanto à gestão da segurança na instituição;
- as referências de apoio à política de segurança (normas/procedimentos de segurança mais detalhados em certos casos, e.g.).

⁷⁵ Quadro construído com o emprego de ideias expostas por Nakamura e Geus (2014).

Ao planejamento em debate se mostram úteis algumas diretrizes (NAKAMURA; GEUS; 2014):

- conhecimento e consideração da estrutura e das peculiaridades da própria entidade/organização em que opera o sistema computacional (processos, pessoas e regras de negócio, e.g.);
- conhecimento dos potenciais atacantes da organização;
- identificação e exame do maior número possível de riscos/vulnerabilidades e ameaças de segurança;
- atenção à multiplicidade de espécies de vulnerabilidades existentes (vulnerabilidades físicas, inclusive);
- avaliação da relação "custo & benefício" dos potenciais investimentos em segurança;
- controle de informações privilegiadas sobre a segurança;
- minimização dos serviços, funcionalidades e permissões de acesso e uso dos sistemas computacionais e das redes de comunicação;
- reconhecimento da necessidade de contínua e constante vigilância da entidade e consequente reflexão sobre recursos úteis a este fim;
- reconhecimento da natural complexidade da segurança e das implicações desta decorrentes à regularidade das operações da organização e à sua sobrevivência.

Considerados os recursos disponíveis e as atividades da entidade/organização, planeja-se a política de segurança, estabelecendo-se variadas versões de documentos com diferentes níveis de detalhamento, para facilitação da compreensão por seus destinatários (NAKAMURA; GEUS, 2014). No Quadro 27, apresentam-se algumas observações relativas aos níveis de detalhamento/compreensão das políticas de segurança.

Quadro 27 - Níveis de compreensão e detalhamento das políticas de segurança.

NÍVEIS DE COMPREENSÃO & DETALHAMENTO DAS POLÍTICAS DE SEGURANÇA			
DESTINATÁRIO/ INTÉRPRETE-ALVO	NÍVEL DE COMPREENSÃO DO DESTINATÁRIO/ INTÉRPRETE- ALVO	NÍVEL DE DETALHAMENTO DA POLÍTICA DE SEGURANÇA	EXEMPLOS DE ITENS INTEGRANTES
DIREÇÃO DA ORGANIZAÇÃO/ ENTIDADE	Baixo	Baixo	Diretriz geral da Segurança na entidade
USUÁRIOS	Moderado	Moderado	Papéis, procedimentos operacionais e permissões associadas
ADMINISTRADORES/ GESTORES DA SEGURANÇA	Alto	Alto	Procedimentos técnicos (Regras de Filtragem, e.g.)

Fonte: Autor (2019) ⁷⁶.

Do exame do Quadro 27, resulta a percepção de que, com foco no pleno entendimento das políticas de segurança, há de se reconhecer o relacionamento diretamente proporcional entre o nível de compreensão do intérprete-alvo e o nível de detalhamento do documento que representa a política de segurança. Assim sendo, é imperioso que se observe que um usuário com baixo nível de compreensão não precisa receber informações densas sobre a política de segurança. Um usuário com maior nível de conhecimento técnico, contudo, precisa de uma versão mais detalhada da política de segurança. Um indivíduo do corpo técnico de segurança, em razão de sua própria função na entidade, tem mais conhecimento sobre segurança e precisa, para o desempenho eficiente de suas atividades, de uma versão ainda mais detalhada da política de segurança.

Caso se façam necessários planos detalhados para subáreas/setores da organização, definem-se subpolíticas setoriais de segurança, subpolíticas estas que integram a política geral da entidade.

Nakamura e Geus (2014) prevêm a potencial utilidade das seguintes

⁷⁶ Quadro construído após reflexão acerca de ideias expostas por Nakamura e Geus (2014).

subpolíticas:

- política de segurança para senhas;
- política de segurança para *firewalls*;
- política de segurança para acesso remoto.

No Quadro 28, expõem-se, de modo breve, notas sobre as políticas referidas.

Quadro 28 - Políticas de segurança.

POLÍTICAS DE SEGURANÇA		
POLÍTICA	FINALIDADE	EXEMPLOS DE ATAQUES-ALVOS
POLÍTICA DE SEGURANÇA PARA SENHAS	Mitigação dos riscos de sujeição a ataques de acesso e uso não autorizado mediante a descoberta de senhas, ou uso desautorizado de senha	• Ataques de captura de senhas com <i>Sniffers</i> • Ataques de descoberta de senhas com dicionários (Ataques com <i>Cracks</i>) • Ataques de captura de senha com <i>Password Guessing</i> • Ataques de captura de senhas com força bruta • Ataques de uso com o emprego de senha por usuário não mais autorizado
POLÍTICA DE SEGURANÇA PARA FIREWALLS	Minimização e mitigação do desautorizado acesso/uso externo de serviços/informações mediante bloqueios e filtragens	• Invasões
POLÍTICA DE SEGURANÇA PARA ACESSO REMOTO	Minimização e mitigação do acesso remoto não autorizado	• Invasões

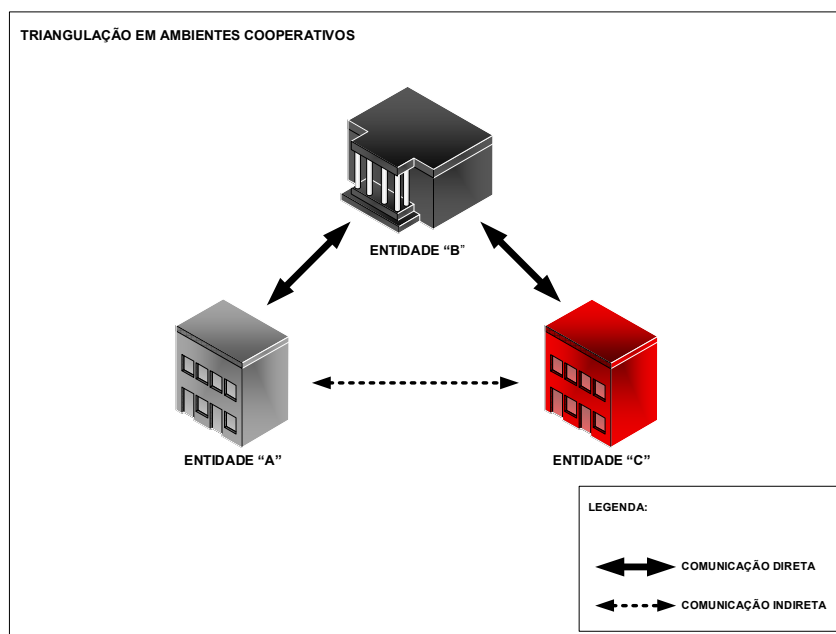
Fonte: Autor (2019) ⁷⁷.

⁷⁷ Quadro elaborado com o emprego de observações tecidas por Nakamura e Geus (2014).

Conclusivamente acerca do planejamento e das espécies de políticas de segurança, é válido se tecer alguns comentários para o caso da segurança em ambientes ditos *cooperativos*, i.e., ambientes em que entidades diversas e com diferentes políticas individuais de segurança, para o pleno desenvolvimento de suas atividades/negócios, interagem entre si, acessando sistemas/módulos de sistemas comuns.

Em ambientes cooperativos, um fenômeno relevante há de ser considerado no planejamento das políticas de segurança: a triangulação. Diz-se que há triangulação quando, como ilustrado na Figura 35, uma entidade não autorizada A acessa, mediante outra entidade devidamente autorizada B, os dados de terceira entidade C.

Figura 35 - Triangulação em ambientes cooperativos.



Fonte: Autor (2019) ⁷⁸.

Para se lidar com a triangulação, Nakamura e Geus (2014) sugerem a previsão, nas políticas de segurança, de "bolsões de segurança", estruturas em que se definem áreas e funcionalidades acessíveis externamente, restringindo-se, no entanto, o acesso às demais, dadas as naturais dificuldades para a constituição de uma política de segurança conjunta.

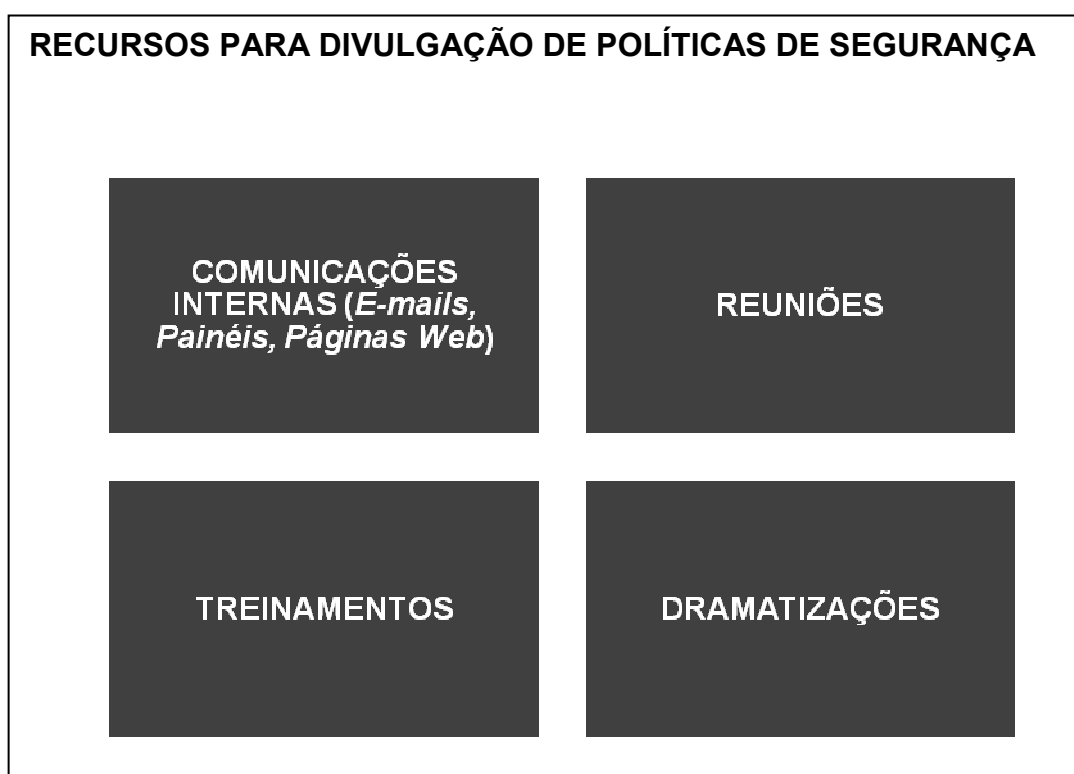
⁷⁸ Adaptação de ilustração produzida por Nakamura e Geus (2014).

- **Implementação das políticas de segurança**

Concebida a política de segurança, passa-se, com foco em sua efetividade operacional, à sua implementação e à sua divulgação.

A mencionada divulgação é indispensável, vez que, através dela, conscientizam-se os colaboradores da organização acerca da importância da segurança, esclarecendo-se os seus papéis nela. Quatro são os principais recursos de divulgação de políticas de segurança, como ilustrado na Figura 36.

Figura 36 - Recursos para divulgação de políticas de segurança.



Fonte: Autor (2019) ⁷⁹.

De acordo com Nakamura e Geus (2014), a implantação da política de

⁷⁹ Representação concebida a partir reflexão sobre exposição de Nakamura e Geus (2014).

segurança envolve, além de sua divulgação:

- a implementação concreta de mecanismos e recursos tecnológicos (Sistemas de Autenticação, *Firewalls*, Sistemas de Monitoramento e Detecção de Intrusões e Controle de Acesso, e.g.);
- o monitoramento da organização;
- a realização de auditorias periódicas independentes, para aferição da conformidade da atuação dos indivíduos que acessam e utilizam os recursos da organização;
- a aplicação de sanções aos indivíduos que desrespeitem ou descumpram as prescrições da política de segurança;
- a verificação da efetividade da política de segurança (avaliação da espécie, volume e impacto dos incidentes de segurança registrados, e.g.);
- a análise do custo e do impacto da segurança ao negócio da entidade;
- a revisão eventual da política de segurança.

- **Obstáculos às políticas de segurança**

Diversos obstáculos podem se opor às políticas de segurança. Nakamura e Geus (2014), analisando tal tema, apontam os seguintes fatores como obstáculos às políticas de segurança:

- escassez de recursos na organização/entidade;
- baixa prioridade da segurança na visão dos dirigentes da organização;
- desconhecimento, pelos dirigentes da entidade e usuários, dos benefícios resultantes de políticas de segurança efetivas;
- baixo convencimento dos dirigentes da entidade acerca da essencialidade da segurança, inclusive para a sobrevivência do empreendimento;

- insuficiente engajamento da direção da organização na concepção e na implantação da política de segurança;
- desconhecimento acerca da insuficiência da mera definição formal de políticas de segurança e da relevância de sua efetividade;
- desconhecimento da complexidade da segurança e dos fatores que nela repercutem (procedimentos de trabalho dos usuários, e.g.);
- falta de liderança e conhecimento técnico, na organização, acerca de Segurança Computacional;
- resistência e medo individuais em face da segurança (receio de perda de poder/prestígio, temor a inovações e conservadorismo em práticas/procedimentos, e.g.);
- incompletude da visão de segurança na organização, ou incompletude da disciplina da segurança em caso de violação (ausência/não aplicação de sanções em caso de descumprimento da política de segurança).

- **Elementos do documento refletivo da política de segurança**

Ainda que as políticas de segurança devam refletir aspectos peculiares da entidade/organização por elas tuteladas, é possível se identificar elementos comuns em suas estruturas. Na Figura 37, apresenta-se um exemplo de elementos integrantes das políticas de segurança.

Figura 37 - Elementos usuais dos documentos refletivos das políticas de segurança.

ELEMENTOS USUAIS DOS DOCUMENTOS REFLETIVOS DAS POLÍTICAS DE SEGURANÇA
1 INTRODUÇÃO
1.1 POLÍTICA DE SEGURANÇA
1.1.1 Informações Gerais
1.1.2 Objetivos
1.2 ESTRUTURAS DE RESPONSABILIDADE ORGANIZACIONAL
1.2.1 Responsáveis
1.2.1.1 Serviços de Informação Corporativa
1.2.1.2 Serviços de Informação de Unidades de Negócio
1.2.1.3 Organizações Internacionais
1.2.1.4 Encarregados
1.2.2 Padrões de Segurança
1.2.2.1 Confidencialidade
1.2.2.2 Integridade
1.2.2.3 Autorização
1.2.2.4 Acesso
1.2.2.5 Uso Apropriado
1.2.2.6 Privacidade dos Usuários
2 DESCRIÇÃO DO SISTEMA
2.1 PAPEL DO SISTEMA
2.1.1 Tipos de Informação Manipulada pelo Sistema
2.1.2 Tipos de Usuários
2.1.3 Número de Usuários
2.1.4 Classificação dos Dados Quanto à Acessibilidade
2.1.5 Quantidade em Bytes de Dados
2.1.6 Configuração do Sistema
2.1.6.1 Número de Terminais
2.1.6.2 Número de Consoles de Controle
2.1.6.3 Número e Tipos de Terminais (Inteligentes, Burros, de Impressão, etc.)
2.1.6.4 Arranjos para Carregamento de Mídia
2.1.6.5 Software de Base (Sistema Operacional e Versão)
2.1.6.6 Interconexões (LAN e WAN)
3 REQUISITOS DE SEGURANÇA E MEDIDAS DE SEGURANÇA
3.1 AMEAÇAS À CONFIDENCIALIDADE, À INTEGRIDADE E À DISPONIBILIDADE DOS DADOS
3.2 NATUREZA E RECURSOS DE POTENCIAIS ATACANTES E ATRATIVIDADE DO SISTEMA E DOS DADOS COMO ALVO
3.3 IMPACTOS DO COMPROMETIMENTO ACIDENTAL DE DADOS
4 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA
4.1 PREPARAÇÃO E PLANEJAMENTO DA RESPOSTA A INCIDENTES
4.2 NOTIFICAÇÃO E PONTOS DE CONTATO
4.3 IDENTIFICAÇÃO DE UM INCIDENTE
4.4 RESPOSTA A UM INCIDENTE
4.5 CONSEQUÊNCIAS DE UM INCIDENTE
4.6 FORENSE COMPUTACIONAL E IMPLICAÇÕES LEGAIS
4.7 CONTATOS DE RELAÇÕES PÚBLICAS
4.8 PASSOS-CHAVES
4.8.1 Contenção
4.8.2 Erradicação
4.8.3 Recuperação
4.8.4 Acompanhamento
4.8.5 Consequências/ Lições Aprendidas
4.9 RESPONSABILIDADES
5 CONTATOS E OUTROS RECURSOS
6 REFERÊNCIAS

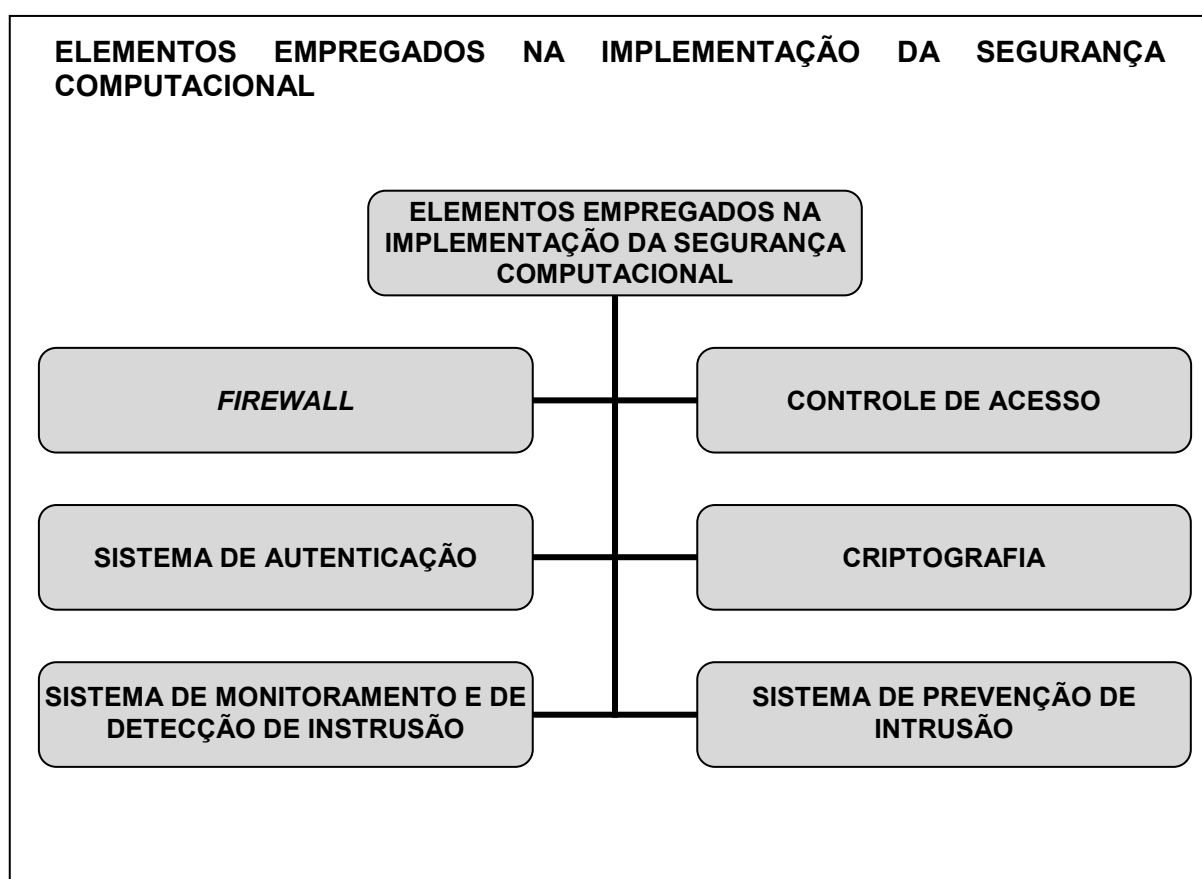
Fonte: Autor (2019) ⁸⁰.

⁸⁰ Figura concebida a partir da adaptação de estrutura apresentada por Nakamura e Geus (2014).

4.5.4.2 Técnicas, procedimentos e recursos

Para efetiva implementação da Segurança Computacional, empregam-se técnicas, procedimentos e recursos diversos, como os referidos na Figura 38.

Figura 38 – Elementos empregados na implementação da Segurança Computacional.



Fonte: Autor (2019) ⁸¹.

No Quadro 29, apresentam-se breves notas sobre os elementos referidos na Figura 38.

⁸¹ Figura elaborada após reflexão acerca de exposição de Nakamura e Geus (2014).

Quadro 29 – Elementos empregados na implementação da Segurança Computacional.

ELEMENTOS EMPREGADOS NA IMPLEMENTAÇÃO DA SEGURANÇA COMPUTACIONAL		
ELEMENTO	DESCRIÇÃO BÁSICA	EXEMPLOS
FIREWALL	Conjunto protetor de componentes através dos quais circulam os dados entre duas ou mais redes em um ambiente com controle, registro e autenticação do tráfego	• Filtros de pacotes • Filtros de pacotes baseado em estados • Proxies • <i>Firewall</i> híbrido • <i>Firewall</i> adaptativo • <i>Firewall</i> reativo • <i>Firewall</i> individual/pessoal
CONTROLE DE ACESSO	Mecanismo restritivo do acesso a recursos computacionais que faculta o acesso e manejo de sistemas computacionais apenas por pessoas autorizadas	• Controle de acesso por autenticação do usuário • Controle de acesso por Listas de Controle de Acesso – <i>Access Control Lists (ACLs)</i> • Interfaces de usuários restritivas • Rotulação de dados
SISTEMA DE AUTENTICAÇÃO	Sistema voltado à validação da identificação de usuários em ambientes e sistemas computacionais	• Autenticação por senha • Autenticação com <i>token</i> ou cartão • Autenticação por biometria
CRİPTOGRAFIA	Conjunto de técnicas e algoritmos que efetivam a cifragem de mensagens, impedindo sua compreensão por entes não autorizados que a eles tenham acesso, evitando, outrossim, que comunicações oriundas de emissores falsos sejam recebidas como legítimas	• Criptografia de chave privada ou simétrica • Criptografia de chave pública ou assimétrica
SISTEMA DE MONITORAMENTO E DETECÇÃO DE INTRUSÃO	Sistema que, como indica sua própria denominação, é voltado ao monitoramento do tráfego de informações e da rede, com foco na identificação de ataques e intrusões	• <i>Host-Based Intrusion Detection System (HIDS)</i> • <i>Network-Based Intrusion Detection System (NIDS)</i> • <i>Hybrid Intrusion Detection System (Hybrid IDS)</i>
SISTEMA DE PREVENÇÃO DE INTRUSÃO	Sistema especial de detecção de ataques/intrusões que também atua na prevenção	• <i>Host-Based Intrusion Prevention System (HIPS)</i> • <i>Network-Based Intrusion Prevention System (NIPS)</i>

Fonte: Autor (2019) ⁸².⁸² Quadro construído após reflexão acerca das ideias expostas por Nakamura e Geus (2014).

Dada a possibilidade, apesar de todos os eventuais esforços empreendidos, de insucesso no gerenciamento da Segurança ocasionar danos, torna-se necessário discorrer, brevemente, acerca da responsabilização por danos e sobre a Ética, temas do Capítulo 5 e do Capítulo 6, respectivamente.

5 RESPONSABILIDADE POR DANOS

De modo usual, pode-se asseverar que os humanos são seres gregários que, com foco na consecução de seus objetivos, convivem em um mesmo espaço, interagindo entre si (DINIZ, 2012). Esta interação, inúmeras vezes, realiza-se sem maiores sobressaltos, havendo, contudo, ocasiões e momentos em que conflitos de interesses emergem.

Diversas são as espécies de conflitos potencialmente emergentes nas sociedades humanas, sobressaindo-se, porém, os atinentes à responsabilidade, quando evidenciados danos a um indivíduo pelas condutas comissivas/omissivas de outro, ou quando constatada a assunção formal do encargo por riscos de dano (AZEVEDO, 1977).

Emergindo conflitos de tal sorte e não se estando, mais, em eras de autotutela e de autocomposição de litígios (CINTRA; GRINOVER; DINAMARCO, 2009), valem-se os homens e o Estado de normas diversas refletivas dos valores sociais para a solução de controvérsias (normas de cunho moral, ético e jurídico, e.g.). Entre as normas mencionadas, sobressaem-se as de natureza jurídica, razão pela qual, nas seções seguintes, discorre-se, de modo breve e genérico, acerca da responsabilidade sob tal enfoque.

5.1 CONSIDERAÇÕES PRELIMINARES

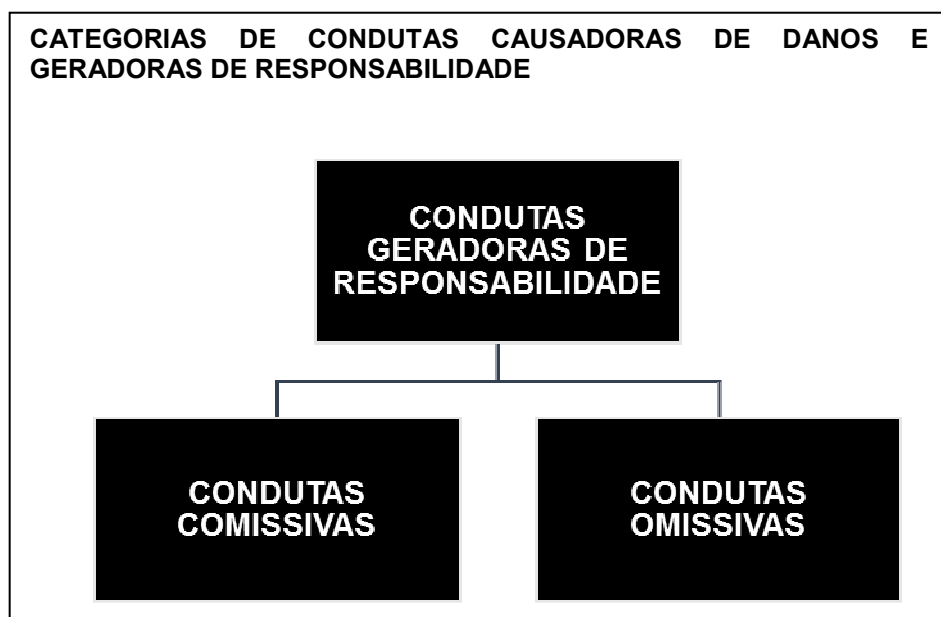
Usualmente, a responsabilidade por dano, no Direito, é concebida como ônus decorrente de contrato/lei, ou, ainda, como obrigação que exsurge do descumprimento de dever encargo contratual/legal (CAVALIERI FILHO, 2014). O aludido ônus/descumprimento pode dar causa à reparação e/ou à indenização pelo dano, tal como ocorre, por exemplo, no caso de dano decorrente do abalroamento de veículo regularmente parado no semáforo.

Tem-se, assim, para o caso exemplificado (abalroamento de veículo regularmente parado no semáforo), que a responsabilidade se constitui no vínculo obrigacional materializado quando um indivíduo/ente pratica uma conduta lesiva a

interesses/patrimônio de um outro ente/indivíduo (MIRANDA, 2012). Na hipótese ilustrada, o condutor do veículo que se chocou com o automóvel regularmente parado trafegava em velocidade superior à permitida na via e não reduziu o ritmo a tempo, colidindo seu automóvel com o veículo no semáforo. Lesados os interesses do condutor do veículo regularmente parado no semáforo com a colisão (integridade do veículo, especialmente), há responsabilidade do condutor do automóvel colidente pelos danos.

É importante que se observe que a conduta lesiva pode, considerada sua natureza, ser inserta em duas categorias macroscópicas, como ilustrado na Figura 39.

Figura 39 - Categorias macroscópicas de condutas causadoras de danos e geradoras de responsabilidade.



Fonte: Autor (2019) ⁸³.

No Quadro 30, apresentam-se notas distintivas das categorias referenciadas na Figura 39.

⁸³ Representação construída considerando-se exposição de Tartuce (2016).

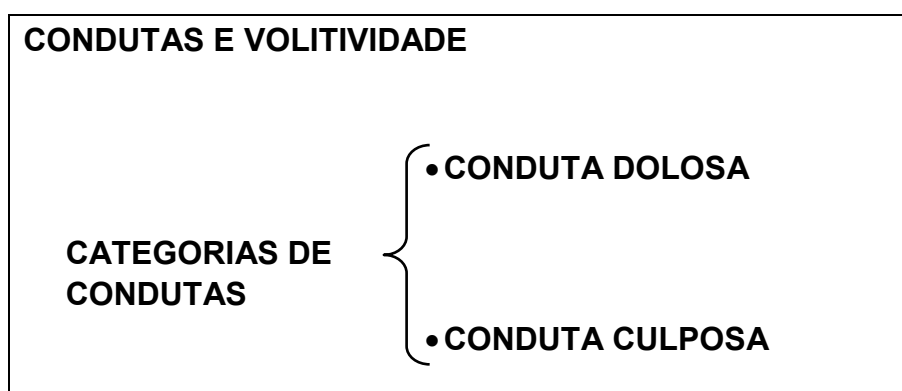
Quadro 30 - Categorias macroscópicas de condutas causadoras de danos e geradoras de responsabilidade.

CONDUTAS CAUSADORAS DE DANOS E GERADORAS DE RESPONSABILIDADE		
CATEGORIA DE CONDUTA	CARACTERÍSTICA DISTINTIVA	EXEMPLOS
CONDUTA COMISSIVA	Conduta materializada com a realização de atos concretos por parte do agente	• Disparo de uma arma por um ladrão • Desferimento de facadas • Condução de veículo em estado de embriaguez
CONDUTA OMISSIVA	Conduta materializada com a inércia/omissão do agente	• Negativa de socorro a transeunte acidentado em via pública • Realização de procedimento cirúrgico sem as devidas cautelas de assepsia e higiene

Fonte: Autor (2019) ⁸⁴.

Há de se atentar, ainda, para o fato de que as condutas também podem ser classificadas em função do elemento volitivo, o ânimo de promoção de dano (*animus nocendi*), como representado na Figura 40.

Figura 40 - Condutas e volitividade.



Fonte: Autor (2019) ⁸⁵.

No Quadro 31, apresentam-se notas sobre as categorias representadas na Figura 40.

⁸⁴ Quadro elaborado com a consideração de ideias expostas por Tartuce (2016).

⁸⁵ Ilustração concebida a partir de reflexão sobre observações de Cavalieri Filho (2014).

Quadro 31 - Condutas e volitividade.

CONDUTAS E VOLITIVIDADE		
CATEGORIA DE CONDUTA	ELEMENTO DISTINTIVO	EXEMPLOS
CONDUTA DOLOSA	Dolo, i.e., intenção de produzir o resultado lesivo com a realização da conduta	• Sequestro de animal para obtenção de resgate junto à sua família humana • Disparo de arma de fogo com o propósito de matar alguém • Furto de coisa alheia para proveito próprio
CONDUTA CULPOSA	Culpa, i.e., a ausência de intenção de produção específica do resultado, mas sua ocorrência por negligência, imprudência ou imperícia	• Realização de procedimento cirúrgico sem a observância das normas gerais de assepsia • Morte por asfixia de criança "esquecida" por seu genitor dentro de veículo automotor

Fonte: Autor (2019) ⁸⁶.

Acerca da responsabilidade, importa ressaltar, também, que múltiplos são os critérios empregáveis em sua classificação, sobressaindo-se, contudo, os relativos à fonte obrigacional e os atinentes à esfera preponderante de Direito aplicável, como representado na Figura 41.

⁸⁶ Quadro construído com o emprego de considerações de Cavalieri Filho (2014).

Figura 41 - Classificação da responsabilidade.



Fonte: Autor (2019) ⁸⁷.

Apresentam-se, no Quadro 32, observações basilares acerca dos critérios e classificações representados na Figura 41.

Quadro 32 - Classificação da responsabilidade.

CLASSIFICAÇÃO DA RESPONSABILIDADE		
CRITÉRIO	CATEGORIA	DESCRIÇÃO
1º CRITÉRIO: FONTE	RESPONSABILIDADE CONTRATUAL	Responsabilidade originária do descumprimento de cláusulas/condições de contrato/avença previamente definido(a) entre as partes envolvidas
	RESPONSABILIDADE EXTRACONTRATUAL/AQUILIANA	Responsabilidade originária do descumprimento da legislação em sentido amplo

⁸⁷ Figura construída com a consideração de exposição feita em Azevedo (1977), Tartuce (2016) e Cavalieri Filho (2014).

CLASSIFICAÇÃO DA RESPONSABILIDADE		
CRITÉRIO	CATEGORIA	DESCRIÇÃO
2º CRITÉRIO: DIREITO PREPONDERANTE APLICÁVEL	RESPONSABILIDADE ADMINISTRATIVA	Responsabilidade em que o Direito Administrativo se faz mais presente, objetivando ressarcimento e aplicação de sanções administrativas
	RESPONSABILIDADE CRIMINAL/PENAL	Responsabilidade regrada precipuamente por normas de Direito Penal, com foco na aplicação de sanções (penas)
	RESPONSABILIDADE CIVIL	Responsabilidade regida, essencialmente, por normas de Direito Civil, que visa, em geral, o ressarcimento de danos
3º CRITÉRIO: TEORIA JUSTIFICADORA NA ESFERA CÍVEL	RESPONSABILIDADE SUBJETIVA	Responsabilidade fundada na Teoria da Culpa, em que a culpa em sentido amplo (dolo ou culpa em sentido estrito) há de ser identificada para a imputação de consequências ao agente causador de dano
	RESPONSABILIDADE OBJETIVA	Responsabilidade, baseada na Teoria do Risco, configurável através da simples constatação do resultado lesivo, sendo irrelevante a presença de dolo/culpa do agente causador

Fonte: Autor (2019) ⁸⁸.

Quanto ao Direito aplicável ao regramento da responsabilidade, é válido salientar que se fala em Direito preponderantemente aplicável, não havendo, assim, que se cogitar de um isolamento hermético impeditivo da incidência de normas de outros ramos jurídicos. Com efeito, há, inclusive, de se reconhecer que, em casos específicos (controvérsias em que se apresentam, simultaneamente, dano civil e ofensa a bem penalmente protegido, e.g.), incidem normas de dois ou mais ramos do Direito e que, eventualmente, as conclusões a que se chega em uma esfera (esfera penal, v.g.) podem repercutir em outra (esfera civil), tal como ocorre, no Direito Brasileiro, quando, negada a ocorrência do fato em âmbito penal, deixa de

⁸⁸ Quadro elaborado a partir de observações de Azevedo (1977), Tartuce (2016) e Cavalieri Filho (2014).

subsistir controvérsia civil relativa a qualquer direito indenizatório⁸⁹.

Diante da possibilidade teórica de atribuição de responsabilidade civil aos que produzem/fornecem bens e serviços, inclusive os produtos e serviços que apresentem vulnerabilidades de segurança em *software*, faz-se, na Seção seguinte, ágil digressão geral sobre este tema.

5.2 RESPONSABILIDADE CIVIL

5.2.1 Definição e justificativa

Apesar de não se esperar que normas vigentes sejam descumpridas, há de se definir, nos ordenamentos jurídicos, medidas voltadas à sua inibição e à sua repressão, bem como à reparação pela injusta violação de direito. Com este propósito, concebeu-se, na esfera cível, o instituto da responsabilidade civil.

Usualmente, a responsabilidade civil pode ser compreendida como o encargo de reparação que surge quando, arbitral ou judicialmente, é declarado que a conduta de um indivíduo/ente, injustificadamente, promove lesão ao patrimônio de outro (NADER, 2016, v. 7).

Há de se observar, contudo, como observado por Pereira (2005, v. III), que não se apresenta a criação de uma nova obrigação, mas, sim, a transmutação de obrigação pré-existente, qual seja, a concernente ao respeito à integridade pessoal e patrimonial de terceiros⁹⁰. Esta transmutação e sua consequência principal (ônus de reparação) são ilustradas na Figura 42.

⁸⁹ É o que se depreende, no ordenamento pátrio, da leitura do artigo 935, do Código Civil (BRASIL, 2002).

⁹⁰ Nos exatos dizeres de Pereira (2005, V. III), p. 324 - 325: "Não se extingue a obrigação, nem nasce outra cujo objeto sejam as perdas e danos. É a mesma obrigação que sofre mutação objetiva. A prestação é que difere, em razão de ter o devedor ficado em falta. E, como o seu inadimplemento impõe ao credor um dano e lhe traz uma perda, o devedor é obrigado a cobrir os prejuízos causados pela sua conduta, de forma que o equilíbrio se restabeleça."

Figura 42 - Transmutação de obrigações na responsabilidade civil.

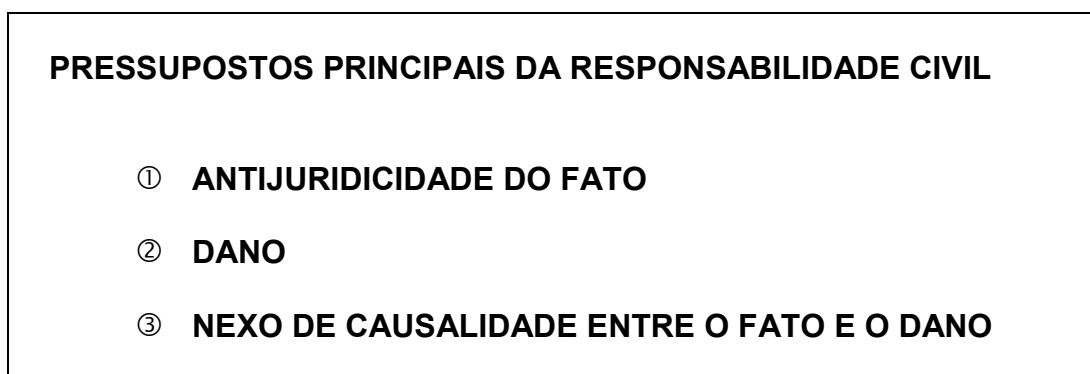


Fonte: Autor (2019) ⁹¹.

5.2.2 Pressupostos

Para que se evidencie a responsabilidade civil, assevera-se, doutrinariamente, que três pressupostos principais devem ser atendidos (CARRÁ, 2004), tal como ilustrado na Figura 43.

Figura 43 - Pressupostos principais da responsabilidade civil.



Fonte: Autor (2019) ⁹².

Tem-se, assim, que, para o surgimento da responsabilidade civil, deve:

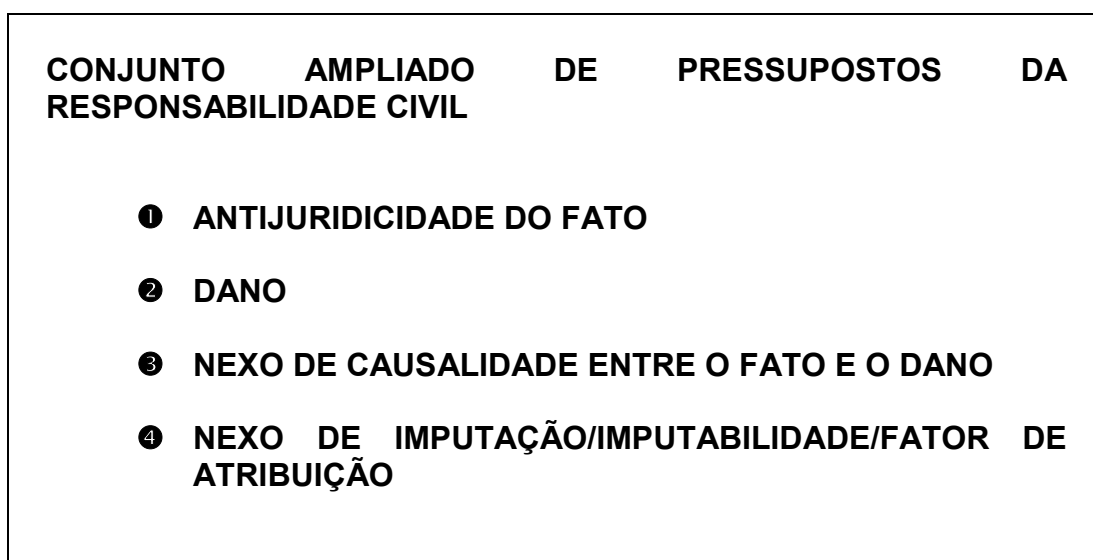
⁹¹ Representação concebida com a reflexão sobre exposição de Pereira (2005, v. III).

⁹² Ilustração concebida a partir de observações de Carrá (2004).

a) ter havido a consumação de um fato antijurídico, i.e., um fato contrário ao Direito (lei ou contrato); b) ter ocorrido um dano; e c) haver, entre o fato antijurídico e o dano, um liame de ligação, ou seja, o dano deve resultar da ocorrência do fato antijurídico.

É crescente, contudo, o entendimento de que, em verdade, um conjunto mais amplo de pressupostos há de ser atendido para configuração da responsabilidade civil, inserindo-se neste um Fator de Atribuição/Nexo de Imputação, como representado na Figura 44.

Figura 44 - Conjunto ampliado de pressupostos da responsabilidade civil.



Fonte: Autor (2019) ⁹³.

Nas subseções seguintes, discorre-se, brevemente, sobre os pressupostos do conjunto ampliado.

5.2.2.1 Antijuridicidade do fato

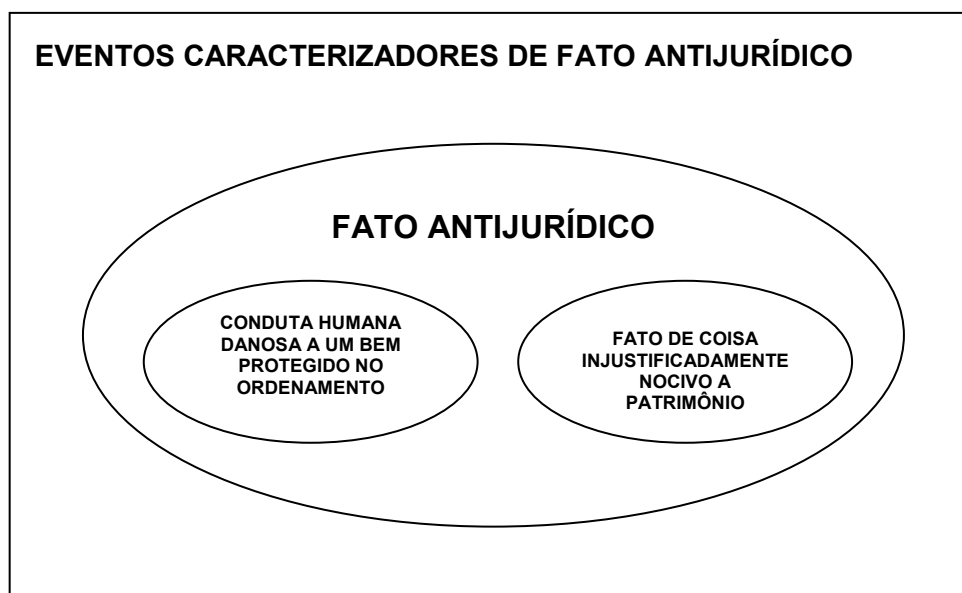
A responsabilidade costuma ser associada à ocorrência de um ato ilícito, ou seja, defende-se que uma conduta humana omissiva/comissiva contrária ao Direito que resulte danos patrimoniais a um ente/indivíduo constitui um ato ilícito gerador de responsabilidade (VENOSA, 2004).

Este entendimento, todavia, é objeto de críticas, vez que, com esta

⁹³ Representação construída com o emprego de ideias expostas em Carrá (2004).

associação, refogem ao campo de incidência da responsabilidade hipóteses em que ela, por lei ou contrato, se faz efetivamente presente (CARRÁ, 2004). Diante desta crítica, fala-se, então, que mais apropriada é a referência a fato antijurídico como pressuposto da responsabilidade, pois, com esta denominação, abarca-se bloco mais completo de eventos em que há responsabilidade civil, como representado na Figura 45.

Figura 45 - Eventos configuradores de fato antijurídico.



Fonte: Autor (2019) ⁹⁴.

Vale salientar quanto aos fatos antijurídicos, que os mesmos, para fins de responsabilidade civil, não restam, necessariamente, descaracterizados por condições que, eventualmente, afastem a ilicitude de uma conduta (exercício regular de direito, e.g.), como registrado em Carrá (2004) e como consignado no direito pátrio civilista⁹⁵. Dito de outra forma, ainda que se apresente excludente de ilicitude na conduta, pode persistir a responsabilidade por um resultado danoso ao patrimônio de outrem, vez que não elidida a configuração de fato antijurídico.

⁹⁴ Ilustração concebida a partir de exposição feita em Carrá (2004).

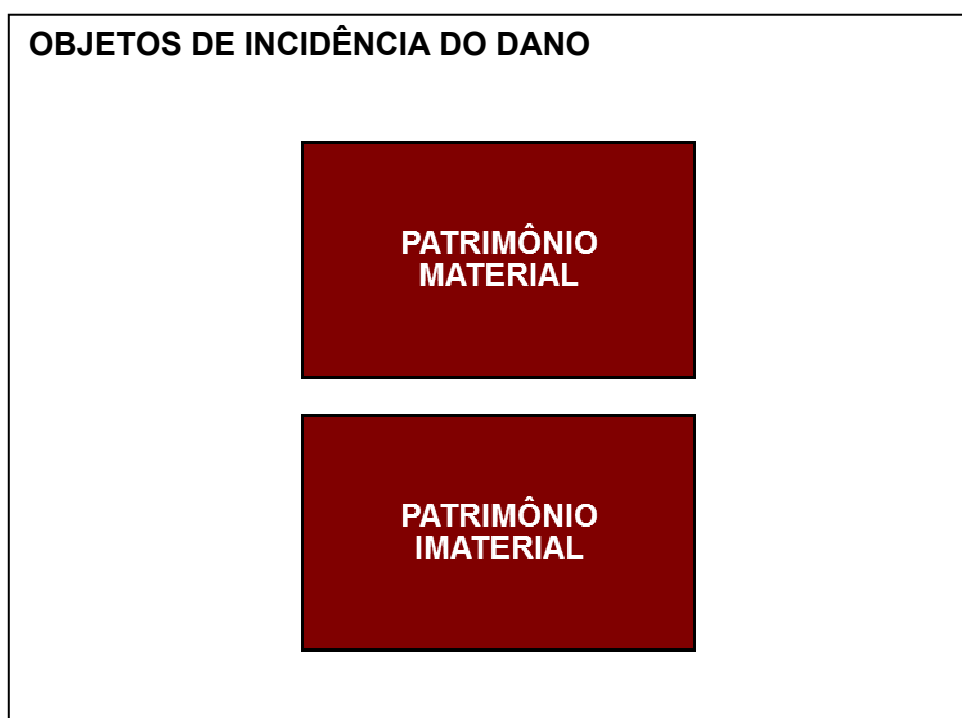
⁹⁵ É o que se depreende da leitura conjunta dos artigos 188, 927, 928, 929 e 930, do Código Civil (BRASIL, 2002).

5.2.2.2 Dano

No Direito Civil, o dano pode ser concebido como uma diminuição em um patrimônio. Esta diminuição se evidencia com a constatação de diferenças entre o patrimônio em um estado prévio e o patrimônio em um estado que sucede um fato antijurídico, i.e., um fato que se apresenta em desconformidade com a lei ou com contrato (CARRÁ, 2004), afetando um bem jurídico tutelado no ordenamento.

A diminuição em debate pode atingir duas distintas principais categorias de objetos, como representado na Figura 46.

Figura 46 - Objetos de incidência do dano.

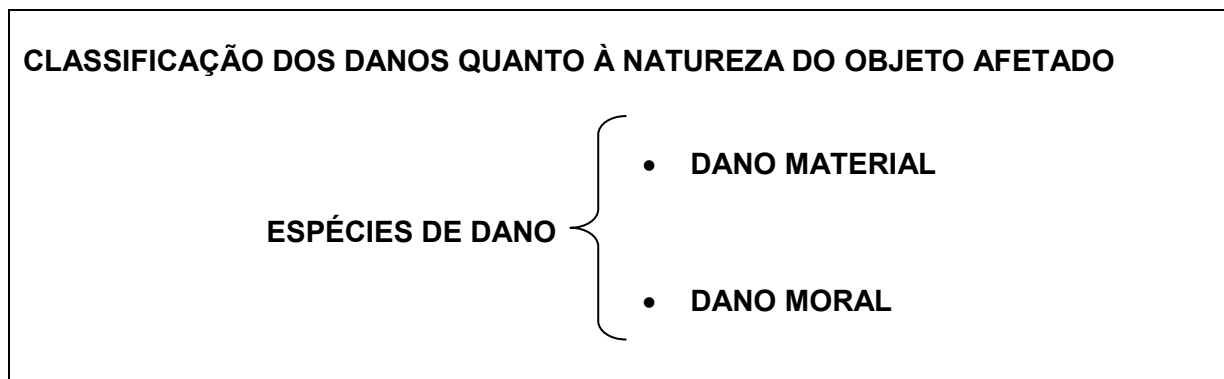


Fonte: Autor (2019) ⁹⁶.

Consideradas as naturezas dos objetos referidos na Figura 46, é corrente a classificação do dano, como ilustrado na Figura 47.

⁹⁶ Representação produzida, neste estudo, para ilustração dos objetos de incidência do dano, consideradas as exposições de Carrá (2004) e Pereira (2009, v. I; II), especialmente.

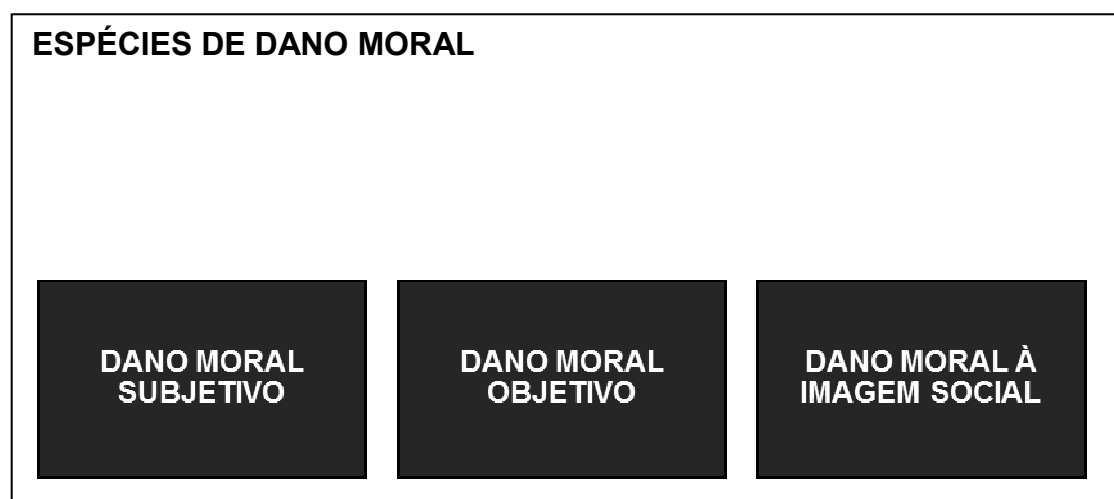
Figura 47 - Classificação dos danos quanto à natureza do objeto afetado.



Fonte: Autor (2019) ⁹⁷.

Como se depreende da Figura 47, recaindo o dano sobre o patrimônio material, tem-se configurado Dano Material. Incidindo o dano sobre o patrimônio moral de um ente/indivíduo (seus valores, suas crenças, suas convicções, sua tranquilidade de ânimo e sua percepção em sociedade, e.g.), tem-se presente o Dano Moral, dano este também passível de classificação, tal como representado na Figura 48.

Figura 48 - Espécies de dano moral.



Fonte: Autor (2019) ⁹⁸.

⁹⁷ Representação criada, neste documento, para ilustração das espécies de dano em função da natureza dos objetos afetados, a partir de comentários tecidos por Carrá (2004) e por Pereira (2009, v. I;II).

⁹⁸ Ilustração concebida com base em exposição de Carrá (2004).

No Quadro 33, apresentam-se alguns comentários basilares sobre as espécies de dano moral referidas na Figura 48.

Quadro 33 - Espécies de dano moral.

ESPÉCIES DE DANO MORAL		
ESPÉCIE	NÚCLEO	EXEMPLOS
DANO MORAL SUBJETIVO	Dor interna suportada pelo indivíduo em razão de desrespeito a íntimos valores seus	Mágoa gerada em deficientes ao visualizarem, em uma rede social, conteúdo discriminatório
DANO MORAL OBJETIVO	Ofensa pública/privada a direitos de personalidade	Dano resultante da demora de uma dada rede social em retirar da Internet perfil/página com conteúdo de ódio indiscriminado a deficientes físicos, a despeito de ter sido alertada por grupo de deficientes de que a criação de conteúdo de tal tipo os desrespeitaria
DANO MORAL À IMAGEM SOCIAL	Desgaste decorrente da exposição à avaliação social depreciativa	Dano resultante da pública divulgação da real orientação sexual de um candidato a cargo eletivo, a qual foi descoberta com a violação de sua comunicação eletrônica por falha de Segurança Computacional, e que, veiculada na mídia, acabou levando à modificação na preferência de seus eleitores conservadores

Fonte: Autor (2019) ⁹⁹.

Há de se observar, todavia, a possibilidade de classificação dos danos em categorias outras, adotadas óticas de observação diversas. Entre as óticas

⁹⁹ Quadro elaborado com o emprego de comentários tecidos por Carrá (2004), tendo os exemplos sido elaborados pelo próprio pesquisador.

mencionadas, sobressai-se, no Direito Civil, a que analisa os danos considerado o cabimento de indenização, tal como ilustrado na Figura 49.

Figura 49 - Classificação dos danos quanto ao cabimento de indenização.



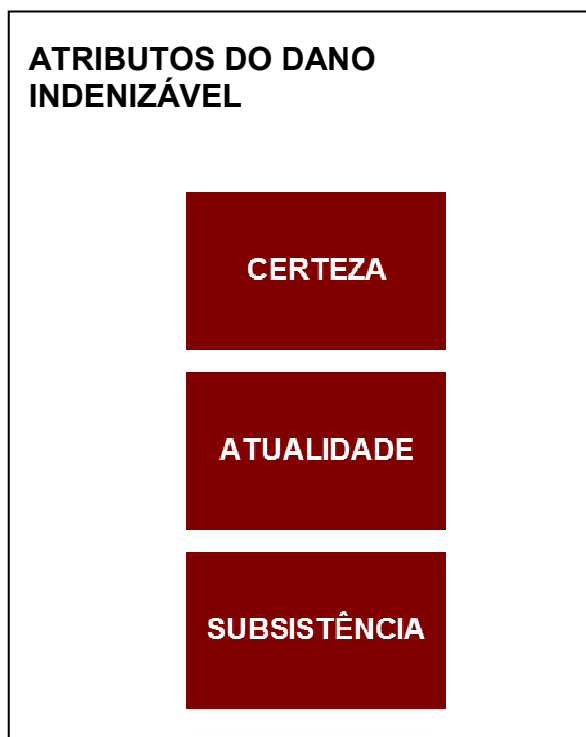
Fonte: Autor (2019) ¹⁰⁰.

Como se depreende da Figura 49, na esfera cível, os danos podem ser inseridos em dois grupos macroscópicos segundo o potencial cabimento de indenização. São indenizáveis os danos qualificados pelo direito e não indenizáveis os demais.

A distinção essencial entre os grupos macroscópicos mencionados é feita em função de atributos conjuntamente identificáveis no dano. Na Figura 50, apresentam-se os atributos que tornam indenizável um dano.

¹⁰⁰ Ilustração produzida a partir de ideias expostas em Carrá (2004).

Figura 50 - Atributos do dano indenizável.



Fonte: Autor (2019) ¹⁰¹.

Para que um dano seja, assim, indenizável no Direito Civil, deve apresentar, conjuntamente, os três atributos indicados na Figura 50, ou seja, o dano deve ser certo, atual e subsistir.

Quanto à atualidade do dano, alguns comentários se fazem necessários. Ao se falar em atualidade, não se restringe o escopo de indenização aos danos que apresentem apenas repercussões presentes ou contemporâneas, vez que, em verdade, as repercussões futuras também se mostram indenizáveis, em condição certa. Admite-se a indenização de repercussões futuras quando o dano já existente produza efeitos/consequências em momento ulterior (CARRÁ, 2004).

Por fim, quanto ao potencial de indenização do dano, vale destacar que não apenas os sujeitos diretamente por ele afetados podem vir a ser indenizados, dado o reconhecimento da existência do "Dano Ricochete", dano que, indiretamente causa prejuízos a pessoa não qualificável como vítima do dano. Dito de outra forma,

¹⁰¹ Representação produzida em função de observações tecidas em Carrá (2004).

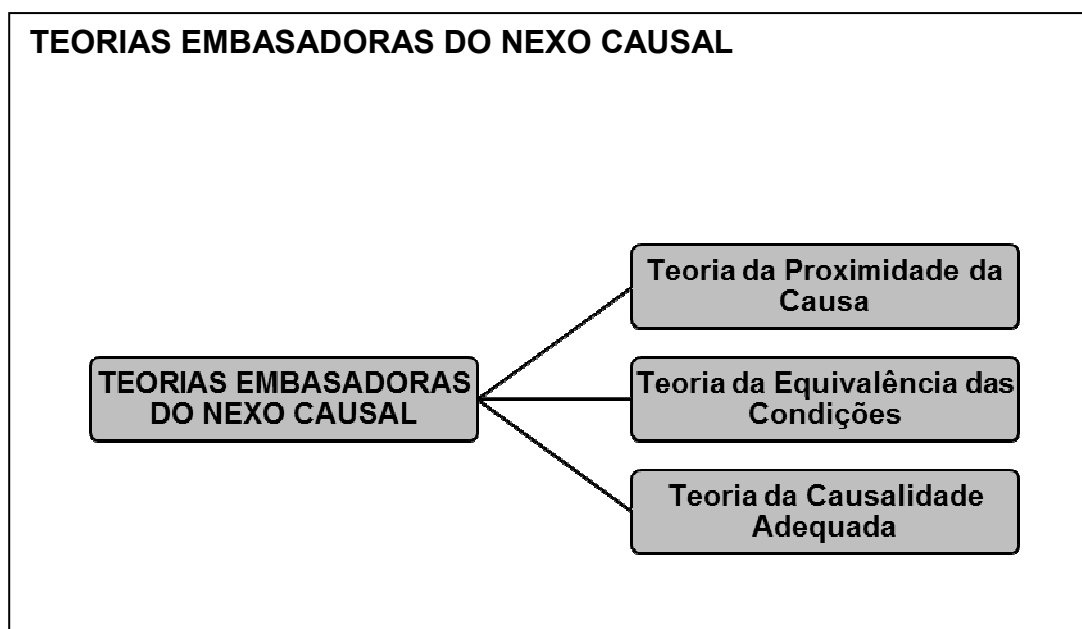
o prejuízo sofrido reflexamente por pessoa ligada à vítima também pode vir a ser qualificado como dano, ensejando indenização reparatória (CARRÁ, 2004).

5.2.2.3 Nexo de causalidade

De modo sintético, o nexa de causalidade pode ser concebido como o elemento de ligação entre um fato jurídico e um dano (CARRÁ, 2004). A identificação deste liame, todavia, pode não ser tarefa trivial, em razão de dificuldades de prova e de dificuldades de identificação do fato jurídico do dano, mormente quando há múltiplas causas para este (causalidade múltipla) (CARRÁ, 2004; NADER, 2016, v. 7; PEREIRA, 2009, v. II, III; STOCO, 2004).

Com o propósito de se abrandar as dificuldades para a identificação do nexa de causalidade, propuseram-se teorias próprias, como ilustrado na Figura 51.

Figura 51 - Teorias embasadoras do nexa causal.



Fonte: Autor (2019) ¹⁰².

No Quadro 34, apresentam-se notas rápidas sobre as teorias indicadas

¹⁰² Representação elaborada a partir de exposição feita em Carrá (2004).

na Figura 51.

Quadro 34 - Teorias embasadoras do nexo causal.

TEORIAS EMBASADORAS DO NEXO CAUSAL		
TEORIA	IDEIA ESSENCIAL	CRÍTICAS
TEORIA DA PROXIMIDADE DA CAUSA	O nexo de causalidade se constitui no evento de ocorrência mais próxima da consumação do dano	Com a Teoria da Proximidade da Causa, pode-se não chegar a apreciar o evento decisivo para a consumação do dano, já que este não precisa, necessariamente, anteceder o dano de modo imediato
TEORIA DA EQUIVALÊNCIA DAS CONDIÇÕES	Qualifica-se como nexo de causalidade qualquer meio que produza o resultado lesivo, seja este meio causa (vetor que obrigatoriamente leva ao resultado) ou condição que propicie o ambiente ideal para a produção de efeitos deletérios (vetor que antecede a causa)	A Teoria da Equivalência das Condições mostra-se excessivamente ampla, possibilitando "regressão infinita" sem lastro, de modo que, injustamente, entes/indivíduos venham a ser apontados como responsáveis, a despeito de não terem concorrido para os atos decisórios geradores do dano
TEORIA DA CAUSALIDADE ADEQUADA	Dentre os fatos antecedentes ao dano, há de se avaliar qual, efetivamente, tem aptidão para promover a produção do resultado danoso, não se considerando os demais fatos como causa, vez que irrelevantes a este fim	Há, na Teoria da Causalidade Adequada, grande espaço para subjetivismos na identificação do fato relevante, já que não delimitados critérios precisos para a avaliação da importância do fato na configuração do resultado danoso

Fonte: Autor (2019) ¹⁰³.

Por fim, faz-se necessário registrar uma observação adicional acerca da já referida causalidade múltipla. Evidenciadas múltiplas causas para um resultado danoso, respondem todos os envolvidos por cada um desses eventos, na medida de sua participação (STOCO, 2004).

¹⁰³ Quadro produzido a partir de considerações tecidas por Carrá (2004) e Nader (2016, v. 7).

5.2.2.4 Fator de imputação

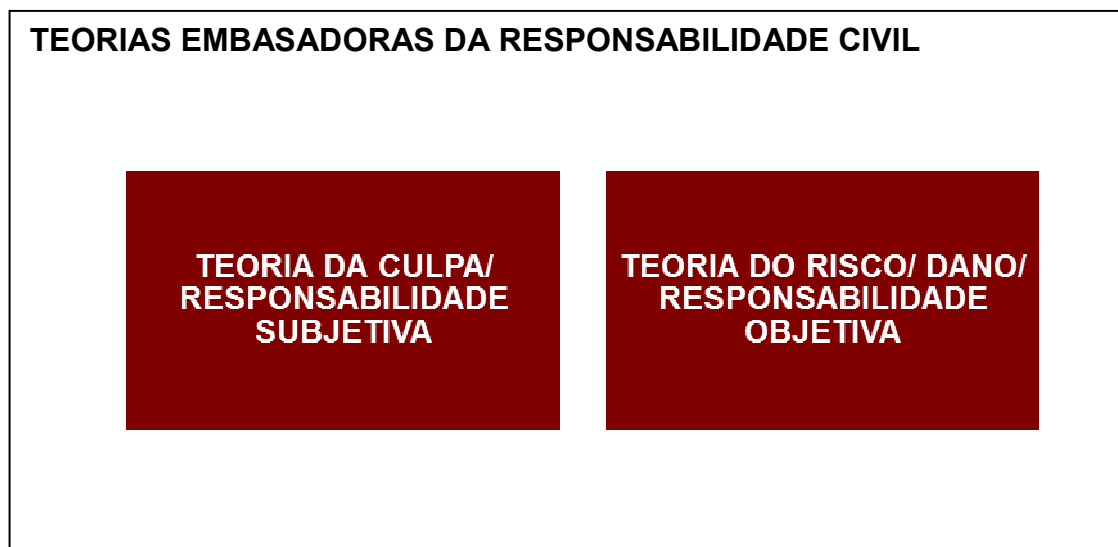
O Nexo de Imputação (Imputabilidade/Fator de Atribuição) há de ser compreendido como um vetor normativo que, na ocorrência de um dano, indica o ente por ele responsável, ou seja, o ente/indivíduo que deve arcar com as consequências do evento danoso, ainda que, eventualmente, não tenha sido seu causador (CARRÁ, 2004).

Para os que defendem o referido conjunto ampliado de pressupostos da responsabilidade civil, o Fator de Atribuição/Nexo de Imputação é elemento indispensável, já que é possível, em contextos específicos, que o agente causador do dano não seja responsável por sua reparação, cabendo esta a terceiros em função de disposição legal ou contratual¹⁰⁴. Para estes, a responsabilidade civil é vinculada pelo Princípio da Imputação.

5.2.3 Teorias

Dentre as teorias aplicadas à compreensão, ao estudo e ao regramento da responsabilidade civil, sobressaem-se as referidas na Figura 52.

Figura 52 - Teorias embasadoras da responsabilidade civil.



Fonte: Autor (2019) ¹⁰⁵.

¹⁰⁴ No ordenamento civil brasileiro, isto se observa, por exemplo, através do exame dos artigos 932, 936, 937 e 938, do Código Civil vigente (BRASIL, 2002).

¹⁰⁵ Ilustração concebida a partir de exposições de Pereira (2009, v. I, II, III), Carrá (2004), Stoco (2004) e Venosa (2009).

Considerações basilares sobre as teorias referidas na Figura 52 são expostas no Quadro 35.

Quadro 35 - Teorias embasadoras da responsabilidade civil.

TEORIAS EMBASADORAS DA RESPONSABILIDADE CIVIL						
TEORIA	IDEIAS ESSENCIAIS	CULPA COMO PRESSUPOSTO	EVENTOS DESENCADEANTES DA RESPONSABILIDADE	JUSTIFICATIVA ORIGINAL	CRÍTICAS PRINCIPAIS	EXEMPLOS ASSOCIADOS
TEORIA DA RESPONSABILIDADE CIVIL SUBJETIVA	A responsabilidade surge quando há dolo/intenção, ou culpa do agente causador do dano	SIM	• Intenção (dolo) de produção do resultado danoso • Assunção da possibilidade de produção do dano • Violação do dever de cuidado imposto pelo Direito (Negligência, Imprudência ou Imperícia)	• Ideia moral de que os indivíduos e seus bens são sagrados, não devendo ser admitidos injustos danos aos mesmos	• Dificuldades eventuais na demonstração da culpa em casos concretos	• Responsabilidade de uma empresa pelo vazamento dos dados seus clientes, já que a aludida empresa, apesar de devidamente alertada por especialistas de segurança, não fez a instalação de alguns <i>patches</i> • Responsabilidade de uma empresa desenvolvedora de <i>software</i> que, reputando apenas relevante a <i>performance</i> de um sistema, tenha desativado no <i>software</i> de seu cliente todos os recursos voltados à preservação da Segurança Computacional • Responsabilidade da empresa desenvolvedora se antivírus "VIRAL" pelo desenvolvimento de novo vírus que

TEORIAS EMBASADORAS DA RESPONSABILIDADE CIVIL						
TEORIA	IDEIAS ESSENCIAIS	CULPA COMO PRESSUPOSTO	EVENTOS DESENCADEANTES DA RESPONSABILIDADE	JUSTIFICATIVA ORIGINAL	CRÍTICAS PRINCIPAIS	EXEMPLOS ASSOCIADOS
						justifique a compra de seu novo pacote de antivírus Responsabilidade da empresa desenvolvedora de <i>software</i> “X” por novo sistema por ela criado para o Banco “Y” sem que tenha sido considerado qualquer requisito de Segurança, a despeito de a instituição bancária ter assinalado a importância de tal elemento
RESPONSABILIDADE CIVIL OBJETIVA	A responsabilidade civil independe do dolo e da culpa do agente causador do dano, decorrendo, na verdade, de disposição normativa (lei ou contrato) que imponha o dever de reparação	NÃO	- Exploração de atividade empresarial que resulte em dano - Produção/comércio de bens/serviços que apresentem dano associado, independentemente de culpa	- Solução dos problemas de responsabilidade emergentes com a Industrialização (despersonalização das relações de produção & dificuldades de identificação da culpa e de comprovação da culpa, especialmente) - Inadmissibilidade do exercício impune de	- Cerceamento da liberdade e da autonomia das pessoas e entes - Desestímulo à atividade produtiva	- Responsabilidade da empresa prestadora de um serviço <i>web</i> pela inoperância do citado serviço, já que prevista esta responsabilidade em contrato - Responsabilidade de uma empresa fornecedora de um dado <i>software</i> por vulnerabilidade de segurança não corrigida em até 6 (seis) meses após a

TEORIAS EMBASADORAS DA RESPONSABILIDADE CIVIL						
TEORIA	IDEIAS ESSENCIAIS	CULPA COMO PRESSUPOSTO	EVENTOS DESENCADEANTES DA RESPONSABILIDADE	JUSTIFICATIVA ORIGINAL	CRÍTICAS PRINCIPAIS	EXEMPLOS ASSOCIADOS
				atividades produtivas diante dos riscos potenciais que delas podem emergir para outras pessoas e entes • Razoabilidade da exigência de reparação por aqueles que se beneficiam economicamente de uma atividade produtiva quanto aos riscos decorrentes desta atividade produtiva para terceiros		sua identificação, se houver diploma legal neste sentido

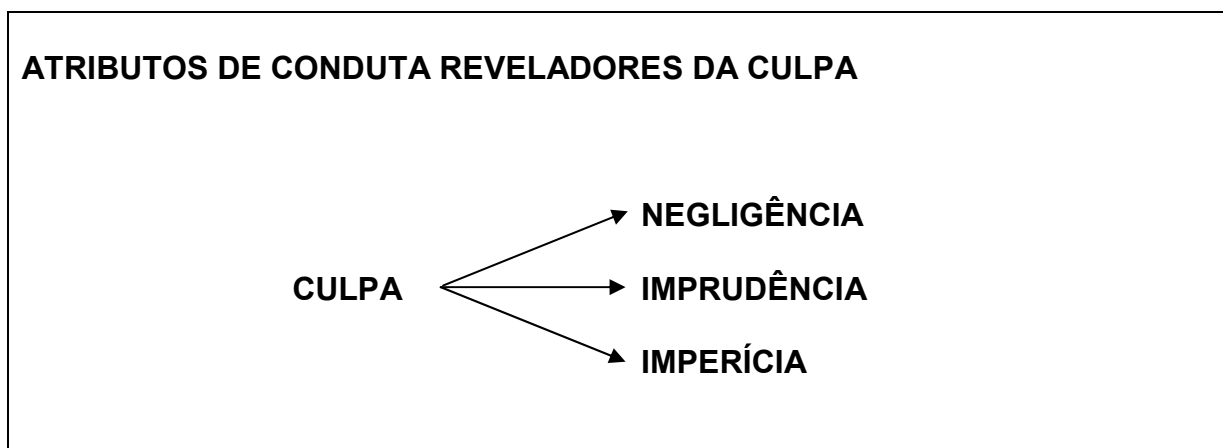
Fonte: Autor (2019) ¹⁰⁶.

¹⁰⁶ Quadro elaborado a partir de observações tecidas por Pereira (2009, v. I, II, III), Carrá (2004), Stoco (2004) e Venosa (2009), tendo os exemplos sido criados pelo próprio pesquisador.

5.2.3.1 Notas adicionais sobre a culpa na Teoria da Responsabilidade Subjetiva

Como asseverado na Seção 5.2.3, a culpa é requisito da responsabilidade na Teoria da Responsabilidade Subjetiva. Nesta teoria, diz-se que há culpa quando evidenciado, na conduta do agente causador do dano, ao menos um dos atributos constantes da Figura 53.

Figura 53 - Atributos de conduta reveladores da culpa do agente causador do dano.



Fonte: Autor (2019) ¹⁰⁷.

É importante se observar, contudo, que a simples identificação dos mencionados atributos não configura a culpa, pois há de se avaliar a coexistência dos elementos indicados na Figura 54 (PEREIRA, 2005, v.III).

¹⁰⁷ Representação construída a partir das ideias expostas por Reale (2003), Carrá (2004) e Pereira (2009, v. I).

Figura 54 - Elementos da culpa.



Fonte: Autor (2019) ¹⁰⁸.

Ainda que a culpa, usualmente, possa ser tida como una, é válido salientar que, em arcabouços normativos alienígenas, ela pode ser classificada em função da gradação da falta cometida, como representado no Quadro 36, e que, em função desta gradação, dá-se a responsabilização.

Quadro 36 - Classificação da culpa em função da gradação da falta cometida.

CLASSIFICAÇÃO DA CULPA EM FUNÇÃO DA GRADAÇÃO DA FALTA COMETIDA	
CATEGORIA	ESPÉCIE DE FALTA
<i>Culpa Levis /Culpa Média</i>	Falta de diligência mediana a que deveria atentar o homem normal
<i>Culpa Lata /Culpa Grave</i>	Negligência mais grave evitável por homem inferior ao homem médio
<i>Culpa Levíssima</i>	Falta que poderia ser cometida pelo homem médio, mas não pelo homem efetivamente diligente

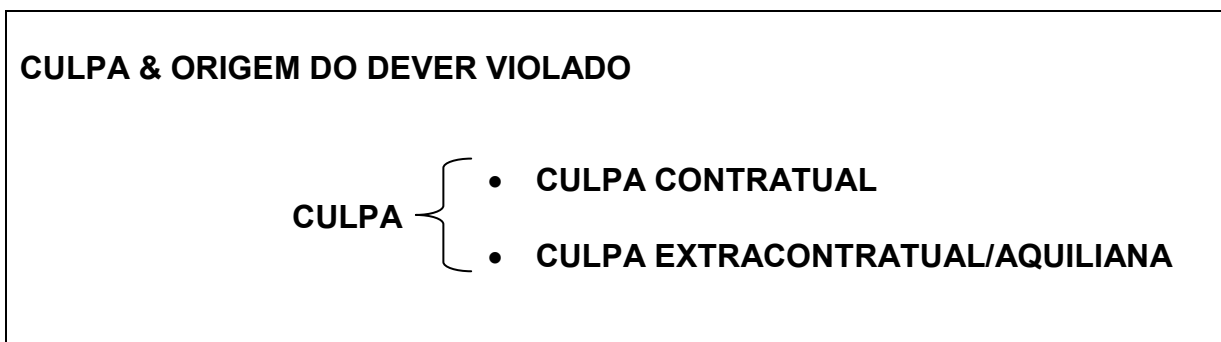
Fonte: Autor (2019) ¹⁰⁹.

A culpa pode, também, ser objeto de classificação em função da origem do dever violado, como se depreende da Figura 55.

¹⁰⁸ Ilustração concebida com base em comentários de Pereira (2005, v. III).

¹⁰⁹ Quadro elaborado a partir de observações tecidas por Pereira (2005, v. III) e Tartuce (2016).

Figura 55 - Classificação da culpa em função da origem do dever violado.



Fonte: Autor (2019) ¹¹⁰.

Como se observa da Figura 55, há culpa contratual quando o dever inadimplido encontra-se previsto em avença previamente pactuada pelos envolvidos. Apresenta-se culpa extracontratual/aquiliana, quando em afronta a disposição legal positiva e não a norma contratual, é violado o dever de respeito a bem jurídico alheio, ou o ônus de não causar danos a outrem.

A mencionada distinção da culpa a partir da origem do dever violado, apesar da unicidade geral da culpa, apresenta relevância prática no contexto de sua comprovação, como representado no Quadro 37.

Quadro 37 - Culpa & ônus da prova.

CULPA & ÔNUS DA PROVA	
ESPÉCIE DE CULPA	ÔNUS DA PROVA
CULPA CONTRATUAL	Afastamento da culpa dependente de comprovação oferecida pelo agente/apontado como responsável
CULPA EXTRACONTRATUAL/AQUILIANA	Reconhecimento da culpa dependente da apresentação de provas pela vítima (provas do dano, do fato antijurídico, do nexo de causalidade e do fator de atribuição, especialmente)

Fonte: Autor (2019) ¹¹¹.

¹¹⁰ Figura produzida após reflexão acerca de exposição de Pereira (2005, v. III) e Tartuce (2016).

¹¹¹ Quadro elaborado a partir de exposição de Pereira (2005, v. III) e Tartuce (2016).

Acerca da classificação da culpa, uma observação adicional se faz necessária. É possível, ainda, a sua classificação quanto ao modo de atuação do agente que causa o dano, como ilustrado no Quadro 38.

Quadro 38 - Classificação da culpa quanto à conduta do agente causador do dano.

CULPA & CONDUTA DO AGENTE CAUSADOR DO DANO	
ESPÉCIE DE CULPA	CONDUTA DO AGENTE CAUSADOR DO DANO
<i>CULPA IN VIGILANDO</i>	Desatenção/falha no dever de zelo
<i>CULPA IN COMITTENDO</i>	Negligência, imprudência ou imperícia na efetiva realização de um ato, na comissão
<i>CULPA IN OMITTENDO</i>	Indevida abstenção/omissão no cumprimento de dever legal
<i>CULPA IN ELIGENDO</i>	Falha na escolha da pessoa que deve realizar uma tarefa e por tal vir a ser responsabilizada
<i>CULPA IN CONTRAHENDO</i>	Dano na contratação, i.e., lesão a contratante na pactuação de avença

Fonte: Autor (2019) ¹¹².

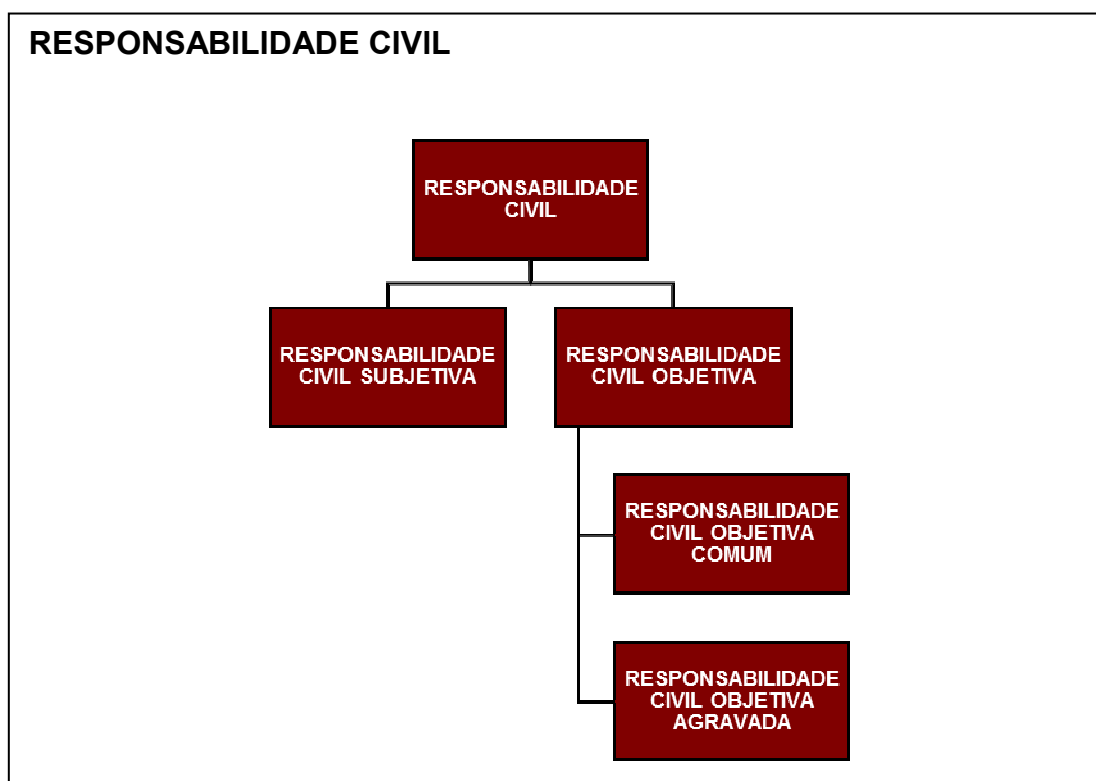
Por fim, há de se ressaltar, conclusivamente, a possibilidade de configuração de *Culpa Pré-Contratual*, quando, iniciadas negociações em bons termos, prejuízos ocorrem em virtude da injustificada interrupção de entendimentos.

5.2.4 Espécies

É corrente a classificação da responsabilidade civil em função da teoria que a embasa, como representado na Figura 56.

¹¹² Quadro construído a partir de comentários tecidos por Pereira (2005, v. III) e Tartuce (2016).

Figura 56 - Classificação da responsabilidade civil fundada nas teorias de base.



Fonte: Autor (2019) ¹¹³.

No Quadro 39, expõem-se comentários básicos sobre as categorias apresentadas na Figura 56.

Quadro 39 - Classificação da responsabilidade civil fundada nas teorias de base.

CLASSIFICAÇÃO DA RESPONSABILIDADE CIVIL EM FUNÇÃO DA TEORIA DE BASE		
CATEGORIA	NOTA DISTINTIVA	EXEMPLOS
RESPONSABILIDADE CIVIL SUBJETIVA	Responsabilidade em que o dolo/culpa é elemento indispensável	Responsabilidade a que se sujeitaria uma empresa construtora de aviões (Companhia Construtora Global – nome fictício), a qual, apesar de ter sido alertada por pilotos de teste, considerou irrelevante possível perda de controle das aeronaves com suposta indevida ativação

¹¹³ Ilustração elaborada após reflexão acerca das ideias tecidas por Pereira (2005, v. III), por Carrá (2004) e por Venosa (2009, v. 4).

CLASSIFICAÇÃO DA RESPONSABILIDADE CIVIL EM FUNÇÃO DA TEORIA DE BASE		
CATEGORIA	NOTA DISTINTIVA	EXEMPLOS
		automática do sistema anti-stall por um sensor, o que, se confirmado fosse, poderia implicar impossibilidade total de controle dos aviões pelos pilotos e quedas iminentes
RESPONSABILIDADE CIVIL OBJETIVA COMUM	Responsabilidade independente de dolo/culpa em que há liame íntegro entre o fato antijurídico e o dano, podendo vir a ser suprimida ou mitigada em casos específicos, quando este liame deixa de existir (Seção 5.2.5)	Responsabilidade da empresa seguradora “R”, contratada pela empresa construtora de aviões, em caso de sinistro envolvendo as aeronaves produzidas por esta
RESPONSABILIDADE CIVIL OBJETIVA AGRAVADA	Responsabilidade independente de dolo/culpa em que não se apresenta liame íntegro entre o fato antijurídico e o dano e que persiste em atenção a interesses sociais reputados relevantes	Responsabilidade da instituição bancária “X” por fraude no lançamento de inexistente transação eletrônica em desfavor de um cliente seu, pouco importando se o lançamento inexistente se deu por dolo ou culpa da instituição bancária, desde que não configurada forma maior ou culpa da própria suposta vítima

Fonte: Autor (2019) ¹¹⁴.

Acerca da responsabilidade civil objetiva agravada, vale acrescentar que:

- sua existência se funda na necessidade de se salvaguardar interesses sociais, preservando-se o dever de indenizar mesmo em situações que, à primeira vista, qualificam-se como caso fortuito/força maior;
- a responsabilidade civil objetiva agravada se apresenta, usualmente, no desempenho de atividades econômicas, quando riscos inerentes a estas atividades não configuram caso fortuito/força maior;
- apenas em caso de fortuito externo, cessa a responsabilidade civil objetiva

¹¹⁴ Quadro construído após reflexão acerca das ideias tecidas por Pereira (2005, v. III), por Carrá (2004) e por Venosa (2009, v. 4), tendo os exemplos sido idealizados pelo próprio pesquisador.

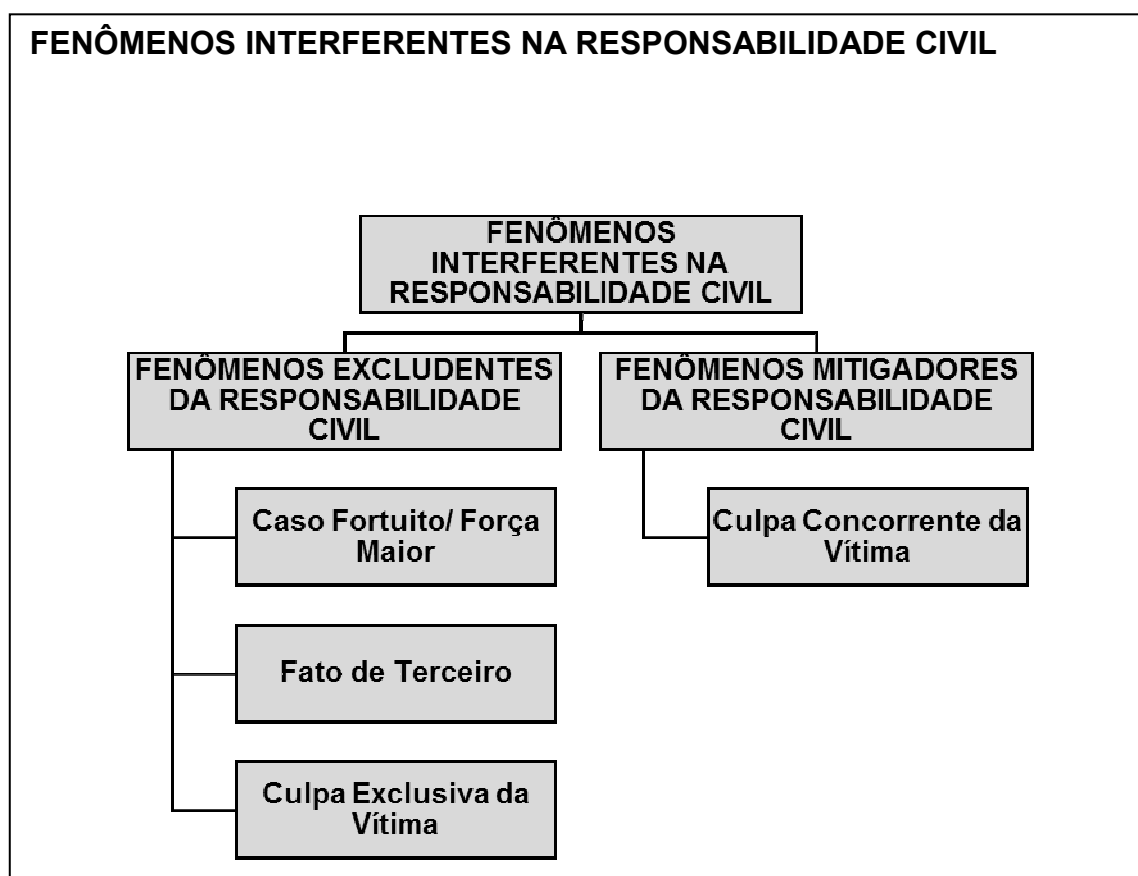
agravada;

- fato de terceiro não é, geralmente, questionável para o afastamento da responsabilidade civil objetiva agravada.

5.2.5 Exclusão e mitigação da responsabilidade civil

Constatados fato antijurídico, dano, nexo de causalidade e fator de imputação, há, em princípio, responsabilidade civil. Esta responsabilidade, todavia, pode ser afastada ou mitigada, quando evidenciada a ocorrência de fenômenos que a excluem ou diminuem, tal como os representados na Figura 57.

Figura 57 - Fenômenos de exclusão e mitigação da responsabilidade civil.



Fonte: Autor (2019) ¹¹⁵.

¹¹⁵ Figura concebida com a consideração de comentários tecidos em Carrá (2004), Stoco (2004) e Venosa (2009). As ideias relativas ao Estado de Necessidade e à Legítima Defesa não foram consideradas na concepção desta ilustração, vez que, no Direito Civil, sua significância não é tão patente quanto no Direito Penal e que o foco último, no estudo ora relatado, não envolve situações excepcionálíssimas geradoras de dano, mas, sim, apenas as usuais e corriqueiras atividades de fornecimento e de prestação de serviços com *software*.

No Quadro 40, apresentam-se algumas notas sobre os fenômenos referidos na Figura 57.

Quadro 40 - Fenômenos interferentes na responsabilidade civil.

FENÔMENOS INTERFERENTES NA RESPONSABILIDADE CIVIL			
CATEGORIA FENÔMENICA	FENÔMENO	IDEIA ESSENCIAL	EXEMPLOS RELACIONADOS A SOFTWARE
FENÔMENOS EXCLUDENTES DA RESPONSABILIDADE CIVIL	CASO FORTUITO/ FORÇA MAIOR	Havendo evento exterior imprevisível e impeditivo da adoção de conduta diversa, afasta-se a responsabilidade civil, vez que não possível se esperar que o agente, com sua prudência, perícia e diligência, evite todo e qualquer resultado danoso	Inoperância de um sistema <i>web</i> em razão da destruição do parque computacional de uma empresa por um <i>tsunami</i> de proporções severas
	FATO DE TERCEIRO	Em situações em que o dano, efetivamente, resulta da conduta de terceiro (pessoa diversa do ente que é apontado como agente e da vítima), não há que se falar em responsabilidade civil do ente apontado, já que inexistente nexo de causalidade, ressalvada, contudo, as hipóteses em que o terceiro age sob ordens do ente apontado ou em que há disposição legal/contratual definidora de responsabilidade excepcional	- Impossibilidade de um dado cliente utilizar um sistema <i>desktop</i> antes instalado em seu computador pela empresa “X” porque, por falha no serviço de fornecimento de energia elétrica prestado pela empresa “Y”, houve sobrecarga na rede elétrica e o computador citado foi fisicamente danificado por tensão excessivamente elevada, tendo se derretido a placa-mãe, o processador e os <i>hard disks</i> (inclusive os do sistema de <i>backup</i>) - Perda de todos os dados da entidade “X” instalados nos computadores do seu setor de pessoal e pagamento, relativos ao sistema cliente-servidor a ele fornecido pela empresa “Y”, em virtude de todos os computadores referidos terem sido atingidos por lamaçal oriundo do estouro de barragem mantida pela Companhia Mineradora “W”, já que esta Mineradora, desconsiderando orientação de

FENÔMENOS INTERFERENTES NA RESPONSABILIDADE CIVIL			
CATEGORIA FENÔMENICA	FENÔMENO	IDEIA ESSENCIAL	EXEMPLOS RELACIONADOS A SOFTWARE
			engenheiros, não procedeu aos reforços estruturais indispensáveis à estabilidade da barragem Perda de todos os dados da instituição “X” (dados relativos ao sistema por ela usado, mas fornecido pela empresa “Y”) em virtude de um ex-funcionário da empresa “X”, fanático por jogos antigos que passou 36 (trinta e seis) horas seguidas jogando <i>Wolfenstein 3D</i> © após a sua demissão, ter retornado ao Centro de Processamento de Dados da empresa “X” e atirado em todos os computadores e dispositivos de <i>backup</i> com uma <i>bazooka</i> e incendiado o prédio inteiro depois disso
	CULPA EXCLUSIVA DA VÍTIMA	Quando o resultado danoso decorre de culpa exclusiva da vítima, resta excluída a culpa de terceiros, eis que integralmente afastado o nexo de causalidade entre a conduta destes e o dano	- Mau funcionamento de um sistema utilizado pela empresa “X” (sistema fornecido pela empresa “Y”), já que a empresa “X” desconsiderou recomendação da empresa “Y” para que o aludido sistema apenas fosse executado em um ambiente/sistema operacional de versão igual ou superior à indicada no contrato de aquisição/uso - Perda de dados sensíveis da empresa “X” (dados associados ao sistema a ela fornecido pela empresa “Y”), em razão de um grupo de <i>hackers</i> ter explorado uma vulnerabilidade de segurança que não mais deveria existir, já que

FENÔMENOS INTERFERENTES NA RESPONSABILIDADE CIVIL			
CATEGORIA FENÔMENICA	FENÔMENO	IDEIA ESSENCIAL	EXEMPLOS RELACIONADOS A SOFTWARE
			a empresa “Y”, ao identificar a vulnerabilidade referida, alertou a empresa “X” da necessidade de instalação de um <i>patch</i> e a empresa “X” não fez isso porque seus dirigentes não achavam isso relevante e temiam, enquanto a instalação ocorresse, que o sistema apresentasse lentidão
FENÔMENOS MITIGADORES DA RESPONSABILIDADE CIVIL	CULPA CONCORRENTE DA VÍTIMA	Em casos em que a vítima contribui para a produção do resultado danoso, sua culpa reduz a responsabilidade de terceiros também envolvidos na produção do dano	Perda de todos dados da empresa “X” relativos ao sistema por ela usado fornecido pela empresa “Y” e impossibilidade de restauração do <i>backup</i> do dia anterior em razão de funcionário desatento da empresa “Y” ter deletado a base de dados existente em um servidor remoto e de um nada diligente funcionário da empresa “X” ter formatado os dispositivos de <i>backup</i> e copiado nos mesmos seu acervo pessoal de fotos

Fonte: Autor (2019) ¹¹⁶.

¹¹⁶ Quadro produzido com a consideração das ideias expostas por Carrá (2004), Stoco (2004) e Venosa (2009) e exemplos elaborados pelo próprio pesquisador.

Acerca do caso fortuito, não é supérfluo destacar, mais uma vez, que apenas os fortuitos externos podem vir a excluir a responsabilidade do agente, o mesmo não ocorrendo quanto aos fortuitos ditos internos, pois a falta de diligência, prudência e de perícia, bem como falhas humanas não suprimem o nexo de causalidade.

5.2.6 Sanções

Para a reparação dos efeitos deletérios de danos de ordem pessoal e patrimonial decorrentes do descumprimento de normas jurídicas e para se coibir a ocorrência de fatos antijurídicos que resultem danos, impõem-se sanções aos que dão causa aos mencionados descumprimentos (AMARAL NETO, 1977), tal como representado na Figura 58.

Figura 58 - Descumprimento de dever jurídico e sanção.

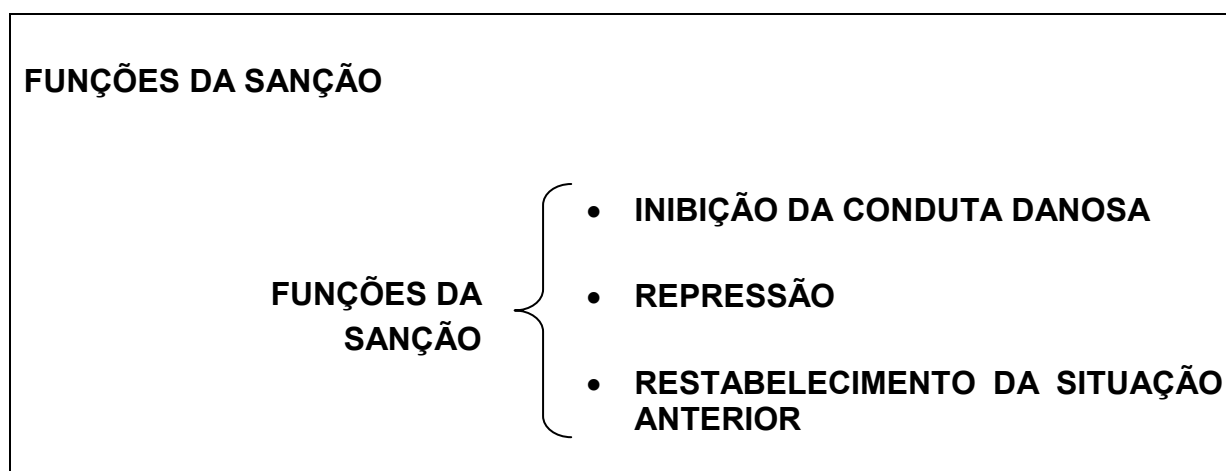


Fonte: Autor (2019) ¹¹⁷.

Apesar de, usualmente, serem associadas às sanções as duas funções antes referidas, há de se observar que existe, ainda, uma terceira finalidade, tal como ilustrado na Figura 59: a repressão.

¹¹⁷ Ilustração produzida após reflexão acerca das ideias expostas por Carrá (2004), Stoco (2004), Venosa (2009) e Pereira (2009, v. I, II, III).

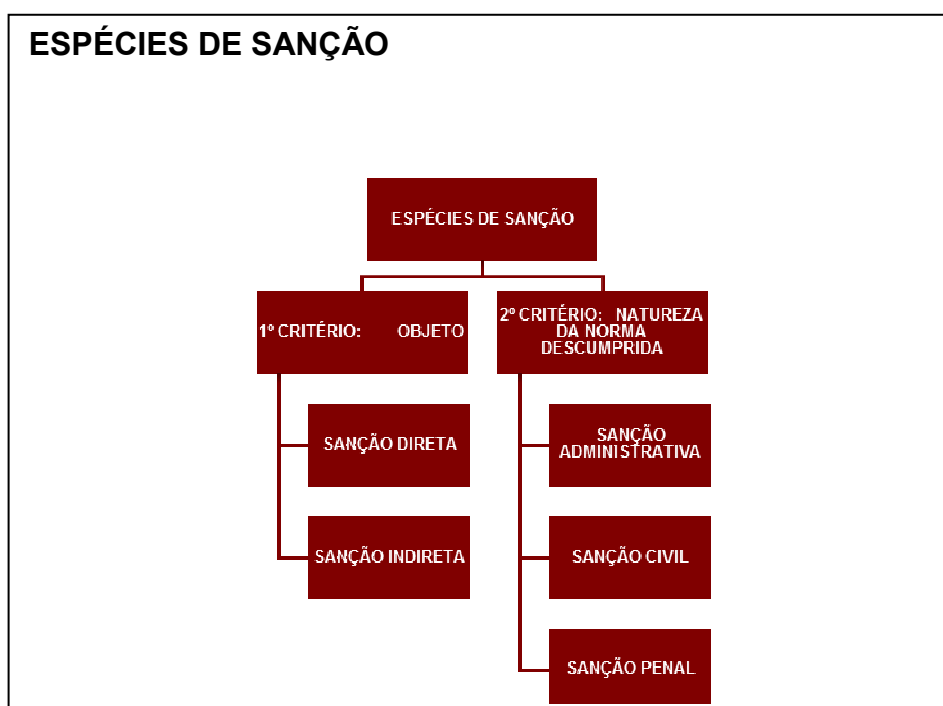
Figura 59 - Funções da sanção.



Fonte: Autor (2019) ¹¹⁸.

De modo geral, pode-se asseverar, considerados critérios variados, que há distintas espécies de sanções, como se depreende da Figura 60.

Figura 60 - Espécies de sanção.



Fonte: Autor (2019) ¹¹⁹.

No Quadro 41, apresentam-se alguns comentários sobre as espécies de sanção referidas na Figura 60.

¹¹⁸ Representação elaborada a partir de ideias expostas em Carrá (2004), Nader (2016, v. 7).

¹¹⁹ Figura concebida a partir de observações de Amaral Neto (1977).

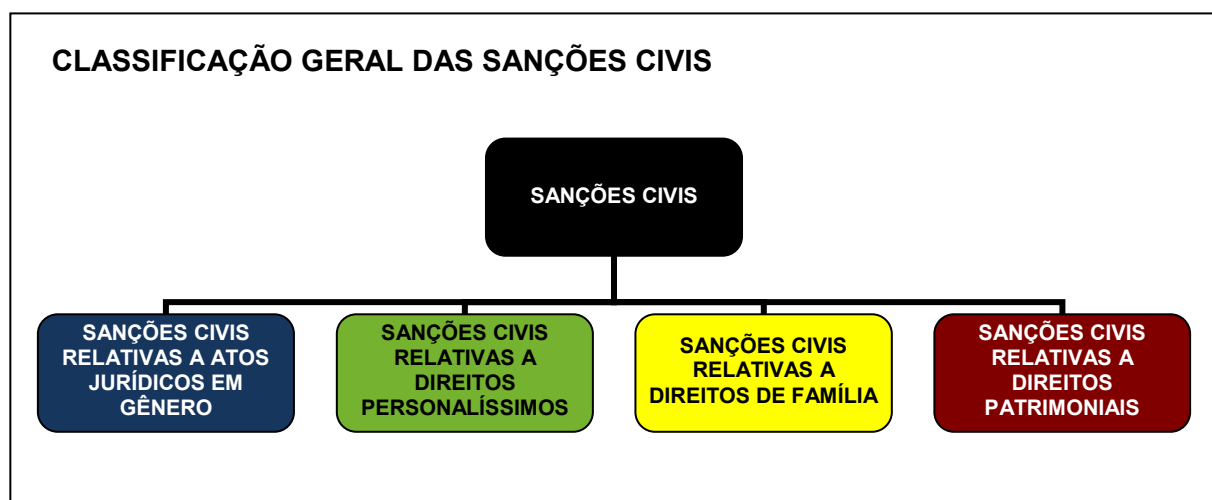
Quadro 41 -Espécies de sanção.

ESPÉCIES DE SANÇÃO		
CRITÉRIO	ESPÉCIE	DESCRIÇÃO
OBJETO DA SANÇÃO	SANÇÃO DIRETA	Sanção destinada ao restabelecimento da situação anterior ao descumprimento da norma jurídica
	SANÇÃO INDIRETA	Sanção destinada à reparação do prejuízo causado por um descumprimento normativo, quando impossível o restabelecimento do <i>status quo ante</i> , i.e., do estado anterior ao citado descumprimento
NATUREZA DA NORMA DESCUMPRIDA	SANÇÃO ADMINISTRATIVA	Sanção impositiva na esfera administrativa em razão do descumprimento de norma de mesma natureza
	SANÇÃO CIVIL	Sanção originária do descumprimento de norma civil
	SANÇÃO PENAL	Sanção originária do descumprimento de norma penal

Fonte: Autor (2019) ¹²⁰.

As sanções civis, por seu turno, costumam, também, ser objeto de classificação, tal como ilustrado na Figura 61.

Figura 61 - Classificação geral das sanções civis.



Fonte: Autor (2019) ¹²¹.

¹²⁰ Quadro construído após reflexão sobre as ideias de Amaral Neto (1977).

¹²¹ Figura elaborada com base em exposição de Amaral Neto (1977).

Como se depreende da Figura 61, as sanções civis, relativamente ao objeto tutelado, podem ser classificadas em quatro categorias principais, as categorias das Sanções Civis Relativas a Atos Jurídicos em Gênero, das Sanções Civis Relativas a Direitos Personalíssimos, das Sanções Civis Relativas a Direitos de Família e das Sanções Civis Relativas a Direitos Patrimoniais.

As sanções civis relativas a ofensas a direitos personalíssimos e a direitos patrimoniais, sanções de especial interesse para a responsabilidade civil, materializam-se com a imposição de obrigações voltadas à reparação. Entre estas obrigações encontram-se o restabelecimento de situação prévia e o pagamento de indenização (CARRÁ, 2004; CAVALIERI FILHO, 2014; PEREIRA, 2009, v. I, II, III).

Ainda que o tema indenização não se insira no escopo da pesquisa ora relatada, discorre-se brevemente sobre o mesmo na Seção 5.2.6.1.

5.2.6.1 Breves comentários sobre indenizações

Em linhas gerais, as indenizações podem ser concebidas como os pagamentos a que um ente é condenado em virtude da configuração de danos a outros entes.

Para a realização de pagamentos de tal sorte, indispensável se faz a apuração dos danos, o que se verifica, geralmente, mediante arbitramento de perdas, em juízos de probabilidade (PEREIRA, 2009, v. I, II, III). Nesta apuração, consideram-se, de modo usual, o prejuízo efetivo presente, os danos emergentes e os lucros cessantes. Carrá (2004), contudo, entende que o montante indenizatório também pode abarcar parcelas agravantes de natureza propedêutica e punitiva.

Especial atenção há de ser dada, na definição do *quantum* indenizatório, à proporcionalidade entre este e o prejuízo a ser indenizado, evitando-se a fixação de montantes excessivamente onerosos que favoreçam o enriquecimento sem causa.

Por fim, é válido registrar, no pagamento em debate, que a atualização monetária é indispensável, para se garantir a expressividade das indenizações, e que o pagamento de indenizações, em princípio, não elide a incidência e o dever de cumprimento de sanções penais.

5.2.7 Regresso

Quanto à responsabilidade civil, é válido se tecer, ainda, algumas observações acerca do direito de regresso.

Em casos de responsabilidade objetiva, é reconhecido o direito de regresso dos responsáveis legais por um dano contra o ente/indivíduo que, sob seu comando, efetivamente deu causa ao dano. Assim, aquele que repara o dano pode exigir compensação desta reparação em relação àquele que, de fato, laborou para a consumação do fato antijurídico (CARRÁ, 2004).

5.2.8 Transferência de responsabilidade civil

A transferência é tema recorrente relativo à responsabilidade civil. Através dela, o que se efetiva é o mero repasse do encargo pelos danos (dever de reparar e/ou indenizar), não se cogitando, em sentido estrito, da transferência do dolo ou da culpa.

Como observado por Pereira (2009, v. I, II, III), a transferência de responsabilidade civil, atualmente, efetiva-se com:

- a pactuação de contratos de seguro;
- a definição de limites de ressarcimento;
- a estipulação de cláusulas de não indenizar, condições que, suprimindo o dever de indenizar do agente causador do dano, acabam por transferir ao próprio ente lesado os custos pelo prejuízo a que o primeiro deu causa.

Embora haja entendimento doutrinário favorável à transferência dos encargos decorrentes da responsabilidade civil, como o posicionamento defendido por Pereira (2009, v. I, II, III), para quem tal transferência é manifestação legítima da autonomia da vontade e consequência natural da força cogente das obrigações convencionais, tal questão permanece como polêmica, já que também relevantes os argumentos dos que a combatem.

Independentemente da filiação à corrente permissiva da transferência ou à corrente que rejeita o repasse em discussão, há hipóteses que afastam a

validade das cláusulas exoneradoras do dever de indenizar (PEREIRA, 2009, v. I, II, III):

- a constatação de dolo do agente;
- a ocorrência de atentado à ordem pública;
- situações em que não seja permitido o estabelecimento de negócio jurídico contratual;
- a configuração de ofensa a direito expresso.

5.3 RESPONSABILIDADE CIVIL POR DANOS DECORRENTES DA EXPLORAÇÃO DE VULNERABILIDADE DE SEGURANÇA EM SOFTWARE

Ainda que, em linhas gerais, não haja diferenças entre a responsabilidade civil por vulnerabilidade de segurança em *software* e outras espécies de responsabilidades por danos, é útil pontuar algumas observações sobre tal tema.

Em princípio, importa esclarecer que, para o indivíduo/entidade lesado pelo dano em debate, são irrelevantes o momento, ao longo da etapa de desenvolvimento de *software*, em que configurada a vulnerabilidade e a identificação do desenvolvedor por ela responsável. O que importa, para o ente lesado, é que a vulnerabilidade teria ocorrido e que, se a empresa produtora/fornecedora de *software* tivesse sido diligente, isso não aconteceria. Assim sendo, não se faz, neste tipo de demanda, “caça às bruxas”, o que não impede, todavia, que a entidade produtora/fornecedora de *software*, por si mesma, busque identificar o problema em sua linha produtiva, bem como possíveis agentes responsáveis, os quais pode vir a acionar por via regressiva, como registrado na Seção 5.2.7 deste documento.

Tem-se, deste modo, simplesmente a constatação do dano com a consequente apuração da indenização devida, considerados os vultos dos prejuízos causados pela exploração da vulnerabilidade e isso se observa no tocante aos *softwares* comerciais e aos *softwares* ditos proprietários.

6 ÉTICA PROFISSIONAL

6.1 CONSIDERAÇÕES PRELIMINARES

Como registrado no Capítulo 5, os seres humanos são ditos seres gregários que, almejando sobreviver e atingir seus objetivos, coabitam um espaço comum. A coexistência referida, como também já destacado no Capítulo 5, nem sempre se efetiva de maneira tranquila, pois há momentos em que conflitos de interesses emergem (HOBBS, 2017), cabendo o destaque de que entre estes conflitos se sobressaem os relacionados à responsabilização.

Usualmente, os conflitos envolvendo responsabilização surgem quando uma pessoa ou entidade sofre danos como resultado de (in)ações de outra pessoa/ente. Sendo os conflitos de tal espécie de extrema importância para as sociedades humanas e suas relações comerciais, é corrente a sua abordagem pela Moral, pelo Direito e pela Ética.

Em termos genéricos, a Ética pode ser concebida como o ramo da Filosofia Moral que estuda e avalia o caráter e as condutas humanas, consideradas as tradições socialmente aceitas, os usos e os costumes (BITTAR, 2016) (MASIERO, 2008). Entre os temas de interesse da Ética, incluem-se, como observado por Nalini (2015), os seguintes:

- a compreensão das diferenças entre o certo e o errado;
- a existência de uma boa vida;
- a tomada de decisões éticas;
- direitos e responsabilidades.

Frequentemente, diz-se que há diversos ramos de concepção da Ética (BRITISH BROADCASTING CORPORATION, [2014?]), como brevemente exposto no Quadro 42.

Quadro 42 – Ramos da Ética.

RAMOS DA ÉTICA	
RAMOS	DESCRIÇÃO BÁSICA
Metaética	Ética encarregada da natureza dos julgamentos morais, bem como das origens e do significado dos princípios éticos
Ética Normativa	Ética que lida com o conteúdo do julgamento moral e com os critérios empregados na compreensão do que é certo ou não
Ética Aplicada	Ética encarregada da análise ética de um tema/assunto particular

Fonte: Autor (2019) ¹²².

No contexto da responsabilidade originária de relações comerciais e atividades profissionais, a Ética Aplicada revela sua especial importância e utilidade. Como consequência desta relevância, é usual a consolidação de documentos que tratam das condutas comerciais e profissionais que podem dar origem a danos a indivíduos e empreendimentos: os Códigos de Ética.

6.2 CÓDIGOS DE ÉTICA PROFISSIONAL

Os Códigos de Ética Profissional constituem diretivas centrais para profissionais de variados domínios. Em essência, estas diretivas se destinam a promover boas condutas e comportamentos entre profissionais, de forma que os mesmos possam exercer regularmente suas atividades laborais com custo mínimo para eles mesmos, seus colegas de trabalho, empregadores e para a sociedade civil (DAVIS, 1991).

A ideia principal por trás dos Códigos de Ética Profissional envolve, então, o favorecimento das atividades profissionais através da prescrição de princípios e regras focados na evitação e na minimização dos riscos e danos potencialmente decorrentes de práticas profissionais ruins e procedimentos como: a) condutas irrazoáveis; b) exploração do cliente/público; c) negligência, imprudência ou imperícia profissional; d) pressões externas; e) competição profissional perniciosa.

¹²² Quadro elaborado a partir das considerações observadas em British Broadcasting Corporation (2018).

Usualmente, diz-se, como anotado por Davis (1991), que os Códigos de Ética são necessários porque:

- embora os profissionais tenham suas próprias consciências, estas consciências variam em um amplo espectro;
- outros profissionais, a sociedade e o público em geral não devem ficar vulneráveis a esta ampla variação espectral, sendo extremamente importante uma proteção mínima aos seus interesses e bem-estar;
- dada a possibilidade de os atos profissionais causarem danos e prejuízos em virtude de más práticas, pode advir responsabilidade profissional, nos termos do Direito e dos Códigos de Ética propriamente ditos.

Como mencionado antes, os Códigos de Ética são uma realidade em uma variedade de domínios, sendo, frequentemente, estabelecidos por sociedades/associações profissionais com o propósito de mostrar ao público em geral a capacidade de uma determinada profissão regular a si mesma (ANDERSON et al, 1993). Em diferentes ramos das Engenharias, diversas sociedades profissionais definiram seus Códigos de Ética. Entre estas sociedades, algumas se destacam (FLEDDERMANN, 2012), como o Institute of Electrical and Electronics Engineers (IEEE), a National Society of Professional Engineers (NSPE), a American Society of Mechanical Engineers (ASME), a American Society of Civil Engineers (ACSE), o American Institute of Chemical Engineers (AIChE) e a Sociedade de Engenheiros Civi do Japão.

A Engenharia de *Software*, como segmento humano de atividade produtiva, é também sujeita à Ética e, em especial, à Ética Aplicada, já que a responsabilidade não pode ser dissociada das atividades de desenvolvimento de *software* porque do uso/construção do *software* podem resultar danos (IEEE COMPUTER SOCIETY; ASSOCIATION FOR COMPUTING MACHINERY, 1999). Seguindo esta ideia, o IEEE e a Association for Computing Machinery (ACM) elaboraram, em 1999, um Código de Ética próprio para este segmento: o Código de Ética IEEE/ACM para Engenharia de *Software*.

6.3 CÓDIGO DE ÉTICA IEEE/ACM PARA ENGENHARIA DE *SOFTWARE*

Em 1994, o IEEE e a ACM, como parte de uma iniciativa focada na definição da Engenharia de *Software* como uma profissão, criaram um comitê conjunto com uma missão especialíssima: o estabelecimento de “um conjunto apropriado de padrões para a prática profissional da Engenharia de *Software* em que decisões industriais, certificação profissional e currículos educacionais pudessem se basear” (GOTTERBARN, MILLER, ROGERSON; 1997).

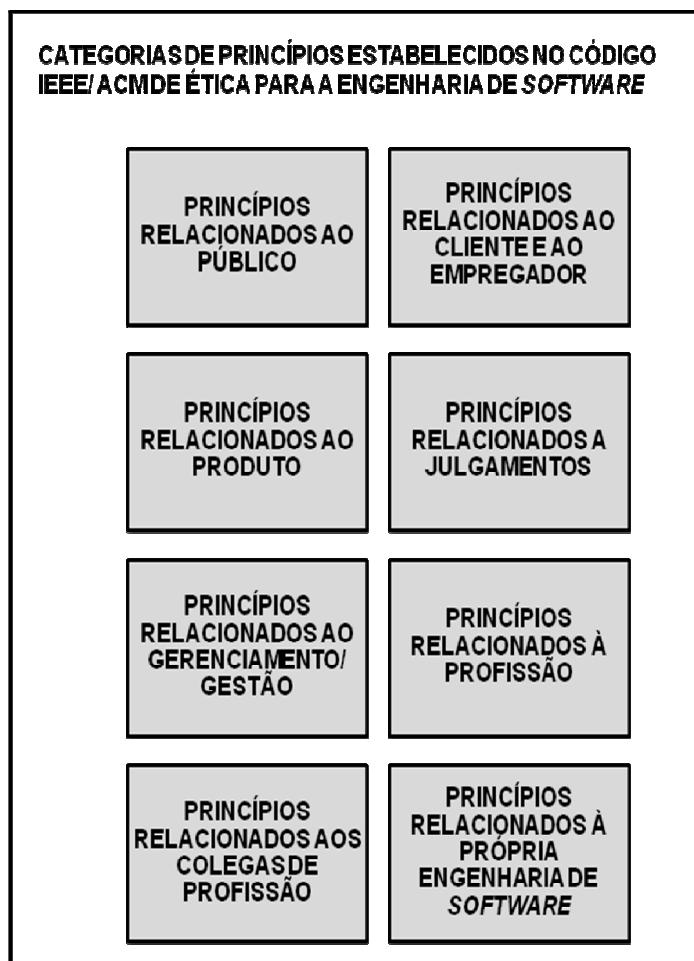
Para realizar a mencionada missão, o referido comitê estabeleceu diversas forças-tarefas. Uma dessas forças-tarefas ficou encarregada de elaborar um Código de Ética para a Engenharia de *Software*. Uma versão preliminar foi elaborada e submetida à crítica em 1997. Após a análise das críticas e comentários feitos, o Código de Ética IEEE/ACM para Engenharia de *Software* foi aprovado em 1999 (GOTTERBARN, MILLER, ROGERSON; 1999) ¹²³.

O Código IEEE/ACM para Engenharia de *Software* contém conjuntos de princípios¹²⁴ que, para o bem da profissão, dos engenheiros/desenvolvedores de *software* e do público em geral, deveriam ser seguidos (IEEE COMPUTER SOCIETY; ASSOCIATION FOR COMPUTING MACHINERY; 1999). Estes conjuntos de princípios são agrupados nas categorias apresentadas na Figura 62.

¹²³ No anexo B, reproduz-se o atual Código de Ética IEEE/ACM para Engenharia de *Software*.

¹²⁴ Acerca da estruturação do Código de Ética IEEE/ACM para Engenharia de *Software*, vale salientar um importante ponto que contribui para a sua permanente atualidade: a sua apresentação sob a forma de enxutos princípios. Tal como a Constituição dos Estados Unidos da América, o Código de Ética IEEE/ACM para Engenharia de *Software* foca-se no básico, no elementar, não descendo a minúcias que poderiam torná-lo obsoleto com o passar do tempo e a evolução tecnológica. Sendo um diploma de princípios, o Código de Ética IEEE/ACM para Engenharia de *Software* pode ser empregado, em tese, como subsídio na solução de problemas éticos indeterminados e infinitos passíveis de ocorrência ao longo de todo o processo de desenvolvimento de *software*. A estruturação do Código sob a forma de princípios foi, indubitavelmente, uma apropriada estratégia adotada por seus elaboradores, que fez com que o Código de Ética IEEE/ACM para Engenharia de *Software*, ao contrário, por exemplo, da maior parte dos diplomas normativos brasileiros, se mantivesse atual e aplicável de forma perene independentemente de sucessivas e reiteradas revisões. O Código de Ética IEEE/ACM pode, então, ser tido como um documento atemporal de irrestrita aplicabilidade.

Figura 62 – Categorias de princípios no Código de Ética IEEE/ACM para Engenharia de *Software*.



Fonte: Autor (2019) ¹²⁵.

A análise dos conjuntos de princípios apresentados na Figura 63 leva a algumas inferências, como:

- a sociedade civil e os interesses públicos devem ser respeitados pela Engenharia de *Software*;
- a Engenharia de *Software* deve ser guiada pela Ética e pelo Direito, o que significa dizer que é tarefa dos engenheiros/desenvolvedores de *software* lidar com questionamentos envolvendo tais temas em seus trabalhos, sendo esta tarefa, também, ônus de gerentes/líderes de desenvolvimento de *software* e de todas as pessoas envolvidas na produção de *software*;
- em suas atividades laborais, similarmente ao que acontece para profissionais de

¹²⁵ Ilustração concebida a partir de leitura do Código de Ética IEEE/ACM para Engenharia de *Software* (IEEE COMPUTER SOCIETY; ASSOCIATION FOR COMPUTING MACHINERY, 1999).

outros segmentos, os engenheiros/desenvolvedores de *software* devem oferecer o seu melhor, empregando as melhores técnicas/métodos disponíveis, continuamente se atualizando e compreendendo completamente as especificações necessárias às suas atividades de trabalho;

- profissionais envolvidos no desenvolvimento de *software* são responsáveis pelo que realizam e, assim, somente devem entregar produtos que acreditem preencher altos padrões de qualidade, segurança física (*safety*) e de segurança computacional (*security*);
- a privacidade das pessoas afetadas pelo *software* deve ser assegurada, o que torna gerentes e líderes de equipes de desenvolvimento de *software* responsáveis por garantir que desenvolvedores conheçam políticas de privacidade e, também, políticas de segurança;
- com foco na melhoria da qualidade do *software* e na redução dos riscos a ele associado, gerentes e líderes de equipes/times de desenvolvimento de *software* devem comunicar diretivas a serem adotadas pelos desenvolvedores em seus trabalhos, definindo, também, recursos para a melhoria da qualidade e para a redução de ameaças em *softwares*;
- gerentes e líderes de equipes/times de desenvolvimento de *software* não devem requerer que os profissionais de desenvolvimento pratiquem qualquer ato contra a Ética;
- desenvolvedores de *software* devem agir de forma a contribuir para a boa reputação da Engenharia de *Software*;
- em suas atividades profissionais, engenheiros/desenvolvedores de *software* devem considerar valores humanos em seus julgamentos.

Por fim, importa ressaltar que o Código de Ética IEEE/ACM para Engenharia de *Software* não é o único diploma a disciplinar práticas nos domínios da Computação, havendo outros textos, como o Código de Ética da Sociedade Brasileira de Computação (SBC). Não se exploram, ao longo desta Tese, contudo estes outros textos porque:

- tais diplomas, como é o caso do Código de Ética da SBC (SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 2013), não foram especialmente

desenvolvidos com foco na Engenharia de *Software*, destinando-se, em verdade, ao regramento de uma ampla gama de atividades relacionadas à Computação de forma inespecífica;

- estes mesmos Códigos, sendo frutos de sociedades/instituições locais, i.e., não transnacionais, não têm, de imediato, independentemente do ulterior estabelecimento de acordos, aplicabilidade internacional;
- em uma era de ubiquidade do *software* e de sua produção globalizada, um diploma ético de potencial aplicação internacional é indispensável;
- o Código de Ética IEEE/ACM para Engenharia de *Software*, como indica o seu próprio nome, é especialmente voltado à Engenharia de *Software* e, tendo sido produzido por instituições reconhecidas internacionalmente no universo acadêmico e industrial, pode vir a ser adotado globalmente de maneira espontânea, não havendo, pois, a necessidade, para a sua aplicação, do estabelecimento de acordos, convenções ou tratados internacionais, o que, obviamente, demandaria tempo e poderia encontrar obstáculos nas soberanias de algum Estado;
- estando já pronto o aludido Código de Ética IEEE/ACM para Engenharia de *Software* e tendo ele potencial aplicação internacional, não há necessidade de se reinventar a roda, sendo, outrossim, evidente, pelas razões já expostas, que a eventual defesa, em Capítulos subsequentes desta Tese, de sua adoção e difusão não resulta de complexo de inferioridade (Complexo de Vira-lata, e.g.), decorrendo de racional avaliação.

7 PANORAMA ATUAL DA SEGURANÇA EM SOFTWARE

Avaliações fundadas em revisão não sistemática da literatura e em observações informais de grupos desenvolvedores de *software* sugerem que, no momento presente, a Segurança, de modo usual, é tratada *a posteriori*, i.e., somente após o desenvolvimento do *software* é que se pensa a respeito do tema. Esta conclusão é confirmada quando se reflete acerca de amostra atual de dados de análises de segurança obtida junto à *Tempest Security Intelligence*, empresa de Segurança Computacional atuante em países variados.

Antes de se passar ao exame da citada amostra de dados, importa registrar algumas observações sobre a sua utilidade e a sua validade aos fins almejados com a investigação conduzida, já que, obviamente, o emprego de dados obtidos por terceiros (*Tempest Security Intelligence*, no caso), usualmente, pode suscitar questionamentos diversos, dada a impossibilidade de o pesquisador, por si mesmo, assegurar a veracidade, confiabilidade, a fidedignidade e a exatidão de insumo que não foi produzido por ele próprio.

A despeito, no contexto do uso de dados de terceiro, da inevitável sujeição dos resultados da pesquisa à coleta não realizada pelo próprio investigador, mostrou-se apropriado, no presente caso, o emprego dos dados coletados pela *Tempest Security Intelligence*, já que:

- tencionava-se traçar um panorama relativo à (in)segurança no *software* ao longo dos últimos tempos;
- para se traçar o aludido panorama mediante coleta direta de dados, seria necessário despender recursos com a realização de *pentests* por intervalo de tempo considerável, mesmo quando já existentes os dados necessários em poder de empresa de Segurança Computacional, ou seja, empregar-se-iam recursos expressivos de forma ineficiente, em verdadeiro desperdício;
- mesmo que o pesquisador se dedicasse pessoal e exclusivamente à tarefa de

realização de *pentests*, o resultado de suas averiguações, provavelmente, não se mostraria tão valioso quanto o produzido pela mencionada empresa de Segurança Computacional, já que o pesquisador, não atuando diretamente no domínio em debate, não deteria o *know-how* e a *expertise* indispensáveis ao cumprimento de tal missão com perfeição, i.e., não se poderia afastar a possibilidade de o pesquisador, apesar de seus esforços, não identificar uma vulnerabilidade existente;

- ainda que o pesquisador tivesse a habilidade e a experiência requeridas à realização de *pentests*, o produto de seu labor neste domínio, refletindo os esforços de um único indivíduo, não seria tão significativo quanto os dados em poder da *Tempest Security Intelligence*, já que os dados desta foram obtidos com a atuação de vários especialistas em Segurança Computacional (uma verdadeira equipe, cuja primordial função de trabalho é a identificação de vulnerabilidades de Segurança em *software*) e não por apenas um único indivíduo;
- em princípio, a amostra de dados cedida pela *Tempest Security Intelligence* se mostrou digna de confiança, já que a referida empresa goza de boa reputação no mercado e que, em suas atividades, quando contratada a realizar *pentests*, ela, auferindo, também, rendas em função do número de vulnerabilidades identificadas e concretamente indicadas aos seus clientes, tem, obviamente, todo o interesse em identificar o maior número possível de vulnerabilidades;
- a amostra em debate ainda se apresentou como útil à investigação em razão de nela se inserirem dados de *softwares* produzidos globalmente, dado que a empresa de Segurança Computacional referida já atuava em âmbito internacional e que, nas análises de segurança por ela realizadas, o foco não era restrito a *software* produzido em um único local, buscando-se, mediante *pentests*, identificar vulnerabilidades independentemente da origem de produção, do nicho/segmento de uso do *software* e da camada de um sistema em que utilizado o *software*.

Feitos estes breves comentários acerca da utilidade da amostra de dados considerada na produção do panorama atual da segurança no *software*, passa-se, na Seção seguinte, à efetiva apreciação dos dados desta amostra, colocando-se, inicialmente, no que pertine à Segurança Computacional, em xeque o próprio uso da terminologia Engenharia de *Software*, em razão do grande número de

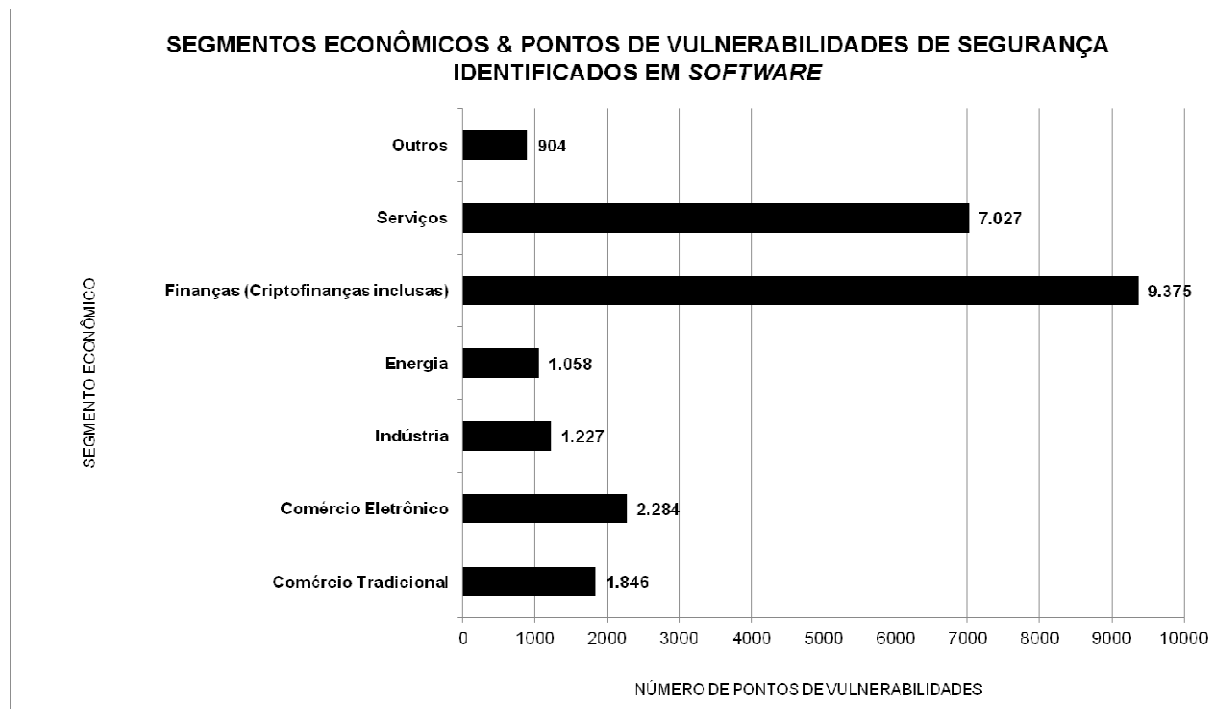
vulnerabilidades identificada via *pentests* e da peculiar natureza da Engenharia de *Software*.

7.1 ENGENHARIA OU NÃO ENGENHARIA? EIS **AINDA** A QUESTÃO

A amostra de dados em discussão foi obtida a partir de análises de segurança realizadas pela *Tempest Security Intelligence* ao longo de 66 (sessenta e seis) meses, no período compreendido entre Janeiro/2013 e Junho/2018. Essencialmente, foram consideradas 1.046 (mil e quarenta e seis) análises efetivadas com o uso de *pentests* sob a forma *Black Box* e *Gray Box*, ou seja, sem a realização geral de revisão de código¹²⁶.

Nas análises em debate (diretrizes no apêndice I), 11.182 (onze mil cento e oitenta e duas) diferentes vulnerabilidades de segurança foram identificadas. Algumas destas vulnerabilidades foram observadas mais de uma vez, resultando em um total de 23.721 (vinte e três mil e setecentos e vinte e um) pontos de vulnerabilidades de segurança (replicação média de vulnerabilidade correspondendo a 2 - dois). Estes pontos de vulnerabilidade foram encontrados de forma heterogênea nas três camadas de sistemas de informação (infraestrutura, comunicações e aplicação) de diversos segmentos econômicos, como ilustrado no Gráfico 1.

¹²⁶ Para uma melhor compreensão da diferenciação existente entre os *pentests* sob a forma *Black Box*, *White Box* e *Grey Box*, recomenda-se leitura de Hafele (2004).

Gráfico 1 – Segmentos econômicos & Pontos de vulnerabilidades de segurança em *software*.

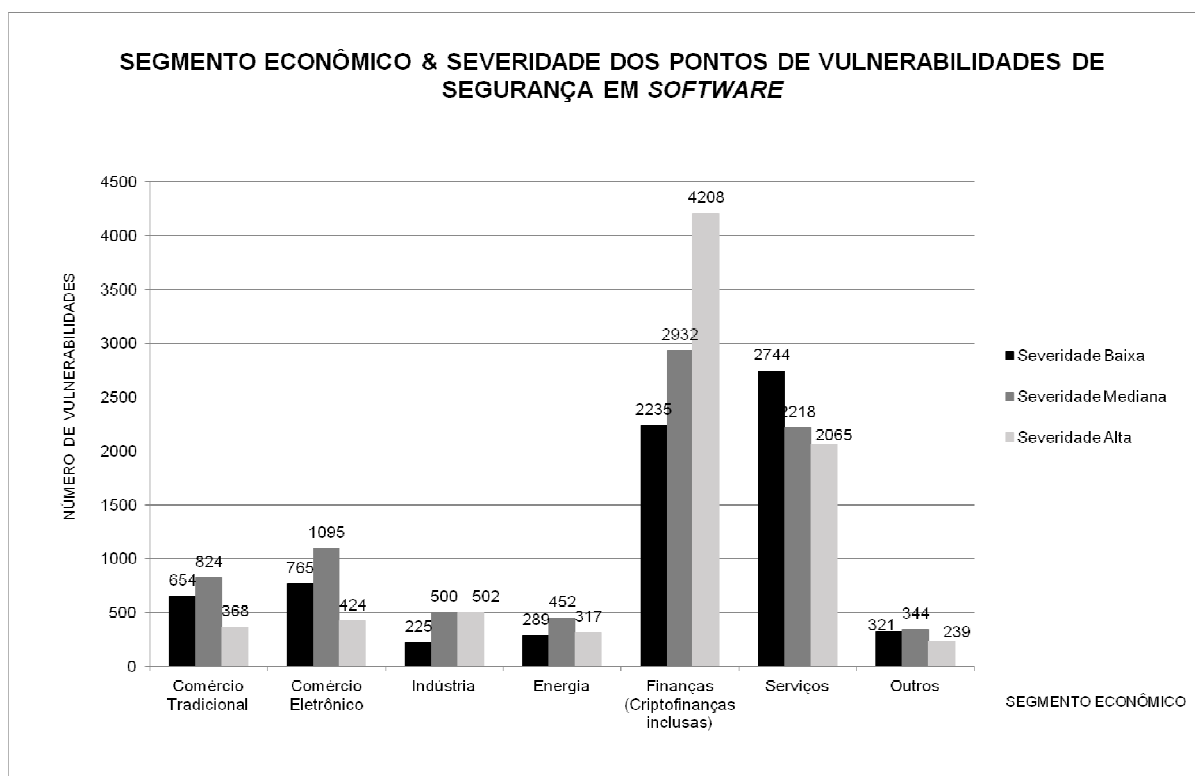
Fonte: Autor (2019) ¹²⁷ ¹²⁸.

Considerada a severidade dos pontos de vulnerabilidades¹²⁹, também não houve homogeneidade nos números absolutos de vulnerabilidades dos distintos segmentos, como se depreende do Gráfico 2.

¹²⁷ Gráfico elaborado para a presente tese a partir de amostra de dados obtida junto à *Tempest Security Intelligence*.

¹²⁸ A título meramente explicativo, esclarece-se que, quando se faz alusão ao termo “Cripto finanças”, está se falando em Finanças baseadas em criptomoedas, ou seja, em moedas não convencionais, mais precisamente em ativos virtuais/digitais fundados nas ideias associadas ao *bitcoin*, à criptografia e ao *blockchain*. Não se inserindo no escopo do presente trabalho os temas mencionados, remetem-se eventuais interessados sobre os mesmos às obras de Ulrich (2014) e Mougayar (2017), bem como de Tapscott e Tapscott (2017).

¹²⁹ Usualmente, o grau de severidade de uma vulnerabilidade é associado ao impacto do dano que a sua exploração pode ocasionar, ou seja, diz-se, em linhas gerais, por exemplo, que uma vulnerabilidade é de alta severidade quando a sua exploração por um *hacker* pode resultar em grandes/devastadores efeitos organizacionais adversos. Há diversos sistemas de cálculo do grau de severidade de uma vulnerabilidade, sobressaindo-se o *OWASP Risk Rating Methodology* (OWASP, 2019) e o *Common Vulnerability Scoring System* (CVSS), um sistema industrial aberto e gratuito de pontuação a este fim destinado baseado em métricas distintas (FIRST, 2019) (POKORNY, 2019) (HACKERONE, 2019). Na amostra cuja análise foi feita na investigação ora relatada, não se utilizaram a metodologia OWASP nem o CVSS na avaliação do grau de severidade, mas, sim, sistema próprio de avaliação de vulnerabilidade adotado pela empresa de Segurança Computacional.

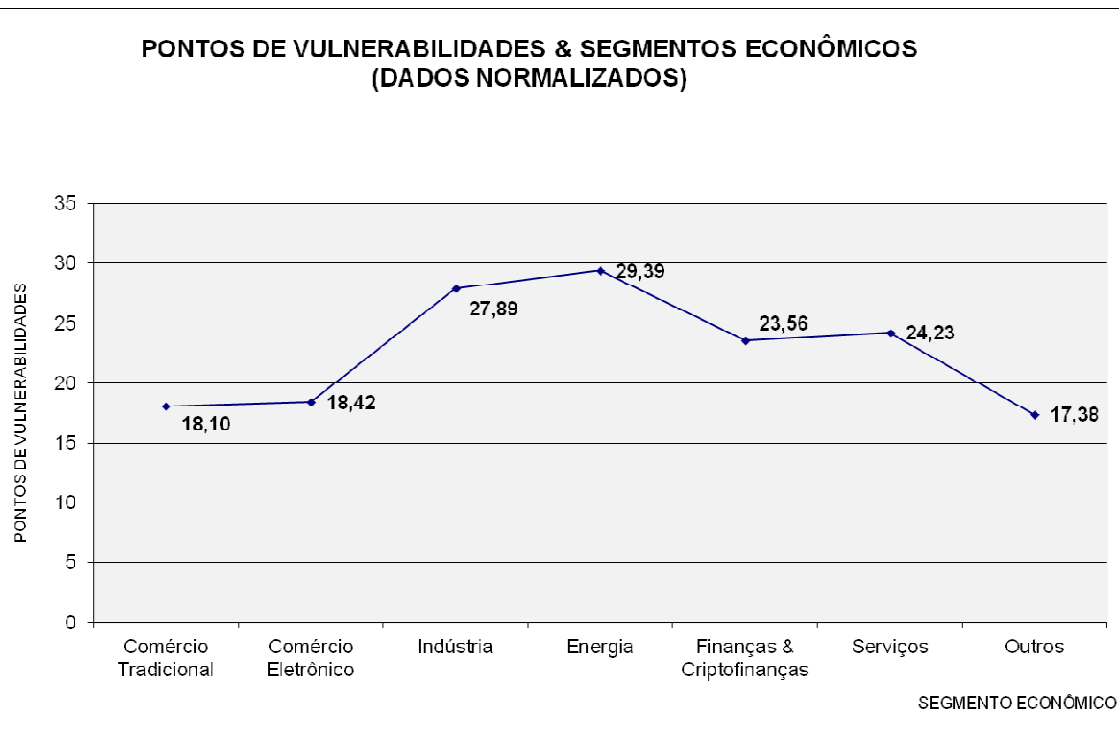
Gráfico 2 – Segmentos & Severidade dos pontos de vulnerabilidades de segurança em *software*.

Fonte: Autor (2019) ¹³⁰.

Como exposto nos Gráficos 1 e 2, Serviços e Finanças foram os segmentos com maiores números absolutos de vulnerabilidades de segurança em *software*, apresentando, também, o maior quantitativo de vulnerabilidades altamente severas. Estas observações, contudo, podem conduzir a percepções falsas. A leitura de números isolados pode levar à equivocada percepção de que vulnerabilidades são mais frequentemente identificadas em *software* utilizado nestes dois segmentos. Dados normalizados, revelaram, entretanto, relativa homogeneidade nos montantes globais de pontos de vulnerabilidades, como representado no Gráfico 3.

¹³⁰ Representação construída para este estudo com o emprego da amostra de dados cedida pela *Tempest Security Intelligence*.

Gráfico 3 – Pontos de vulnerabilidades & Segmentos econômicos (Dados normalizados).



Fonte: Autor (2019) ¹³¹.

A diferença entre os montantes globais de vulnerabilidades identificadas nos diversos segmentos econômicos reside, então, na frequência com que *pentests* foram feitos em cada segmento. Quanto mais *pentests* foram feitos, mais vulnerabilidades foram identificadas e exploradas, independentemente do segmento econômico de atuação da empresa em que o *software* analisado era utilizado.

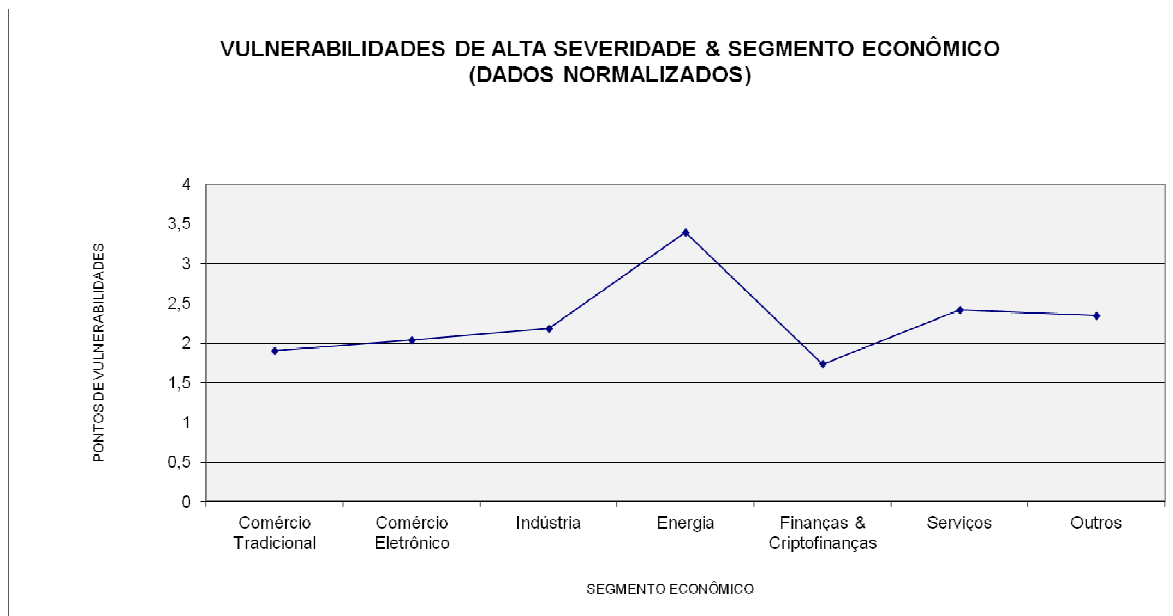
Desse modo, o grande número de pontos de vulnerabilidades nas Finanças (Criptofinanças inclusas) pode ser explicado por uma maior preocupação com Segurança neste segmento. Quanto maior a preocupação, maior a quantidade de análises de segurança e maior, por conseguinte, o número de vulnerabilidades identificadas.

Quando considerado o grau de severidade, mais uma vez, os dados normalizados revelam uma conclusão diferente acerca dos segmentos econômicos e das vulnerabilidades em seus *softwares*. O maior número de vulnerabilidades altamente severas foi encontrado no segmento energético e o menor número no

¹³¹ Normalização produzida mediante a conjunta consideração dos números dos pontos de vulnerabilidades e da quantidade de análises realizadas em cada segmento.

segmento das Finanças, como ilustrado através do Gráfico 4.

Gráfico 4 – Vulnerabilidades de alta severidade & Segmento econômico (Dados normalizados).



Fonte: Autor (2019) ¹³².

Globalmente considerados, os dados indicam, então, que o segmento econômico não é fator determinante nos montantes de pontos de vulnerabilidades. Os mesmos dados indicam que as maiores quantidades de vulnerabilidades altamente severas não estão nos segmentos das Finanças e dos Serviços. Dentre todos os setores examinados, o setor energético é o mais afetado por vulnerabilidades com alta severidade porque a exploração de suas vulnerabilidades apresenta maior potencial de afetação de ativos com repercussão em série, ou seja, de produção de impactos em ativos não apenas da própria organização do setor energético como também de vasto número de organizações/entidades, dada a inevitável dependência social de energia para a produção de bens e o fornecimento de serviços de um modo geral.

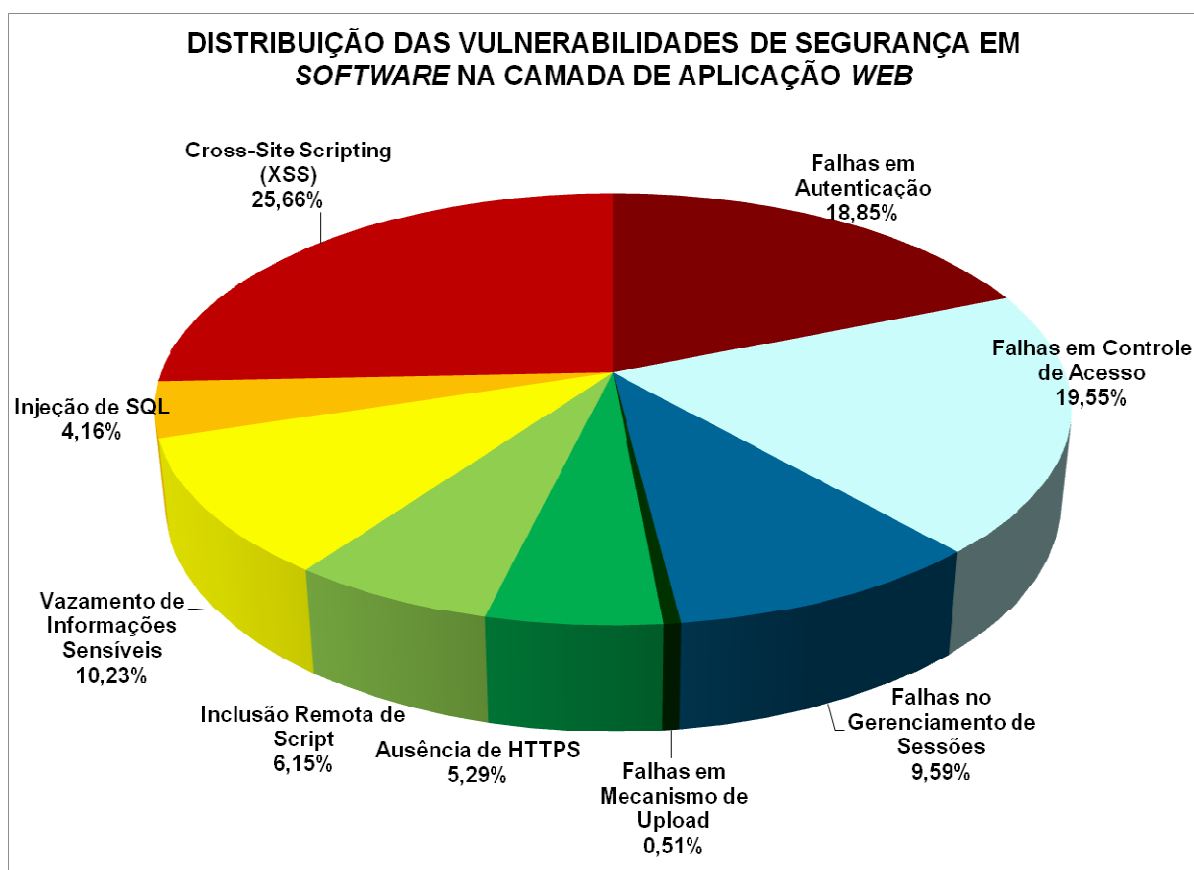
Observando-se, mais detidamente, os dados relativos à camada de aplicação *web*, identificaram-se 7.431 (sete mil e quatrocentas e trinta e uma) pontos de vulnerabilidade, como exposto na Tabela 1 e nos Gráficos 5 e 6.

¹³² Normalização realizada com a observância do quantitativo de análises de segurança realizadas para cada segmento.

Tabela 1 – Pontos de vulnerabilidade na camada de aplicação *web*.

PONTOS DE VULNERABILIDADE DE SEGURANÇA NA CAMADA DE APLICAÇÃO WEB	
CATEGORIA DE VULNERABILIDADES	QUANTIDADE
Falhas em Autenticação	1.401
Falhas em Controle de Acesso	1.453
Falhas no Gerenciamento de Sessões	713
Falhas nos Mecanismos de <i>Upload</i>	38
Ausência de <i>HTTPS</i>	393
Inclusão Remota de <i>Scripts</i>	457
Vazamento de Informações Sensíveis	760
Injeção de <i>SQL</i>	309
<i>Cross-Site Scripting (XSS)</i>	1.907
TOTAL	7.431

Fonte: Autor (2019) ¹³³.

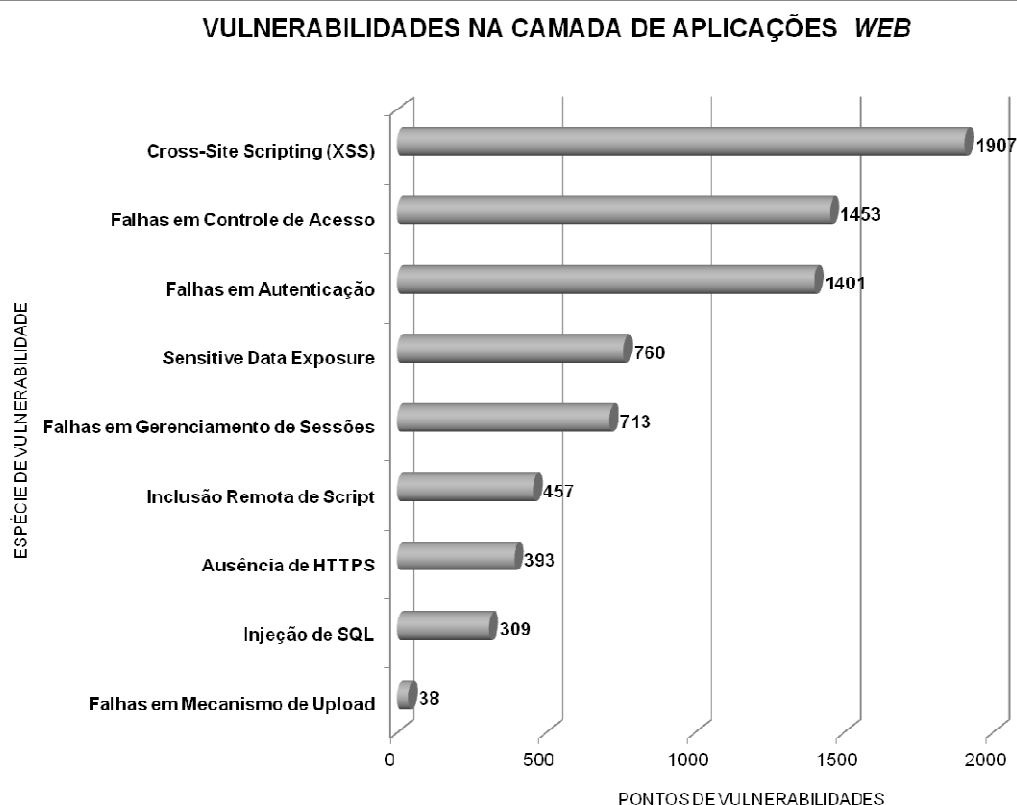
Gráfico 5 – Distribuição dos pontos de vulnerabilidade de segurança na camada de aplicação *web*.

Fonte: Autor (2019) ¹³⁴.

¹³³ Tabela produzida a partir da análise de amostra de dados obtida junto à *Tempest Security Intelligence*.

¹³⁴ Gráfico construído com base nas informações apresentadas na Tabela 1.

Gráfico 6 – Pontos de vulnerabilidade na camada de aplicações web.



Fonte: Autor (2019) ¹³⁵.

Do exame da Tabela 1, bem como dos Gráficos 5 e 6, infere-se que, na camada de aplicação, diferentes tipos de vulnerabilidades foram encontrados no período de realização dos *pentests*. As três espécies mais frequentes de vulnerabilidades identificadas foram *Cross-Site Scripting (XSS)*, Falhas em Autenticação e Falhas em Controle de Acesso¹³⁶.

Além de possibilitar aos interessados a adoção de planos para gerenciamento dos riscos resultantes, a identificação das citadas vulnerabilidades permite inferir que, atualmente, a despeito dos esforços empreendidos na Engenharia de *Software*, vulnerabilidades de segurança em *software* são frequentemente encontradas nas três camadas dos sistemas de informação.

A partir da análise dos dados coletados através dos *pentests*, constata-se, em síntese, ademais, que:

¹³⁵ Gráfico produzido com o emprego dos dados expostos na Tabela 1.

¹³⁶ Para informações adicionais acerca das vulnerabilidades mencionadas, tema fora do escopo do presente trabalho, recomenda-se consulta a Samuel (2007).

- uma mesma espécie de vulnerabilidade pode aparecer mais de uma vez em um dado sistema, de modo que é pertinente se falar em pontos de vulnerabilidades;
- a quantidade de pontos de vulnerabilidades identificados e explorados através dos *pentests* é significativa;
- embora os números absolutos sugiram discrepâncias na distribuição dos pontos de vulnerabilidade nos sistemas de diferentes segmentos econômicos, dados normalizados revelam o oposto. Não há grande diferença nas quantidades normalizadas de pontos de vulnerabilidades de segurança de sistemas de diferentes segmentos, ainda que dois segmentos se sobressaíam neste aspecto: Energia e Indústria;
- não se identificam maiores números de vulnerabilidades nos setores de Finanças. Os altos números isolados de vulnerabilidades identificadas nestes setores decorrem da maior realização de avaliações de segurança em seus sistemas, dada uma natural maior preocupação com este tema em tais segmentos. Maior a preocupação, maior a frequência de realização de *pentests*. Maior a quantidade de *pentests* feitos, maior a quantidade de vulnerabilidades de segurança identificadas;
- considerando-se apenas a camada de aplicação (camada de aplicação *web*), identificaram-se 7.431 (sete mil quatrocentos e trinta e um) pontos de vulnerabilidades. *Cross-Site Scripting* (XSS), Falhas em Autenticação e Falhas em Controle de Acesso foram as três espécies de vulnerabilidades mais identificadas, o que é compatível com o quadro *Open Web Application Security Project* (OWASP)¹³⁷ dos 10 mais frequentes riscos de segurança (OWASP, 2017), como se depreende do Quadro 43.

¹³⁷ O *Open Web Application Project* (OWASP) constitui-se em projeto aberto destinado à promoção da Segurança Computacional na camada de aplicações *web*, tendo por missão básica habilitar organizações a desenvolver, adquirir e manter aplicações e *Application Programming Interfaces* (APIs) confiáveis. Informações adicionais sobre o OWASP podem ser encontradas no link www.owasp.org.

Quadro 43 – Vulnerabilidades de Segurança mais frequentes na camada de aplicações de acordo com o OWASP.

VULNERABILIDADES DE SEGURANÇA MAIS FREQUENTES NA CAMADA DE APLICAÇÕES SEGUNDO O OWASP		
POSIÇÃO NO RANKING	ESPÉCIE DE VULNERABILIDADE	IDEIAS NUCLEARES
1 ^a	FALHAS DE INJEÇÃO	Falhas de injeção (Injeção SQL, entre outras) ocorrem quando dado não confiável é enviado até um interpretador como parte de um comando ou consulta, podendo ludibriar o interpretador e promover a execução de comandos indesejados ou o acesso não autorizado a dados
2 ^a	Quebra de Autenticação	Funções de aplicações relacionadas à autenticação e ao gerenciamento de sessão são frequentemente implementadas de forma incorreta, permitindo o comprometimento de senhas, chaves ou <i>tokens</i> de sessão, bem como a exploração de outras falhas de implementação, possibilitando a temporária ou permanente assunção da identidade de um usuário legítimo por um atacante
3 ^a	Exposição de Dados Sensíveis	Diversas aplicações <i>web</i> não protegem apropriadamente dados sensíveis (dados financeiros, dados de saúde e informações pessoalmente identificáveis, e.g.), o que permite aos atacantes roubar/modificar registros, cometendo crimes de naturezas variadas (fraude com cartão de crédito e roubo de identidade, por exemplo), os quais poderiam ser evitados/minimizados, se adotadas medidas adicionais (criptação de dados em repouso e em trânsito, i.e., encriptação de dados situados sob a proteção de um <i>firewall</i> /antivírus e dados utilizados em uma base diária sem a aludida proteção através de <i>browsers</i>)

VULNERABILIDADES DE SEGURANÇA MAIS FREQUENTES NA CAMADA DE APLICAÇÕES SEGUNDO O OWASP		
POSIÇÃO NO RANKING	ESPÉCIE DE VULNERABILIDADE	IDEIAS NUCLEARES
4 ^a	Entidades Externas em <i>Extensible Markup Language (XML)</i>	Processadores <i>XML</i> antigos e mal configurados avaliam referências a entidades externas através de arquivos <i>XML</i> , os quais podem ser utilizados para revelar arquivos internos mediante o emprego de manipuladores de localizadores de recursos, bem como para compartilhar arquivos internos, realizar varreduras de portas internas, executar remotamente código e negar o regular serviço
5 ^a	Quebra de Controle de Acesso	Frequentemente, não são definidas restrições apropriadas ao que os usuários autenticados podem fazer nos sistemas, o que acaba por possibilitar aos atacantes explorar falhas de acesso não autorizado, tais como: acesso de dados de outros usuários, visualização de dados sensíveis, modificação de dados dos usuários, modificação de direitos de acesso, etc.
6 ^a	Má Configuração de Segurança	Resultando do indevido uso de configurações padronizadas e incompletas ou <i>ad hoc</i> , bem como de abertura do armazenamento em nuvem, da má configuração de cabeçalhos <i>Hypertext Transfer Protocol (HTTP)</i> e da exibição de mensagens de erro com conteúdo sensível, a má configuração permite, no geral, a exploração de brechas de Segurança
7 ^a	XSS	Falhas XSS ocorrem quando a aplicação inclui dados não confiáveis em uma página <i>web</i> sem a validação própria, ou quando, por problemas de validação/atualização, uma página <i>web</i> pode remeter dados fornecidos pelo usuário para a aplicação criar um código <i>Hypertext Markup Language (HTML)</i> ou <i>JavaScript</i> , os quais, se executados por potenciais atacantes, poderiam

VULNERABILIDADES DE SEGURANÇA MAIS FREQUENTES NA CAMADA DE APLICAÇÕES SEGUNDO O OWASP		
POSIÇÃO NO RANKING	ESPÉCIE DE VULNERABILIDADE	IDEIAS NUCLEARES
		sequestrar sessões do usuário, redirecionar o usuário para <i>sites</i> maliciosos ou apresentar como verdadeiro falso <i>site</i> sob o controle de <i>hackers</i>
8ª	Desserialização Insegura	Falhas de desserialização ocorrem quando dados em transmissão sob a forma de caracteres codificados estão sujeitos à manipulação indevida, o que pode, no seu destino, levar a vulnerabilidades permissivas de injeção, escalação de privilégios e repetição/retardo na transmissão de mensagem inidônea
9ª	Uso de Componentes com Vulnerabilidades Conhecidas	Componentes executáveis com os mesmos privilégios da aplicação (bibliotecas de código e outros módulos de <i>software</i>) com vulnerabilidades conhecidas associadas e não corrigidas podem possibilitar ataques com perda de dados relevantes ou, até mesmo, com a perda do controle do próprio servidor em benefício dos atacantes
10ª	Insuficiente <i>Login</i> e Monitoramento	Falhas no controle de <i>logins</i> podem não ser tratadas rapidamente, em virtude de falhas no monitoramento e de inaptidão à pronta resposta/solução, possibilitando a exploração de vulnerabilidades por <i>login</i> indevido

Fonte: Autor (2019) ¹³⁸.

A análise dos dados coletados via *pentest* torna possível, por fim, uma reflexão maior, cujos limites transpassam os da Segurança Computacional. Sua maior contribuição está na reflexão e nas críticas que dela podem se originar.

Se quanto mais *pentests* são feitos, mais vulnerabilidades de segurança são encontradas e se os montantes de pontos de vulnerabilidades, de acordo com os dados examinados, são independentes de nicho, a incidência de

¹³⁸ Quadro elaborado a partir das considerações expostas em OWASP (2017).

vulnerabilidades se mostra como uma constante.

Se a incidência de vulnerabilidades se apresenta como uma constante, pode-se cogitar que as quantidades de pontos de vulnerabilidades de segurança e a consequente insegurança dos *softwares* estejam relacionadas à Engenharia envolvida na construção dos sistemas de informação.

Engenharia ou não Engenharia? Eis **ainda** a questão. Vinte e oito anos após a publicação do notório artigo de Mary Shaw (SHAW, 1990), esta **ainda** é a questão!

Em 1990, a mencionada autora discorreu sobre o usual emprego, desde 1968, da terminologia “Engenharia de *Software*” e sobre as deficiências associadas a esta terminologia, que poderiam resultar em questionamentos acerca da própria natureza da Engenharia de *Software*.

Em essência, a citada autora expressava, em uma perspectiva otimista, sua convicção pessoal de que, concentrando-se esforços em pesquisa e educação, não seria inapropriado se referenciar um novo ramo de Engenharia: a Engenharia de *Software*.

Vinte e oito anos após a defesa de Shaw relativa à Engenharia de *Software* e cinquenta anos após a primeira vez em que o termo foi empregado, embora tenham sido empreendidos inegáveis grandes esforços pela Academia e pela Indústria de Tecnologia de Informação, ainda parece questionável o uso da terminologia em debate, especialmente quando considerada, atualmente, a Segurança no *software*.

Seriam aceitáveis em outros ramos da Engenharia falhas nos montantes identificados no presente estudo com o auxílio de *pentests*? **Em 66 (sessenta e seis) meses de *pentesting*, 23.721 (vinte e três mil e setecentos e vinte e um) pontos de vulnerabilidades de segurança foram identificados por uma única empresa de Segurança Computacional mediante o emprego de uma única estratégia de identificação de vulnerabilidades.** Este número não é insignificante e sua expressividade sugere que o que está sendo chamado de Engenharia pode, no momento, de fato, constituir um ofício artesanal, quando considerado o atributo da Segurança.

Desde 1968, métodos de desenvolvimento têm sido criados, novas linguagens foram concebidas e novos paradigmas emergiram. Respeitados entendimentos em sentido diverso (MEIRA; BURÉGIO; BORBA; GARCIA;

ALBUQUERQUE; SOARES, 2016), estas iniciativas, todavia, como empiricamente demonstra a amostra de dados de *pentesting* utilizada nesta investigação, não tornaram a Engenharia de *Software* uma realidade de fato. Parafraseando noção muito utilizada na seara jurídica quando se discute acerca da existência de direito adquirido, tem-se, no máximo, em verdade, como se infere obliquamente da análise da utópica percepção de Shaw (1990), bem como das otimistas impressões de Meira, Burégio, Borba, Garcia, Albuquerque e Soares (2016), uma mera **expectativa** de que, em um inespecífico e incerto futuro, exista, efetivamente, uma Engenharia de *Software* porque são diversos os dilemas enfrentados no desenvolvimento de *software* (IIVARI, 1996) e porque permanece atual a afirmação de Brooks no sentido de que “não há bala de prata” (BROOKS, 1987).

Na busca por uma Engenharia de *Software* real, em que a Segurança não desempenhe papel similar ao de mero figurante em uma produção cinematográfica/teatral, muito precisa ainda ser feito e, como esforços isolados não resultaram em uma nova Engenharia viável e madura (ao menos no que pertine à Segurança no *software*), talvez, a chave para uma mudança verdadeira envolva integração, envolva, **ao longo de todo o processo de desenvolvimento**, a reunião de esforços, envolva pensar globalmente e não com o foco estanque, compartimentado e restrito em disciplinas de Ciência de Computação, já que, de fato, a Ciência, afinal, é uma só.

Em nova analogia, é preciso, assim, que cada um dos agentes impactantes no desenvolvimento de *software* (acadêmicos, dirigentes da Indústria de *Software* e desenvolvedores) deixe, tal qual o pescador que, originariamente, se encanta mais com a sua própria rede que com o mar, de olhar única e exclusivamente para os seus próprios instrumentos de trabalho, passando a observar que a realidade, o todo, é muito maior que o que cada um dos agentes produz e que o mar, o Universo verdadeiro, é integrado, também, pelas ações de terceiros (*hackers*, por exemplo), as quais podem apresentar repercussões diretas e indiretas no que é produzido com fins legais e lícitos.

Sem o pensar global, sem o pensar holístico, a produção de *software* que se tem por ora, quando considerada a Segurança e os números de pontos de vulnerabilidades apontados nesta investigação, não pode, por todo o exposto, ser tida como o resultado de um processo de Engenharia.

Considerada a importância da Segurança e os citados números obtidos

via *pentesting*, não é, também, leviano se dizer que se está, hoje, ainda, na “Era do *Software* de Padaria”, em que o *software*, feitas as devidas ressalvas de diligentes agentes produtores isolados, é elaborado, geralmente, como se não se estivesse em um momento de ubiquidade interconectada, como se, ainda, se estivesse na década de 80 do século passado, quando, no máximo, havia, para o público comum, aplicações isoladas sendo executadas em pequenos computadores pessoais para usos muito restritos e simplórios sem grande repercussão social (*softwares* voltados ao controle de estoque e folha de pagamento de pequenos empreendimentos comerciais, por exemplo).

O ponto é que este nostálgico momento de aplicações isoladas não mais representa a realidade e, nesta nova realidade que se tem atualmente de interconexão e ubiquidade, é preciso mais e é preciso mais de forma imediata e urgente.

Desde que o primeiro computador foi criado e desde que foi desenvolvido o primeiro *software*, houve, sim, significativos e relevantes avanços. A descoberta de materiais semicondutores, o desenvolvimento de circuitos integrados e a miniaturização de componentes (BOYLESTAD; NASHELSKY, 1986) levaram, em um curto intervalo de tempo, a uma expressiva popularização no uso de computadores digitais e, conseqüentemente, a uma difusão na necessidade e no uso de *softwares* de uma maneira geral.

Considerada a história da Humanidade, em um brevíssimo interregno de tempo, passou-se a ter à disposição do público comum um valioso instrumento, o *software*, e não se nega a importância do *software* e das atividades voltadas à sua produção.

Não se nega, também, a evidente evolução nos processos de desenvolvimento de *software* (evolução de linguagens de programação, na construção de ambientes de desenvolvimento, na criação de metodologias de desenvolvimento e na elaboração de paradigmas/*frameworks* de trabalho) e na própria qualidade do *software* como produto final.

Ocorre, porém, que, dada a exponencialmente crescente e irreversível importância do *software* para a sociedade atual, não houve, apesar dos muitos esforços empreendidos pela Academia, pela Indústria e pelos próprios desenvolvedores, a evolução necessária quando se pensa a respeito da Segurança e é imperioso que isso mude, sob pena de se consolidar algo socialmente nefasto e

de o conceito associado às Engenharias como um todo, e não apenas à Engenharia de *Software*, vir a ser descaracterizado/deturpado¹³⁹.

7.2 ALGO DE PODRE NO REINO DA INDÚSTRIA DE *SOFTWARE*

O volume de vulnerabilidades e pontos de vulnerabilidades exposto na Seção precedente indica uma relativa imaturidade da Engenharia de *Software* e sugere, ainda, que a produção de *software* seguro não é uma prioridade geral para a indústria de desenvolvimento de sistemas.

Vulnerabilidades foram identificadas em sistemas de distintos segmentos econômicos, o que indica que o problema do tratamento da segurança não é exclusivo de um nicho. Mesmo que os números absolutos de vulnerabilidades identificadas difiram entre segmentos, não há variação significativa nos dados normalizados. Em outras palavras, a insegurança está, literalmente, em todo lugar.

Os dados obtidos também revelaram uma repetição de vulnerabilidades, i.e., vulnerabilidades identificadas apareceram mais de uma vez em um mesmo sistema de informação, originando os já referidos *pontos de vulnerabilidades*. Esta reiterada repetição de vulnerabilidades, por seu turno, leva a crer que as potenciais falhas de segurança em discussão não resultaram de meros equívocos, sendo, em verdade, produto de erros decorrentes do desconhecimento de temas relativos à Segurança e/ou, resultado direto da desconsideração de tais temas quando do desenvolvimento de sistemas.

Na percepção dos dois especialistas em Segurança Computacional

¹³⁹ Acerca da comparação entre a Engenharia de *Software* e as demais Engenharias, algumas observações adicionais se mostram necessárias no tocante à abstração. Não afeta a comparação e os questionamentos suscitados nesta investigação o fato de haver, na Engenharia de *Software*, certo grau de abstração quanto ao seu produto final (*software*), porque, nas demais Engenharias e em diversos outros segmentos produtivos, também há abstração, independentemente de objeto final construído parecer meramente concreto. A simples concepção de um novo modelo de automóvel por exemplo, é algo extremamente abstrato. Se a concepção de um novo modelo de automóvel não fosse abstrata, não haveria significativas diferenças, por exemplo, entre um Bugatti, uma Ferrari e um Novo Uno. Se não houvesse abstração, não haveria espaço para a criatividade nem para a inovação, produzindo todas as grandes montadoras automóveis integralmente idênticos. O mesmo pode ser dito, ilustrativamente, no tocante às Engenharias Mecânica, Química, Civil, etc. Assim sendo, pelo exemplo dado, depreende-se que todas as demais Engenharias têm, sim, graus de abstração associados e todas elas possuem meios próprios para lidar com estas abstrações e suas consequências. Suposta abstração do *software* não justifica a identificação de vultoso número de vulnerabilidades de Segurança. Suposta abstração do *software* não torna a Engenharia de *Software* uma Engenharia peculiar imune a questionamentos quanto à qualidade do seu produto. Suposta abstração do *software* não constitui salvo-conduto para que os integrantes da Engenharia de *Software* ajam como bem entendam sem arcar com as repercussões de suas condutas.

entrevistados ao longo desta investigação¹⁴⁰, este cenário possui uma potencial explicação. Na visão destes especialistas:

- durante o desenvolvimento de *software*, há, provavelmente, uma priorização em favor dos requisitos funcionais;
- a priorização referida é, em alguns casos, consequência da metodologia de desenvolvimento¹⁴¹;
- os requisitos de segurança, como outros requisitos não funcionais, são negligenciados, já que, muitas vezes, não são visíveis ao usuário final e ao público em geral;
- o “desenvolvedor médio” não tem um conhecimento mínimo acerca da Segurança Computacional, cometendo, em suas atividades laborais, ingênuas escolhas ruins que facilitam as ações dos *hackers*.

A situação vislumbrada pelos citados especialistas é confirmada com a análise de pequeno *survey* conduzido entre estudantes de graduação e de pós-graduação, vinculados ao Centro de Informática da UFPE (CIn/UFPE)^{142 143 144 145},

¹⁴⁰ Tendo os especialistas referidos sido entrevistados com garantia de anonimato, registra-se, para sua maior qualificação no relato da pesquisa, que se trata de profissionais com mais de vinte anos de experiência na área, formados localmente, mas com atuação internacional.

¹⁴¹ Não se pode, por óbvio, a partir dos dados coletados na investigação, rechaçar, ainda que ausente menção pelos especialistas em Segurança Computacional entrevistados, a possibilidade de haver outros elementos que contribuam para a mencionada priorização dos requisitos funcionais, como a urgência e a cobrança pelo pronto fornecimento do *software*. Ainda que tais pontos não tenham sido suscitados pelos aludidos especialistas, há de se observar que a sua invocação, por si só, não justifica eventual priorização dos requisitos funcionais em detrimento da Segurança porque, se vulnerabilidades de Segurança forem exploradas, o próprio comportamento “normal” de um sistema pode vir a ser integralmente subvertido pela ação de *hackers*, não persistindo, pois, qualquer funcionalidade dita “normal” ou “regular”.

Mesmo que a insegurança, por si mesma, não constituísse uma ameaça às próprias funcionalidades, a urgência e a cobrança pela entrega não justificariam, de forma similar ao que ocorre em outros domínios produtivos humanos, a desconsideração de essencial requisito (Segurança) porque, quando se exerce alguma atividade produtiva, há responsabilidade associada que não é afastada por “pressões”.

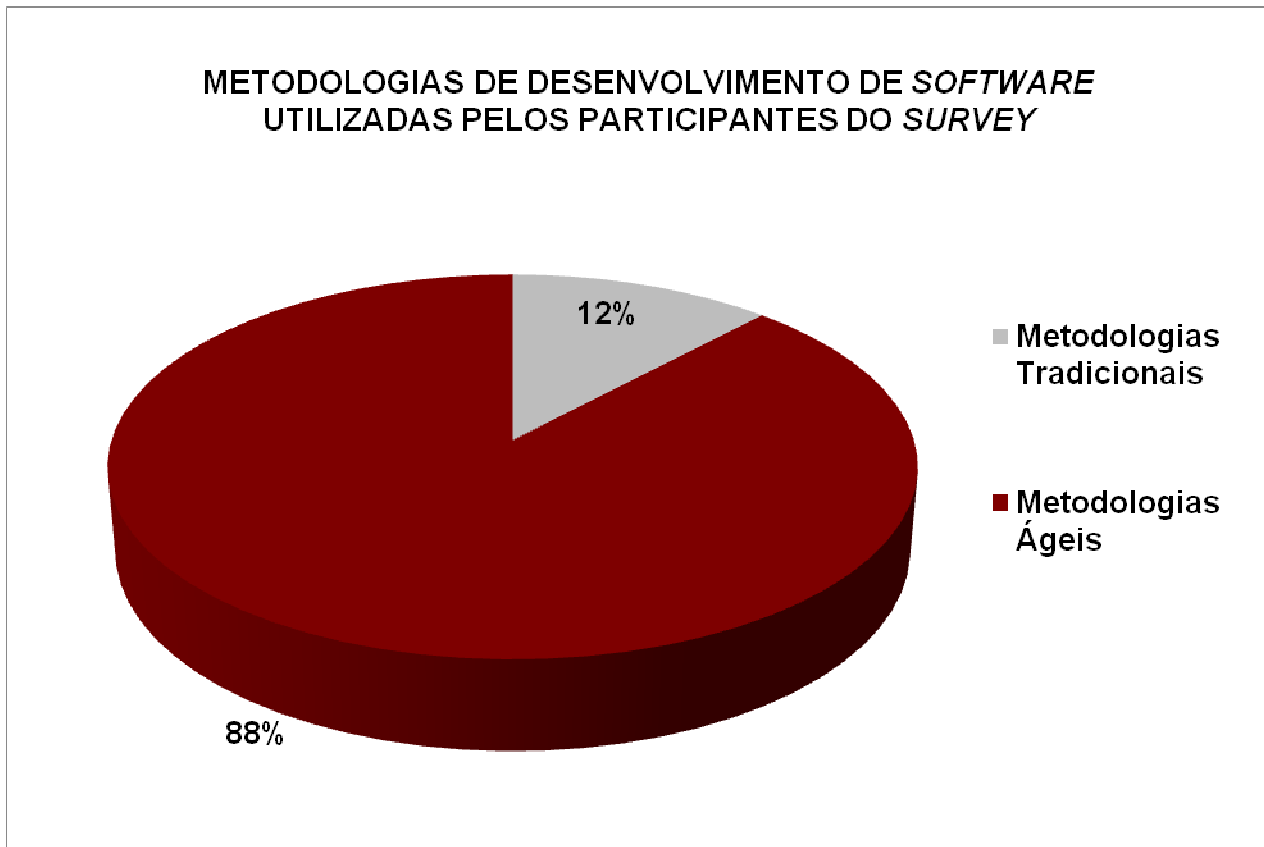
Todo aquele, entidade ou indivíduo, que se dispõe a produzir algo, tem que prezar por um mínimo de qualidade no que faz e não há, de fato, qualidade, quando não se tem um mínimo de Segurança. Um Médico, por exemplo, não pode realizar apressadamente uma cirurgia sem analisar os indispensáveis exames perioperatórios porque o seu paciente deseja viajar ou tem algum outro compromisso agendado. Ilustrativamente, também, um Engenheiro Civil não pode, em virtude de urgência em se iniciar a fase de acabamento de uma edificação para a “ágil” entrega das unidades habitacionais aos respectivos compradores, dar por terminadas as estruturas antes de concluído o processo de cura do concreto. Um Professor não pode, em situação regular, antes da conclusão de todas as aulas de um semestre letivo, dar por vistos os assuntos elencados na ementa de uma disciplina e lançar, sem a efetiva avaliação, as notas dos alunos porque informado de pretensa urgência.

Há sempre responsabilidade e esta responsabilidade, como antes ressaltado, não é suprimida por suposta cobrança/urgência. Suposta urgência/cobrança não justificam a elaboração de um produto ruim e deficiente em aspecto essencial: Segurança, no caso do *software*.

¹⁴² A amostra em discussão foi definida em função da reputação de que goza o CIn/UFPE no mercado e do seu conceito junto à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Com o escopo de se obter um dos melhores cenários reais, definiu-se tal amostra, já que, se este cenário, o cenário formado a partir dos dados obtidos junto aos discentes do CIn fosse ruim no tocante à Segurança Computacional, o cenário

que também trabalham como desenvolvedores na indústria de *Software* geral, empregando metodologias tradicionais e ágeis em suas atividades de produção de sistemas, na proporção exposta no Gráfico 7.

Gráfico 7 – Metodologias de desenvolvimento de *software* empregadas pelos participantes do survey.



Fonte: Autor (2019) ¹⁴⁶ ¹⁴⁷.

mediano real, por lógica trivial, seria pior, o que era esperado a partir dos dados obtidos via *pentesting* e das entrevistas realizadas com os especialistas em Segurança Computacional.

¹⁴³ Acerca da reputação do CIn, vale registrar, ainda, que não se desconhece o fato de que, neste Centro, não há ênfase na pesquisa e no ensino atinentes à Segurança, o que poderia, em princípio, levar à falsa percepção de inutilidade da amostra em discussão, uma amostra possivelmente fraca neste aspecto. Ocorre que esta característica do CIn, em verdade, corrobora com o que foi apurado na investigação e ora é relatado neste documento, pois como poderia, hoje, neste momento de ubiquidade do *software*, uma instituição de ensino ser tida como de excelência se nela a Segurança não desempenha papel relevante? Seria apropriada a sistemática de avaliação da CAPES para os cursos de Ciência da Computação, Engenharia da Computação e Sistemas de Informação, com a desconsideração da importância da Segurança na pesquisa e no ensino? Tem-se aqui novo problema de pesquisa a ser objeto de trabalhos futuros.

¹⁴⁴ Sobre os respondentes deste survey, alguns comentários merecem destaque. Houve, neste universo de respondentes, preponderância masculina (79,41%). Não se apresentou uniformidade etária, estando 29% dos respondentes na faixa dos 20 aos 24 anos, 17,64% na faixa dos 25 aos 29 anos, 29% na faixa dos 30 aos 34 anos e 20,58% na faixa dos 35 aos 40 anos. Quanto à escolaridade (titulação máxima à época), também não houve uniformidade, já que, dos respondentes, 8,82% possuíam Doutorado, 35,19% tinham concluído um Mestrado, 5,88% cursaram uma especialização, 32,35% eram graduados e 14,70%, ainda sendo alunos de graduação, tinham apenas o Ensino Médio completo.

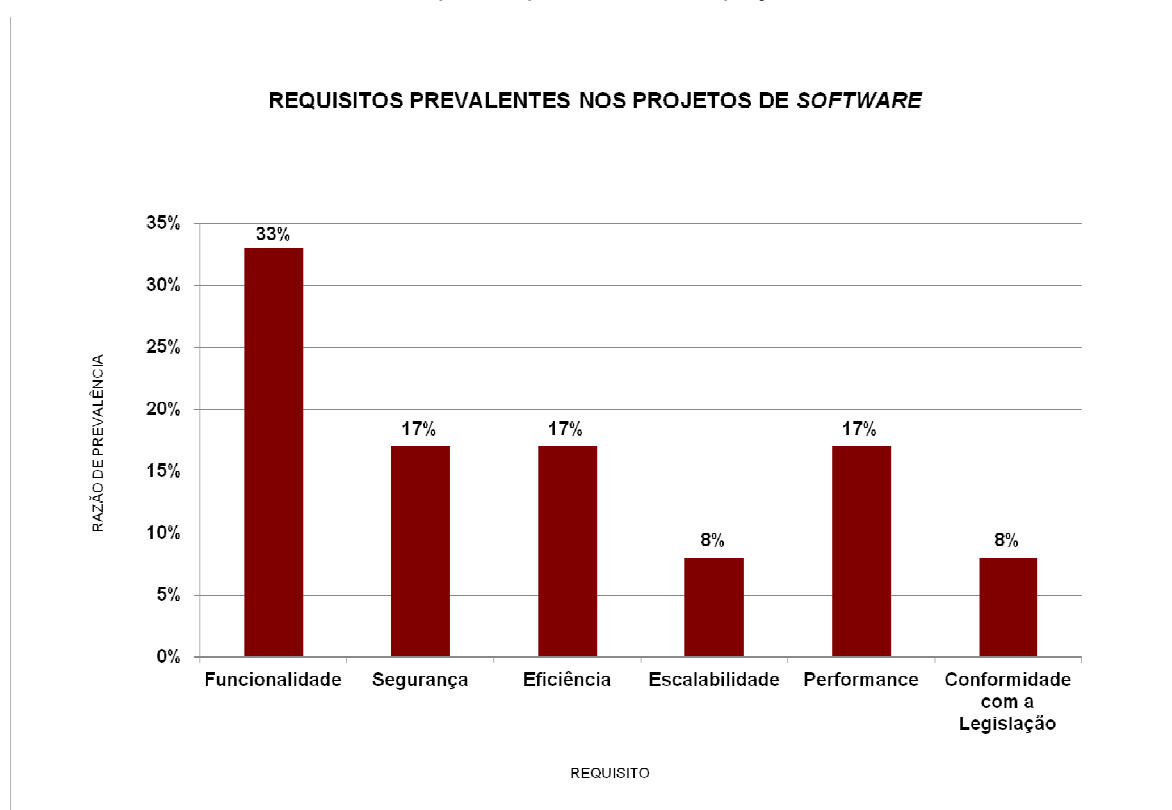
¹⁴⁵ Para captação de potenciais respondentes, encaminharam-se, às listas de *e-mails* dos discentes do CIn, mensagens solicitando voluntária participação na pesquisa.

¹⁴⁶ Gráfico produzido com base nos dados obtidos no survey referido.

¹⁴⁷ Importa esclarecer, neste ponto, que o estudo ora relatado não teve por escopo a detalhada análise de possível associação entre a adoção de uma dada metodologia de desenvolvimento e eventual impropriedade no tratamento dos requisitos de segurança. Fez-se a inclusão de tal informação apenas porque, considerada a

No *survey* referido, 34 (trinta e quatro) desenvolvedores de *software* participaram como respondentes anônimos de forma voluntária. De acordo com suas respostas a questionário acessível através da *web* (modelo no apêndice C), infere-se que, embora eles reconhecessem, por si mesmos, a importância dos Requisitos de Segurança, esta categoria de requisito não foi tratada como prioridade nos projetos em que eles trabalharam. Os respondentes que puderam detalhar parte dos projetos em que trabalharam, um total de 12 (doze) desenvolvedores de *software*, também afirmaram que os requisitos ditos funcionais sempre prevaleceram, como ilustrado no Gráfico 8.

Gráfico 8 – Requisitos prevalentes nos projetos de *software*.



Fonte: Autor (2019) ^{148 149}.

distribuição observada na amostra, não se poderia, de plano, afastar a possibilidade de haver, sim, algum relacionamento entre a insegurança no *software* e a metodologia empregada em sua construção, mormente quando considerado o fato de que, em razão de suas próprias naturezas, as metodologias ditas ágeis não propiciam ampla margem para reflexão acerca das muitas questões impactantes no desenvolvimento, uma vez que a agilidade se constitui no foco principal. A efetiva avaliação, contudo, da possível associação em debate é questão que fica para exame em trabalhos futuros.

¹⁴⁸ Gráfico elaborado a partir dos dados coletados no citado *survey*.

¹⁴⁹ Ainda que já tenha sido feito o destaque, no Capítulo 2, de que, em algumas ocasiões, poderia haver mútua excludência entre requisitos, registra-se, mais uma vez, agora, esta possibilidade, consignando-se, em antecipação a ideias debatidas ulteriormente ao longo deste documento, que, na percepção do pesquisador, a mútua excludência mencionada não justificaria, por si só, eventual preterição da Segurança, já que sem Segurança, não se teria, por exemplo, nem mesmo funcionalidades, dado que, da exploração de vulnerabilidades, poderia resultar subversão do funcionamento “normal” de um sistema.

A prevalência referida pode resultar, em parte, de deliberadas opções feitas ao longo do desenvolvimento do *software*, quando dilemas são enfrentados [IIVARI, 1996]. Ainda assim, não se pode afastar a possibilidade de a preterição/negligência em debate se originar, também, na Academia.

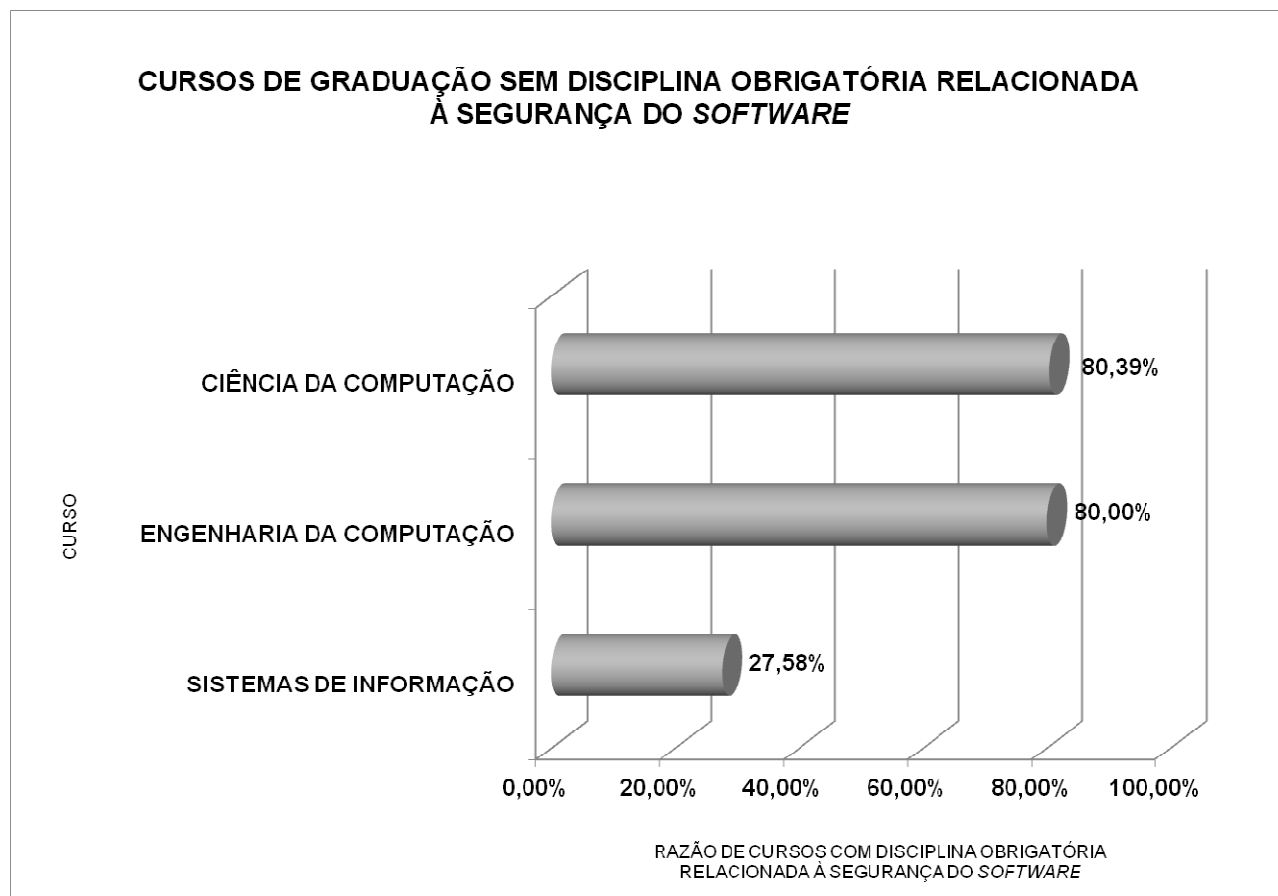
Com efeito, os Requisitos de Segurança parecem não ser relevantes em algumas instituições de ensino nacionais, já que um grande número de discentes conclui seus estudos sem cursar qualquer disciplina obrigatória sobre este tema ou sobre Segurança Computacional em geral. Isso é o que revela a análise curricular de 115 (cento e quinze) cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de 64 (sessenta e quatro) instituições brasileiras de ensino (diretrizes de análise apresentadas no apêndice H)^{150 151 152}, como ilustrado no Gráfico 9.

¹⁵⁰ Antevendo-se, por observações empíricas, um panorama ruim neste sentido, optou-se por buscar informações do “melhor cenário”, já que, se o “melhor cenário”, como esperado, fosse ruim, o cenário real, obviamente, seria pior. Para tanto, decidiu-se examinar as grades curriculares dos cursos de Ciência da Computação, Engenharia da Computação e Sistemas de Informação de instituições de ensino que também mantivessem um programa de pós-graduação regular junto à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), do Ministério da Educação. Se os cursos destas instituições, supostamente as melhores nacionais, não apresentassem as disciplinas em discussão, o mais provável, por lógica, seria que os cursos das demais instituições de ensino superior também não tratassem do assunto. Consideraram-se, desse modo, na pesquisa ora relatada, os cursos de graduação referidos com programas de pós-graduação ativos junto à CAPES, cujas grades curriculares estivessem divulgadas na Internet.

¹⁵¹ No tocante à origem dos desenvolvedores e instituições de ensino consideradas nesta investigação, uma observação se faz necessária. A origem dos desenvolvedores e instituições de ensino não foi considerada um grande promotor de viés neste estudo porque, atualmente, há grande mobilidade nacional e internacional entre os profissionais de *software*. Devido à mencionada mobilidade, espera-se que haja, globalmente, similaridade nas grades curriculares de instituições de ensino e no *background* dos engenheiros de *software* de diferentes países e culturas.

¹⁵² Relação das instituições de ensino, cujos cursos foram considerados nesta pesquisa, é apresentada no apêndice J.

Gráfico 9 – Razão de cursos de graduação sem disciplina obrigatória relacionada à Segurança.



Fonte: Autor (2019) ¹⁵³.

Como exposto no Gráfico 9, mesmo que, nos cursos de Sistemas de Informação, mais de 70% (setenta por cento) das grades incluam disciplinas obrigatórias em Segurança, persiste uma expressiva lacuna de disciplinas relacionadas à Segurança nos cursos de Ciência da Computação e Engenharia da Computação, já que cerca de 80% deles não apresentam disciplina obrigatória voltada à Segurança.

Se as disciplinas relacionadas à Segurança não são obrigatórias nos cursos de graduação cujas grades foram examinadas, é provável, embora não se possa rechaçar a hipótese de suplementação da lacuna com o autodidatismo, que os profissionais que tenham feito tais cursos não possuam um conhecimento razoável sobre Segurança.

Ao mesmo tempo em que os dados indicam problemas relacionados à efetiva e à eficiente inclusão de requisitos de segurança no *software*, bem como no tocante ao conhecimento teórico dos desenvolvedores/engenheiros relativamente à

¹⁵³ Gráfico construído com o emprego dos dados coletados no já referido *survey*.

Segurança¹⁵⁴, o exame dos *End User License Agreements (EULAs)* e dos *Terms of Service (ToS)* sugere que a Indústria de *Software* tenta se evadir da responsabilidade pelos produtos/serviços que desenvolve/fornece, inserindo-se nesta almejada isenção de responsabilidade também questões atinentes à Segurança.

O citado exame dos *EULAs/ToSs* envolveu, basicamente, a coleta e a análise das disposições de 150 (cento e cinquenta) *EULAs/ToS*, disponíveis na Internet, de 67 (sessenta e sete) variadas companhias de porte significativo produtoras/fornecedoras de *software/serviços de software*^{155 156 157}, originárias de distintas localidades geográficas, como revelam a Tabela 2 e o Gráfico 10.

Tabela 2 – Origem geográfica das empresas produtoras/fornecedoras de *software*.

DISTRIBUIÇÃO DAS EMPRESAS PRODUTORAS/FORNECEDORAS DE SOFTWARE CONSIDERADA SUA ORIGEM GEOGRÁFICA	
ORIGEM GEOGRÁFICA	QUANTIDADE DE EULAS/TOSS CONSIDERADOS NA PESQUISA
ALEMANHA	3
AUSTRÁLIA	1
ÁUSTRIA	1
CANADA	1
CURAÇÃO	1
ESTADOS UNIDOS	118
FRANÇA	4
HOLANDA	6
IRLANDA	1
JAPÃO	3
MAURÍCIA	1
REINO UNIDO	6
RÚSSIA	2
SUÉCIA	1
SUIÇA	1
TOTAL	150

Fonte: Autor (2019) ¹⁵⁸.

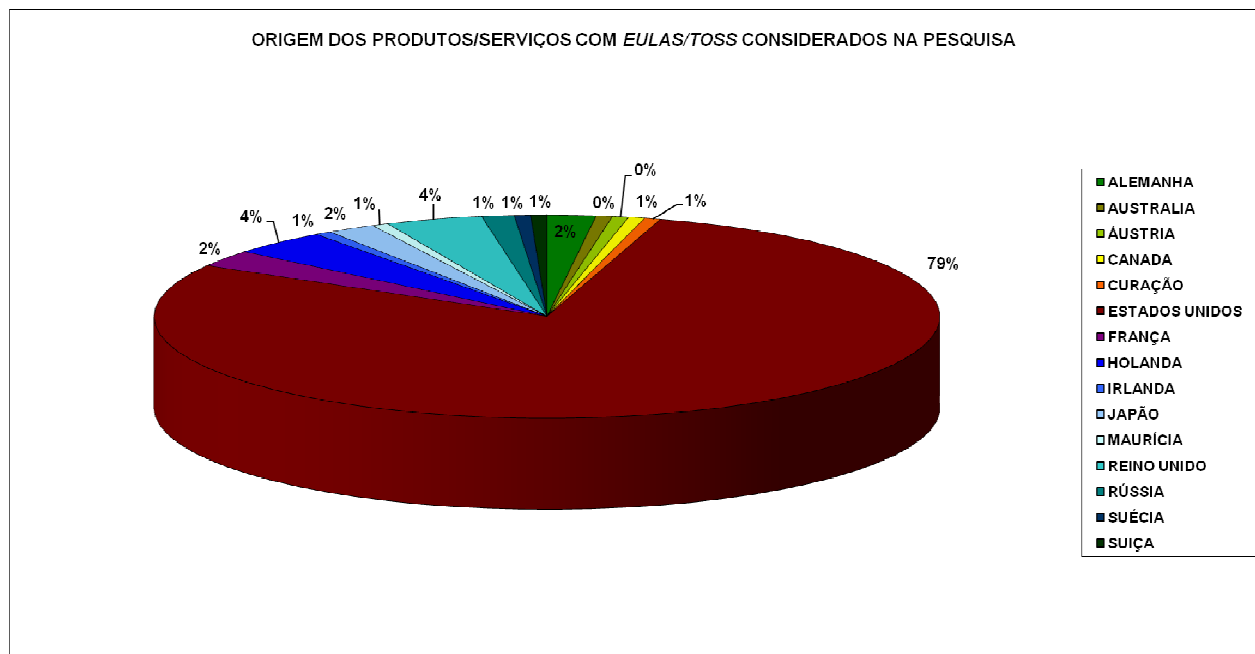
¹⁵⁴ Importa registrar, quanto ao desconhecimento mencionado, que, em outros Estados, também há indícios de insuficiente domínio de noções de Segurança Computacional, como observado por Porup (2019), quando referida, na compilação de dispositivos IoT, a não ativação das características de compilação segura.

¹⁵⁵ Na seleção dos *EULAs/ToSs* que seriam examinados, empregaram-se as diretrizes apresentadas no apêndice B, segundo as quais, por opção do pesquisador, a busca por novos *EULAs/ToSs* cessaria, se atingido o número mínimo de 150 (cento e cinquenta) documentos coletados sem que novas inovações quanto à responsabilidade surgissem. Cabe ressaltar que a busca realizada foi feita em função de documentos e não em função das empresas produtoras. Chegou-se ao exame de *EULAs/ToSs* de 67 (sessenta e sete) distintas empresas de forma não intencional mediante simples tabulação e contagem, nos documentos referidos, das ocorrências relativas a cada empresa.

¹⁵⁶ Rol dos *EULAs* e *ToSs* examinados é exposto no apêndice K.

¹⁵⁷ Listagem alfabética das empresas que tiveram *EULAs/ToSs* examinados é apresentada no apêndice L. Relação alfabética condensada das empresas produtoras/fornecedoras de *software/serviços de software* e dos seus respectivos produtos/serviços cujos *EULAs/ToSs* foram considerados na investigação é exposta no apêndice M.

¹⁵⁸ Tabela produzida com o uso dos dados de *EULAs/ToSS* coletados para esta pesquisa.

Gráfico 10 – Origem geográfica das empresas produtoras/fornecedoras de *software*.

Fonte: Autor (2019) ¹⁵⁹.

Os *softwares*/serviços em *software* cujos *EULAs* e *ToSs* foram examinados, em livre classificação adotada neste estudo¹⁶⁰, foram inseridos nas categorias referidas na Figura 63, em distribuição representada na Tabela 3.

¹⁵⁹ Gráfico elaborado a partir das informações apresentadas na Tabela 2.

¹⁶⁰ A livre opção pelas categorias empregadas deu-se em função da pretensão de ulterior análise segmentada, considerados a natureza e o domínio do produto/serviço.

Figura 63 – Categorias dos *softwares/serviços* em *software* considerados na pesquisa.

Fonte: Autor (2019) ¹⁶¹.

Tabela 3 – Distribuição dos *softwares/serviços* em *software* considerados no estudo em função da livre taxonomia adotada.

CATEGORIAS DOS SOFTWARES COM EULAS/TOSS CONSIDERADOS NA INVESTIGAÇÃO	
CATEGORIAS	QUANTIDADE
APLICATIVO/UTILITÁRIO	136
INSTALAÇÃO, CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDOR	4
SERVIÇO WEB	18
AMBIENTE/SISTEMA OPERACIONAL	6
TOTAL	164

Fonte: Autor (2019) ¹⁶².

Esclarecendo-se um pouco a natureza dos *softwares* cujos *EULAs* e *ToSs* foram considerados na pesquisa, registra-se, no tocante à instalação, configuração e gerenciamento de servidores, que foram analisados *EULAs/ToSs* de *softwares* voltados à criação, visualização e gerenciamento de máquina virtual, bem como à instalação, configuração e gestão de servidor de *e-mails*. Para se expor, superficialmente, a natureza dos aplicativos/utilitários e dos serviços *web* cujos *EULAs/ToSs* foram examinados na pesquisa, apresentam-se as Tabelas 4 e 5.

¹⁶¹ Categorização livre, definida em função do escopo da presente pesquisa.

¹⁶² Tabela elaborada a partir dos dados coletados nos *EULAs/ToSs*.

Tabela 4 – Domínios dos aplicativos/utilitários considerados cujos *EULAs/ToSs* foram considerados na pesquisa.

DOMÍNIOS DOS APLICATIVOS E UTILITÁRIOS CUJOS <i>EULAs/TOSS</i> FORAM CONSIDERADOS NA PESQUISA	QUANTIDADE
ACESSO A NUVEM DE SERVIÇOS	1
ADMINISTRAÇÃO PREDIAL	1
AMOSTRAGEM E ENSAIO PARA DIAGNÓSTICO MOLECULAR, TESTES	1
APLICADOS E PESQUISAS ACADÊMICAS/CIENTÍFICAS	1
ANÁLISE DE DADOS E GERAÇÃO DE RELATÓRIOS SOBRE PACIENTES	1
ANÁLISE LABORATORIAL	1
ANÁLISE QUALITATIVA DE DADOS	1
ANTIVÍRUS	3
ANTIVÍRUS, ANTISPYWARE E ANTIMALWARE	1
APRENDIZADO DE IDIOMA	2
APRESENTAÇÃO DE CONTEÚDO RELACIONADO AO CINEMA AMERICANO	1
ARMAZENAMENTO DE DADOS EM REDE	1
ATUALIZAÇÃO AUTOMÁTICA DE ARQUIVOS EM DISPOSITIVOS DIFERENTES	1
AUTOCONFIGURAÇÃO DE DISPOSITIVOS DE REDE	1
AUTOMAÇÃO DOMÉSTICA	1
BARRA INTEGRADA DE BUSCA WEB	1
CAD 3D	1
CÁLCULO ESTATÍSTICO DE DADOS CENSITÁRIOS	1
CERTIFICAÇÃO DIGITAL	1
CLIENTE DE CORREIO-ELETRÔNICO	2
CLIENTE PARA COMPUTAÇÃO EM NUVEM	1
COMPACTAÇÃO DE ARQUIVOS	2
COMUNICAÇÃO INSTANTÂNEA	1
COMUNICAÇÃO INSTANTÂNEA EM AMBIENTES CORPORATIVOS	1
CONFIGURAÇÃO DE REDE	2
CONFIGURAÇÃO DE SMARTPHONE	1
CONSTRUÇÃO, DEBUGGING E OTIMIZAÇÃO DE PERFORMANCE DE APLICAÇÕES ACELERADAS POR RECURSOS NVIDIA	1
CRIAÇÃO DE APRESENTAÇÕES PARA DISPOSITIVOS MÓVEIS	1
CRIAÇÃO DE INTERFACES PARA A WEB E PARA APLICAÇÕES DESKTOP	1
CRIAÇÃO DE LIVROS ELETRÔNICOS EM FORMATOS ESPECÍFICOS	1
CRIAÇÃO DE PORTAIS/INTRANETS, GESTÃO DE CONTEÚDO E PUBLICAÇÃO DE APLICAÇÕES WEB	1
CRIAÇÃO DE SLIDES E APRESENTAÇÕES	11
CRIAÇÃO, ORGANIZAÇÃO, VISUALIZAÇÃO E PUBLICAÇÃO DE CONTEÚDO DIGITAL	1
CRIAÇÃO/GESTÃO DE COMUNIDADES/FORUNS DE DISCUSSÃO	1
DEFINIÇÃO DE REDE POR <i>SOFTWARE</i>	1
DESENHO/EDIÇÃO DE GRÁFICOS VETORIAIS	1
DESENVOLVIMENTO DE <i>SOFTWARES</i>	2
DESENVOLVIMENTO E GESTÃO DE PROJETOS	1
DIVULGAÇÃO DE INFORMAÇÃO SOBRE CANAL DE TELEVISÃO	1
DIVULGAÇÃO E COMPRAS EM PARQUE TEMÁTICO	1
DRIVER PARA PLACA-MÃE/PLACA DE VÍDEO	1
EDITORIAÇÃO ELETRÔNICA	5

DOMÍNIOS DOS APLICATIVOS E UTILITÁRIOS CUJOS <i>EULAS/TOSS</i> FORAM CONSIDERADOS NA PESQUISA	QUANTIDADE
ENGENHO DE BUSCA	1
EXTENSÃO PARA MODELAGEM BPMN	1
FACILITAÇÃO DO APRENDIZADO	1
GERAÇÃO DE EXPERIÊNCIAS PARA CLIENTES	2
GERENCIAMENTO DE DADOS EM NUVEM	1
GERENCIAMENTO DE IMAGENS FOTOGRÁFICAS	2
GERENCIAMENTO DE <i>SOFTWARE</i> COMO SERVIÇO	1
GRAVAÇÃO DE CD/DVD	1
HELPDESK	1
IDENTIFICAÇÃO DECENTRALIZADA COM SUPORTE A BLOCKCHAINS E CRIPTOMOEDAS	1
INSTALAÇÃO E CONFIGURAÇÃO DE MÁQUINAS ATM	1
INTEGRAÇÃO ENTRE HARDWARE E <i>SOFTWARE</i>	1
INTEGRAÇÃO ORACLE-BLACKBERRY	1
JOGO ELETRÔNICO	3
LEITURA DE LIVROS ELETRÔNICOS EM FORMATOS ESPECÍFICOS	2
LIMPEZA DE DISCO	1
METABUSCA	1
MONITORAMENTO E SUPORTE EM CASO DE INJÚRIA BUCAL POR ATLETA	1
NAVEGAÇÃO VEICULAR	1
NAVEGAÇÃO WEB	3
NOTEBOOK VIRTUAL	1
OTIMIZAÇÃO E CONFIGURAÇÃO DE PLACA DE VÍDEO	1
PLANILHA ELETRÔNICA	14
PROCESSAMENTO DE TEXTOS	10
PRODUÇÃO DE ÁUDIO/VÍDEO	4
PROJETO 3D	3
PROJETO DE DISPOSITIVOS BLUETOOTH DE BAIXO CONSUMO ENERGÉTICO	1
PROJETO DE ENGENHARIA	1
PROJETO DE PLACA DE CIRCUITO IMPRESSO	1
PROJETO INDUSTRIAL DE VEÍCULOS E INSTALAÇÕES MARÍTIMAS	1
RECOLHIMENTO DE INFORMAÇÃO E COLABORAÇÃO MULTIUSUÁRIO	1
REPRODUÇÃO DE ÁUDIO EM ALTA RESOLUÇÃO	1
SEGURANÇA E FORENSE COMPUTACIONAL	1
SISTEMA DE GERENCIAMENTO DE BASES DE DADOS	2
SUPORTE À PESQUISA DE LITERATURA CIENTÍFICA	1
SUPORTE A RECURSOS MULTIMÍDIA	1
SUPORTE EDUCACIONAL EM DISPOSITIVOS MÓVEIS	1
VIDEOCONFERÊNCIA	2
TOTAL	136

Fonte: Autor (2019) ¹⁶³.

¹⁶³ Tabela construída a partir dos dados coletados de *EULAs/ToSs* nesta pesquisa.

Tabela 5 – Domínios dos serviços *web* cujas *EULAs/ToSs* foram considerados no estudo.

RELAÇÃO DOS DOMÍNIOS DOS SERVIÇOS WEB CUJAS <i>EULAs/TOSS</i> FORAM CONSIDERADOS NO ESTUDO	QUANTIDADE
ARMAZENAMENTO EM NUVEM	1
COMPUTAÇÃO EM NUVEM	2
CORREIO-ELETRÔNICO WEB	2
DICIONÁRIO	1
ELABORAÇÃO DE PROJETOS/DESENHOS	1
INTEGRAÇÃO EM NUVEM	1
JOGO ON-LINE	3
NEGOCIAÇÃO AUTOMATIZADA DE CRIPTOMOEDA	1
PAGAMENTOS E TRANSAÇÕES COM MOEDAS	1
REDE SOCIAL	3
REPRODUÇÃO DE MÍDIA	1
STREAMING DE MÚSICA	1
TOTAL	18

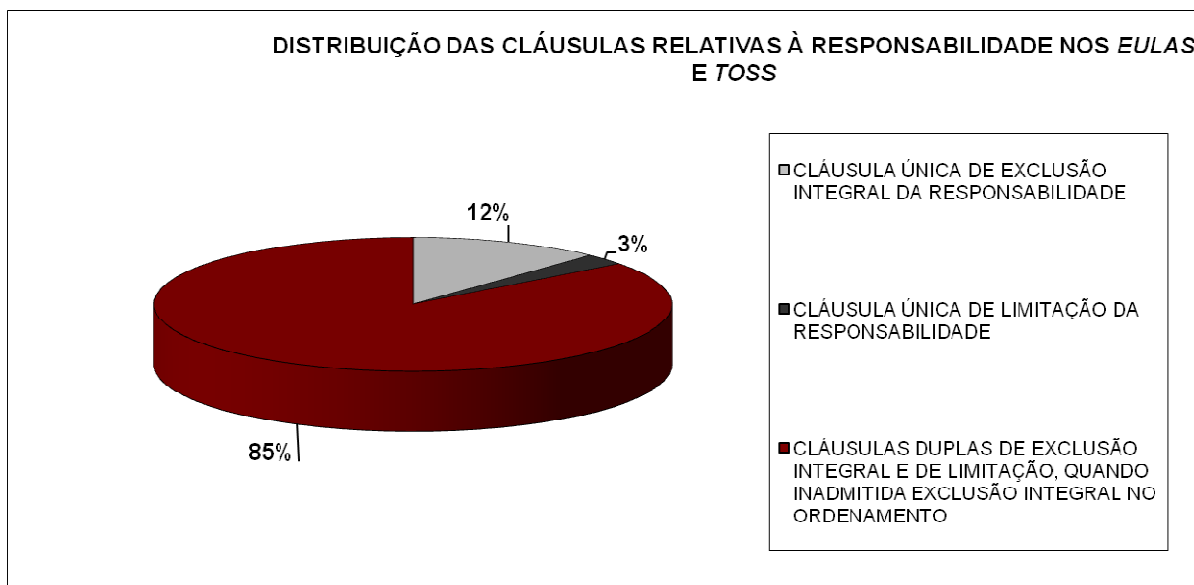
Fonte: Autor (2019) ¹⁶⁴.

Independentemente do domínio e da origem geográfica dos *softwares/serviços* em *software* considerados, observou-se como se depreende da Tabela 6 e do Gráfico 11, que em 100% (cem por cento) dos *EULAs/ToSs*, havia alguma variante de cláusula limitante ou isentiva de responsabilidade por danos resultantes do uso do *software* (danos por vulnerabilidades de segurança implícitos) e o estabelecimento de uma condição para o citado uso: a irrestrita aceitação das cláusulas limitantes ou excludentes de responsabilidade.

Tabela 6 –Responsabilidade nos *EULAs/ToSs*.

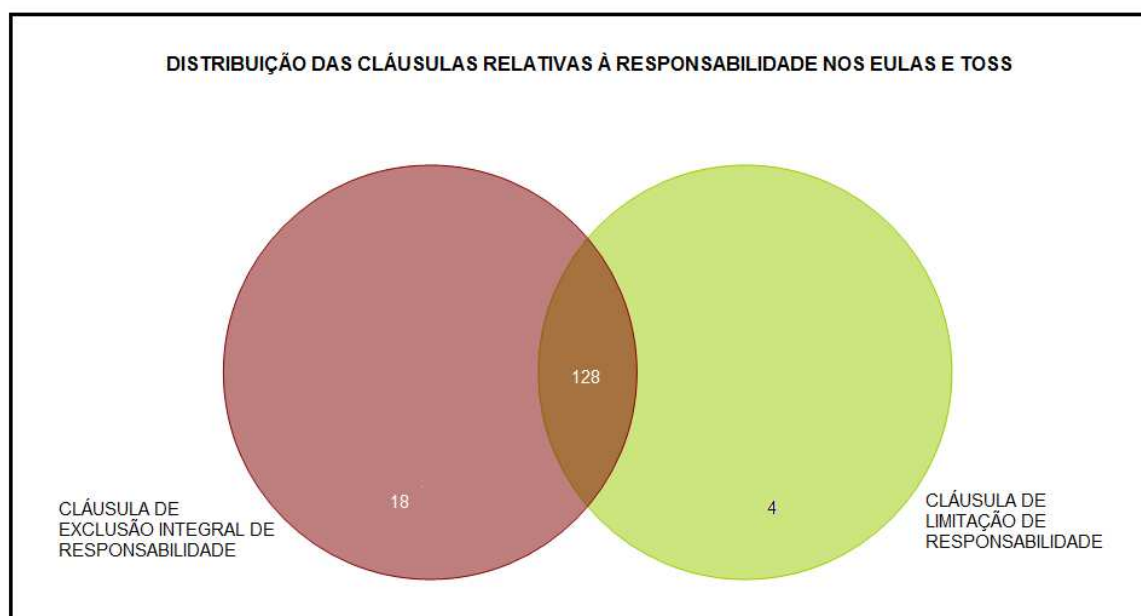
RESPONSABILIDADE NOS <i>EULAs/TOSS</i>	
CLÁUSULAS RELATIVAS À RESPONSABILIDADE IDENTIFICADAS EM CADA <i>EULA/TOS</i>	QUANTIDADE
Cláusula única de exclusão integral de responsabilidade	18
Cláusula única de limitação de responsabilidade	4
Cláusulas duplas de exclusão integral e de limitação de responsabilidade, quando não admitida exclusão integral no ordenamento jurídico	128

Fonte: Autor (2019) ¹⁶⁵.¹⁶⁴ Tabela elaborada com o emprego dos dados dos *EULAs/ToSs* coletados nesta investigação.¹⁶⁵ Tabela construída mediante análise dos dados de *EULAs/ToSs* coletados.

Gráfico 11 – Responsabilidade nos *EULAs* e *ToSs*.

Fonte: Autor (2019) ¹⁶⁶.

Ilustrando de outra forma a expressividade das cláusulas excludentes e limitantes de responsabilidade nos *EULAs* e *ToSs*, apresenta-se o Gráfico 12.

Gráfico 12 – Responsabilidade nos *EULAs* e *ToSs*.

Fonte: Autor (2019) ¹⁶⁷.

Relativamente às cláusulas de limitação de responsabilidade, importa

¹⁶⁶ Gráfico elaborado a partir das informações expostas na Tabela 6.

¹⁶⁷ Diagrama de Venn montado em função do exame dos *EULAs/ToSs* considerados nesta investigação.

registrar a usual existência de tetos de responsabilização em cerca de 88% (oitenta e oito) por cento delas. Comumente, tais limites máximos consistem no preço de aquisição do produto/serviço ou soma previamente fixada pelo produtor/fornecedor do produto/serviço.

Vale salientar, ainda, em virtude de alguns *EULAs/ToSs* referirem mais de um produto/serviço em *software*¹⁶⁸, que se teve, no total, o exame de disposições contratuais relativas a 164 (cento e sessenta e quatro) produtos/serviços em *software* das distintas categorias/segmentos antes referidos.

Considerados os segmentos citados, observou-se, como representado na Tabela 7 e no Gráfico 13, que:

- em todos os segmentos, estão presentes cláusulas de integral exclusão de responsabilidade, havendo um segmento em que, contudo, a integral exclusão de responsabilidade não se dá como nos demais: o segmento dos *softwares* voltados à instalação, configuração e gerenciamento de servidores;
- no segmento dos *softwares* de instalação, configuração e gerenciamento de servidores, para a amostra considerada, é cerca de 50% (cinquenta por cento) menos frequente a inclusão, nos *EULAs* e *ToSs*, de condições de integral exclusão de responsabilidade;
- no tocante à limitação de responsabilidade, não se observa grandes variações entre segmentos, feita a normalização dos dados.

Tabela 7 – Exclusão/limitação de responsabilidade x segmento do produto/serviço.

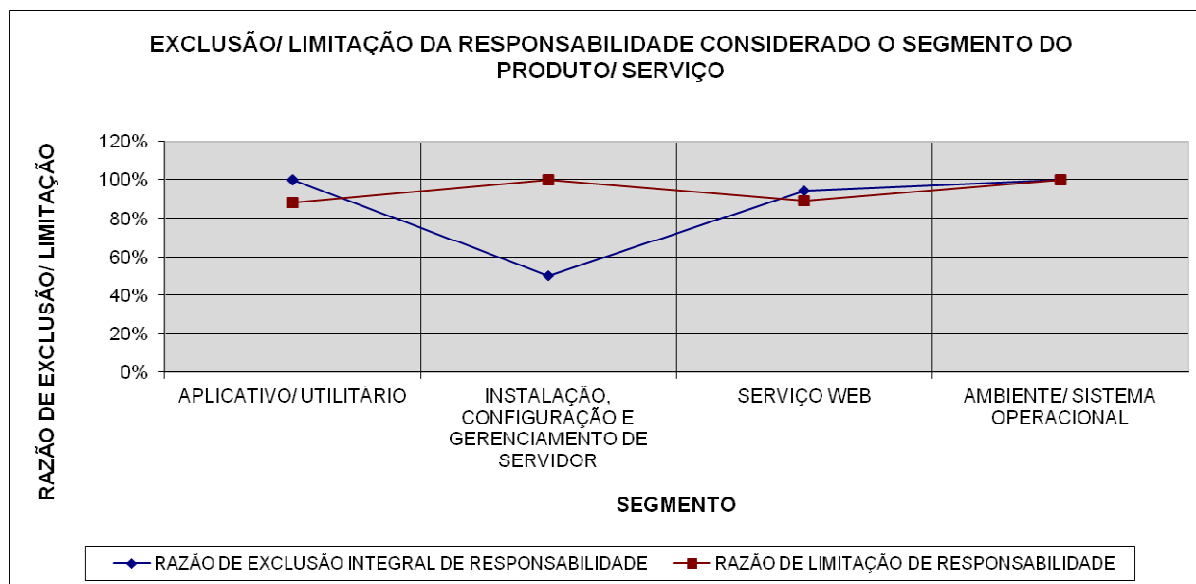
EXCLUSÃO/LIMITAÇÃO DA RESPONSABILIDADE CONSIDERADO O SEGMENTO DO PRODUTO/SERVIÇO		
SEGMENTO	RAZÃO DE EXCLUSÃO INTEGRAL DE RESPONSABILIDADE	RAZÃO DE LIMITAÇÃO DE RESPONSABILIDADE
APLICATIVO/UTILITÁRIO	100%	88,23%
INSTALAÇÃO, CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDOR	50%	100%
SERVIÇO WEB	94,44%	88,88%
AMBIENTE/SISTEMA OPERACIONAL	100%	100%

Fonte: Autor (2019) ¹⁶⁹.

¹⁶⁸ Exemplo de tal situação se verificou quando são consideradas suítes/pacotes de *softwares* comercializados em conjunto (Microsoft Office, e.g.).

¹⁶⁹ Tabela construída com a consolidação e a análise dos dados dos *EULAs/ToSs* coletados neste estudo.

Gráfico 13 – Exclusão/limitação de responsabilidade x segmento do produto/serviço.



Fonte: Autor (2019) ¹⁷⁰.

Ocultando-se atrás de *EULAs/ToSs* isentivos e/ou limitantes de responsabilidade, segmentos da Indústria de *Software*, ainda, paradoxalmente, propalam aos quatro ventos que comercializam produtos seguros, o que, como bem observado por um dos especialistas de Segurança Computacional é impossível se certificar.

De fato, não há, no geral, como se garantir formal e matematicamente, a integral Segurança de nenhum Sistema Computacional, dado que as vulnerabilidades podem se manifestar em diversas camadas de um sistema e que o fator humano, mesmo não sendo elemento integrante do *software* em si, não pode ser desconsiderado.

Não havendo, assim, como se garantir a Segurança, seria possível, no máximo, eventualmente, caso rotineiramente adotados teoremas matemáticos, métodos formais e linguagens formais de especificação¹⁷¹, produzir descrições e modelos abstratos claros e unívocos para parcelas ou módulos de um sistema. Há que se ressaltar, contudo, que esta especificação/modelagem não ambígua não implicaria, de forma absoluta, correção perfeição do módulo/parcela, uma vez que a

¹⁷⁰ Gráfico elaborado a partir dos dados referidos na Tabela 7.

¹⁷¹ Aos interessados em linguagens formais de especificação (Z, em particular), recomenda-se conferência de Potter, Till e Sinclair (1996) e de Woodcock e Davies ([S.d.]).

sua efetiva implementação, mais uma vez, é dependente do fator humano, sujeitando-se, obviamente, a escolhas ruins e a falhas.

Neste contexto de generalizada proliferação de vulnerabilidades, de significativo desconhecimento quanto à importância da Segurança e de priorização de outros requisitos em detrimento da Segurança, de impossibilidade de se atestar, formal e matematicamente, a integral segurança de um sistema e de ocultação da Indústria de *software* através de *EULAS/ToSs* com a antagônica divulgação da comercialização/uso de *software* seguro, alguns questionamentos relevantes surgem.

Se as empresas da amostra obtida nesta pesquisa assim procedem (empresas de relativo porte, ou de significativa participação em seus respectivos nichos mercadológicos), o que se poderia esperar dos demais empreendimentos que desenvolvem/fornecem *software*? Se é difundida, hoje, como se depreende do discurso de empreendimentos e desenvolvedores de *software* (como revela, por exemplo, extrato de conversa entre desenvolvedores de jogos apresentada no anexo A¹⁷²), a equivocada crença de que é trivial a definição de *EULAs/ToSs* isentivos ou limitantes de responsabilidade, o que se poderia esperar dos demais empreendimentos referidos? Se é comum que significativa parcela da Indústria de *Software*, partindo da premissa de que o indivíduo comum não lê ou não compreende *EULAs* e *ToSs*, defina absurdas e irrealizáveis condições gerais para o uso de seus produtos/serviços, o que se poderia imaginar das cláusulas que, direta ou indiretamente, refiram-se a questões de Segurança?¹⁷³ Se há, atualmente,

¹⁷² A visualização, na própria origem, da discussão referida, caso ainda acessível livremente na *web*, é possível em GameDev (2013).

¹⁷³ Ilustrando-se o caráter absurdo e abusivo de certos *EULAs* e *ToSs*, citam-se, de forma mera exemplificativa, os seguintes condicionamentos, referidos em Hoffman (2012), Dean (2017), Winder (2009), Newitz (2005) e Newman (2012):

- condicionamento do uso de determinado *software* à irrevogável cessão da alma do usuário em favor da empresa fornecedora do *software*;
- condicionamento do uso de dado *software* ao direito do fornecedor do *software* a realizar irrestritas e infinitas auditorias nas atividades do usuário;
- condicionamento do uso de navegador *web* à irrestrita e total concessão de direitos autorais e de propriedade original do usuário à empresa produtora do referido navegador;
- condicionamento do uso de *browser* especialmente elaborado para determinado ambiente operacional a sua não instalação em ambientes de tal espécie;
- condicionamento do uso de player de áudio e vídeo ao comprometimento de não criar mísseis, bem como armas químicas, biológicas ou nucleares;
- condicionamento do uso de jogo a inespecífica moral;
- condicionamento do uso do *software* à renúncia de eventual participação em ações coletivas;
- condicionamento do uso do *software* ao comprometimento irrevogável do usuário em não tecer comentários acerca da qualidade do *software*;
- condicionamento do uso do *software* a não utilização de qualquer ferramenta/solução *antispyware*;
- condicionamento do uso do *software* a contínua monitoração pela entidade fornecedora do *software*;
- condicionamento do uso do *software* a não utilização de produtos de empresas/fornecedoras concorrentes.

inclusive, sítios *web* voltados à automatizada criação de *EULAs/ToSs*, o que se pode antever da futura conduta da Indústria de *Software*¹⁷⁴? Se até mesmo os supostos geradores automatizados de *EULAs* e *ToSs* possuem seus próprios *EULAs* e *ToSs* isentivos e limitantes de responsabilidade, como é o caso, do *LawDepot Free EULA* ([2019?]) e do *TermsFeed EULA Generator* (TERMSFEED, [2019?]), o que se pode esperar da Indústria de *Software* como um todo? O que se pode esperar considerando, também, o fato de que, como observado por Whittaker (2018), parte da Indústria, em iniciativa qualificável como censura a liberdade fundamental, protocoliza ações judiciais voltadas a impedir que pesquisadores e *white-hat hackers* divulguem publicamente informações relativas a vulnerabilidades de segurança por eles identificadas?

Seria razoável se acreditar e se esperar que os pequenos e médios produtores de *software*, dispondo, em tese, de menos recursos técnicos e financeiros, agissem de forma diferente? Seria plausível a tese de que a sociedade civil, mais dependente do *software* a cada dia, quedasse resignada a respeito da conduta evasiva da Indústria de *Software*? Seria razoável se esperar que esta mesma Indústria, por seu comportamento pretérito e atual, espontânea a livremente, passasse, sem a intervenção de algum novo fenômeno, a trabalhar de forma diferente no tocante aos requisitos de segurança no *software*?

A provável resposta a estas perguntas constitui um problema simples de lógica informal.

O quadro traçado a partir de todos os dados apresentados até o momento leva a reflexões sobre o comportamento dos desenvolvedores de *software*, da Academia e da Indústria de *Software*. De plano, as ações destes agentes não parecem ideais, corretas ou, em alguns casos, éticas.

Se um indivíduo ou entidade é pago para criar algo, como ele poderia ser exonerado de responsabilidade por sua criação? Este tipo de comportamento é aceitável? Este tipo de comportamento é ético? É ético, neste processo criativo, não

¹⁷⁴ A identificação de produtos comerciais e não comerciais voltados à automatizada criação de *EULAs* e *ToSs* é procedimento simples, realizável através, por exemplo, de trivial consulta em navegador *web*. Entre os “geradores automatizados” de *EULAs/ToSs* divulgados na Internet, destacam-se o *TermsFeed Eula Generator* (TERMSFEED, [2019?]), que apresenta, inclusive, interessante vídeo ilustrativo de sua utilidade no mercado, e o *Kuikie Eula Generator* (SINEVIA, [2019?]). Também é corrente a divulgação de modelos (*templates*), para que o interessado, por si próprio, crie seu *EULA/ToS*. Entre os repositórios/sítios de *templates*, sobressaem-se o *Law Depot Free EULA* (LAWDEPOT, [2019?]), o *FormSwift End User License Agreement Form* (FORMSWIFT, [2019?]), o *SEQ Legal EULA* (SEQ LEGAL, [2019?]), o *EULA Template* (EULATEMPLATE, [2019?]) e o *Legal Templates Free End User License Agreement* (LEGAL TEMPLATES, [2019?]).

se empregar os melhores recursos, métodos e técnicas disponíveis? É ético se focar apenas na redução do tempo de desenvolvimento, dispensando-se atenção somente ao que *stakeholders* e usuários veem (requisitos funcionais, principalmente)? Pode-se falar em *Minimum Viable Product (MVP)* ¹⁷⁵, quando não se consideram requisitos de Segurança? É certo, atualmente, não se considerar a Segurança como um aspecto relevante do *software*, mormente quando patente que se está em uma era de onipresença do *software* e da Internet das Coisas/Internet de Tudo? É ético e aceitável que um indivíduo ou entidade venda um pacote de *software* ou um serviço de *software* e estabeleça cláusulas limitantes/excludentes de responsabilidade em *EULAs* e *ToSs*, isentando-o de qualquer ônus mesmo em caso de negligência, imprudência ou imperícia? É aceitável e ético que a Indústria de *Software* tenha aviltante e leonina conduta, tal qual o Mefistófeles de Goethe (1997)?

Em uma nova “analogia literária”, Victor Frankenstein poderia se isentar de qualquer encargo/responsabilidade ao dar origem à sua criatura (SHELLEY, 2014)? Deveria Victor Frankenstein ter agido sem refletir sobre as consequências dos seus atos? Deveria ele ter dado ânimo a uma nova vida por mero deleite e para satisfação de sua vaidade, sem as devidas cautelas e sem avaliar repercussões potenciais?

Em um contexto diferente, em nova analogia, analogia técnica, dessa vez, se um profissional especializado agisse de tal forma, isso seria aceitável? Seria aceitável, por exemplo, que um cirurgião somente realizasse cirurgias com foco na minimização do tempo dos procedimentos? Seria aceitável que este mesmo cirurgião apenas empregasse metodologias rápidas para operações e, por este motivo, negligenciasse o diagnóstico pré-operatório de seus pacientes? Seria ético que este cirurgião não adotasse medidas profiláticas contra infecções durante as operações porque isso demandaria mais tempo e consumiria mais de seus esforços pessoais? Seria aceitável e ético que este cirurgião não empregasse os seus melhores esforços quando manipulasse órgãos internos, já que nem o paciente ou qualquer outra pessoa poderia ver o que foi feito internamente? Seria aceitável que este cirurgião se esquecesse de retirar algum instrumento cirúrgico do corpo do

¹⁷⁵ De forma extremamente sintética, o *Minimum Viable Product* pode ser definido como aquele produto que, com reduzido conjunto de funcionalidades/recursos, tem aceitação potencial no mercado. Dito de outra forma, o MVP seria o produto menos complexo que um ente poderia fornecer e encontrar aceitação no mercado. Tratando-se de tema estranho ao objeto central do presente trabalho, remetem-se os interessados em tal assunto a Duc e Abrahamsson (DUC, ABRAHAMSSON, 2016), bem como a Münch *et al* (2013).

paciente antes de terminar o procedimento? Seria aceitável se a principal (se não a única) preocupação do cirurgião se relacionasse às cicatrizes, às aparências das incisões? Seria aceitável que este cirurgião não desse atenção a aspectos pessoais da vida do paciente (comorbidades, por exemplo), quando da definição dos planos da cirurgia? Seria aceitável que este cirurgião, ainda, quando contratado por um paciente, dissesse não ser responsável por qualquer resultado adverso, mesmo quando não prestasse a devida atenção ao que estava fazendo?

A resposta geral a todas estas perguntas é “Não, não seria aceitável. Seria antiético. O comportamento do cirurgião no exemplo dado não é correto. Há um Código de Ética para Médicos e Cirurgiões. O cirurgião do exemplo deveria seguir este Código. O cirurgião é responsável pelo que faz.”. Os mesmos argumentos se aplicam aos engenheiros/desenvolvedores de *software* nos domínios do tratamento dos requisitos de Segurança ao longo de todo o processo de desenvolvimento e não é difícil perceber isso. Na verdade, é imprescindível reconhecer isso, considerando que existe, inclusive, desde o final da década de 90, um código de ética internacionalmente aplicável no desenvolvimento de *software*: o *Código de Ética para a Engenharia de Software* produzido pela IEEE Computer Society e pela Association for Computing Machinery (1999).

Se é antiético não endereçar os requisitos de Segurança ao longo de todo o processo de desenvolvimento¹⁷⁶ e se também é antiético definir irrestritas cláusulas de limitação/exclusão de responsabilidade em *EULAs* e *ToSs*, é urgente uma modificação no comportamento dos indivíduos e entidades que compõem a Indústria de *Software*. Irrestritas cláusulas isentivas/limitantes de responsabilidades devem ser suprimidas de *EULAs* e *ToSs* e os requisitos de Segurança não mais podem ser negligenciados.

Consoante relato de um dos especialistas de segurança entrevistados, uma parte da Indústria de *Software* e dos desenvolvedores reconhece a inadequação das práticas citadas e já está “fazendo a coisa certa” desde o princípio, ou seja, já está agindo de forma ética e assumindo a responsabilidade pelo que produz, atentando para qualidade e para os requisitos de Segurança. Ainda assim,

¹⁷⁶ Frisa-se, mais uma vez, a necessidade de consideração da Segurança ao longo de todo o processo de desenvolvimento e não apenas em um único momento porque, como antes asseverado, as vulnerabilidades de segurança são observadas em todas as camadas de um sistema, de modo que, hipotéticos isolados tratamentos *a posteriori* (exclusiva instalação de *firewalls* e *softwares antimalware*, por exemplo) não poderiam, por óbvio, evitar, com eficácia e eficiência a exploração de brechas por *hackers*.

diante do vulto das vulnerabilidades identificadas neste estudo e da frequência com que se encontram *EULAs* e *ToSs* abusivos, é evidente que mais precisa ser feito.

É chegada a hora de uma mudança na Indústria de *Software* e esta mudança é urgente, sob pena de a própria Indústria de *Software* e a sociedade civil virem a arcar com custos elevados demais.

7.3 MUITO BARULHO POR NADA

Estando-se em uma era de *software* ubíquo e de alto número de pontos de vulnerabilidades de Segurança, é patente, como exposto nas seções precedentes, que não se pode mais negligenciar a Segurança no *software*, sendo indispensável a aludida modificação de paradigma de conduta na Indústria de Tecnologia da Informação. Discorrer sobre tal assunto não equivale a fazer “muito barulho por nada”. Tal assunto é vital para a sociedade civil e, também, para a própria Indústria que, como mencionado antes, pode vir a arcar com elevado custo resultante de suas próprias condutas, já havendo, inclusive, indícios robustos deste inestimável custo.

Apesar de, até hoje, se ter, de certa forma, um “anárquico estado de liberdade” na Indústria de *Software*, uma vez que o setor não é regulamentado em países diversos e que, conseqüentemente, esta mesma Indústria pode, em tais locais, agir a seu bel-prazer, há discussões iniciais acerca do licenciamento de profissões relacionadas ao desenvolvimento de *software*, como se observa, por exemplo, em Laplante (2005), dadas a relevância do labor dos atuantes em tal segmento e a importância das potenciais repercussões/consequências deste trabalho^{177 178}.

¹⁷⁷ Analisando-se a questão da regulamentação profissional a partir da realidade brasileira, pode-se, apesar da plausibilidade dos argumentos dos que rechaçam esta ideia, visualizar, em um futuro não longínquo, o efetivo estabelecimento de requisitos para a atuação na Engenharia de *Software*, já que isso se verifica em diversas outras Engenharias e atividades produtivas com motivação legítima: a proteção dos interesses da sociedade civil. Não se pode, hoje, por exemplo, construir edificações de determinado porte sem que haja um Engenheiro Civil responsável. Não se pode, atualmente, por exemplo, produzir medicamentos, sem que químicos, médicos ou farmacêuticos estejam envolvidos, devendo tais profissionais deter uma formação acadêmica mínima fixada em lei. Não se pode, hoje, nem mesmo comercializar remédios em uma farmácia, sem que haja, de plantão, um farmacêutico responsável para o saneamento de questionamento emergencial de algum comprador. Nada disso é possível porque existe um interesse social subjacente que não pode ser desconsiderado ou relegado a um segundo plano. Se o *software*, no mundo atual, tem a importância que tem por permear praticamente todas as atividades produtivas, por que estariam imunes ao licenciamento profissional os profissionais que atuam nos domínios da Engenharia de *Software*? Haveria “imunidade” apenas por ser este um domínio peculiar com necessidades próprias e continuamente mutantes? Esta peculiaridade e a característica mutante não se observariam nas demais profissões? Não estaria a Medicina a sofrer contínuos avanços sempre? Não deveriam os médicos sempre se manter atualizados? Não se observaria o mesmo para um Engenheiro Civil, ou um

Há, também, debates acerca de iniciativas externas de regulação¹⁷⁹

das atividades que envolvam o desenvolvimento de *software* (WERTH, 1998), cabendo o destaque de que uma delas (legislação, especialmente) vem sendo tida como ineficaz (PARK, 2019)^{180 181 182}.

Farmacêutico? Deveria haver “imunidade” por ser relativamente nova a Engenharia de *Software*? A tenra “idade” desta Engenharia serviria de escusa para tudo, tornando os seus agentes, a despeito das consequências de suas ações, inimputáveis civil e penalmente? A tenra idade mencionada dispensaria a necessidade de os profissionais de Engenharia de *Software* terem uma formação acadêmica ou técnica mínima? A tenra idade referida dispensaria a necessidade de avaliação da aptidão destes profissionais, ou concederia à própria Indústria amplos poderes para a sua realização segundo critérios seus? A tenra idade e a suposta escassez de profissionais com formação deveriam permitir que qualquer indivíduo se arvorasse a desenvolver *software* com fins econômico-produtivos? O que, no contexto exposto, deveria determinar o licenciamento profissional, a “antiguidade”/“idade” de uma profissão ou a sua relevância e as potenciais repercussões dela decorrentes? As respostas a estas perguntas levam, sim, à constatação de que há argumentos relevantes para o licenciamento profissional e estes argumentos acabarão por ser objeto de deliberação no Congresso Nacional em razão da existência de variados Projetos de lei em tramitação na Câmara dos Deputados sobre o tema (Projeto de lei nº 3.065/2015, Projeto de lei nº 4.408/2016 e Projeto de lei nº 5.101/2016, por exemplo). Acerca dos citados Projetos de lei, importa esclarecer alguns pontos. Nos Projetos de lei nº 3.065/2015 e nº 5.101/2016, defende-se o licenciamento em função de variados argumentos, mas, no Projeto de lei nº 5.101/2016, já se faz, de forma breve, a inclusão da Segurança na justificação. No Projeto de lei nº 4.408/2016, em liberalismo extremo, defende-se que o mercado de *software* se regule por si mesmo, não devendo haver licenciamento ou exigência de formação acadêmica mínima, tendo tal projeto sido, inclusive, apoiado pela SBC, a qual reputa desnecessária a ingerência em debate, imputando a ela a qualidade de nociva por ameaçar os ideais de liberdade (SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 2016). Não se refuta a relevância dos ideais de liberdade, mas, diante da importância do *software* na sociedade atual e do quadro observado nesta investigação no tocante à Segurança, estariam, realmente, a Indústria de *Software* e os seus profissionais a agir de forma apropriada, tornando-se desnecessário algum nível de licenciamento e de regulação? A discussão envolveria, como defende de forma simplista a SBC, apenas a reserva de mercado profissional? Não se deveria buscar uma contínua maior qualificação dos profissionais que integram a Indústria de *Software*? Não seria razoável se esperar uma maior qualificação dos profissionais, se fosse exigida alguma formação acadêmica/técnica mínima? Hoje, para se ocupar o posto de gari, exige-se formação acadêmica mínima (ensino fundamental ou ensino médio, a depender do ente contratante). Não deveria, para os profissionais da Engenharia de *Software*, ser exigida alguma formação? Qualificar-se-iam todos os que atuam na Engenharia de *Software* como indivíduos de intelecto elevadíssimo que dispensasse educação formal? Há muito espaço para reflexão e tal questão, definitivamente, é complexa o suficiente para inúmeros outros trabalhos futuros, já que não insere diretamente no objeto da investigação ora relatada.

¹⁷⁸ Ainda quanto ao licenciamento profissional, o que pensariam a Indústria de *Software* e os desenvolvedores de *software*, se o “inovativo” e “diligente” Legislador (Legislador brasileiro, por exemplo) cogitasse do condicionamento da profissão à submissão de contínuas e periódicas avaliações e reavaliações, tais como as que se submetem os condutores de veículos automotores, para atestar a aptidão profissional no tocante à Segurança? Se há algo similar para o exercício, por exemplo, da Advocacia, por que não algo parecido para os Engenheiros de *Software*? Seria tal tipo de medida bem recebido? Não seria mais inteligente e produtivo se a Indústria, a Academia e os desenvolvedores passassem a lidar melhor com a Segurança, para evitar tal espécie de “inventividade” legislativa?

¹⁷⁹ Ao se fazer referência à regulação, torna-se importante anotar alguns comentários basilares. Em princípio, pode-se falar, nos Estados em que os meios de produção e o exercício das atividades econômico-produtivas não ficam no controle governamental, na eventual necessidade, para se coibir abusos da exploração de tais atividades pelos particulares e para se garantir um mínimo de bens e serviços à sociedade civil, de regramento estatal da citada exploração pelo setor privado. Este regramento, ou melhor, esta regulação (regulação externa de um setor pelo governo/ente supranacional) pode se dar de variadas formas (o estabelecimento de normas de disciplina da atuação de alguma indústria/segmento econômico, sujeição da atuação de seus empreendimentos à autoridade de um órgão central de regulação, a definição de requisitos para o exercício profissional e a constituição de arcabouço tributário/fiscal próprio para os atuantes, e.g.), limitadas apenas pelo ordenamento jurídico de base (Constituição, em essência) e pela criatividade do Legislador, que, como se pode observar da realidade brasileira, tende ao infinito.

¹⁸⁰ Ainda que, em diversas ocasiões, legislar, definitivamente, não resolva problema algum, faz-se necessário, em alguns casos, a explícita definição de normativo próprio, para se evitar que os agentes envolvidos não se furtem às suas responsabilidades, deixando o público comum à mercê de suas ações. Com este escopo protetivo, observa-se, em Estados diversos, uma espécie de reforço no arcabouço legal, para se deixar mais claros aspectos e tópicos que um determinado segmento produtivo deve observar em seu mister. Tal reforço vem sendo estabelecido nos domínios da Indústria de *Software* tanto no Brasil como em outras Nações. É o que se depreende quando se verifica que, por exemplo, na União Europeia foi implantada a *General Data Protection*

Vislumbram-se incipientes estigmatização e execração dos profissionais que desenvolvem *software* e da Indústria que eles integram, como se depreende, por exemplo, ainda que em hipótese não diretamente relacionada a questões de Segurança no *software*, no caso da falha no *software* da aeronave Boeing 737 MAX 8¹⁸³.

Regulation e que, no Brasil, foram editados o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Sendo relativamente recentes os aludidos diplomas normativos, a sua eficácia real é questão que somente poderá ser avaliada com o decorrer de mais tempo, cabendo destacar, contudo, que se antevê, sim, utilidade em tais normas, dada a previsão, como mecanismo de regulação, do estabelecimento de reprimendas que atingem o “órgão mais sensível” de todos os indivíduos e empreendimentos: o bolso. Ainda que não revertam danos já consumados, sanções sob a forma de multas podem, sim, vir a constituir um interessante recurso para se “conscientizar” a Indústria de *Software* da necessidade de revisão de algumas de suas práticas no tocante à Segurança Computacional.

¹⁸¹ Valendo-se da mesma capacidade criativa do Legislador pátrio antes referida, poder-se-ia pensar, inclusive, na suposta utilidade da criação e da implantação, com foco na regulação, de uma nova contribuição tributária extrafiscal, incidente, exclusivamente, sob o faturamento das empresas que integram a Indústria de *Software*. Dada a relevância da Segurança para a sociedade atual, o “sagaz” e “imaginativo” Legislador nacional, utilizando-se de toda a sua força “inovadora”, poderia vir a defender, diante do elevado número de sinistros de Segurança Computacional, que a Indústria de *Software* se sujeitasse ao pagamento provisório, i.e., enquanto não melhorado o panorama da insegurança no *software*, de uma “singela” contribuição (0,5% - meio por cento do faturamento bruto, por exemplo), que seria destinada a um “Fundo” (não o “Fundo do Abismo”, mas, sim, o “Fundo para a Erradicação e o Combate à Insegurança no *Software*”) voltado ao estudo e ao desenvolvimento da Segurança Computacional no País. Se o Legislador pátrio fosse ainda mais “arrojado”, poderia, inclusive, cogitar da exação desta nova contribuição não apenas em relação às empresas que integram a Indústria de *Software*, mas, sim, de todas as empresas que utilizassem algum tipo de *software* (até mesmo o anteriormente mencionado “Software de Padaria”), estabelecendo-se alíquotas diferenciadas em função de avaliação de riscos de Segurança Computacional operada por algum agente/órgão governamental, tal como ocorre com a cobrança do Seguro contra Acidentes do Trabalho (SAT). Expostas estas breves ideias produzidas de forma inédita neste documento de Tese para esta nova contribuição extrafiscal, pergunta-se ao leitor se esta medida, a criação de uma contribuição para o “Fundo para a Erradicação e o Combate à Insegurança no *Software*”, como outras contribuições já criadas no Brasil (Contribuição Provisória sobre Movimentação Financeira - CPMF, por exemplo), resolveria o problema da Segurança Computacional? A CPMF resolveu o problema da Saúde Pública no Brasil? Qual seria, de fato, para a Indústria de *Software*, para os demais segmentos produtivos e para a sociedade civil, a verdadeira repercussão da criação destas hipotéticas contribuições para a Segurança Computacional? Seria a sujeição da Indústria de *Software* a uma nova cobrança bom para esta Indústria? Encerrando-se estes sintéticos comentários sobre regulação e extrafiscalidade, indicam-se a eventuais interessados em tributação as obras de Nogueira (1990), Baleeiro (2015) e Ataliba (1975).

¹⁸² Outra interessante possibilidade para o Legislador “diligente” e “preocupado” com a Segurança no *software* poderia resultar, também, em maior ingerência no próprio processo de desenvolvimento e/ou no funcionamento da Indústria de *Software*. E se o Legislador impusesse à cada empresa que integrasse a Indústria de *Software* o encargo de manter em seus quadros um determinado número de especialistas em Segurança Computacional, constituindo algo como uma Comissão Interna de Prevenção de Sinistros de Segurança, tal como se exige, hoje, na legislação trabalhista, para a prevenção de acidentes do trabalho? E se o Legislador criasse uma agência regulatória (uma variante da Agência Nacional de Vigilância Sanitária, por exemplo), para a fiscalização da qualidade do *software*? Esta nova “relevante” agência, mediante amostragens, analisaria o *software* produzido por diversas empresas, impondo penalidades em caso de excessivo número de vulnerabilidades de segurança identificadas (multas, essencialmente) e, na hipótese de reincidência/recalcitrância, poderia suspender as atividades da empresa que não tratasse a Segurança Computacional de forma apropriada. O que pensariam a Indústria de *Software* e os desenvolvedores de *software*, se uma ideia como esta fosse construída pelo Legislador? E, pior ainda, se o Legislador, reputando a Segurança no *software* imperativa à própria Segurança Nacional ou a relevante interesse coletivo, valendo-se das disposições constantes do artigo 173 da Constituição Federal, achasse por bem estabelecer que, a partir de um dado momento, toda a produção de *software* ficaria a cargo exclusivo do Estado, definindo-se um monopólio tal qual, em décadas passadas, no tocante às Telecomunicações e à Energia Elétrica através de empresas públicas e sociedades de economia mista? Ficariam a Indústria de *Software* nacional e os seus desenvolvedores extasiados diante da criação de uma “EMBRASOFTWARE” ou de uma “SOFTWAREBRAS” (nomes fictícios inventados pelo pesquisador)? Muito provavelmente, não haveria, de forma alguma, êxtase ou contentamento geral.

¹⁸³ Para uma breve compreensão das questões envolvidas no caso da aeronave Boeing 737 MAX 8, sugere-se leitura de Leopold, G. (2019), Yoshida, J. (2019), B. Fernando (2019), Sing, A. (2019), Campbell, D. (2019), Gregg, A. *et al* (2019), Pontefract (2019), B. (2019), Singh (2019), Campbell (2019), Leopold (2019a), Leopold

Anteveem-se, como no caso da referida empresa de aeronaves, perdas na participação de mercados em virtude de decréscimo em sua reputação com a utilização/desenvolvimento de *software* falho, o que, provavelmente, também, de forma similar, pode se dar em relação a *software* deficiente no tocante à Segurança Computacional (JEONG; LEE; LIM, 2019). Especificamente em relação a falhas de segurança, cabe destacar que as aludidas perdas de participação no mercado não são, de forma absoluta, obstadas pela mera assunção dos prejuízos causados a terceiros, como, usualmente, ocorre com as instituições bancárias, as quais, quando comprovada a delituosa ação de *hackers*, acabam por fazer acordos com seus clientes. Mesmo quando as citada instituições garantem que seus clientes não sofram com o prejuízo financeiro decorrente da exploração de vulnerabilidades de segurança, a perda de reputação persiste e, muitas vezes, a despeito da percepção de compensação pelos prejuízos, o cliente perde a confiança na instituição bancária e, na primeira oportunidade, migra para outro banco, ou, simplesmente, divulga o episódio em seu círculo social, o que também abala a imagem da referida instituição, agora em relação, inclusive, a não clientes e a clientes em potencial.

Reconhece-se como verossímil a tese de que, inerte/omissa a Indústria de *Software* no tocante à Segurança, pode-se formar um novo nicho a ser explorado em Cortes de Justiça e em Cortes de Arbitragem, proliferando demandas individuais e coletivas voltadas à responsabilização e à composição de danos decorrentes de falhas/vulnerabilidades de segurança em *software* (KASPERSKY, 2018) (UNIVERSITY BUSINESS, 2016)^{184 185 186}.

(2019b), Yoshida (2019), MacMillan (2019), Gregg *et al* (2019), Yglesias (2019), Stewart (2019), Travis (2019a) e Travos (2019b).

¹⁸⁴ Acerca da judicialização em comento, importa registrar que falhas em *software* não relacionadas à Segurança Computacional têm, no momento, chamado a atenção da sociedade civil, o que se vê, por exemplo, no tocante ao antes citado caso da aeronave Boeing 737 MAX 8, com a protocolização, inclusive, de ação coletiva (*class action*) por mais de 400 (quatrocentos) pilotos contra a produtora da referida aeronave. Se, no momento, a sociedade civil opta, com grande vigor, por questionar judicialmente possível falha em *software* não relacionada à Segurança Computacional, em uma ocasião diversa, o mesmo também poderá ser observado em relação a falhas de Segurança Computacional. Para detalhes sobre a ação coletiva antes mencionada relacionada ao caso Boeing 737 MAX 8, recomenda-se conferência de Vox Media (2019), Yahoo (2019), Australian Aviation (2019), Australian Corporation Broadcasting (2019) e Baler (2019).

¹⁸⁵ Acerca da responsabilização da Indústria de Software pela produção/fornecimento de software falho no tocante à Segurança, importa registrar, em termos jurídicos, na mesma linha das discussões sobre a responsabilidade da Indústria de Armas quando do uso de armas para o cometimento de crimes, a absoluta impossibilidade de subtração da responsabilidade com o emprego do argumento de que ela, a Indústria, não poderia ser acionada por atos indevidos praticados por terceiros porque não se está debatendo acerca de mau uso (uso para o cometimento de crimes), mas, sim, sobre uso regular que é afetado por deficiência intrínseca ao produto. Dito de outra forma, não se pode cogitar de incabível responsabilização da Indústria de Armas pelos homicídios cometidos com as armas que ela produz porque, fora das hipóteses de exclusão da culpabilidade (legítima defesa, estado de necessidade ou estrito exercício de dever legal), o uso de armas para a prática de homicídios é qualificado como mau uso. Se, no entanto, um indivíduo que tenha a posse legal de armas utiliza, em sua própria defesa pessoal (durante um assalto em sua residência, por exemplo), uma arma e esta arma

Com a mencionada hipotética proliferação de demandas judiciais e de ações de arbitragem, ficam as empresas/entidades produtoras de *softwares/serviços* em *software* sujeitas a prejuízos/perdas financeiras em virtude de potenciais condenações ao pagamento de indenizações por danos decorrentes da exploração de vulnerabilidades de segurança (UNIVERSITY BUSINESS, 2016).

Sob motivação real ou ficta de proteção da sociedade civil de um dado Estado a eventuais falhas de segurança em *software*, podem ganhar força iniciativas de questionável utilidade voltadas à limitação do acesso das empresas de *software* a mercados internacionais.

Invocando-se a proteção da coletividade, podem emergir e se tornar difundidos “selos e certificações de qualidade em segurança” que “atestem” o inatestável, ou seja, que, falaciosamente, propalem, como antes já mencionado, o que, formal e matematicamente, não pode ser demonstrado (a integral segurança de um *software*), induzindo a sociedade civil em erro. Sobre tal ponto, vale, mais uma vez, para se afastar, de pronto, ideias em sentido diverso, enfatizar que:

- não é possível, como antes já ressaltado, assegurar a segurança de nenhum *software*;
- se um selo/certificação sugerisse garantia de segurança no *software*, haveria, em verdade, falácia, sendo difundida convicção enganosa entre o público comum;
- no máximo, um selo/certificação poderia, talvez, na melhor hipótese, indicar uma preocupação com a Segurança ao longo de um processo de desenvolvimento, servindo, assim, apenas para registrar, perante a sociedade civil, que uma dada instituição produtora/fornecedora de *software* sabe que isso é sua responsabilidade também e está tentando fazer algo a respeito;
- não se mostra, em princípio, útil a criação e a divulgação de um “processo de desenvolvimento de *software* seguro” porque, como observado por Brooks

falha, há, sim, a possibilidade de se acionar a Indústria de Armas porque a arma não se prestou ao fim destinado, a arma, por deficiência dela, não tinha corte suficiente, se fosse arma branca, ou não disparou o projétil ao comando, se fosse arma de fogo, por exemplo.

¹⁸⁶ Especificamente no tocante a falhas de Segurança Computacional em *software*, importa destacar que, ainda que de forma incipiente, já tem havido iniciativas de judicialização voltadas à composição de danos. Isso se observa, por exemplo, quando se consideram as demandas envolvendo a Intel (WARREN, 2018; CLARK, 2018, WALTON, 2019), ADT Home Security (TOP CLASS ACTIONS, 2018), Microsoft (WIRED, 2003), Lenovo-Superfish (HALFACREE, 2019; SEALS, 2018), Hewlett-Packard (Glynn, 2011), Jeep (MCCARTHY, 2019) e a Symantec (SCHUBERT JONCKHEER & KOLBE, 2018), bem como a Adobe e diversas instituições de ensino superior (UNIVERSITY BUSINESS, 2016). Estas ações, contudo, não tiveram, na mídia, a mesma exposição que vem tendo o referido caso da aeronave Boeing. Tivessem tido a mesma divulgação entre o público comum, o volume de autores e lides, provavelmente, seria maior.

(1987), “não há bala de prata” e porque, como demonstra a História da Computação, processos veem e vão, ficando, em realidade, o que verdadeiramente importa, a essência de suas ideias e propósitos, que, obviamente, não se mostram, de plano, como incompatíveis com qualquer que seja o processo de desenvolvimento de *software* adotado por uma instituição;

- a Indústria de *Software*, quando desconsidera a Segurança ao longo do processo de desenvolvimento, não tem, ademais, a sua responsabilidade elidida pela mera existência, no mercado, de outras instituições/empresas que se dedicam, quando contratadas, a identificar vulnerabilidades de segurança em *software*. Quem produz/fornece algo é, em termos jurídicos e éticos, responsável pelo que faz e as suas falhas não podem ser tidas como inexistentes apenas porque haveria, hipoteticamente, outros entes que pudessem identificar estas falhas. Não é possível, de forma direta e sem questionamento, a transferência desta responsabilidade porque se está falando de empresas/instituições distintas e que não se confundem (empresa produtora/fornecedora de *software* e empresa de Segurança Computacional) e porque as empresas de Segurança Computacional, como antes já salientado, não podem assegurar a segurança de nada, limitando-se a buscar vulnerabilidades e a apontar as vulnerabilidades que encontrar aos seus clientes, quando contratadas para tanto¹⁸⁷;
- não sendo, pois, as empresas de Segurança Computacional passíveis de responsabilização por vulnerabilidades em *software*, não haveria, por fim, qualquer utilidade real em se divulgar, por exemplo, que o *software* produzido pela empresa “X” teria sido auditado/examinado pela empresa de Segurança Computacional “Y”.

Feitas as observações *supra*, vale anotar, ainda, sob o manto dos

¹⁸⁷ Ilustrando o que ocorre no mundo real, imaginem-se, por exemplo, a empresa “X” produtora/fornecedora de *software* e a empresa “Y” atuante no segmento de Segurança Computacional. A empresa “X”, por um motivo qualquer, resolve contratar a empresa “Y”, para avaliar a Segurança do *software* que ela produz. Não sendo, como destacada anteriormente, factível a garantia de Segurança, a empresa “Y” se limita a tentar identificar vulnerabilidades de segurança no *software* e a apontar as vulnerabilidades que identificar à sua cliente, a empresa “X”. Em seu trabalho, a empresa “Y” poderia, por exemplo, ter encontrado apenas as vulnerabilidades “A”, “B” e “C”, comunicando a empresa cliente sobre a existência destas vulnerabilidades. O fato de a empresa “Y” ter encontrado somente as vulnerabilidades “A”, “B” e “C” não implica inexistência de outras vulnerabilidades, ou seja, não afasta, de forma alguma, a possibilidade de um outro ente/indivíduo qualquer (um *hacker*, por exemplo) identificar outras vulnerabilidades e vir a explorá-las. Não afastada a possibilidade de existência de outras vulnerabilidades, não se pode, sem leviandade, afirmar que o *software* em debate é seguro. Pode-se apenas dizer que nele não foram encontradas as vulnerabilidades “A”, “B” e “C”. Não pode, assim, a empresa “Y” atestar a segurança do *software* produzido pela empresa “X”.

referidos “selos e certificações em segurança de *software*”, a possibilidade de surgimento de monopólios e cartéis na Indústria de *Software*, aniquilando-se as oportunidades de estruturação de novos empreendimentos desenvolvedores de *software* e se instalando um estado de controle e dominação decorrente de eventual irreversível dependência/sujeição coletiva aos monopólios e cartéis mencionados.

Por fim, cumpre salientar, também, a possibilidade, em âmbito internacional, de estabelecimento de descabidas reservas protecionistas de mercado fundadas na falsa premissa de “garantia da Segurança no *software*”¹⁸⁸.

A identificação das potenciais nocivas repercussões antes referidas não é tarefa difícil nem mesmo para o dito “homem médio”/“homem comum”, já tendo sido antevista, em um contexto inespecífico sem foco específico na Segurança, por Meira, Burégio, Borba, Garcia, Albuquerque e Soares (2016), quando consignada a necessidade de se atentar ao Primeiro Mandamento da Engenharia de *Software*. Para se perceber a nocividade em debate, basta se examinar global e retrospectivamente a história da Indústria como um todo que se chega às hipóteses brevemente apontadas.

Por todo o exposto nesta Seção, percebe-se, em síntese, que a manutenção da conduta atual da Indústria de *Software* no tocante à Segurança Computacional pode provocar efeitos adversos a ela própria, com o favorecimento de:

- ações voltadas ao licenciamento das profissões relacionadas ao desenvolvimento de *software*;
- iniciativas externas de regulação¹⁸⁹;
- estigmatização e pública execração dos profissionais que lidam com o desenvolvimento de *software*;
- perdas empresariais de participação em determinados mercados¹⁹⁰;

¹⁸⁸ Em retrospectiva análise da realidade brasileira, não é difícil constatar que o protecionismo e a reserva de mercados, a despeito da eventual legitimidade de seus propósitos e do teórico favorecimento do Estado protecionista (GRAU, 1990), em alguns casos, não resultam benefícios nem mesmo para o próprio ente instituidor. Isso se observa, por exemplo, quando se consideram alguns dos deletérios efeitos colaterais decorrentes da Lei nº 7.232/84 (BRASIL, 1984), já que não considerado o potencial do mercado externo para a vazão de eventual produção nacional (O ESTADO DE SÃO PAULO, 2014) (ISTO É DINHEIRO, 2009) e que irreversível o estabelecimento de mercados transnacionais com a globalização (IKEHARA, 1997).

¹⁸⁹ Embora exista entidade, como a Thales eSecurity, que sugira haver uma possível boa receptividade e aceitação da Indústria de *Software* a iniciativas regulatórias (THALES, 2018), não se evidencia, de plano, em contato direto com desenvolvedores de *software*, a aceitação mencionada, ao menos não em âmbito interno.

- proliferação de demandas judiciais voltadas à composição de danos decorrentes de *software* falho no tocante à Segurança;
- sujeição da Indústria de *Software* ao pagamento de indenizações por danos originados do uso dos produtos/serviços que oferece;
- limitações de acesso a mercados internacionais com a definição de reservas protecionistas de propósito verdadeiro questionável;
- surgimento de monopólios e cartéis na Indústria de *Software*;
- estagnação da sociedade civil por irrestrita irreversível dependência dos citados potenciais monopólios e cartéis.

É, assim, chegado o momento de uma mudança na Indústria e esta mudança é urgente porque a inércia, neste caso, pode favorecer, entre outros, os pontos já mencionados, temas que, obviamente, não interessam a todos os atores envolvidos na produção de *software*. É chegado o momento da Engenharia de *Software* Ética, especialmente no tocante à Segurança Computacional.

Antes, contudo, de se passar, no Capítulo 8, a discorrer sobre a Engenharia de *Software* Ética relativamente à Segurança, importa consignar que não se teve, ao longo deste Capítulo 7, de forma alguma, o propósito de se denegrir a Engenharia de *Software*, a Indústria de *Software*, a Academia ou os desenvolvedores, ao se definirem os provocativos subtítulos das Seções que integram este Capítulo. Utilizaram-se subtítulos ácidos e graves porque, a despeito de parte dos agentes envolvidos atuar diligentemente, os ácidos subtítulos mencionados se mostram pertinentes e apropriados quando considerado o vulto das vulnerabilidades de *software* identificadas e suas potenciais repercussões. O mesmo há de ser dito no tocante às ideias expostas ao longo do Capítulo.

Por mais áridas, desagradáveis e de difícil assimilação que sejam as críticas construídas neste Capítulo, há pertinência e propriedade. Não mais é possível ignorar a (in)segurança no *software* e a mudança desse *status*, como antes mencionado, é urgente, apesar de, obviamente, esta mudança envolver, sim, despesas para a própria Indústria, a qual teria, é claro, que incluir em seus custos de produção os gastos decorrentes do desenvolvimento de *software* com foco na

¹⁹⁰ Para maiores informações sobre os diversos custos (custos com perdas de participação em mercados, inclusive), para as empresas em geral, decorrentes da exploração de vulnerabilidades de segurança em *software*, indica-se análise feita pelo Ponemon Institute (2017).

Segurança, como:

- despesas com contínua capacitação de seus profissionais no tocante à Segurança;
- possível maior custo global do processo produtivo de desenvolvimento de *software* em razão de possível menor agilidade, dada a necessidade de a Segurança ser considerada ao longo de todas as fases de construção do *software*;
- despesas com a contratação de auditorias externas para avaliação dos *softwares* produzidos;
- gastos adicionais para a eventual revisão do *software*, caso encontradas, em auditorias externas, vulnerabilidades que mereçam tratamento.

Estes custos e despesas, todavia, não constituiriam, por si mesmos, escudos para se rechaçar a indispensável mudança em debate porque, evidentemente, seria consequência natural o seu repasse ao valor final do produto/serviço de *software*, tal como ocorre em todas as demais Engenharias e segmentos econômicos. Como se diz em algumas nações, *“there is no such a thing as a free lunch”* e, em se tratando de atividade comercial e produtiva, não se espera caridade ou prejuízo para quem produz/fornece um bem/serviço.

Ilustrando este ponto, tem-se, por exemplo, o caso da Construção Civil. Uma empresa construtora de apartamentos, em suposto benefício da redução do preço final das unidades habitacionais e de uma consequente maior facilidade de comercialização destas, não poderia/não deveria, por exemplo, subdimensionar a estrutura de um edifício de médio porte, deixando, hipoteticamente, de realizar a avaliação do solo, de elaborar as fundações e de utilizar aço de boa qualidade nos pilares, cogitando seus diretores/gerentes, íntima e previamente, da eventual possibilidade, caso acontecesse algum sinistro e a edificação desabasse, de pagar ínfimas somas a potenciais prejudicados em demorados processos indenizatórios. Ainda que esta ideia pudesse, em termos imediatistas, parecer mais atrativa à construtora hipotética, esta conduta não seria correta. A construtora deveria, sim, preparar boas estruturas, mas incluir, por óbvio, as despesas pertinentes no preço final da unidades habitacionais.

Do mesmo modo, um dentista, em prol do barateamento e da redução

última do custo para os seus pacientes, não deveria, salvo situação extraordinária (paciente toxicômano que não deve se expor a certos tipos de drogas, v.g.), realizar um tratamento de canal sem qualquer anestesia/sedação. O suposto dentista deveria, sim, utilizar anestesia/sedação para que o paciente não sentisse dor, incluindo tais despesas no preço do tratamento.

Similarmente, um cirurgião não deveria deixar de utilizar luvas em um procedimento sob a escusa de economizar material, tendo, é claro, que utilizar as mencionadas luvas para preservação da integridade sua e de seu paciente e que incluir os custos com a aquisição das citadas luvas no valor final da cirurgia.

Da mesma forma que em todos estes exemplos, uma empresa produtora/fornecedora de *software* não deveria, diante das potenciais nocivas repercussões da insegurança, desconsiderar a Segurança Computacional porque isso encareceria o seu produto/serviço final. O legitimamente esperado desta empresa seria considerar a Segurança em seu processo de desenvolvimento e embutir os custos decorrentes no preço do *software*/serviço em *software*¹⁹¹.

¹⁹¹ Imposta destacar que a o tema relativo aos custos para o desenvolvimento de *software* sem preterição da Segurança não se inseriu no objeto da investigação ora relatada, de modo que a sua menção, nesta seção, foi feita exclusivamente para se afastar, por completo, qualquer possível utilização de tal ponto com vistas à exclusão/minimização de eventual falta da Indústria de *Software*. Independentemente dos custos envolvidos, faz-se o repasse no preço final, não havendo, pois, que se cogitar de pseudojustificativa para a desconsideração da Segurança.

8 SEGURANÇA & DESENVOLVIMENTO ÉTICO DE *SOFTWARE*

8.1 HOUSTON, NÓS PODEMOS TER UM PROBLEMA

Com a análise das considerações expostas no Capítulo 7, infere-se que, para a mudança de paradigma necessária à construção da Engenharia de *Software* Ética relativamente à Segurança, dois fatores são indispensáveis:

- o reconhecimento da importância dos requisitos de Segurança pela Academia e pela Indústria de *Software*, bem como o adequado tratamento dos requisitos de segurança ao longo do processo de desenvolvimento;
- uma modificação na conduta de desenvolvedores e da Indústria de *Software* como um todo, de modo a se ter a Ética como uma constante em todo e qualquer processo que repercute no desenvolvimento do *software*.

O tratamento de tais temas não é questão trivial e envolve não apenas a aquisição, a difusão e a utilização de conhecimento sobre Segurança Computacional. O tratamento em debate envolve, essencialmente, o agir correto, o agir adequado, o agir voltado não somente à satisfação de interesses exclusivamente pessoais dos que fazem a Indústria de *Software*. O agir em debate envolve a Ética. O agir em debate envolve, especialmente, atenção à Ética Profissional.

Em uma era em que há *software* em todo lugar e em que “tudo é *software*” (MEIRA, 2008), os profissionais que atuam nos domínios na Engenharia de *Software* desempenham um relevante papel social devido às potenciais consequências e implicações de seu trabalho no mundo real. As suas condutas e os seus comportamentos são, então, de crucial importância social, o que justifica sua

Com foco em uma exploratória avaliação quantitativa acerca do prévio contato dos desenvolvedores de *software* sobre Códigos de Ética, conduziu-se, inicialmente, no presente estudo, um *survey* de escopo limitado, com um único objetivo: descobrir se as pessoas que desenvolvem *software* profissionalmente sabem, em geral, algo sobre Códigos de Ética (modelo de questionário empregado neste *survey* é apresentado no apêndice D) ¹⁹².

Para atingir tal objetivo, foi aplicado, através da Internet, um questionário a profissionais voluntários que desenvolvessem *software* diariamente e que também participassem como discentes em um programa de pós-graduação em Ciência da Computação (um programa de Mestrado e um programa de Doutorado). O citado questionário possuía apenas uma única questão:

Você já ouviu falar de algum Código de Ética, ou leu algum Código sobre esse assunto?

Almejando-se obter o maior número de respostas possível em uma reduzida fração de tempo (seis dias) ¹⁹³, este questionário foi anunciado como “O Menor Questionário do Mundo”. Esta estratégia foi empregada porque, em iniciativas

¹⁹² Há de se esclarecer que, no presente estudo, não se teve, de forma alguma, o propósito de se construir um panorama relativo às percepções éticas dos desenvolvedores de *software*, não se tencionando, pois, avaliar densamente suas valorações éticas pessoais e profissionais ao longo do processo de produção de *software*. A questão ética, nesta pesquisa, surgiu de forma incidental, quando se anteviu que práticas de parte da Indústria de *Software* e dos desenvolvedores que a integram, no tocante à Segurança Computacional e à evasão de responsabilidade em *EULAs/ToSs*, apresentavam, sim, um viés antiético, o que levou à constatação da utilidade de se saber se os desenvolvedores de *software* já tinham tido algum contato com algum Código de Ética, podendo, por conseguinte, realizar autoavaliações críticas de suas condutas. Ausente, assim, o propósito de mapeamento de percepções éticas dos desenvolvedores, incipiente, consoante revisão não sistemática realizada da literatura especializada, o interesse da Academia por tal questão e não frequentemente abordada a Ética Profissional nas publicações e pesquisas relacionadas à Engenharia de *Software*, optou-se, intencionalmente, por averiguar apenas do contato prévio dos desenvolvedores com algum Código de Ética. Obviamente, contudo, mostra-se útil a obtenção de maiores informações sobre as percepções éticas dos desenvolvedores de *software*, tema que, não se inserindo no objeto da pesquisa ora relatada, poderá ser objeto de trabalhos futuros.

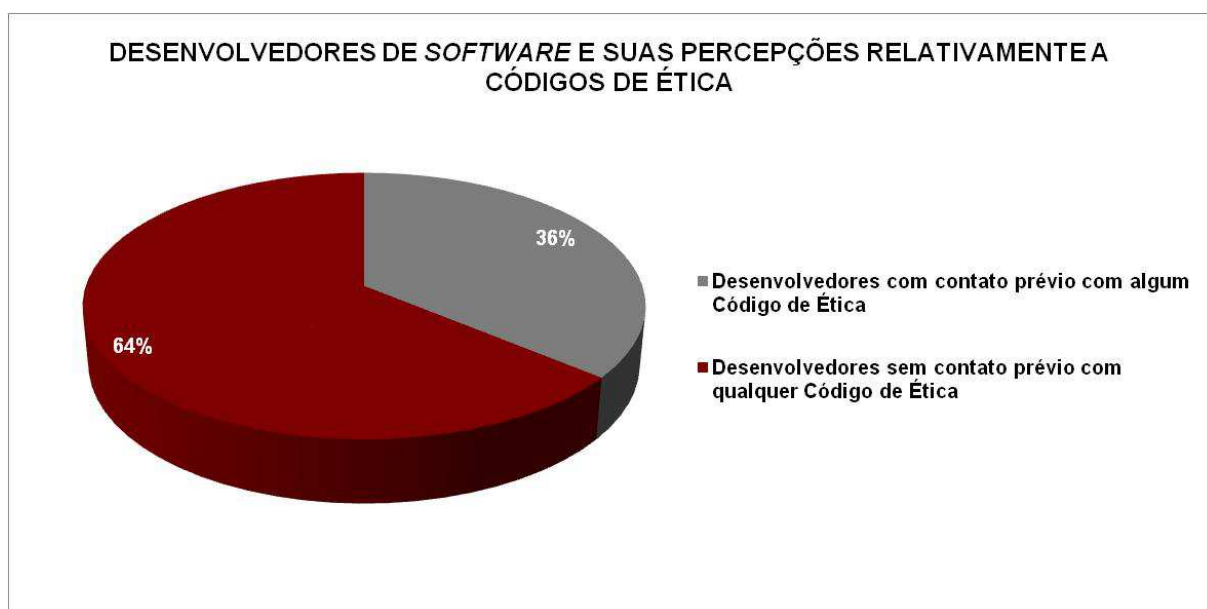
¹⁹³ Inicialmente, teve-se por objetivo coletar respostas aos questionários em um único dia, já que se tencionava aproveitar os dados eventualmente obtidos, caso expressivo o número de respostas, em artigo a ser submetido dois dias após este lapso e que já estava em elaboração. Como houve, extensão da data de submissão do artigo por alguns dias extras, manteve-se o formulário apto a receber respostas por alguns dias adicionais (seis dias no total), no período compreendido entre 7 e 12 de setembro de 2018. O artigo mencionado (“Houston, We may have a problem”) foi aceito em conferência organizada pela IEEE (13th Annual IEEE International Systems Conference – SYSCON 2019), tendo sido apresentado e publicado em abril de 2019 na cidade de Orlando/Fl.

prévias, observou-se que os respondentes-alvos tendiam a não responder questionários grandes.

Os dados coletados via questionário *web* foram tabulados na plataforma em que foi disponibilizado o acesso aos respondentes (Google Form®).

Com a tabulação, constatou-se que 103 (cento e três) desenvolvedores de *software* concordaram em participar voluntariamente do *survey* e que, como ilustrado no Gráfico 14, significativa parcela deles nunca havia tido qualquer contato com qualquer Código de Ética.

Gráfico 14 – Contato prévio dos desenvolvedores de *software* com algum Código de Ética.



Fonte: Autor (2019) ¹⁹⁴.

Como ilustrado no Gráfico 14, apenas 36% dos respondentes, profissionais que desenvolvem *software*, tiveram alguma espécie de contato com algum Código de Ética (qualquer Código de Ética e não necessariamente um Código de Ética relacionado às suas profissões). A grande maioria dos respondentes nunca ouviu falar e nem leu nada a respeito de qualquer espécie de Código de Ética, o que é preocupante quando se pensa sobre:

¹⁹⁴ Gráfico elaborado a partir da tabulação dos dados obtidos com a aplicação do questionário relativo às percepções dos desenvolvedores de *software* quanto à Ética.

- a natureza ubíqua do *software* atualmente;
- a importância do *software* nas atividades diárias do público em geral, bem como nas atividades de diversos segmentos econômicos;
- a inexistência de regulamentação/licenciamento para algumas profissões atuantes na Indústria de *Software*;
- a existência de um Código de Ética especialmente direcionado aos profissionais que desenvolvem *software* (o Código de Ética IEEE/ACM para a Engenharia de *Software*), que não é conhecido pela grande maioria dos participantes no *survey*¹⁹⁵.

Uma explicação inicial para este desconhecimento dos desenvolvedores de *software* quanto a Códigos de Ética em geral e, em especial, para a sua falta de familiaridade com um Código especialmente relacionado ao seu trabalho (o já referido Código de Ética IEEE/ACM para a Engenharia de *Software*, por exemplo) poderia envolver uma omissão na Academia.

Poderia se pensar que estes profissionais não saberiam nada a respeito de Ética porque isso não lhes foi ensinado, porque não lhes foi dada a oportunidade formal de travar uma experiência intelectual relacionada à Ética e a seus Códigos. Estes profissionais, de maneira similar às pessoas aprisionadas na caverna da Alegoria de Platão (PLATÃO, 2013), não poderiam compreender a realidade relacionada à Ética porque, ao longo de suas existências, esta realidade não se apresentou perante os mesmos. Nas sombras de um currículo restritivamente técnico, os desenvolvedores de *software* teriam, então, estado condenados a vivenciar apenas uma parte da realidade: o conhecimento técnico diretamente ligado à Engenharia de *Software*. Embora, obviamente, seja essencial a estes profissionais o domínio de aspectos técnicos de seus trabalhos, não se pode negar que a

¹⁹⁵ Como já consignado na Seção 6.3, ao se destacar a existência do Código de Ética IEEE/ACM para Engenharia de *Software*, não se está a desconsiderar que existem outros relevantes Códigos de Ética nos domínios da Computação. Ocorre, como já consignado na citada Seção, que tais Códigos não se destinam especialmente à Engenharia de *Software* e, tendo sido produzidos por entes locais, não apresentam potencial de imediata aplicação internacional, dada, é claro, a necessidade de se respeitar as soberanias estatais. Ademais, o Código de Ética IEEE/ACM, em verdade, é constituído por um conjunto de princípios, sendo, pois, atemporal, e apresenta legitimidade na Academia e na Indústria, já que, em sua elaboração, foi assegurada a oportunidade de participação social através dos próprios associados do IEEE e da ACM.

ignorância no tocante à Ética os priva de uma integral percepção da realidade e de uma completa compreensão sobre as potenciais consequências de suas condutas profissionais.

A referida hipótese de omissão da Academia, todavia, foi parcialmente descartada quando foram examinados os currículos de 115 (cento e quinze) cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de 64 (sessenta e quatro) instituições de ensino nacionais¹⁹⁶.

A análise curricular (diretrizes no apêndice H) revelou que, correntemente, no Brasil, há disciplinas envolvendo Ética na maioria dos cursos de graduação considerados, como exposto na Tabela 8 e no Gráfico 15.

Tabela 8 – Disciplinas obrigatórias com conteúdo relativo à Ética em cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação.

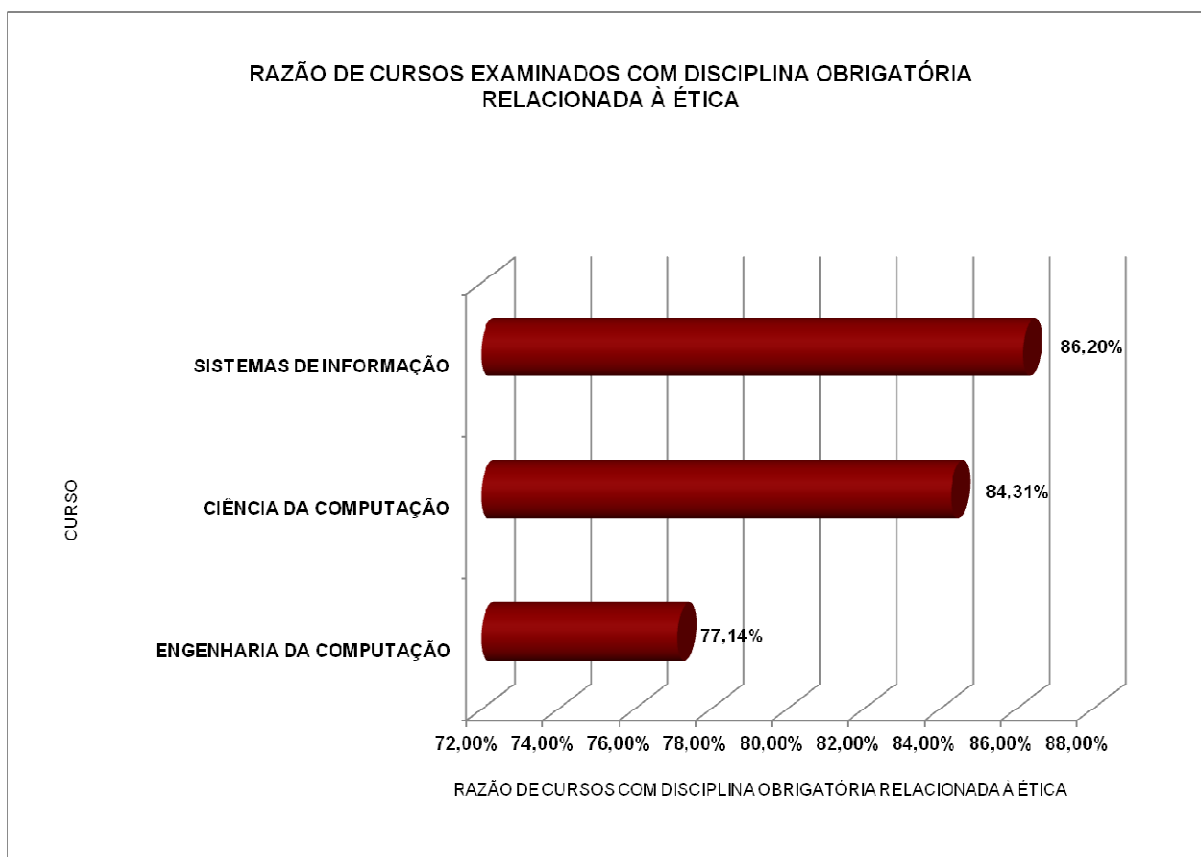
DISCIPLINAS OBRIGATÓRIAS COM CONTEÚDO RELATIVO À ÉTICA EM CURSOS EXAMINADOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO		
CURSO DE GRADUAÇÃO	QUANTITATIVO DE CURSOS COM DISCIPLINA OBRIGATÓRIA ABRANGENDO NOÇÕES DE ÉTICA	QUANTITATIVO DE CURSOS SEM DISCIPLINA OBRIGATÓRIA RELACIONADA À ÉTICA
Ciência da Computação	43	08
Engenharia da Computação	27	08
Sistemas de Informação	25	04

Fonte: Autor (2019) ¹⁹⁷.

¹⁹⁶ A definição de tal amostra se fez com a consideração da mesma estratégia eleita para o levantamento de documentos atinente às disciplinas com conteúdo relativo à Segurança Computacional, referida na Seção 4.2. Ou seja, optou-se por avaliar o “melhor cenário”, analisando-se as grades e as disciplinas de cursos de instituições nacionais de ensino que mantivessem, junto à CAPES, programas de pós-graduação.

¹⁹⁷ Tabela construída a partir dos dados obtidos no *survey* relativo às percepções dos desenvolvedores de *software* quanto a Códigos de Ética.

Gráfico 15 – Razão de cursos de graduação examinados com disciplinas obrigatórias relacionadas à Ética.



Fonte: Autor (2019) ¹⁹⁸.

Se, como exposto no Gráfico 15, mais de 77% dos cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação possuem alguma disciplina obrigatória relacionada à Ética em seus currículos, seria esperado, então, que um significativo número de desenvolvedores de *software* tivesse tido ao menos um contato inicial com a Ética e com algum Código de Ética voltado à sua profissão. Esta expectativa, contudo, não se mostra como uma realidade de fato, já que os resultados obtidos no *survey* referido no início desta Seção indicam o oposto.

Ainda, se, de acordo com a análise curricular das grades atuais, um grande número de desenvolvedores deveria ter travado algum tipo de contato com Códigos de Éticas direcionados a suas profissões, poderia se pensar que:

- no passado, noções de Ética podem não ter feito parte da grande maioria dos

¹⁹⁸ Gráfico elaborado em função dos dados apresentados na Tabela 8.

currículos dos cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação;

- os currículos podem ter evoluído e, agora, há disciplinas obrigatórias com conteúdo relativo à Ética na maioria dos cursos em discussão.

Mesmo que uma grande parte dos profissionais que lidam com *software* conclua seus cursos e graduação após ter algum contato com disciplinas com conteúdo ético, há um número incerto de desenvolvedores que terminaram e ainda terminam seus cursos sem, formalmente, saber nada sobre Ética. Neste contexto de desconhecimento e de incerteza, não seria leviano se afirmar algo como: “Houston, nós podemos ter um problema”. Se a sociedade atual é dependente de *software* e se pode haver um elevado e incerto número de profissionais que não tenham adquirido qualquer conhecimento formal sobre Ética, há, por consequência, um grande problema. Este problema é evidente porque:

- na ausência deste conhecimento, as condutas dos desenvolvedores de *software* dependem exclusivamente das consciências pessoais de cada profissional e porque, como demonstra a História Humana, as consciências pessoais variam amplamente e podem causar grandes impactos aos indivíduos e à sociedade em geral;
- ainda quando as pessoas agem de acordo com suas “consciências” e, seguindo alguma corrente filosófica, acreditam estar fazendo o que é “certo” para um determinado grupo, persistem riscos para a sociedade como um todo e nocivos eventos inaceitáveis podem se consumir. Isso é o que ocorreu, por exemplo, quando, em um determinado país, um “seleto grupo”, almejando construir uma “nação melhor para seus cidadãos” decidiu se filiar a certas ideias utilitaristas (STANFORD, 2014), promovendo extermínio em massa em campos de concentração;
- se grande parte do *software* é produto do trabalho coletivo, a conduta antiética de um único profissional pode “contaminar” o processo de desenvolvimento, outros profissionais de desenvolvimento e o próprio produto final;
- apesar da adoção das teorias que advogam em favor da inaceitabilidade da responsabilização individual do trabalhador em alguns casos (FLORES,

JOHNSON, 1983), há sempre a possibilidade de responsabilização legal do empregador, o que, certamente, não é desejado por nenhum empreendimento;

- em um momento de grande mobilidade entre profissionais de *software* e de mercados globais, *software* deficiente produzido de forma antiética em um país pode provocar consequências internacionais, afetando até mesmo países em que a produção de *software* é eticamente engajada.

8.2 PROPOSIÇÃO PARA O DESENVOLVIMENTO ÉTICO DE *SOFTWARE* NO TOCANTE À SEGURANÇA COMPUTACIONAL

Neste cenário de desconhecimento, de incerteza e, conseqüentemente, de insegurança no *software*, medidas globais são necessárias para mitigação e minimização dos riscos associados a potenciais práticas ruins de engenheiros/desenvolvedores de *software* em todo o mundo e, se o problema, em parte, está na Academia, a solução também nela pode se originar.

Ainda que a oferta de disciplinas com conteúdo ético não assegure um comportamento ético por parte de engenheiros e ainda que haja várias críticas a algumas estratégias de ensino adotadas em disciplinas de tal natureza (ensino focado em processo de decisão individual & ensino focado em processo de decisão contextual, por exemplo) (BUCCIARELLI, 2008) (DAVIS, 2006), a oferta em debate pode proporcionar aos desenvolvedores de *software* um arcabouço de conhecimentos que lhes permita pensar por si mesmos em termos éticos (POEL, ZANDVOORT, BRUMSEN, 2001). Por esta razão macroscópica, o estudo e o ensino da Ética são recomendados por algumas organizações. Nos Estados Unidos da América, por exemplo, esta é a recomendação geral do Accreditation Board for Engineering and Technology (ABET) (BUCCIARELLI, 2008).

O ensino de disciplinas com conteúdo sobre Ética para engenheiros poderia, como observado em Bioética (BAUM, 1980) (TURINE; TURINE; MASIERO, 2000), auxiliar na melhoria deste contexto de desconhecimento ético porque um conhecimento formal mínimo sobre Ética:

- favoreceria a imaginação ético-moral;
- contribuiria para o reconhecimento de questões éticas;
- estimularia o desenvolvimento das competências analíticas necessárias para se

lidar com questões éticas em uma base diária;

- ajudaria na formação de um senso moral de responsabilidade;
- auxiliaria na redução e na tolerância de divergências ético-morais e de ambiguidades.

Por todas estas razões, o Ensino pode vir a ser uma relevante ferramenta na difusão da Ética entre os engenheiros de *software*. Este ensino, como observado previamente em outros trabalhos (POEL, ZANDVOORT, BRUMSEN, 2001), poderia se dar sob uma abordagem multidisciplinar e de diversas formas como, por exemplo, tutoriais gratuitos, *workshops*, cursos livres e disciplinas de conteúdo ético inseridas como obrigatórias nos currículos dos cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação. Esta abordagem miscelânea poderia, assim, também ajudar a solucionar o problema da “falta de familiaridade” com a Ética enfrentada pelo conjunto de desenvolvedores de *software* que se encontram no mercado atualmente e que, tendo terminado suas graduações tempos atrás, não tiveram um contato prévio com tal tema.

Caso a oferta de um denso referencial teórico sobre Ética não se mostrasse viável ou necessária na percepção da Indústria e da própria Academia, um conhecimento mínimo e indispensável poderia ser propagado através do ensino e da divulgação de Códigos de Ética. A questão que se coloca, em tal hipótese, é simples: Qual Código de Ética deveria ser adotado, ensinado e difundido mundialmente?

Atualmente, a definição e a adoção de Códigos de Ética constituem, por si mesmas, um problema próprio devido à globalização (GORNIÁK-KOČIKOWSKA, 1996). Nos domínios da Engenharia de *Software*, este problema também é real e uma potencial solução para ele envolveria a adoção e a difusão de um Código de Ética para Engenharia de *Software* aprovado por entidades profissionais reconhecidas mundialmente. Uma solução para este problema poderia envolver o emprego do Código de Ética para Engenharia de *Software* estabelecido pelo Institute of Electrical and Electronic Engineering (IEEE) e pela Association for Computing Machinery (ACM) em 1999.

De certo que o ensino se mostra como apenas uma parte do trabalho a ser realizado, já que uma entusiástica cultura ética também deveria ser promovida. Ensinar por ensinar, certamente, não implica solução plena. Engajamento e

comprometimento são essenciais e, por esta razão, estratégias adicionais poderiam ser necessárias (medidas de socialização, por exemplo), considerado o grau de envolvimento identificado nos heterogêneos ambientes da Academia e da Indústria.

As ideias até o momento expostas no tocante à Ética (miscelânea abordagem para difusão de noções de conteúdo ético e promoção de cultura própria na Academia e na Indústria) aplicam-se, de forma similar, também, à própria Segurança Computacional.

Se a Segurança Computacional, de forma irreversível, é vital para a sociedade civil e se os resultados da presente pesquisa sugerem que não vem sendo dada a devida atenção a tal tema (grande número de vulnerabilidades em *software* de distintos segmentos, relegação dos requisitos de Segurança e desconhecimento usual dos desenvolvedores sobre questões a ela pertinentes, por exemplo) , é importante que trabalho semelhante ao voltado à difusão de noções sobre Ética também se realize em relação à Segurança¹⁹⁹.

Contatou-se uma lacuna na Academia, já que expressivo número dos cursos, cujas grades atuais foram consideradas na pesquisa, não apresentam disciplinas obrigatórias de Segurança em sua estrutura. Observou-se que, para os profissionais que saíram da Universidade há mais tempo, provavelmente, o desconhecimento sobre Segurança é ainda maior, ressalvada, contudo, a possibilidade de individual superação do desconhecimento através de autodidatismo. Verificou-se que a Segurança é preterida na Indústria, não se podendo afastar a hipótese de tal relegação decorrer, também, do desconhecimento da importância da Segurança, consideradas suas potenciais repercussões.

Para uma modificação significativa de paradigma no desenvolvimento de *software*, faz-se necessário, então, atacar duas frentes principais na Academia e na Indústria, difundindo-se, simultaneamente, conhecimento sobre Ética e sobre Segurança. Medidas isoladas não se mostram suficientes à resolução do problema da insegurança nos *softwares*. Esforços coordenados têm que ser empreendidos e é preciso que estes esforços se iniciem com o reconhecimento, pela própria Academia e pela própria Indústria de *Software*, da necessidade de mudança, sob pena de

¹⁹⁹ Vale salientar, neste ponto, que não se está a sugerir/propor o ensino de uma única disciplina com conteúdo miscelâneo relativo à Ética e à Segurança. Defende-se o ensino de duas autônomas disciplinas porque ambas são relevantes e apresentam, individualmente, conteúdo significativo para um curso independente. A autonomia referida não impede, contudo, que, em cada uma destas disciplinas propostas, aborde-se, com finalidade ilustrativa, tema pertinente da outra.

ambas e a sociedade civil como um todo, pelas razões já mencionadas em seções de Capítulo precedente, arcarem com custo elevado demais.

É, indubitavelmente, necessário um plano de ação, uma estratégia com objetivos de curto, médio e longo prazo, uma “agenda” para tornar o desenvolvimento de *software* ético no tocante à Segurança Computacional.

Não se faz, neste estudo, a imposição do plano mencionado porque, em verdade, para uma efetiva adesão às suas hipotéticas ideias, faz-se necessário o envolvimento/engajamento/alinhamento de todos os atores atuantes no desenvolvimento de *software*, o que não é algo simples de se obter.

Como forma de motivar os envolvidos a efetivamente participar de uma mudança real no tocante à Segurança no desenvolvimento de *software*, propõe-se que o plano em discussão se construa pelos próprios interessados principais (Academia e Indústria, especialmente), que, esclarecidos sobre o panorama atual exposto ao longo deste trabalho, reconheçam a importância de superação do *status quo ante*, deliberem, em conjunto por si mesmos, sobre o que fazer e ajam concretamente.

A construção da estratégia em debate deve partir da própria Academia e da Indústria de *Software* porque o seu envolvimento real é essencial e porque é mais provável que um ente/pessoa se envolva verdadeiramente com algo do qual tenha a oportunidade de participar da concepção, apontando, inclusive, eventualmente, pontos carecedores de atenção para a sua efetiva concretização. A imposição externa de uma agenda de mudança, elaborada sem a participação dos citados atores, não produziria, definitivamente, o mesmo efeito²⁰⁰.

²⁰⁰ Ilustrando-se a necessidade de conjunta construção de estratégias pelos agentes potencialmente envolvidos, cita-se caso em domínio diverso a respeito do qual o pesquisador teve conhecimento por mero acaso através de um contato. Em uma unidade hospitalar inominada, um iluminado indivíduo em posto de gestão, imbuído de excelentes intenções mas desconhecedor da realidade enfrentada pela equipe de médicos (cirurgias gerais habilitados à realização de qualquer procedimento), ao quedar ciente de um grande represamento de pacientes a depender de cirurgias, resolveu, sem qualquer consulta à aludida equipe de médicos, que atribuiria a cada um dos médicos um caso cirúrgico semanal extra, eleito em função da adução de pedido de prioridade pelo paciente. Em princípio, tal medida pareceria apropriada, já que se trataria de casos prioritários e que viria a reduzir, em um menor tempo, o citado represamento. Ocorre, contudo, que o mencionado gestor, não sendo médico, não detinha conhecimento para saber o que era prioritário, terminando por assim qualificar qualquer caso de paciente que perante ele comparecesse e pedisse urgência na realização do seu procedimento cirúrgico. Os inúmeros pleitos de prioridade passaram, então, a ser repassados sem qualquer critério técnico à equipe de médicos, os quais, independentemente dos pacientes que já estivessem a atender, teriam que encontrar uma forma de realizar, também, um controvertido procedimento extraordinário semanal. Quando os pleitos de prioridade começaram a ser recebidos por cada médico da equipe, condutas individuais diferentes foram observadas. Alguns dos médicos, por razões diversas, acabaram por acatar integralmente a determinação do gestor, deixando, com isso, de dar o atendimento necessário aos pacientes que já tinham, i.e., para atender também aos pacientes ditos prioritários, estes médicos tiveram que ser menos detalhistas com os seus demais pacientes, mesmo quando a situação destes (carcinomas metastáticos em avançados graus) fosse, em verdade, mais grave que a dos supostos pacientes prioritários (lipoaspirações e reduções de estômago em pacientes sem

Ainda que o pesquisador, por todo o exposto, verdadeiramente acredite que uma solução efetiva para o problema da insegurança no *software* deva ser produzida coletivamente pelos agentes interessados (Academia, Indústria de *Software* e desenvolvedores, em essência) e que a unilateral produção e imposição de um plano de ação por quem não fosse implementá-lo concretamente e não tivesse o preciso conhecimento dos recursos disponíveis se constituiria em mero desperdício de recurso, entende-se por pertinente, neste documento, para se afastar eventuais equivocadas impressões de que a investigação ora relatada teria sido produzida na flutuante ilha de Laputa (SWIFT, 2011), por apresentar um plano de ação mínimo e hipotético, que, sem a utópica pretensão de resolver por si próprio o problema em debate, servisse, simplesmente, de base/diretriz para a eventual elaboração da solução coletiva antes mencionada.

No Quadro 44, apresenta-se tal plano, cabendo registrar, contudo, que, quando de sua concepção, ele foi idealizado como mera diretriz para um projeto piloto a ser implementado localmente na cidade do Recife, devendo, antes de sua potencial extensão a outros centros, ser avaliado para a averiguação da necessidade de ajustes.

qualquer grau de obesidade mórbida ou doença associada). Tais médicos, em princípio, mostraram-se, perante o gestor, como diligentes e comprometidos. Outro grupo de médicos, contudo, analisando os casos que tinham em suas mãos, não pôde desconsiderar a verdadeira doença que acometia seus pacientes e, percebendo que as doenças destes pacientes era realmente mais severa e crítica que a dos pretensos pacientes prioritários, desconsiderou, em benefício real dos doentes, a diretriz do gestor. Este conjunto de médicos, por deliberação dele mesmo, passou a agendar suas cirurgias com base em suas próprias percepções quanto à gravidade e à urgência do procedimento cirúrgico e, ao assim agirem, acabaram por não atender à determinação do gestor, ainda que o resultado último tenha sido melhor para os pacientes. O que se pretende ilustrar, com este exemplo, é que o plano de ação traçado de forma isolada pelo iluminado gestor não logrou êxito em seu intento porque não foi construído coletivamente ou, ao menos, com uma consulta aos agentes executores, os quais poderiam, se tivessem sido ouvidos previamente, indicar, diante da escassez de recursos (cirurgiões em número suficiente) e da inexistência de prioridade real para os que aguardavam procedimentos eletivos (lipoaspirações e reduções de estômago), a impropriedade da estratégia para o que deveria ser o verdadeiro objetivo deste hospital: o tratamento daqueles pacientes que, de fato, necessitassem de cirurgia. A estratégia, assim, por falta de adesão (ainda que legitimamente justificada a não adesão), não atingiu seu propósito e o represamento não deixou de existir. Tivesse o plano sido construído com a oitiva da equipe, provavelmente, outra solução teria sido desenvolvida, uma solução mais viável e factível.

Quadro 44 – Plano de ação mínimo para o tratamento do problema da insegurança no *software*.

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE				
ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
1º	FORMAÇÃO DE UM GRUPO DE TRABALHO INICIAL	Organização das atividades a serem empreendidas para melhoria do quadro de insegurança no <i>software</i>	Docentes e discentes da UFPE	05 (cinco) dias
2º	DIVULGAÇÃO, VIA E-MAIL OU OUTRA ESPÉCIE DE COMUNICAÇÃO ESCRITA, DA EXISTÊNCIA DO GRUPO JUNTO, ENTRE OUTROS ESTABELECIMENTOS, A: - INSTITUIÇÕES DO ENSINO DA CIDADE DO RECIFE QUE MANTENHAM CURSOS DE GRADUAÇÃO EM QUALQUER ÁREA - CONSELHOS PROFISSIONAIS EM ATUAÇÃO NA LOCALIDADE - SINDICATOS E ASSOCIAÇÕES DE	Divulgação das atividades do grupo e da importância do tema para todos os entes citados, com foco na ulterior captação de interessados na iniciativa	- Membros do grupo de trabalho - Voluntários	03 (três) dias

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	CLASSE • ÓRGÃOS PÚBLICOS FEDERAIS, ESTADUAIS E MUNICIPAIS LIGADOS À COMPUTAÇÃO • TRIBUNAIS FEDERAIS E ESTADUAL • SECRETARIAS/ ÓRGÃOS FAZENDÁRIOS (FEDERAL, ESTADUAL E MUNICIPAL) • HOSPITAIS PÚBLICOS E PRIVADOS • CENTRO DE ESTUDOS E SISTEMAS AVANÇADOS DO RECIFE • PORTO DIGITAL • EMPRESAS			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	PRODUTORAS/ FORNECEDORAS DE SOFTWARE • INSTITUTO DE TECNOLOGIA DE PERNAMBUCO • DEPARTAMENTO DE ESTADUAL DE TRÂNSITO • ADVOCACIA GERAL DA UNIÃO • PROCURADORIAS DO ESTADO E DO MUNICÍPIO DA CIDADE DO RECIFE • MINISTÉRIO PÚBLICO FEDERAL • MINISTÉRIO PÚBLICO ESTADUAL • ÓRGÃOS POLICIAIS			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	(FEDERAIS, ESTADUAIS E MUNICIPAIS) • INSTITUIÇÕES DO SISTEMA PRISIONAL (FEDERAL/ESTADUAL) • EMPRESA FORNECEDORA DE ENERGIA ELÉTRICA • EMPRESA FORNECEDORA DE ÁGUA • EMPRESAS DE TELEFONIA • EMPRESAS PROVEDORAS DE SERVIÇO DE ACESSO À INTERNET • EMPRESAS PRESTADORAS DE SERVIÇOS DE TELEVISÃO A CABO			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	• OPERADORAS DE RÁDIO E TELEVISÃO ATUANTES NA CIDADE • ENTES INTEGRANTES DO GOVERNO FEDERAL/ESTADUAL/MUNICIPAL EM GERAL • PROCON E ÓRGÃOS DE DEFESA DO CONSUMIDOR • ASSOCIAÇÕES DA INDÚSTRIA/COMÉRCIO • CENTRAIS DE ABASTECIMENTO DE ALIMENTOS • ESCOLAS PÚBLICAS/PRIVADAS • EMPRESAS CONTROLADORAS DAS INFRAESTRUTURAS			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	AEROPORTUÁRIA E PORTUÁRIA • EMPRESA CONCESSIONÁRIA DO AEROPORTO • EMPRESAS ATUANTES NO SEGMENTO DE DERIVADOS DE PETRÓLEO (POSTOS DE GASOLINA, INCLUSIVE) • EMPRESAS DE SEGURANÇA COMPUTACIONAL ATUANTES NA LOCALIDADE • GRANDES REDES DE COMÉRCIO E DISTRIBUIÇÃO DE BENS • INSTITUIÇÕES BANCÁRIAS			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	• SEGURADORAS • LABORATÓRIOS CLÍNICAS MÉDICAS E • LABORATÓRIOS CLÍNICAS VETERINÁRIAS E • ÓRGÃOS FEDERAIS E ESTADUAIS DE FOMENTO À AGROPECUÁRIA • INSTITUIÇÕES DE PESQUISA • ÓRGÃOS DA IMPRENSA OFICIAL FEDERAL, ESTADUAL E MUNICIPAL • INSTITUIÇÕES MANIPULADORAS DE MATERIAL NUCLEAR/ RADIOATIVO			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	• REDES HOTELEIRAS • EMPRESAS DE TRÁFEGO AÉREO, MARÍTIMO, FLUVIAL OU RODOVIÁRIO ATUANTES NA CIDADE DO RECIFE • EMPRESAS CONTROLADORAS DE TRÁFEGO AÉREO, MARÍTIMO, FLUVIAL E TERRESTRE • EMPRESAS DE TRANSPORTE PÚBLICO • EMPRESAS GESTORAS DOS SISTEMAS DE SEMÁFOROS DAS VIAS PÚBLICAS • ÓRGÃOS INTEGRANTES DA MARINHA, DO			

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO *SOFTWARE*

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
	EXÉRCITO E DA AERONÁUTICA • REPRESENTAÇÕES CONSULARES			
3º	DIVULGAÇÃO DA EXISTÊNCIA DO GRUPO JUNTO À SOCIEDADE CIVIL, APROVEITANDO-SE, PARA ISSO, DE EVENTOS COMO O REC'N'PLAY	• Divulgação do grupo e da importância da Segurança no <i>software</i> no mundo atual, despertando-se o interesse de eventuais interessados pelo tema	• Membros do grupo de trabalho • Voluntários	05 (cinco) dia
4º	CONVOCAÇÃO DE EVENTUAIS INTERESSADOS EM PARTICIPAR DO PROJETO	• Recrutamento de potenciais colaboradores para o projeto	• Membros do grupo de trabalho • Voluntários	02 (dois) dias
5º	DELIBERAÇÃO SOBRE A NECESSIDADE DE AJUSTE DAS GRADES CURRICULARES DOS CURSOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO NA CIDADE DO RECIFE	• Oitiva dos agentes interessados integrantes da comunidade acadêmica local, para a definição dos ajustes necessários	• Membros do grupo de trabalho • Voluntários • Representantes da Indústria de <i>Software</i> • Interessados eventuais sobre o projeto	03 (três) dias

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
6º	AJUSTE DAS GRADES CURRICULARES DOS CURSOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO OFERECIDOS NA CIDADE DO RECIFE, PARA QUE TAIS CURSOS OFERECEÇAM, AO MENOS, DUAS NOVAS DISCIPLINAS OBRIGATÓRIAS: UMA RELACIONADA À SEGURANÇA E OUTRA À ÉTICA	Inclusão, nas grades dos aludidos cursos, de disciplinas obrigatórias sobre Segurança e Ética, com o escopo de se propiciar a futuros profissionais, noções básicas sobre estes temas	- Membros do grupo de trabalho - Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife - Voluntários	06 (seis) meses
7º	CAPACITAÇÃO DO CORPO DOCENTE DAS INSTITUIÇÕES DE ENSINO LOCAIS PARA O OFERECIMENTO DAS DISCIPLINAS RECÉM-CRIADAS	Preparação dos docentes para atuação como agentes replicadores das ideias básicas sobre Segurança e Ética no desenvolvimento de <i>software</i>	- Membros do grupo de trabalho - Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife	02 (dois) meses

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO *SOFTWARE*

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
			• Docentes • Especialistas em Segurança Computacional • Representantes da Indústria de <i>Software</i> • Voluntários	
8º	OFERECIMENTO DAS DISCIPLINAS RECÉM-CRIADAS NAS INSTITUIÇÕES DE ENSINO SUPERIOR LOCAIS	• Promoção de noções mínimas sobre Segurança e Ética entre os profissionais do futuro	• Membros do grupo de trabalho • Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife • Docentes • Especialistas em Segurança Computacional • Representantes da	Indefinido, iniciando-se, no máximo, em até 12 (doze) meses da formação do grupo de trabalho

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO *SOFTWARE*

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
			Indústria de <i>Software</i>	
9º	ESTRUTURAÇÃO DE CURSOS DE CURTA DURAÇÃO, LIVRES GRATUITOS SOBRE ÉTICA E SEGURANÇA NO DESENVOLVIMENTO DE <i>SOFTWARE</i> A SEREM OFERTADOS SOB A FORMA DE PARCERIA/PATROCÍNIO COM AGENTES/INSTITUIÇÕES LOCAIS	• Elaboração de cursos para oferecimento aos indivíduos atuantes na Indústria de <i>Software</i> que já tenham concluído suas graduações	• Voluntários • Membros do grupo de trabalho • Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife • Docentes • Especialistas em Segurança Computacional • Representantes da Indústria de <i>Software</i> • Voluntários	01 (um) mês

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO *SOFTWARE*

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
10º	DIVULGAÇÃO DA OFERTA DOS CURSOS DE CURTA DURAÇÃO, LIVRES E GRATUITOS SOBRE ÉTICA E SEGURANÇA NO DESENVOLVIMENTO DE <i>SOFTWARE</i>	Recrutamento de interessados em participar dos cursos	- Membros do grupo de trabalho - Voluntários	01 (uma) semana a cada semestre
11º	OFERECIMENTO DOS CURSOS DE CURTA DURAÇÃO, LIVRES E GRATUITOS SOBRE ÉTICA E SEGURANÇA NO DESENVOLVIMENTO DE <i>SOFTWARE</i>	Difusão de noções mínimas sobre Ética e Segurança no desenvolvimento de <i>software</i>	- Membros do grupo de trabalho - Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife - Docentes - Especialistas em Segurança Computacional - Representantes da Indústria de <i>Software</i> - Voluntários	02 (duas) semanas para novas turmas a cada semestre

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO SOFTWARE

ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
12º	PROMOÇÃO DE JORNADAS SOBRE ÉTICA E SEGURANÇA	• Divulgação de noções sobre Ética e Segurança no desenvolvimento de <i>software</i> • Indireta avaliação da repercussão das demais atividades do projeto e da conscientização acerca da relevância da Ética e da Segurança no desenvolvimento de <i>software</i> • Captação de ideias para melhoria da iniciativa	• Membros do grupo de trabalho • Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife • Docentes • Especialistas em Segurança Computacional • Representantes da Indústria de <i>Software</i> • Voluntários	01 (um) dia a cada semestre
13º	AVALIAÇÃO DOS RESULTADOS OBTIDOS COM A INICIATIVA E AJUSTE DO PLANO DE AÇÃO	• Avaliação dos resultados obtidos com foco na melhoria das ações do plano • Ajuste do plano de ação a partir das constatações observadas na avaliação	• Membros do grupo de trabalho • Dirigentes/ Representantes das instituições de Ensino Superior atuantes na cidade do Recife	01 (um) dia a cada semestre

PLANO DE AÇÃO MÍNIMO PARA O TRATAMENTO DO PROBLEMA DA INSEGURANÇA DO <i>SOFTWARE</i>				
ORDEM CRONOLÓGICA	ATIVIDADE	MOTIVAÇÃO/ FINALIDADE	AGENTES ENVOLVIDOS NA EXECUÇÃO	PRAZO PARA CONSUMAÇÃO
			• Docentes • Especialistas em Segurança Computacional • Representantes da Indústria de <i>Software</i> • Voluntários	

Fonte: Autor (2019) ²⁰¹

²⁰¹ O plano em debate foi, nesta investigação, concebido como um simples ponto de partida fundado em noções gerais de gestão de projetos.

Importa consignar, no tocante à divulgação inicial da existência do grupo de trabalho em discussão (2º item do plano, observada a ordem cronológica adotada), que, mesmo sem o propósito de apresentar profecias apocalípticas, sugere-se, sim, o envio de comunicação a todos os entes indicados, consideradas a relevância da Segurança à sociedade atual e o potencial interesse de tais entes em assegurar suas plenas operações/atividades e/ou os interesses/atendimento da população local.

9 CONCLUSÕES E CONSIDERAÇÕES FINAIS

Construídos o referencial teórico sobre os temas relevantes à pesquisa, constatou-se, consideradas a importância e a ubiquidade do *software* no mundo contemporâneo, bem como a irreversível dependência da sociedade civil em relação ao *software*, uma impropriedade no tratamento dispensado à Segurança Computacional, havendo, em verdade, uma Crise de Segurança.

Ao longo do extremamente crítico e interdisciplinar estudo ora relatado, observou-se que se vive, atualmente, uma Crise de Segurança relativamente ao *software*, já que:

- através de simples análise estatística de amostra de dados reais, obtida com o emprego de uma **única estratégia** de identificação e análise de vulnerabilidades (*pentesting*) por **uma única empresa** de Segurança Computacional no período compreendido entre Janeiro/2013 e Junho/2018, constatou-se a ocorrência de expressivo número de distintas espécies de vulnerabilidades de segurança em *softwares* utilizados em diversos segmentos econômicos (Comércio Tradicional, Comércio Eletrônico, Indústria, Energia, Finanças, Serviços e outros), correspondendo este número a 11.182 (onze mil cento e oitenta e duas) distintas espécies de vulnerabilidades com variados graus de severidade;
- as vulnerabilidades referidas manifestaram-se, no geral, mais de uma vez (replicação média de vulnerabilidade correspondendo a 2 - dois), tendo sido identificados, ao todo, **23.721 (vinte e três mil e setecentos e vinte e um) pontos de vulnerabilidades de segurança**;
- embora os números absolutos sugerissem grande discrepância entre os quantitativos de vulnerabilidades/pontos de vulnerabilidades em *softwares* utilizados em segmentos econômicos distintos, os dados normalizados revelaram relativa homogeneidade entre segmentos, havendo ligeiro destaque no tocante

ao número de vulnerabilidades nos *softwares* empregados no segmento energético;

- a discrepância mencionada decorreu, em realidade, do simples fato de que, para alguns segmentos, a Segurança é tida como uma preocupação mais relevante, o que justificou, para entidades destes segmentos, maiores investimentos na identificação de vulnerabilidades, com conseqüentemente maior realização de *pentests* e maior efetiva identificação de pontos de vulnerabilidades;
- afastada, pela razão já citada, a discrepância referida, chegou-se à conclusão de que, quanto maior o número de *pentests* realizados, maior o número de vulnerabilidades/pontos de vulnerabilidades de segurança identificados, não havendo, pois, relação de prevalência do quantitativo de vulnerabilidades em função do segmento econômico em que utilizado o *software*;
- considerada a severidade dos pontos de vulnerabilidade, também não se observou significativa variação nos dados normalizados, cabendo, contudo, o destaque de que discreto maior número de vulnerabilidades mais severas se apresentou no *software* empregado no segmento energético;
- considerada a severidade, ainda, verificou-se que o *software* utilizado nas Finanças apresentou menor quantidade de vulnerabilidades mais severas, devendo este fato, provavelmente, resultar da maior preocupação natural com Segurança que se tem nos *softwares* empregados neste segmento, preocupação esta que deve levar a um *software* menos inseguro desde a sua concepção inicial e a sucessivas e contínuas reavaliações de conferência voltadas à identificação de vulnerabilidades de segurança com foco em sua eliminação;
- globalmente considerados, os dados mencionados sugerem, assim, que não se apresenta associação entre o quantitativo de pontos de vulnerabilidade de um *software* e o segmento em que ele se utiliza. A insegurança, enfim, não é dependente do nicho de mercado, manifestando-se de forma generalizada em significativos montantes em diversas camadas dos sistemas computacionais;
- na camada de aplicações *web*, observaram-se 7.431 (sete mil e quatrocentas e trinta e um) pontos de vulnerabilidades de variadas espécies (Falhas em Autenticação, Falhas em Controle de Acesso, Falhas no Gerenciamento de Sessões, Falhas nos Mecanismos de *Uploads*, Ausência de Protocolo Seguro de Transferência de Texto (*Hypertext Transfer Protocol Secure – HTTPS*), Inclusão

Remota de *Scripts*, Vazamento de Informações Sensíveis, Injeção de *SQL* e *Cross-Site Scripting*), sendo, em conformidade com quadro OWASP (2017), mais frequentes as vulnerabilidades envolvendo *Cross-Site Scripting*, Falhas em Autenticação e Falhas em Controle de Acesso.

Com a análise da amostra de dados, constatou-se, ademais, que uma consequência maior resulta do quadro de insegurança identificado, pois, apresentando-se a incidência de pontos de vulnerabilidade quase como uma constante (dados normalizados), verificou-se que a insegurança está, literalmente, em todos os lugares, não havendo dependência em função do nicho mercadológico do *software*.

Ausente dependência de nicho e sendo significativos os números de pontos de vulnerabilidades de segurança, chegou-se à inferência de que a insegurança no *software*, ao menos em parte, tem origem na própria Engenharia envolvida em sua construção, persistindo, então, o debate acerca da natureza da Engenharia de *Software*.

Engenharia ou não Engenharia? Eis **ainda** a questão. Quase três décadas após a publicação do popular artigo escrito por Shaw (SHAW, 1990), ainda seria questionável a atribuição da nomenclatura de Engenharia ao conjunto de atividades e disciplinas voltadas ao desenvolvimento de *software*.

Quase três décadas após a publicação do mencionado artigo e cinco décadas após a primeira vez em que foi usado o termo Engenharia de *Software*, apesar de todos os esforços empreendidos pela Academia e pela Indústria, ainda é questionável o uso da terminologia em discussão quando considerada a questão da Segurança no *software* porque, em outros ramos de Engenharia, não seriam aceitas falhas no *quantum* identificado neste estudo. **Em 66 (sessenta e seis) meses de pentesting, 23.721 (vinte e três mil e setecentos e vinte e um) pontos de vulnerabilidades de segurança foram identificados e este número não é insignificante.** Não sendo insignificante este número, tem-se que o que, atualmente, é chamado de Engenharia consiste, em verdade, em Artesania.

As muitas iniciativas adotadas desde o surgimento da “Engenharia de *Software*” (definição de novos métodos de desenvolvimento, criação de novas linguagens e concepção de novos paradigmas, e.g.) não fizeram da Engenharia de

Software, **sob a ótica da Segurança**, uma Engenharia de fato²⁰² porque, em essência, como antes já mencionado ao longo deste documento, são diversos os dilemas enfrentados ao longo dos processos de desenvolvimento de *software* (IIVARI, 1996) e porque, como observado por Brooks, “não há bala de prata” (BROOKS, 1987).

Muito tem sido feito na busca por uma verdadeira Engenharia de *Software*, mas muito ainda tem que ser feito! Se os esforços e as iniciativas isoladas não resultaram, **quando se pensa na Segurança no *software***, em uma Engenharia de *Software* real e madura, o afastamento da já referida Crise de Segurança somente pode ocorrer mediante uma mudança de paradigma fundada, ao longo de todo o processo de desenvolvimento e não apenas em um momento específico, na integração, na reunião de esforços, no pensar de forma holística, tendo a Segurança como alvo, e não com foco estanque e limitado em disciplinas de Ciência da Computação. Integração é vital já que:

- trata-se, em último caso, de questão atinente a conhecimento científico;
- a Ciência, ao final de tudo, é uma só, a despeito de se apresentar, para fins organizacionais e didáticos, sob múltiplos ramos.

Além de indicarem imaturidade da Engenharia de *Software* e relativa inadequação, considerada a Segurança, no uso de tal terminologia ao se fazer referência ao ramo de atividade produtiva que envolve a especificação e o desenvolvimento de *software*, os dados dos *pentests* apontaram, ainda, para uma preterição da Segurança ao longo dos processos de desenvolvimento de sistemas. Dito de outra forma, tem-se como verdadeiro, a partir dos dados da amostra de *pentests*, que a Indústria de *Software* não tem, entre suas prioridades, o desenvolvimento de *software* não inseguro.

Se a insegurança, como antes já mencionado, está em todos os lugares, não dependendo, como demonstraram os dados normalizados, do nicho

²⁰² Mais uma vez, vale registrar que, com a crítica feita, não se objetiva denegrir a Engenharia de *Software*, almejando-se, em verdade, a melhoria desta, dada a sua exponencialmente crescente e irreversível importância à sociedade como um todo. O ponto é que, a despeito de toda esta essencialidade e relevância, quando considerada a Segurança, não se tem, de fato, hoje, Engenharia e se mostra, sim, inapropriado o uso da terminologia Engenharia de *Software*, como demonstram os dados apurados na investigação ora relatada. Independentemente do mal estar e do descontentamento que esta crítica pudesse causar, ela tinha que ser feita, pois esta conclusão é apontada pelos resultados da pesquisa.

mercadológico dos *softwares* e se foram identificadas repetições de uma mesma vulnerabilidade em cada um dos *softwares* da amostra analisada (pontos de vulnerabilidades), chegou-se à constatação de que as falhas de segurança identificadas não decorreram de meros equívocos, sendo, em realidade, consequências do desconhecimento de temas relativos à Segurança Computacional e/ou resultado direto da desconsideração de tais temas ao longo dos processos de desenvolvimento de *software*. Esta constatação, registre-se, foi corroborada, também, pelos especialistas de Segurança Computacional entrevistados e por um dos *surveys* realizados na pesquisa.

A partir dos dados das entrevistas citadas e do mencionado *survey* em que se coletaram impressões de 34 (trinta e quatro) desenvolvedores de *softwares*, observou-se que:

- na produção de *software*, é usual a preterição dos requisitos de Segurança em favor de outros requisitos (Requisitos Funcionais, especialmente), uma vez que estes requisitos, ao contrário de outros, não têm visibilidade imediata para o usuário final e o público em geral;
- em alguns casos, a preterição referida decorre, também, da metodologia de desenvolvimento empregada;
- os desenvolvedores não têm, em geral, conhecimento mínimo sobre Segurança Computacional, incorrendo em falhas primárias que tornam fáceis as ações dos *hackers*.

Considerada a constatação do desconhecimento dos desenvolvedores acerca da Segurança Computacional, cogitou-se da possibilidade de a preterição/negligência se originar, também, na Academia, hipótese essa que foi corroborada por análise documental das grades curriculares de 115 (cento e quinze) cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de 64 (sessenta e quatro) instituições de ensino brasileiras.

Com a análise documental referida, verificou-se que:

- quase de 30% dos cursos de Sistemas da Informação não apresentam disciplina obrigatória relacionada à Segurança Computacional em suas grades curriculares;

- cerca de 80% dos cursos de Ciência da Computação e Engenharia da Computação não apresentam nenhuma disciplina obrigatória que envolva, diretamente, Segurança Computacional em suas estruturas;
- não havendo, pelo exposto, ainda hoje, obrigatoriedade de participação discente em disciplinas relativas à Segurança Computacional, é pertinente se pensar, apesar de não ser possível se afastar a possibilidade de suplementação autônoma por autodidatismo, que parte da causa para o desconhecimento dos desenvolvedores tem, sim, também, origem na Academia.

Ao mesmo tempo em que constatados o grande volume de pontos de vulnerabilidades de Segurança em *software*, bem como a já mencionada preterição dos requisitos de Segurança, o desconhecimento teórico dos discentes e profissionais sobre tal tema e a parcial origem deste desconhecimento na Academia, observou-se que a Indústria de *Software*, ainda, tenta se esquivar de qualquer responsabilidade pelo que produz (responsabilidade por falhas de Segurança inclusas), valendo-se, para isso, de abusivos *EULAs/ToSs* isentivos ou limitantes de responsabilidade, como revelou o exame de 150 (cento e cinquenta) documentos de tais espécies adotados por 67 (sessenta e sete) empresas, sediadas em localidades geográficas variadas, produtoras/fornecedoras de *software*/serviços de *software* insertos nas categorias seguintes:

- aplicativo/utilitário;
- instalação, configuração e gerenciamento de servidor;
- serviço *web*;
- ambiente/sistema operacional.

Constatou-se, através do exame dos *EULAs/ToSs*, que:

- em 100% (cem por cento) dos casos, as empresas produtoras/fornecedoras de *software*/serviços em *software* tentaram se evadir da responsabilidade pelo que produziram/forneceram, valendo-se de cláusulas diversas isentivas e/ou limitantes de responsabilidade, impondo-se, ainda, uma cláusula básica ao uso do *software*: a irrestrita e incondicionada aceitação do que constasse dos respectivos *EULAs* e *ToSs*;

- na maior parte dos *EULAs* e *ToSs*, 85% (oitenta e cinco por cento deles) em termos mais específicos, foram simultaneamente definidas cláusulas isentivas e cláusulas limitantes, quando não possível se afastar *in totum*, a responsabilidade nos ordenamentos jurídicos considerados;
- em 12% (doze por cento) dos *EULAs* e *ToSs*, foram definidas cláusulas únicas de integral isenção de responsabilidade;
- a adoção de cláusulas de integral isenção de responsabilidade realizou-se de forma relativamente homogênea nos *EULAs/ToSs* analisados, havendo, contudo, um segmento em que este tipo de cláusula não foi inserto em 50% (cinquenta por cento) dos casos: o segmento dos *softwares* voltados à instalação, à configuração e ao gerenciamento de servidores, o que sugere que, talvez, nesse segmento, haja uma efetiva maior preocupação com a qualidade do produto/serviço em *software*;
- apenas em 3% (três por cento) dos documentos referidos, incluíram-se somente cláusulas limitantes de responsabilidade;
- em 88% (oitenta e oito por cento) dos *EULAs* e *ToSs* com cláusulas limitantes, definiram-se tetos de responsabilização, os quais, comumente, foram fixados com a consideração do preço de aquisição do produto/serviço ou soma previamente fixada pelo próprio produtor/fornecedor do *software/serviço* em *software*.

Observou-se, ademais, que mesmo se furtando à responsabilidade pelo que produzissem/fornecessem, algumas das empresas de *software/serviços* em *software* consideradas na pesquisa, em contraditória atitude, propalavam aos quatro ventos informação falsa e não cientificamente verificável: a segurança de seus produtos/serviços.

Se não há, matematica e formalmente, como mencionado no Capítulo 7 deste trabalho, como se conceber, construir, implantar e operar *software/serviço* de *software* inequívoca e infalivelmente seguro, a conduta dos agentes da Indústria de *Software* não se mostra apropriada, socialmente aceitável ou ética.

A conduta referida se mostra antiética e é urgente uma modificação nela, sob pena de a sociedade civil, a própria Indústria de *Software* e seus agentes virem a arcar com custos elevados demais.

Especialmente para a Indústria de *Software* e os seus agentes, não é exagerado discorrer sobre a necessidade de premente alteração de conduta, pois, entre os custos que a estes podem ser impostos e que, obviamente, não se inserem entre seus interesses, sobressaem-se os elencados no Quadro 45:

Quadro 45 – Repercussões da manutenção da postura atual da Indústria de *Software* e de seus agentes em relação à Segurança Computacional.

REPERCUSSÕES DA MANUTENÇÃO DA POSTURA ATUAL DA INDÚSTRIA DE SOFTWARE E DE SEUS AGENTES EM RELAÇÃO À SEGURANÇA COMPUTACIONAL	
REPERCUSSÕES POTENCIAIS PARA A INDÚSTRIA DE SOFTWARE	REPERCUSSÕES HIPOTÉTICAS PARA OS DESENVOLVEDORES DE SOFTWARE
• Subordinação a iniciativas externas de regulação (legislação, principalmente) • Decréscimo de reputação • Perda de participação em mercados • Figuração como rés em demandas judiciais e arbitrais • Sujeição a prejuízos financeiros em virtude de condenação ao pagamento de indenizações em virtude de falhas de Segurança em produtos/serviços • Sujeição a “selos” e “certificações” falaciosos, que atestem o inastestável: a segurança de um <i>software</i> • Sujeição a monopólios, cartéis e a descabidas reservas de mercado fundadas em motivação falsa e/ou protecionista	• Sujeição a normas de licenciamento profissional • Estigmatização e execração pública em caso de grande impacto social decorrente de falhas nos produtos/serviços que elaboram ou com que lidam em suas atividades profissionais

Fonte: Autor (2019) ²⁰³.

²⁰³ Este Quadro foi elaborado a partir das inferências produzidas ao longo da pesquisa ora relatada e expostas, essencialmente, nos Capítulos 7 e 8, de modo que, caso o leitor repute necessário relembrar alguns destes temas, sugere-se consulta aos aludidos Capítulos.

Por todo o exposto até o momento, verificou-se que a indispensável mudança de paradigma na Indústria de *Software* envolve, em essência, o estabelecimento de uma Engenharia de *Software* Ética no tocante à Segurança Computacional, o que, como já ressaltado no Capítulo 8 deste texto, somente pode ser alcançado com:

- o reconhecimento da relevância dos requisitos de Segurança pela Academia e pela Indústria de *Software*, bem como o adequado tratamento destes requisitos ao longo de todo o processo de desenvolvimento;
- uma modificação na postura de desenvolvedores e da Indústria de *Software* como um todo, de modo a se ter a Ética como uma constante em todo e qualquer evento que possa repercutir no desenvolvimento do *software*.

Lidar com os temas referidos não é missão simples, uma vez que o foco da mudança real não envolve apenas a Segurança Computacional. Para uma mudança significativa, é necessário que a Indústria e seus agentes passem a ter como objetivo o agir correto, o agir adequado, o agir voltado não somente à efêmera satisfação de seus interesses. O agir em discussão, como destacado no Capítulo 8, envolve a Ética Profissional.

Estando-se em um irreversível estágio de dependência social de *software* ubíquo, todos os que, de alguma forma, integram ou participam do desenvolvimento de *software* devem pautar suas condutas em normas de conteúdo ético, o que, em princípio, parece ser um problema já que, consoante dados obtidos em outro *survey* realizado ao longo da pesquisa, 64% dos profissionais nunca tiveram qualquer contato prévio com qualquer Código de Ética e que os desenvolvedores restantes tiveram algum contato, mas não, necessariamente, com um Código voltado às suas atividades profissionais.

A falta de familiaridade e conhecimento formal dos desenvolvedores de *software* quanto à Ética Profissional é ainda mais preocupante quando se pensa que, de longa data, há um Código internacional especialmente destinado ao regramento de suas condutas laborais: o Código de Ética IEEE/ACM para Engenharia de *Software*.

Além de se constatar os mencionados falta de familiaridade e desconhecimento quanto à Ética Profissional, verificou-se, no presente estudo,

através de nova análise documental (análise das grades curriculares de cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de instituições de ensino brasileiras), que, em parte, a origem disso se dá na Academia, já que, atualmente, parcela dos referidos cursos não apresenta em sua estrutura alguma disciplina relacionada à Ética.

Observou-se, ademais, que:

- embora, no momento atual, significativo montante dos cursos citados tenha em sua grade alguma disciplina de conteúdo ético, é provável, considerado o resultado do *survey* referido, que, no passado, disciplinas de tal conteúdo não constassem das estruturas curriculares, dado que expressivo montante dos profissionais inquiridos no *survey* não teve qualquer contato com qualquer Código de Ética;
- em virtude da presumível pretérita inexistência de disciplinas com conteúdo ético e da ausência, ainda, hoje, de disciplinas de tal espécie em parte dos cursos considerados, persiste uma significativa lacuna de conhecimento quanto à Ética em parte dos profissionais que desenvolvem *software*;
- a aludida lacuna, por seu turno, representa um problema para a sociedade civil, para a Indústria de *Software* e para os próprios profissionais que desta participam, já que se está, hoje, como antes mencionado, em uma era de irreversível dependência dos *softwares*;
- em uma era de dependência de *software*, as condutas de cada desenvolvedor em suas atividades laborais podem apresentar implicações e repercussões sociais, não sendo recomendado, então, que quedem a depender, exclusivamente, das consciências individuais dos próprios desenvolvedores, uma vez que as “consciências individuais” oscilam em um grande espectro e que é indispensável assegurar um mínimo de retidão em tais condutas, para se evitar danos aos demais indivíduos, à própria Indústria de *Software* e para a sociedade civil como um todo;
- a adoção de medidas para se promover um “mínimo ético” entre os profissionais que compõem a Indústria de *Software* é indispensável também quando se cogita da globalização, já que *software* produzido em um dado país pode provocar

deletérias consequências internacionais, afetando, inclusive, países em que a produção de *software* esteja alinhada à Ética.

Diante de todo o panorama visualizado no tocante à Segurança Computacional e à Ética no desenvolvimento de *software*, constatou-se, por fim, que:

- algo há de ser feito para a superação da Crise de Segurança no *software*, sob pena de nefastas consequências;
- parte da solução do problema principal identificado (antiético tratamento da Segurança nos processos de desenvolvimento de *software*) envolve a própria Academia, já que a oferta de compulsórias disciplinas com conteúdo relativo à Segurança Computacional e à Ética, apesar de não assegurar comportamento apropriado, pode contribuir para a uma maior conscientização a respeito de tais temas e o consequente engajamento dos desenvolvedores e da Indústria de *Software* no tocante a essas questões;
- caso não considerado relevante pela Academia e pela Indústria o oferecimento de disciplina com denso conteúdo ético, deve, ao menos, ser difundido o teor de normas éticas de cunho profissional;
- em virtude da globalização do atual mercado de *software* e da grande mobilidade entre os profissionais que integram a Indústria de *Software*, mostram-se, em princípio, interessantes a voluntária adoção e a difusão um Código de Ética comum, ou seja, a adoção e a difusão de um Código de Ética que se mostre internacionalmente aplicável independentemente de ordenamento jurídico;
- existe, desde 1999, um Código de Ética compatível com as ideias *supra* e que pode, sem grandes questionamentos da própria Indústria e da Academia, vir a ser mundialmente adotado: o Código IEEE/ACM de Ética para Engenharia de *Software*;
- com o ataque das duas frentes mencionadas (Segurança e Ética), pode-se superar a antes referida Crise de Segurança no *software*, mas engajamento e alinhamento reais são essenciais a tal fim;
- para o engajamento e alinhamento citados, esforços coordenados da Indústria e da Academia são necessários, cabendo o destaque de que, antes de qualquer

ação, é importante que estes entes reconheçam que, de fato, o problema, a Crise da Segurança, existe e deve, sob pena das nocivas repercussões já expostas ao longo deste trabalho, ser enfrentado;

- reconhecida a relevância do enfrentamento do problema, há de ser traçado um plano de ação, uma estratégia com objetivos de curto, médio e longo prazo, com foco na produção de *software* ético relativamente à Segurança;
- produziu-se, ao longo da presente investigação, com escopo simplesmente ilustrativo, um plano de ação mínimo com natureza de mera diretriz porque, em verdade, para uma efetiva adesão às suas hipotéticas ideias pela Academia, pela Indústria e pelos desenvolvedores de *software*, não é apropriado que este plano seja “imposto”;
- para uma real adesão e uma verdadeira mudança no tocante à Segurança no *software*, o que somente se obtém com engajamento, alinhamento e envolvimento autênticos, o plano em debate deve ser construído pelos próprios agentes referidos (Academia e Indústria, em particular), que cientes do panorama atual exposto neste estudo, reconheçam a importância e a premência de mudança, deliberem em conjunto sobre como proceder e assim o façam de forma concreta;
- a elaboração do plano em discussão deve se iniciar na própria Academia e na Indústria de *Software* porque o seu envolvimento verdadeiro é essencial e porque, como mencionado no Capítulo precedente, um ente/pessoa se envolve mais verdadeiramente com algo do que tem a oportunidade de participar na concepção;
- a elaboração e a imposição externa de uma agenda de mudança, construída sem a participação dos referidos atores, não produziria o mesmo resultado.

Brevemente expostas as conclusões a que se chegou com a realização do estudo ora relatado, há de se tecer alguns comentários sobre suas limitações, destacando-se as seguintes:

- impossibilidade, por inexperiência e insipiência do pesquisador na concreta identificação de vulnerabilidades, de efetiva avaliação da segurança no *software* com base em dados coletados diretamente por ela mesma, sujeitando-se a

acurácia da avaliação referida à exatidão dos dados da amostra cedida por empresa de Segurança Computacional;

- baixo nível estatístico de confiabilidade dos dados obtidos com a aplicação dos questionários, já que diminuto o número de respondentes, considerado o universo amostral (discentes do CIn atuantes na Indústria de *Software*);
- impossibilidade de definição de um universo amostral mais amplo para a aplicação dos questionários, em razão de não se ter obtido acesso a outros núcleos de respondentes de potencial interesse para a pesquisa;
- impossibilidade de integral análise das grandes, ementas e programas de disciplinas dos cursos cujos documentos foram levantados para avaliação do papel da Academia no panorama de insegurança traçado, uma vez que apenas coletados documentos disponíveis na *Internet* e que, em casos diversos, tais documentos não haviam sido disponibilizados *on line*;
- potencial persistência de viés na avaliação dos *EULAs/ToSs* considerados neste estudo, já que coletados documentos de tal espécie de apenas 15 (quinze) diferentes países e que, na apreciação global realizada, não conduzida normalização;
- impossibilidade de efetiva verificação de que as conclusões obtidas neste estudo não podem, em transposição simples, ser aplicadas a universos em que a produção de *software* já se mostre eticamente engajada;
- impossibilidade de realização de retrospectiva avaliação de artefatos de processos de desenvolvimento de *software*, para verificação da efetiva preterição dos requisitos de segurança, já que a utilidade de tal fonte de dados não foi reconhecida antes de a pesquisa ter atingido dado patamar;
- impossibilidade de observação de um maior conjunto de equipes de desenvolvimento de *software* em suas atividades produtivas.

Apesar das limitações referidas, as conclusões produzidas com a pesquisa mostram-se pertinentes, já que as inferências decorrentes da análise da amostra de *pentesting* foram corroboradas pelos resultados obtidos através dos breves *surveys* realizados e das análises documentais conduzidas (análises de *EULAs/ToSs* e das grades curriculares dos cursos de Ciência da Computação, Engenharia da Computação e Sistemas de Informação considerados na pesquisa).

As referidas pertinentes conclusões evidenciam que se está, atualmente, em uma Crise de Segurança e que a superação de tal crise ou, ao menos, a minoração de suas consequências é urgente e dependente de esforços conjuntos da Academia, da Indústria de *Software* e dos desenvolvedores de *software*, os quais, sob pena de nefastas consequências a si próprios e à sociedade civil, devem se conscientizar da importância de seus papéis sociais, passar a valorizar comportamentos éticos e a agir eticamente no tocante à Segurança no *software*.

Em síntese, tem-se, assim, que, concluída a investigação ora relatada, obtiveram-se respostas às perguntas de pesquisa originalmente definidas, como se depreende do Quadro 46.

Quadro 46 - Extrato das respostas às perguntas de pesquisa da investigação relatada.

EXTRATO DAS RESPOSTAS ÀS PERGUNTAS DE PESQUISA DA INVESTIGAÇÃO RELATADA	
PERGUNTA DE PESQUISA	RESPOSTAS OBTIDAS AO LONGO DA INVESTIGAÇÃO
Que proporções assumem as vulnerabilidades de Segurança em <i>softwares</i> atualmente?	Atualmente, as vulnerabilidades de Segurança em <i>software</i> assumem grande proporção, pois, como se infere do exame de uma amostra de <i>pentesting</i> fornecida por uma única empresa de Segurança Computacional para um interregno de 66 (sessenta) e seis meses, foi possível a identificação de 23.721 (vinte e três mil e setecentos e vinte e um) pontos de vulnerabilidades em <i>softwares</i> de distintos segmentos econômicos.
Que fatores concorrem para a insegurança do <i>software</i>?	Múltiplos fatores podem concorrer para a insegurança, sobressaindo-se, como consignado ao longo deste relato de pesquisa, os seguintes: • impossibilidade de garantia formal e matemática da Segurança; • débito técnico dos desenvolvedores no tocante à Segurança Computacional; • débito ético da Indústria de <i>Software</i> quanto ao tratamento dos requisitos de Segurança, os quais costumam ser preteridos em favor dos requisitos ditos funcionais.

EXTRATO DAS RESPOSTAS ÀS PERGUNTAS DE PESQUISA DA INVESTIGAÇÃO RELATADA	
PERGUNTA DE PESQUISA	RESPOSTAS OBTIDAS AO LONGO DA INVESTIGAÇÃO
É possível se associar a existência de vulnerabilidades de Segurança a uma preterição dos Requisitos de Segurança em favor dos Requisitos Funcionais durante o processo de desenvolvimento de <i>software</i> ?	Sim, pois, de acordo com o apurado na investigação, o foco usual, no processo de desenvolvimento, está nas funcionalidades e na urgente entrega do produto/serviço em <i>software</i> .
Os desenvolvedores de <i>software</i> têm, no geral, um conhecimento formal mínimo sobre Segurança Computacional e sobre Segurança em <i>software</i> ?	De acordo com a apuração feita na investigação para o universo considerado na pesquisa (desenvolvedores atuantes no Brasil, em essência), não há conhecimento formal mínimo sobre Segurança Computacional entre os desenvolvedores de <i>software</i> , já que se constatou, também, débito da Academia, dada a não obrigatoriedade, na maioria dos cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação, de disciplinas acerca de Segurança Computacional, o que permite aos discentes concluir seus cursos sem qualquer noção basilar sobre este tema.
O que a Indústria de <i>Software</i> tem feito no tocante à questão da Segurança?	Analisando-se os dados coletados na pesquisa (grande número de vulnerabilidades de Segurança nos <i>softwares</i> , informações prestadas por desenvolvedores e simultânea evasão da responsabilidade em <i>EULAs/ToSs</i> , em particular), chega-se à conclusão de que, para a Indústria de <i>Software</i> a Segurança não apresenta a relevância necessária, sendo frequente a sua preterição em favor de outros requisitos.
Está a Indústria de <i>Software</i> tentando se furtar à responsabilidade pela Segurança do que produz, valendo-se, para isso, do condicionamento do uso de seus produtos/serviços à irrestrita aceitação das condições unilaterais de isenção/limitação de responsabilidade	Considerado o teor dos <i>EULAs/ToSs</i> analisados, tem-se como plausível o argumento de que a Indústria de <i>Software</i> estaria a tentar se evadir da responsabilidade pelo que produz, uma vez que, nos aludidos documentos, são insertas desarrazoadas cláusulas isentivas/limitantes de responsabilidade.

EXTRATO DAS RESPOSTAS ÀS PERGUNTAS DE PESQUISA DA INVESTIGAÇÃO RELATADA

PERGUNTA DE PESQUISA	RESPOSTAS OBTIDAS AO LONGO DA INVESTIGAÇÃO
constantes, usualmente, de <i>EULAs</i> e <i>ToSs</i> ?	
Caso a Indústria de <i>Software</i> esteja se furtando à responsabilidade pelo que produz, é possível sua responsabilização na esfera civil?	No ordenamento jurídico brasileiro e no de diversas outras Nações, tem-se como possível a responsabilização civil da Indústria de <i>Software</i> a despeito da existência de <i>EULAs/ToSs</i> porque tais documentos, fixados em contratos de adesão produzidos unilateralmente pela própria Indústria, são tidos como abusivos por apresentarem cláusulas leoninas. Não faltam, na esfera judicial, exemplos de casos em que empresas produtoras/fornecedoras de <i>software</i> foram condenadas ao pagamento de indenizações ou, antes da condenação, reconhecendo sua culpa, sujeitaram-se a acordos para a retirada da demanda.
Caso se considerem legalmente válidas as disposições excludentes e limitantes de responsabilidade dos <i>EULAs</i> e <i>ToSs</i> , pode-se cogitar da persistência de um viés antiético?	Mesmo nos ordenamentos em que as cláusulas em comento possam vir a ser consideradas legais, persiste um viés antiético nelas, pois se espera que um profissional, ao realizar suas atividades, empregue os recursos que dispuser a este fim, tencionando produzir um produto com qualidade mínima.
Agem eticamente a Indústria e os desenvolvedores de <i>software</i> , ao lidar com os requisitos de Segurança?	Não, considerado o momento atual de ubiquidade e interconexão do <i>software</i> , não agem eticamente a Indústria e os desenvolvedores de <i>software</i> , já que a Segurança, em tal momento de interconectividade ubíqua, revela-se atributo essencial do <i>software</i> .
Que repercussões nocivas podem decorrer da consolidação de um estado de insegurança de <i>software</i> para a sociedade em geral e para a própria Indústria de <i>Software</i> ?	Da consolidação referida, pode resultar, para a sociedade civil, um estado de caos generalizado em que, dada a inevitável e irreversível dependência do <i>software</i> , nem mesmo serviços básicos à população possam ser prestados. Para a Indústria também se visualizam possíveis repercussões nocivas, como: • sujeição à regulação externa (fiscalização/controle externo e tributação extrafiscal diferenciada, inclusive); • estabelecimento de normas para o licenciamento profissional; • impossibilidade de participação em mercados

EXTRATO DAS RESPOSTAS ÀS PERGUNTAS DE PESQUISA DA INVESTIGAÇÃO RELATADA	
PERGUNTA DE PESQUISA	RESPOSTAS OBTIDAS AO LONGO DA INVESTIGAÇÃO
	internacionais; • surgimento de cartéis e monopólios desestabilizantes da concorrência leal.
Há algo a ser feito para se evitar a consolidação citada?	Para se evitar a nefasta consolidação da Crise de Segurança no <i>software</i> , mostra-se necessário a conjunta atuação da Academia, da Indústria de <i>Software</i> e dos desenvolvedores, os quais precisam passar a considerar a Segurança como atributo essencial a ser tratado apropriadamente ao longo de todo o processo de desenvolvimento. Faz-se útil, com este escopo, a elaboração e a implantação de um plano de ação conjunto para reversão do panorama atual.

Fonte: Autor (2019).

As respostas obtidas levaram à confirmação das hipóteses macroscópicas inicialmente cogitadas para o problema da pesquisa:

- a atual impropriedade no tratamento dado pela Indústria de *Software* à Segurança Computacional, mormente quando observadas a preterição dos requisitos de Segurança em um momento de irreversível ubiquidade interconectada, e a antiética tentativa de evasão da responsabilidade com a imposição de abusivos EULAs/ToSs isentivos/limitantes de responsabilidade;
- a existência de débitos técnico e ético a contribuir para o panorama observado;
- a necessidade de reversão do quadro traçado em benefício da sociedade civil e da própria Indústria de *Software*;
- a urgência na reversão referida, a qual somente será possível com a conjunta atuação da Academia, da Indústria de *Software* e dos próprios desenvolvedores.

Na busca por respostas às antes citadas perguntas de pesquisa, foram, outrossim, em virtude do pioneirismo da investigação ora relatada e da consequente impossibilidade de exploração da área, construídas novas perguntas e hipóteses, cujos temas podem servir de base para trabalhos futuros, como:

- averiguação da necessidade, ou não, de educação formal mínima para a atuação como desenvolvedor de *software*, dadas a importância do *software* e da Segurança no mundo atual;
- avaliação, para a Segurança Computacional, da relação custo x benefício associada a eventual licenciamento profissional;
- análise da (im)propriedade de se considerar uma dada instituição de ensino e pesquisa (instituição com cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação) como centro de excelência (modelo de avaliação da CAPES), quando nos cursos da referida instituição de ensino e pesquisa não se confere, nas grades curriculares, a necessária importância às disciplinas de Segurança e quando não há investimento em pesquisas neste domínio;
- avaliação da possível existência de associação entre a adoção de metodologias ágeis de desenvolvimento e um maior número de vulnerabilidades no *software* através destas metodologias produzido;
- mapeamento das percepções pessoais de desenvolvedores de *software* quanto à Ética comum e quanto à Ética profissional, especialmente no tocante à Segurança.

A investigação, além de levar à obtenção das respostas às perguntas de pesquisa antes citadas e de apontar temas para trabalhos futuros, resultou, ainda, em 6 (seis) diferentes artigos submetidos em 9 (nove) distintas ocasiões em conferências internacionais. Um dos mencionados artigos (*“HOUSTON, WE MAY HAVE A PROBLEM: Results of an exploratory inquiry on software developers’ knowledge about Codes of Ethics”*, de coautoria do pesquisador e de seu orientador) foi aceito na *13th Annual IEEE International Systems Conference – SYSCON 2019*, tendo sido apresentado e publicado em abril de 2019, na cidade de Orlando, Flórida, e um dos demais outros artigos se encontra em processo de revisão, aguardando avaliação em nova submissão.

REFERÊNCIAS

ADEODATO, João Maurício. Bases para uma metodologia de pesquisa em direito. **Revista do Centro de Estudos Judiciários**, Brasília, DF, n. 7, p. 143-150, abr. 1999.

ADKINS, Lyssa. **Coaching agile teams**: a companion for scrummasters, agile coaches, and project managers in transition. Boston: Addison-Wesley, 2010.

AGUIAR, Roger Silva. **Responsabilidade civil objetiva**: do risco à solidariedade. São Paulo: Atlas, 2007.

AIP; CASSIDY, David. Quantum Mechanics: The Uncertainty Principle. **Werner Heisenberg (1901-1976)**, College Park, [2011?]. Disponível em: <http://www.aip.org/history/heisenberg/p08.htm>. Acesso em: 12 jun. 2011.

ALLEN, Lee. **Advanced penetration testing for highly-secured environments**: the ultimate security guide. Birmigham: Packt Publishing, 2012.

ALEXANDER, Jonathan. **Codermetrics**: analytics for improving software teams. [Sebastopol?]: O'Reilly, 2011.

ALMEIDA, Marco Romeu Baptista. **Análise da interoperabilidade aplicada ao projeto BIM de estruturas metálicas**. 2015. 89 p. Dissertação de Mestrado (Engenharia Mecânica) - Instituto Superior de Engenharia do Porto, Porto, 2015.

AMARAL NETO, Francisco dos Santos. Responsabilidade Civil - II. In: LIMONGI FRANÇA, R. (Coord.). **Enciclopédia Saraiva do Direito**. São Paulo: Saraiva, 1977. p. 346 - 359.

ANDERSEN, Hans Christian. **A roupa nova do imperador**. São Paulo: Brinque-Book, 1997.

ANDERSON, R. R.; JOHNSON, D. G.; GOTTERBARN, D.; PERROLLE, J. Using the new ACM Code of Ethics in decision making. **Communications of the ACM**, vol. 36, n.2, 1993.

AQUINO, André Carlos Busanelli; PAGLIARUSSI, Marcelo Sanches; BITTI, Eugênio José Silva. Heurística para a composição de referencial teórico. **Revista Contabilidade & Finanças**, São Paulo, v. 19, n. 47, p. 73-88. Disponível em: <http://www.eac.fea.usp.br/cadernos/completos/47/andre-marcelo-eugenio-pg73a88.pdf>. Acesso em: 17 abr. 2011.

ARGHIRE, Ionut. Ransomware Attack Hits Health Firm LabCorp. **Security Week**, [S.l.], jul. 2018. Disponível em: <https://www.securityweek.com/ransomware-attack-hits-health-firm-labcorp>. Acesso em: 9 set. 2019.

ARMERDING, Taylor. The 18 biggest data breaches of the 21st century. **CSO**, Framingham, 2018. Disponível em: <https://www.csoononline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html#tk.cso-fsb>. Acesso em: 9 set. 2019.

ASNAR, Yudistira; GIORGINI, Paolo; MASSACCI, Fabio; ZANNONE, Nicola. From trust to dependability through risk analysis. In: Second International Conference on Availability, Reliability and Security (AreS 2007), 2007, Viena. **AreS 2007**. Disponível em: <http://www.troposproject.org/biblio/author/files/asnar-giorgini-massacci-zannone-ARES.pdf>. Acesso em: 29 abr. 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro, nov. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6024**: informação e documentação: numeração progressiva das seções de um documento escrito: apresentação. Rio de Janeiro, fev. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6027**: informação e documentação: sumário: apresentação. Rio de Janeiro, dez. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6028**: informação e documentação: resumo: apresentação. Rio de Janeiro, nov. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6034**: informação e documentação: índice: apresentação. Rio de Janeiro, dez. 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro, ago. 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 10719**: apresentação de relatórios técnico-científicos. Rio de Janeiro, jun. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 14724**: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro, mar. 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 15287**: informação e documentação: projeto de pesquisa: apresentação. Rio de Janeiro, mar. 2011.

ATALIBA, Geraldo. **Hipótese de incidência tributária**. São Paulo: Revista dos Tribunais, 1975.

AURUM, Aybüke; WOHLIN, Claes (ed). **Engineering and managind in software requirements**. Berlim: Springer, 2005.

AUSTRALIAN AVIATION. Pilots launch class action over boeing 737 max grounding. **Australian Aviation**, 24 June 2019. Disponível em: <https://australianaviation.com.au/2019/06/pilots-launch-class-action-over-boeing-737-max-grounding/>. Acesso em: 24 jun. 2019.

AUSTRALIAN CORPORATION BROADCASTING. Boeing sued by more than 400 pilots in class action over 737 MAX's 'unprecedented cover-up'. **ABC**, 24 June 2019. Disponível em: <https://www.abc.net.au/news/2019-06-23/over-400-pilots-join-lawsuit-against-boeing-over-737-max/11238282>. Acesso em: 24 jun. 2019.

AZEVEDO, Álvaro Villaça. Responsabilidade Civil - I. In: LIMONGI FRANÇA, R. (Coord.). **Enciclopédia Saraiva do Direito**. São Paulo: Saraiva, 1977. p. 331 - 346.

B., Fernando. Boeing 737 MAX 8 Software accountability or lack thereof? **DEV**, 26 Mar. 2019. Disponível em: <https://dev.to/kodaman2/boeing-max-8-software-accountability-or-lack-thereof-2k9k>. Acesso em: 23 jun. 2019.

BAJARIN, Tim. The next big thing for tech: the Internet of Everything. **Time Magazine**, Jan. 13, 2014. Disponível em: <http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/>. Acesso em: 25 jun. 2016.

BALEEIRO, Aliomar, DERZI, Misabel Abreu Machado. **Direito tributário brasileiro**. 13ª ed. [S.l.]: GEN/Forense, 2015.

BALER, Sinéad. More than 400 737 Max pilots are suing Boeing over an 'unprecedented cover-up' of flaws in the plane's design. **Business Insider**, 24 June 2019. Disponível em: <https://www.businessinsider.com/737-max-pilots-sue-boeing-claim-unprecedented-cover-up-issues-2019-6>. Acesso em: 24 jun. 2019.

BALOGH, Rafay. **Ethical hacking and penetration testing guide**. Boca Raton: CRC Press, 2015.

BARANIUK, Chris. Biostar security software 'leaked a million fingerprints'. **BBC**, London, ago. 2019. Disponível em: <https://www.bbc.com/news/technology-49343774>. Acesso em: 9 set. 2019.

BAUM, Robert J. **Ethics and Engineering curricula**. Garrison: The Hastings Center, 1980.

BEAVER, Kevin. **Hacking for dummies**. 4th ed. Hoboken: John Wiley & Sons, 2013.

BERENBACH, Brian; PAULISH, Daniel J.; KAZMEIER, Juergen; RUDORFER, Arnold. **Software & systems requirements engineering in practice**. [New York]: McGraw-Hill, 2009.

BIOLCHINI, Jorge; MIAN, Paula Gomes; NATALI, Ana Candida Cruz; TRAVASSOS, Guilherme Horta. **Systematic review in software engineering**. Rio de Janeiro: [COPPE/UFRJ?], 2005.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte Geral (arts. 1º a 120). 24 ed. rev.ampliada e atualizada. São Paulo: Saraiva Educação, 2018. V. 1.

BITTAR, Eduardo C. B. **Curso de Ética Jurídica**: ética geral e profissional. São Paulo: Saraiva, 2016.

BITTAR, Eduardo C. B.; ALMEIDA, Guilherme Assis de. **Curso de Filosofia do Direito**. 8. ed. São Paulo: Atlas, 2010.

BOOCH, Grady. **The software development team: a rational software white paper**. Cupertino: Rational Software, 1999.

BORGIA, Eleonora. The Internet of Things vision: Key features, applications and open issues. **Computer Communications**, [s.l.], v. 54, p. 1 - 31, Dec. 2014.

BORLAND SOFTWARE CORPORATION. **Mitigating risk with effective requirements engineering**. [S.l.]: Borland Software Corporation, 2005.

BOSE, Sujoy; KURHEKAR, Manish; GHOSHAL, Joydip. Agile methodology in requirements engineering. **SETLabs Briefings Online**, 2008.

BOYLESTAD, Robert, NASHELSKY, Louis. **Dispositivos eletrônicos e teoria de circuitos**. 3ª ed. [São Paulo?]: Prentice Hall do Brasil, 1986.

BRASIL. **Código civil**. Lei nº 10.406, de 10 de janeiro de 2002. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 11 de janeiro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 12 jul. 2016.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 de outubro de 1988.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 30 de outubro de 1984.

BRASIL. Lei nº 12.965/2014, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2 de abril de 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 15 de agosto de 2018.

BRASIL. Câmara dos Deputados. **Projeto de lei nº 3.065/2015**, de 22 de setembro de 2015. Dispõe sobre a regulamentação do exercício das profissões de Analista de Sistemas, Desenvolvedor, Engenheiro de Sistemas, Analista de Redes, Administrador de Banco de Dados, Suporte e suas correlatas, cria o Conselho Federal e os Conselhos Regionais de Informática e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=173856>. Acesso em: 9 set. 2019.

BRASIL. Câmara dos Deputados. **Projeto de lei nº 4.408/2016**, de 17 de fevereiro de 2016. Dispõe sobre o exercício profissional na área de Informática. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=207737>. Acesso em: 9 set. 2019.

BRASIL. Câmara dos Deputados. **Projeto de lei nº 5.101/2016**, de 27 de abril de

2016. Dispõe sobre a regulamentação do exercício da profissão de Analista de Sistemas e suas correlatas. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=208263>. Acesso em: 9 set. 2019.

BRASIL. Conselho Nacional de Saúde. Resolução nº 466, de 12 de dezembro de 2012. Aprova diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 13 de junho de 2013. Seção 1, p. 59.

BRAUSE, Rita S. **Writing your doctoral dissertation**: invisible rules for success. 1st ed. [S.l.]: Routledge, 1999.

BRITISH BROADCAST CORPORATION. Ethics: a general introduction. **Ethics guide**, [2014?], Disponível em: http://www.bbc.co.uk/ethics/introduction/intro_1.shtml. Acesso em: 21 jun. 2019.

BRONTE-STEWART, Malcom. Risk estimation from technology project failure. **EUROMOT 2009 4th European Conference on Management of Technology**, Glasgow, 2009. Disponível em: <http://www.princetwo.pwp.blueyonder.co.uk/PaperE01MalcolmBronteStewart.pdf>. Acesso em 28 abr. 2011.

BROOKS JR., Frederick P. No silver bullet: essence and accidents of Software Engineering. **Computer**, v. 20,. Los Alamitos/California, IEEE Computer Society Press, p. 10 – 19, abri. 1987. Disponível em: <http://worrydream.com/refs/Brooks-NoSilverBullet.pdf>. Acesso em: 17 jan. 2019.

BROOKS JR., Frederick P. **The mythical man-month**: essays on software engineering. Anniversary Edition. [S.l.]: Addison-Wesley, [2002?].

BRUMFIELD, Cynthia. Equifax's data breach disaster: Will it change executive attitudes toward security? **CSO**, Framingham, 24 jul. 2019. Disponível em: <https://www.csoonline.com/article/3411139/equifax-s-billion-dollar-data-breach-disaster-will-it-change-executive-attitudes-toward-security.amp.html>. Acesso em: 9 set. 2019.

BUCCIARELLI, Louis. Ethics and Engineering Education. **European Journal of Engineering Education**, vol. 33, n. 2, 2008.

BUFFA, Ester. A teoria em pesquisa: o lugar e a importância do referencial teórico na produção em educação. **Cadernos de Pós-Graduação**, São Paulo, v. 4, Educação, p. 33-38, 2005. Disponível em: <http://www4.uninove.br/ojs/index.php/cadernosdepos/article/viewFile/1792/1397>. Acesso em: 17 abr. 2011.

CALIFORNIA DEPARTMENT OF TRANSPORTATION (CALTRANS). **Project risk management handbook**. [Sacramento?]: CALTRANS, 2003.

CAMPANÁRIO, Milton de; ROVAI, Ricardo Leonardo; COSTA, Tiago Ribeiro. Metodologia e Níveis de Maturidade em Gestão de Riscos de Projetos nas Empresas de Serviços de Telecomunicações. **Congresso Virtual Brasileiro de**

Administração 04 (CONVIBRA 04). Disponível em: <http://risktrak.com/news/brazil-conference43.pdf>. Acesso em: 01 mar. 2010.

CAMPBELL, Darryl. Redline: The manu human erros that brought down the Boeing 737 MAX. **The Verge**, 2, May 2019. Disponível em: <https://www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa>. Acesso em: 23 jun. 2019.

CARRÁ, Bruno Leonardo Câmara. **Da responsabilidade civil do transportador aéreo**. 2004. 288f. Dissertação de Mestrado (Direito) - Universidade Federal do Ceará, Fortaleza, 2004.

CASTRO, José D'. **Avaliação de riscos em projetos de software a partir do uso de técnicas de inteligência computacional**. 2009. 61 f. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, 2009. Disponível em: <http://tcc.dsc.upe.br/>. Acesso em: 24 fev. 2010.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 11. ed. rev. e ampl. São Paulo: Atlas, 2014.

CERVO, Amado L.; BERVIAN, A. **Metodologia científica**. 5. ed. [S.l.]: Pearson Education, [s.d.].

CHAUÍ, Marilena de Souza. **Convite à Filosofia**. 13. ed. São Paulo: Ática, 2004.

CIN. UNIVERSIDADE FEDERAL DE PERNAMBUCO. Turma de 2010.1 da Disciplina IN1002 do Programa de Pós-Graduação. **Meta-tese**. Recife: CIn/UFPE, 2010.

CIN. UNIVERSIDADE FEDERAL DE PERNAMBUCO. Turma de 2011.1 da Disciplina IN1002 do Programa de Pós-Graduação. **Meta-Projeto**. Recife: CIn/UFPE, 2011.

CINTRA, Antônio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria geral do processo**. 25. ed., rev. e atual. São Paulo: Malheiros, 2009.

CISCO SYSTEMS INC. Connections Counter: The Internet of Everything in Motion. Cisco, july 29, 2013. **Cisco's Technology News Site**. Disponível em: <https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342>. Acesso em: 25 jun 2016.

CLARK, David. L.; GUBA, Egon; SMITH, Reald R. **Functions and definitions of a research proposal**. Bloomington: [College of Education?], 1977.

CLARK, Sam. Intel seeks dismissal of processor vulnerability class action. **Global Data Review**, 22 Oct. 2018. Disponível em: <https://globaldatareview.com/article/1175891/intel-seeks-dismissal-of-processor-vulnerability-class-action>. Acesso em: 24 jun. 2019.

COLLIER, Paul M. **Fundamentals of risk management for accountants and**

managers: Tools and techniques. [Oxford]: Elsevier, 2009.

CONTE, Tatyana Uchôa; MENDES, Emília; TRAVASSOS, Guilherme Horta. **Revisão sistemática sobre processos de desenvolvimento para aplicações web.** Rio de Janeiro: [COOPE/UFRJ?], 2004.

COOK, Deborah J.; MULROW, Cynthia D.; HAYNES, R. Brian. Systematic reviews: synthesis of best evidence for clinical decisions. **Annals of Internal Medicine**, Philadelphia, vol. 126, Mar. 1997. Disponível em: <http://www.annals.org/content/126/5/376.full>. Acesso em: 02 fev. 2010.

COOPER, Dale; GREY, Stephen; RAYMOND, Geoffrey; WALKER, Phil. **Project risk management guidelines:** managing risk in large projects and complex procurements. [West Sussex?]: John Wiley & Sons, 2005.

CORDEIRO, Alexander Magno; OLIVEIRA, Glória Maria de; RENTERÍA, Juan Miguel. Revisão sistemática: uma revisão narrativa. **Revista do Colégio Brasileiro de Cirurgiões**, Rio de Janeiro, vol. 34, nov./dez. 2007. Disponível em: <http://www.scielo.br/pdf/rcbc/v34n6/11.pdf>. Acesso em: 02 fev. 2010.

COURAGE, Catherine; BAXTER, Kathy. **Understanding your users:** a practical guide to user requirements methods, tools and techniques. [San Francisco?]: Morgan Kaufmann, 2005.

COX, Sue; TAIT, Robin. **Safety, reliability and risk management:** and integrated approach. 2nd ed. Oxford: Butterworth-Heinemann, 1998.

CRAFT, Rick *et al.* **An open framework for risk management:** an integrated approach. 2nd ed. Oxford: Butterworth-Heinemann, 1998.

CRENSHAW, Adrian. Ethics of full disclosure concerning security vulnerabilities. **Iron Geek**, [2019?]. Disponível em: <https://www.irongeek.com/i.php?page=security/ethics-of-full-disclosure-concerning-security-vulnerabilities>. Acesso em: 26 jun. 2019.

CRESWELL, John W. **Qualitative inquiry & research design:** choosing among five approaches. 2nd ed. Thousand Oaks: Sage Publications, 2007.

CRUZES, Daniela S.; DYBÅ, Tore. Recommended steps for thematic synthesis in software engineering. **ESEM'11 proceedings of the 2011 International Symposium on Empirical Software Engineering and Measurement, Washington**, [s.p.], 2011. Disponível em: <http://www.idi.ntnu.no/grupper/su/publ/daniela/esem2011-Cruzes-p91-thematic-synth.pdf>. Acesso em: 28 mai. 2013.

DAVIS, Michael. Thinking like an Engineer: the plade of a Code of Ethics in the practice of a profession. **Philosophy and Public Affairs**, vol. 20, n. 2, 1991.

DAVIS, Michael. Engineering Ethics, individuals and organizations. **Science and Engineering Ethics**, vol. 12, n. 2, p. 223 – 231, 2006.

DAWSON, Catherine. **Introduction to research methods:** a pratical guide for everyone undertaking a research project. 4th ed. [Begbroke?]: How To Books, 2009.

DEAN, Lindsey. 10 fantastic hidden clauses in contracts and end user license agreements. **One Legal**, 2017. Disponível em: <https://www.onelegal.com/blog/fantastic-clauses-hidden-in-contracts-and-eulas/>. Acesso em: 24 jun. 2019.

DeMARCO, Tom; LISTER, Timothy. **Peopleware**: como gerenciar equipes e projetos tornando-os mais produtivos. São Paulo: McGraw-Hill, 1990.

DIAS, José de Aguiar. **Da responsabilidade civil**. 10. ed. Rio de Janeiro: Forense, 1997. v. I.

DIAS, José de Aguiar. **Responsabilidade civil em debate**. Rio de Janeiro: Forense, 1983.

DINIZ, Maria Helena. **Compêndio de introdução à Ciência do Direito**. 11. ed. Atual. São Paulo: Saraiva, 1999.

DINIZ, Maria Helena. **Compêndio de introdução à Ciência do Direito**. 23. ed. São Paulo: Saraiva, 2012.

DOOLEY, John. **Software development and professional practice**: writing great programs from start to finish. [New York?]: Apress, 2011.

DRUCKER, Peter Ferdinand. **Managing in a time of great chance**. New York: Truman Talley Books/Dutton, 1995.

DUC, Anh Nguyen, ABRAHAMSSON, Pekka. Minimum Viable Product or Multiple Facet Product? The role of MVP in software startups. **Agile Processes, in Software Engineering, and Extreme Programming. XP 2016**, vol. 251, p. 118-130. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-33515-5_10. Acesso em: 30/01/2019.

DYKSTRA, Josiah. **Essential Cybersecurity Science**: build, test, and evaluate secure systems. 1st ed. Sebastopol: O'Reilly, 2016.

ESTADO DE SÃO PAULO. Sobrou pouco da época da reserva de mercado, **O Estado de São Paulo**, São Paulo, 26 out. 2014. Disponível em: <https://link.estadao.com.br/noticias/geral,sobrou-pouco-da-epoca-da-reserva-de-mercado,10000030238>. Acesso em: 9 set. 2019.

EASTERBROOK, Steve; SINGER, Janice; STOREY, Margaret-Anne; DAMIAN, Daniela. Selecting empirical methods for engineering research. **Guide to advanced empirical software engineering**, [s.l.]: Springer, 2007.

ESTRELLA GUTIÉRREZ, Graciela N. Messina de. **La responsabilidad civil en la era tecnológica**: tendencias y prospectiva. 2. ed. Buenos Aires: Abeledo Perrot, 1997.

EVANS, Isabel. **Achieving software quality through teamwork**. Norwood: Artech House, 2004.

EULA TEMPLATE. **Eula Templates**, [2019?]. Disponível em:

<https://www.eulatemplate.com/>. Acesso em: 24 jun. 2019.

FERGUSON, Scott. Gearbest Database Leaks 1.5 Million Customer Records. **Data Breach Today**, Princeton, mar. 2019. Disponível em: <https://www.databreachtoday.com/gearbest-database-leaks-15-million-customer-records-a-12198>. Acesso em: 9 set. 2019.

FERGUSON, Scott. Volusion Payment Platform Sites Hit by Attackers. **Bank Info Security**, Princeton, out. 2019. Disponível em: <https://www.bankinfosecurity.com/volusion-payment-platform-sites-hit-by-attackers-a-13229>. Acesso em: out. 2019.

FIRST. **Common Vulnerability Scoring System version 3.1**: User Guide. Cary: First, 2019. Disponível em: <https://www.first.org/cvss/user-guide>. Acesso em: 9 set. 2019.

FLEDDERMANN, C. B. **Engineering Ethics**. Upper Saddle River: Pearson, 2012.

FLORES, Fabiana F. S. **Riscos em projetos de software**: genéricas considerações sobre riscos e seu atual tratamento no desenvolvimento de sistemas. 2010. 175 p. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, 2010. Disponível em: tcc.ecomp.poli.br/20101/TCC_final_Fabiana.pdf. Acesso em: 25 mar. 2016.

FLORES, Albert; JOHNSON, Deborah G. Collective responsibility and professional roles. **Ethics**, vol. 93, n. 3, p. 537 – 545, Apr., 1983.

FOGLIATTO, Flavio; SILVEIRA, Giovani da; RIBEIRO, José Luis Duarte. Diretrizes para elaboração do Referencial Teórico e Organização de Textos Científicos. **Seminário de Pesquisa 2**, [s.l.], 2007. Disponível em: http://www.producao.ufrgs.br/arquivos/disciplinas/146_seminario_de_pesquisa_2_dirtrizes_referencial_teorico.doc. Acesso em: 17 abr. 2011.

FORMSWIFT. **FormSwift End User License Agreement Form**, [2019?]. Disponível em: <https://formswift.com/end-user-licensing-agreement>. Acesso em: 24 jun. 2019.

FRUHLINGER, Josh. The OPM hack explained: Bad security practices meet China's Captain America. **CSO**, Framingham, 2018. Disponível em: <https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.amp.html>. Acesso em: 9 set. 2019.

GAMEDEV. When is an EULA necessary? **GameDev.net**, 2013. Disponível em: <https://www.gamedev.net/forums/topic/643142-when-is-an-eula-necessary/>. Acesso em: 24 jun. 2019.

GARCIA, Vinicius Cardoso. **Rise Reference Model for Software Reuse Adoption in Brazilian Companies**. 2010. Tese (Doutorado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2010.

GATLAN, Sergiu. Zendesk Security Breach May Impact Orgs Like Uber, Slack, and FCC. **Bleeping Computer**, Huntington Station, out. 2019. Disponível em:

<https://www.bleepingcomputer.com/news/security/zendesk-security-breach-may-impact-orgs-like-uber-slack-and-fcc/>. Acesso em: 9 out. 2019.

GIBBS LAW GROUP. Sony /BMG Digital Rights Management Lawsuit. **Gibbs Law Group**, [S.d.]. Disponível em: <https://www.classlawgroup.com/sony-digital-rights-management-lawsuit/>. Acesso em: 24 jun. 2019.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GLYNN, Fergal. HP Faces Class Action Lawsuit Over Printer Software Vulnerability. **Veracode**, 6 Dec. 2011. Disponível em: <https://www.veracode.com/blog/2011/12/hp-faces-class-action-lawsuit-over-printer-software-vulnerability>. Acesso em: 24 jun. 2019.

GOETHE, Johann Wolfgang. **Fausto**. 4. ed. [S.l.]: Itatiaia, 1997.

GOMES FILHO, Marcílio José Albuquerque. **Um processo de avaliação da portabilidade de unidades de software**. 2005. 70 p. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Centro de Informática da UFPE, Universidade Federal de Pernambuco, 2005.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**: contratos e atos unilaterais. 9. ed. São Paulo: Saraiva, 2012. v. 3.

GORNIACK-KOCIKOWSKA, Krystyna. The Computer Revolution and the Problem of Global Ethics. **Science and Engineering Ethics**, vol. 2, n. 2, p. 177 – 190, June 1996.

GOTTERBARN, D., MILLER, K., ROGERSON, S. Software Engineering Code of Ethics. **Communications of the ACM**, vol. 40, n. 11, 1997.

GOTTERBARN, D., MILLER, K., ROGERSON, S. Software Engineering Code of Ethics is approved: The exhaustive efforts of the ACM and IEEE-CS has resulted in the adoption of a code of professional practices for software engineers to consider – and use. **Communications of the ACM**, vol. 43, n. 10, 1999.

GRAU, Eros Roberto. A reserva de mercado, no Brasil, para a produção de bens de informática. **Revista da Faculdade de Direito**, Universidade de São Paulo, São Paulo, v. 84/85, p. 204 – 217, 1990. Disponível em: <http://www.periodicos.usp.br/rfdusp/article/view/67140/69750>. Acesso em: 9 set. 2019.

GRAY, Carole; MALINS, Julian. **Visualizing research**: a guide to the research process in Art and Design. Aldershot: Ashgate, 2004.

GREAT BRITAIN. **The Parliamentary Debates**. East Lansing: Reuter's Telegram Company, 1906.

GREGG, Aaron, O'CONNELL, Jonathan, TRAN, Andrew Ba, SIDDIQUI, Faiz. At tense meeting with Boeing executives, pilots fumed about being left in dark on plane software. **Washington Post**, 13 Mar. 2019. Disponível em:

https://www.washingtonpost.com/business/economy/new-software-in-boeing-737-max-planes-under-scrutiny-after-second-crash/2019/03/13/06716fda-45c7-11e9-90f0-0ccfeec87a61_story.html?utm_term=.1ed8ffb8eb49. Acesso em: 23 jun. 2019.

GUTIÉRREZ, Graciela N. Messina de Estrella. **La responsabilidad civil en la era tecnológica**: tendencias y prospectiva. 2. ed. act. Buenos Aires: Abeledo-Perrot, 1997.

HACKERONE. Severity. **HackerOne Docs**, [San Francisco?], 2019. Disponível em: <https://docs.hackerone.com/hackers/severity.html>. Acesso em: 9 set. 2019.

HAFELE, David M. **Three different shades of ethical hacking**: black, white and gray. [S.l.]: Sans Institute, 2004. Disponível em: <https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390>. Acesso em 20 jun. 2019.

HALFACREE, Gareth. Lenovo class-action could pay out \$55 per user. **Bit-tech**, 21 Feb. 2019. Disponível em: <https://bit-tech.net/news/tech/software/lenovo-class-action-could-pay-out-55-per-user/1/>. Acesso em: 24 jun. 2019.

HANNAY, Jo E.; SJØBERG, D.; DYBÅ, Tore. A systematic review of theory use in software engineering experiments. **IEEE Transactions on Software Engineering**, [s.l.], vol. 33, no. 2. Feb. 2007.

HANSSON, M. Berndtsson; LUNDELL, B. Olsson. **Thesis projects**: a guide for students in Computer Science and Information Systems. 2nd ed. [London?]: Springer, 2008.

HASS, Kathleen B. The blending of traditional and agile management. **PMWorld Today**, [s.l.], vol. IX, issue V, May 2007. Disponível em: <http://www.pmforum.org/library/tips/2007/PDFs/Hass-5-07.pdf>. Acesso em: 03 mai. 2010.

HENRIQUES, Antonio; MEDEIROS, João Bosco. **Monografia no curso de direito: trabalho de conclusão de curso**: metodologia e técnicas de pesquisa, da escolha do assunto à apresentação gráfica. 3. ed. São Paulo: Atlas, 1999.

HIDALGO, Antonio; ALBORS, José. New innovation management paradigms in the knowledge-driven economy. **Management of technology innovation and value creation**: selected papers from the 16th International Conference on Management of Technology, Toh Tuck Link – Singapore, p. 3 - .19, 2008.

HIGGINS, Julian P. T.; GREEN, Sally. (Edit). **Cochrane handbook for systematic reviews of interventions**. Oxford: The Cochrane Collaboration, 2009. Disponível em: <http://www.cochrane-handbook.org/>. Acesso em: 01 mar. 2010.

HM TREASURY. **The orange book**: management of risks – principles and concepts. [London?]: HM Treasury, 2004.

HOBBS, Thomas. **Léviathan: traité de la matière, de la forme et du pouvoir ecclésiastique et civil**. Chicoutimi: Université du Québec, 2017. DOI=<http://dx.doi.org/doi:10.1522/cla.hot.lev>.

HOFFMAN, Chris. 10 ridiculous EULA clauses that you may have already agreed to. **MakeUseOf**, 2012. Disponível em: <https://www.makeuseof.com/tag/10-ridiculous-eula-clauses-agreed/>. Acesso em: 24 jun. 2019.

HOOD, Colin; WIEDMANN, Simon; FLICHTINGER, Stefan.; PAUTZ, Urte. **Requirements management**: the interface between requirements development and all other systems engineering processes. [S.l.]: Springer, 2008.

HULL, Elizabeth; JACKSON, Ken; DICK, Jeremy. **Requirements engineering**. 2nd ed. [S.l.]: Springer, 2011.

HULL, Elizabeth; JACKSON, Ken; DICK, Jeremy. **Requirements engineering**. 3rd ed. [Kent?]: Springer, 2005.

IBGE. **Normas de apresentação tabular**. 3. ed. Rio de Janeiro: IBGE, 1993. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/monografias/GEBIS%20-%20RJ/normastabular.pdf>. Acesso em: 08 mai. 2010.

IKEHARA, Hideharu Carlos. A reserva de mercado de Informática no Brasil e seus resultados. **Akrópolis – Revista de Ciências Humanas da UNIPAR**, Umuarama, v. 5, n. 18, 1997. Disponível em: <http://revistas.unipar.br/index.php/akropolis/article/view/1694>. Acesso em: 9 set. 2019.

IEEE COMPUTER SOCIETY, ASSOCIATION FOR COMPUTING MACHINERY. **Software Engineering Code of Ethics**. [S.l.]: IEEE/ACM, 1999. Disponível em: <https://www.computer.org/web/education/code-of-ethics>. Acesso em: 21 jan. 2019.

IIVARI, Juhani. Dilemmas of IS Development. **Proceedings of the Fifth International Conference on Information Systems Development**, Gdansk/Polônia, p. 35 – 53, Sept. 1996. Disponível em: https://www.researchgate.net/publication/259331745_Dilemmas_of_IS_Development. Acesso em: 17 jan. 2019.

ILASCU, Ionut. Details of 92 million Brazilians auctioned on underground forums. **Bleeping Computer**, Nova York, 4 out. 2019. Disponível em: <https://www.bleepingcomputer.com/news/security/details-of-92-million-brazilians-auctioned-on-underground-forums/>. Acesso em 10 out. 2019.

ISTO É DINHEIRO. Os efeitos colaterais da Lei de Informática. **Isto é Dinheiro**, São Paulo, 21 out. 2009. Disponível em: <https://www.istoedinheiro.com.br/noticias/mercado-digital/20091021/efeitos-colaterais-lei-informatica/11861>. Acesso em: 9 set. 2019.

JEONG, Christina Y., LEE, Sang-Yong Tom, LIM, Jee-Hae. Information security breaches and IT security investments: impacts on competitors. **Information & Management**, v. 56, p. 681-695, July 2019.

JEYNES, Jacqueline. **Risk management**: 10 principles. Oxford: Buitenworth-Heinemann, 2001.

JUTTE, Bart. **Ten golden rules of project risk management**. [S.l.]: Concilio business solutions for professionals, 2008.

KANELL, Michael E. Two years after breach, Equifax costs top \$1.25 billion. **AJC**, Atlanta, 13 maio 2019. Disponível em: <https://www.ajc.com/business/two-years-after-breach-equifax-costs-top-billion/EJ4QQQx1vltPJDsvC4EqOM/>. Acesso em: 9 set. 2019.

KANG, Xie; LIU, Mei; ZHENBANG, Rong; YONG, Hu . A neural network approach for software risk analysis. In: ICDM Workshops 2006, 2006, Hong Kong. **Sixth IEEE International Conference on Data Mining Workshops**. Hong Kong: ICDM Workshops, 2006. Disponível em: http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=4063720&queryText%3DA+Neural+Networks+Approach+for+Software+Risk+Analysis%26openedRefinements%3D*%26searchField%3DSearch+All. Acesso em: 16 mar. 2010.

KANT, Immanuel. **Crítica da razão pura**. Rio de Janeiro: Tecnoprint, [1982?].

KASPERSKY. IoT security leads to legal headaches. **Kaspersky Daily**, 20 aug. 2018. Disponível em: <https://www.kaspersky.com/blog/insecurity-of-iot-legal-issue/23527/>. Acesso em: 26 jun. 2019.

KEIL, Mark; LI, Lei.; MATHIASSEN, L.; ZHENG, Guangzhi. The influence of checklists and roles on software practitioner risk perception and decision-making. In: HICSS'06, 2006, Hawaii. **Proceedings of the 39th Annual Hawaii International Conference on System Sciences**. Hawaii: HICSS06, 2006. Disponível em: http://ieeexplore.ieee.org/search/freesrchabstract.jsp?=&arnumber=1579760&querytext%3DThe+Influence+of+Checklists+andRoles+on+Software+Practitioner+Risk%26openedRefinements%3D*%26searchField%3DSearch+All. Acesso em: 16 mar. 2010.

KELLY, Allan. **Changing software development: learning to become agile**. West Sussex: John Wiley & Sons, [2008?].

KITCHENHAM, B.; CHARTERS, Stuart. Guidelines for performing systematic literature reviews in software engineering. **EBSE Technical Report**, version 2.3, EBSE-2007-01, 2007.

KOTHARI, C. R. **Research methodology: methods & techniques**. New Delhi: New Age International, 2004.

KOTONYA, Gerald; SOMMERVILLE, Ian. **Requirements engineering: processes and techniques**. Wiltshire: John Wiley & Sons, 2003.

KREBS, Brian. Credit Union Sues Fintech Giant Fiserv Over Security Claims. **KrebsOnSecurity**, [S.l.], 3 may 2019. Disponível em: <https://krebsonsecurity.com/2019/05/credit-union-sues-fintech-giant-fiserv-over-security-claims/>. Acesso em: 9 set. 2019.

KREBS, Brian. Breach at Hy-Vee Supermarket Chain Tied to Sale of 5M+ Stolen Credit, Debit Cards. **KrebsOnSecurity**, [S.l.], 22 ago 2019. Disponível em: <https://krebsonsecurity.com/2019/08/breach-at-hy-vee-supermarket-chain-tied-to-sale-of-5m-stolen-credit-debit-cards/>. Acesso em: 9 set. 2019.

KURBEL, Karl. E. **The making of information systems: software engineering and**

management in a globalized world. Frankfurt: Springer, 2008.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. São Paulo: Atlas, 1991.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia Científica**. 2. ed. São Paulo: Atlas, 1992.

LANDIS, Sean. **Agile hiring**: transform how you hire software professionals. 1st printing. Walnut Creek: Artima, 2011.

LAPLANTE, Phillip A. Professional licensing and the social transformation of software engineers. **IEEE Technology and Society Magazine**, v.24, issue 2, p. 40 – 45, June 2005.

LAW DEPOT. **Free EULA**, [2019?]. Disponível em: <https://www.lawdepot.com/contracts/software-license-agreement/?loc=US#.XRFVRj9KjIV>. Acesso em: 24 jun. 2019.

LEFFINGWELL, Dean. **Agile software requirements**: lean requirements practices for teams, programs, and the enterprise. Boston: Addison-Wesley, 2011.

LEGAL TEMPLATES. **Free End User License Agreement**, [2019?]. Disponível em: <https://legaltemplates.net/form/end-user-license-agreement/>. Acesso em: 24 jun. 2019.

LEYDEN, John. Foxit PDF reader devs admit data breach impacted users. **The Daily Swig**, Knutsford, set. 2019. Disponível em: <https://portswigger.net/daily-swig/foxit-pdf-reader-devs-admit-data-breach-impacted-users>. Acesso em: 9 set. 2019.

LEOPOLD, George. Software won't fix Boeing's 'Faulty' Airframe. **EE Times**, 27 Mar. 2019. Disponível em: https://www.eetimes.com/document.asp?doc_id=1334482. Acesso em: 23 jun. 2019.

LEOPOLD, George. Boeing 737 MAX: A Question of Ethical Engineering. **EET India**, 28 Mar. 2019. Disponível em: <https://www.eetindia.co.in/news/article/Boeing-737-MAX-A-Question-of-Ethical-Engineering>. Acesso em: 23 jun. 2019.

LEITE, Eduardo de Oliveira. **A monografia jurídica**. 6. ed. São Paulo: Revista dos Tribunais, 2004.

LENZA, Pedro (Coord.). **Direito civil esquematizado**. São Paulo: Saraiva, 2011. v. I.

LEVENSON, Nancy. Medical Devices: The Therac-25. In: **Safeware: system safety and computers**. [S.l.]: Addison-Wesley, 1995.

LEVY, Yair; ELLIS, Timothy J. A systems approach to conduct an effective literature review in support of information systems research. **Informing Science Journal**, florida, vol. 9, p. 181 – 212, 2006. Disponível em: <http://inform.nu/Articles/Vol9/V9p181-212Levy99.pdf>. Acesso em: 24 fev. 2010.

LIMA JÚNIOR, Orlando Fontes. **Manual de orientação ao Pesquisador**. Campinas: UNICAMP, 2004. Disponível em: http://www.fec.unicamp.br/~oflimaj/Manual_Pesquisador_2004.pdf. Acesso em: 12 mai. 2011.

MACMILLAN, Douglas. "Safety was just a given": Inside Boeing's boardroom amid the 737 Max crisis. **Washington Post**, 5 May 2019. Disponível em: https://www.washingtonpost.com/business/2019/05/06/safety-was-just-given-inside-boeings-boardroom-amid-max-crisis/?noredirect=on&utm_term=.3c7cbc85d6ca. Acesso em: 23 jun. 2019.

MACZYK, Geoffrey; DE MATTEO, David; FESTINGER, David. **Essentials of research design and methodology**. Hoboken: John Wiley & Sons, Inc., 2005.

MADSEN, Annette. Count Lucanor by Don Juan Manuel as inspiration for Hans Christian Andersen and other European writers. **The Hans Christian Andersen Centre**, Odense, 2015. Disponível em: https://andersen.sdu.dk/forskning/konference/tekst_e.html?id=10922. Acesso em 9 set. 2019.

MANBER, Udi. Introduction to Algorithms: a creative approach. 1st ed. [S.l.]: Addison-Wesley, 1989.

MAIWALD, Eric. **Network security**: a beginner's guide. 3rd ed. [S. l.]: McGraw Hill, 2013.

MASIERO, Paulo Cesar. **Ética em Computação**. São Paulo: EDUSP, 2008.

MATSAKIS, Louise; LAPOWSKY, Issie. Everything We Know About Facebook's Massive Security Breach. **Wired**, set. 2018. Disponível em: <https://www.wired.com/story/facebook-security-breach-50-million-accounts/amp>. Acesso em: 9 set. 2019.

MAYER, N.; DUBOIS, E.; RIFAUT, A. Requirements Engineering for improving Business/IT alignment in security risk management methods. **Enterprise interoperability II**, [S.l.], Springer, p. 15 - 26, 2007.

McCARTHY, Kieren. Jeep hacking lawsuit shifts into gear for trial after US Supremes refuse to hit the brakes. **The Register**, 8 Jan. 2019. Disponível em: https://www.theregister.co.uk/2019/01/08/jeep_hacking_supreme_court/. Acesso em: 24 jun. 2019.

McNEILS, Alexander J.; FREY, Rüdiger; EMBRECHTS, Paul. **Quantitative risk management**: concepts, techniques and tools. Princeton: Princeton University Press, 2005.

MEIRA, Silvio Romero de Lemos. tudo é software... **dia a dia, bit a bit**, [s.l.], 27 ago. 2008. Disponível em: <http://boletim.de/silvio/tudo-e-software/>. Acesso em: 25 jun. 2016.

MEIRA, Silvio, BURÉGIO, Vanilson, BORBA, Paulo, GARCIA, Vinicius, ALBUQUERQUE, Jones, SOARES, Sérgio. Programming the Universe: the first

commandment of Software Engineering for all varieties of information systems. **30th Brazilian Symposium on Software Engineering**, Maringá, set. 2016.

MENEZES JÚNIOR, Júlio Venâncio de. **RBTTool**: proposta de ferramenta de automação das atividades de teste baseado em riscos. 2009. 63 f. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, 2009. Disponível em: <http://tcc.dsc.upe.br>. Acesso em: 01 mar. 2010.

MERRIAM, Sharan B. **Qualitative research**: a guide to design and implementation. Jossey-Bass, San Francisco; Jossey-Bass, 2009.

MEHROTRA, Kartikay. Facebook Must Face Lawsuit Over 29 Million-User Data Breach. **Bloomberg**, Nova York, jun. 2019. Disponível em: <https://www.bloomberg.com/amp/news/articles/2019-06-24/facebook-must-face-lawsuit-over-29-million-user-data-breach>. Acesso em: 9 set. 2019.

MEYER, Bertrand. Dependable software, to appear in Dependable Systems; Software, Computing Networks, eds. Jürg Kohlas, Bertrand Meyer, André Schiper, **Lectures Notes in Computer Science**, [S.l.], Springer-Verlag, 2006. Disponível em: inf.ethz.ch/~meyer/publications/lncs/dependability.pdf. Acesso em: 28 abr. 2016.

MIRANDA, Pontes de. **Direito das obrigações: direitos das obrigações, fatos ilícitos absolutos...** Atualização de Rui Stoco. São Paulo: Revista dos Tribunais, 2012. (Coleção Tratado de Direito Privado: parte especial). Tomo III.

MOLAK, Vlasta. **Fundamentals of risk analysis and risk management**. [Boca Raton]: Lewis Publishers, 1997.

MOREIRA, Marcílio Marques; REIS, Fábio Wanderley; COSTA, Caio Túlio; LA TAILLE, Yves de; TIBA, Içami. **Cultura das transgressões no Brasil**: visões do presente. São Paulo: Saraiva, 2009.

MORETTI, Neuza (Coord.). **Manual de metodologia científica**: como elaborar trabalhos acadêmicos. [Cafelândia?]: União de Ensino Superior de Cafelândia, 2008.

MOUGAYAR, William. **Blockchain para negócios**: promessa, prática e aplicação da nova tecnologia. Rio de Janeiro: Alta Books, 2017.

MÜLLER, Mary Stela; CORNELSEN, Julce Mary. **Normas e padrões para teses, dissertações e monografias**. 5. ed. Londrina: Editora da Universidade Estadual de Londrina, 2003.

MÜNCH, Jürgen; FAGERHOLM, Fabian; JOHNSON, Patrik; PIIRTTILAHTI, Janne; TORKKEL, Jua; JÄRVINEN, Janne. Creating Minimum Viable Products in Industry-Academy collaborations. **Lean Enterprise Software and Systems (LESS)**, Springer, Berlin, vol. 167, p. 137-151, 2013.

NADER, Paulo. **Curso de Direito Civil**: parte geral. 10. ed. rev. atual. e ampl. Rio de Janeiro: Forense, 2016. v. 1.

NADER, Paulo. **Curso de Direito Civil**: responsabilidade civil. 6. ed. rev. atual. e

ampl. Rio de Janeiro: Forense, 2016. v. 7.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes corporativos**. 1. ed. 7. reimp. São Paulo: Novatec, 2014.

NALINI, José Renato. **Ética geral e profissional**. São Paulo: Revista dos Tribunais, 2015.

NASCIMENTO, Dinalva. **Metodologia do trabalho científico**: teoria e prática. Rio de Janeiro: Forense, 2002.

NASCIMENTO, Leandro Marques do. **SMADL – The social machines architecture description language**. 2014. Tese (Doutorado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2014.

NÉLO, Ana Maria. Metodologia científica: um enfoque referente à estrutura da pesquisa contábil. **Revista Brasileira de Contabilidade**, [s.l.], n. 99, [s.d.]. Disponível em: http://www.bahai.org.br/virtual/metodologia_cientifica.htm. Acesso em: 12 mai. 2011.

NEVES, José Luis. Pesquisa qualitativa: características, usos e possibilidades. **Caderno de Pesquisas em Administração**, São Paulo, v.1, n. 3, 1996. Disponível em: <http://www.ead.fea.usp.br/cad-pesq/arquivos/C03-art06.pdf>. Acesso em: 28 mai. 2011.

NEVES, Luiz Antônio Pereira. **Pesquisa**: escolha do método. Joinville: Universidade do Estado de Santa Catarina, [s.d.]. Disponível em: http://www.joinville.udesc.br/sbs/professores/neves/materiais/Prof_Neves___Aula_3___Metodo_Cientifico.pdf. Acesso em: 12 mai. 2011.

NEWITZ, Annalee. Dangerous terms: a user's guide to EULAs. **Electronic Frontier Foundation**, 2005. Disponível em: <https://www.eff.org/wp/dangerous-terms-users-guide-eulas>. Acesso em: 24 jun. 2019.

NEWMAN, Jared. Top EULA gotchas: website fine-print hall of shame. **PCWorld**, 2012. Disponível em: https://www.pcworld.com/article/249396/top_eula_gotchas_website_fine_print_hall_of_shame.html. Acesso em: 24 jun. 2019.

NOGUEIRA, Ruy Barbosa. **Curso de Direito tributário**. São Paulo: Saraiva, 1990.

NORTHOVER, Mandy; BOAKE, Andrew; KOURIE, Derrick G.; GRUNER, Stefan. Towards a philosophy of software development: 40years after the birth of software engineering. **Journal for general Philosophy of Science**, [New York?], v. 39, n.1. Sept. 2008. Disponível em: <http://www.springerlink.com/content/m7723416410k21g4/>. Acesso em: 16 mar. 2010.

NUNES, Luiz Antonio Rizzatto. **Manual de monografia jurídica**: como se faz: uma monografia, uma dissertação, uma tese. 3. ed. São Paulo: Saraiva, 2001.

OGATA, Katsuhiko. **Engenharia de controle moderno**. 3. ed. Rio de Janeiro: Prentice-Hall do Brasil, 1998.

OLIVEIRA, Djalma de Pinho Rebouças. **Administração de processos**: conceitos, metodologia, práticas. 3. ed. São Paulo: Atlas, 2009.

OLIVEIRA, Keldjan Alves de. **Um modelo para identificação de riscos no teste de software**. 2008. 55 f. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Escola Politécnica de Pernambuco, Universidade de Pernambuco, Recife, 2008. Disponível em: <http://tcc.dsc.upe.br/>. Acesso em: 01 mar. 2010.

OLIVEIRA, Sílvio Luiz. **Metodologia científica aplicada ao direito**. São Paulo: Pioneira Thomson Learning, 2002.

OWASP, The OWASP Foundation. **OWASP Risk Rating Methodology**. Maryland: The OWASP Foundation, jun. 2019. Disponível em: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. Acesso em: 9 set. 2019.

OWASP, The OWASP Foundation. **OWASP Top 10 – 2017**: The Ten most critical web application security risks. Maryland: The OWASP Foundation, 2017. Disponível em: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. Acesso em: 9 set. 2019.

PAGANINI, Pierluigi. Jackson County paid \$400,000 to crooks after ransomware attack. **Security Affairs**, [S.l.], mar. 2019. Disponível em: <https://securityaffairs.co/wordpress/82218/cyber-crime/jackson-county-ransomware-attack.html>. Acesso em: 9 set. 2019.

PAGANINI, Pierluigi. Lake City agreed to pay \$500,000 in ransom, is the second case in Florida in a week. **Security Affairs**, [S.l.], jun. 2019. Disponível em: <https://securityaffairs.co/wordpress/87621/hacking/lake-city-500k-ransom.html>. Acesso em: 9 set. 2019.

PAGANINI, Pierluigi. The Riviera Beach City pays \$600,000 in ransom. **Security Affairs**, [S.l.], jun. 2019. Disponível em: <https://securityaffairs.co/wordpress/87381/breaking-news/riviera-beach-city-ransomware.html>. Acesso em 9 set. 2019.

PAGANINI, Pierluigi. Global Shipping and mailing services firm Pitney Bowes hit by ransomware attack. **Security Affairs**, [S.l.], out. 2019. Disponível em: <https://securityaffairs.co/wordpress/92526/malware/pitney-bowes-ransomware-attack.html>. Acesso em: 16 out. 2019.

PAGANINI, Pierluigi. Click2Mail suffered a data breach that potentially impacts 200,000 registrants. **Security Affairs**, [S.l.], 15 out. 2019. Disponível em: <https://securityaffairs.co/wordpress/92529/data-breach/click2mail-data-breach.html>. Acesso em: 16 out. 2019.

PANDIAN, C. Ravindranath. **Applied software risk management**: a guide for software managers. [Boca Raton: Auerbach Publications, 2007].

PAQUETTE, Danielle. Le rôle du cadre de référence théorique dans une recherche monographique constructiviste. **Recherches qualitatives**, Quebec, vol. 27(1), p. 3-

21, 2007. Disponível em: <http://www.recherche-qualitative.qc.ca/numero27%281%29/paquette.pdf>. Acesso em: 28 abr. 2011.

PARK, Sangchul. Why information security law has been ineffective in addressing security vulnerabilities: evidence from California data breach notifications and relevant court and government records. **International Review of Law and Economics**, v. 58, p. 132 – 145, June 2019.

PLATÃO. **O mito da caverna**. [Belém?]: EDUFPA, 2013.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. 12. ed. Rio de Janeiro: Forense, 2005. v. I, II, III.

PEREIRA, Caio Mário da Silva. 22. ed. Rio de Janeiro: Forense, 2009. v. I, II, III.

PETTICREW, Mark; ROBERTS, Helen. **Systematic review in the social sciences: a practical guide**. Oxford: Blackwell Publishing, 2006.

PICHLER, Roman. **Agile product management with scrum**: creating products that customers will love. 1st printing. Boston: Addison-Wesley, 2010.

POEL, Ibo van de; ZANDVOORT, Henk; BRUMSEN, Michiel. Ethics and Engineering Courses at Delft University of Technology: contents, educational setup and experiences. **Science and Engineering Ethics**, v. 7., n. 2, June 2001.

POKORNY, Zane. Is that vulnerability critical? Judging the severity of threats with threat intelligence, **Recorded Future**, Boston, mar. 2019. Disponível em: <https://www.recordedfuture.com/judging-threat-severity/>. Acesso em: 9 set. 2019.

PONEMON INSTITUTE. **2017 Cost of Data Breach Study**: global overview. Traverse City: Ponemon Institute, 2017. Disponível em: <https://www.ibm.com/downloads/cas/ZYKLN2E3>. Acesso em: 9 set. 2019.

PONTEFRAC, Dan. Boeing's 737 MAX Crisis is a Leadership Issue. **Forbes**, 18 Mar. 2019. Disponível em: <https://www.forbes.com/sites/danpontefract/2019/03/18/boeings-737-max-crisis-is-a-leadership-issue/#673a5d306a0a>. Acesso em: 23 jun. 2019.

PORUP, J. M. IoT vendors ignore basic security best practices, CITL research finds. **CSO**, Framingham, 10 set. 2019. Disponível em: . Acesso em: 10 set. 2019.

POTTER, Ben; TILL, David; SINCLAIR, Jane. **An introduction to formal specification and Z**. Upper Saddle River: Prentice Hall, 1996.

PRESSBURGER, Thomas; FEATHER, Martin. S.; DI VITO, Ben; HINCHEY, Michael; MARKOSIN, Lawrence; TREVINO, Luis C. Infusing software assurance research techniques into use. **IEEE Aerospace Conference # 1506**, Manhattan Beach, v.1, Sept. 2005. Disponível em: <http://trs-new-jpl.nasa.gov/dspace/bitstream/2014/38052/1/05-3175.pdf>. Acesso em: 10 fev. 2010.

PRESSMAN, Roger S. **Ingeniería del Software**: un enfoque práctico. 5 ed. Madrid:

McGraw-Hill, 2002.

PROJECT MANAGEMENT INSTITUTE. **A guide to the project management body of knowledge**. 3rd ed. Newton Square, Pennsylvania: Project Management Institute, 2004.

PROJECT MANAGEMENT INSTITUTE. **PMBOK guide**: a guide to the project management body of knowledge. Newton Square, Pennsylvania: Project Management Institute, 2000.

PROJECT MANAGEMENT INSTITUTE. **Um guia do conjunto de conhecimentos em gerenciamento de projetos**: guia PMBOK. 3. ed. Newton Square, Pennsylvania: Project Management Institute, 2004.

PYMNTS. The Data Breach Case Against Facebook Is Moving Forward. **PYMNTS**, [S.l.], jun 2019. Disponível em: <https://www.pymnts.com/facebook/2019/data-breach-case/amp/>. Acesso em: 9 set. 2019.

RANDOPH, Justus J. A guide to writing the dissertation literature review. **Practical Assessment**, Research & Evaluation, [s.l.]: [s.n.], 2009.

RASHID, Fahmida Y. The Target data breach settlement sets a low bar for industry security standards. **CSO**, Framingham, mai. 2017. Disponível em: <https://www.csoonline.com/article/3199064/the-target-data-breach-settlement-sets-a-low-bar-for-industry-security-standards.html>. Acesso em: 9 set. 2019.

REALE, Miguel. **Fundamentos do Direito**. 2. ed. rev. São Paulo: Revista dos Tribunais, 1972.

REALE, Miguel. **Estudos preliminares do Código Civil**. São Paulo: Revista dos Tribunais, 2003.

REALE, Miguel. **História do novo Código Civil**. São Paulo: Revista dos Tribunais, 2005.

REIS, Adelson Pacheco dos. **Análise de vulnerabilidades de segurança em sistemas de Internet Banking utilizando ferramentas de código aberto**. 2018. 46 p. Trabalho de Conclusão de Curso (Sistemas de Informação) – Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em: <https://repositorio.ufu.br/bitstream/123456789/24152/3/An%C3%A1liseVulnerabilidadesSeguran%C3%A7a.pdf>. Acesso em: 9 set. 2019.

RIBEIRO, Lucio; GUSMÃO, Cristine; FEIJÓ, Wilmar; BEZERRA, Vicente. A case study for the implementation of an agile risk management process in multiple projects environments. **PICMET 2009 Proceedings**, Oregon, Aug. 2009. Disponível em: <http://ieeexplore.ieee.org/Xplore/login.jsp?reload=true&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5230479%2F5261733%2F05262002.pdf%arnumber%3D5262002&authDecision=-203>. Acesso em: 16 mar. 2010.

RUIZ, João Álvaro. **Metodologia científica**: guia para eficiência nos estudos. 5. ed. São Paulo: Atlas, 2002.

SAMUEL, Sabrina. **Coding policies for secure web applications**. 2007. 126 f. Dissertação (Mestrado em Matemática e Ciência da Computação) - Technische Universiteit Eindhoven, Eindhoven, 2007. Disponível em: https://www.owasp.org/images/e/e9/Sample_Coding_Policies_for_Secure_Web_Applications.doc. Acesso em: 23 jun. 2019.

SANCHES CUNHA, Rogério. **Manual de Direito Penal**: Parte Geral (arts. 1 ao 120). 7. ed. Salvador: Juspodium, 2019.

SANDELOWSKI, Margarete; BARROSO, Julie. **Handbook for synthesizing qualitative research**. New York: Springer Publishing Company, 2007.

SCHUBERT JONCKHEER & KOLBE. Consumers File Class Action Lawsuit Against Symantec for Defective AntiVirus Software. **CISION PR Newswire**, 8 Nov. 2018. Disponível em: <https://www.prnewswire.com/news-releases/consumers-file-class-action-lawsuit-against-symantec-for-defective-antivirus-software-300746568.html>. Acesso em: 24 jun. 2019.

SCHWARTZ, Mathew J. Wendy's Reaches \$50 Million Breach Settlement With Banks. **Bank Info Security**, Princeton, fev. 2019. Disponível em: <https://www.bankinfosecurity.com/wendys-reaches-50-million-breach-settlement-banks-a-12032>. Acesso em 9 set. 2019.

SCHWARTZ, Mathew J. Malware Knocks Out Accounting Software Giant Wolters Kluwer. **Information Security Media Group**, Princeton, maio 2019. Disponível em: <https://www.databreachtoday.com/malware-knocks-out-accounting-software-giant-wolters-kluwer-a-12462>. Acesso em 9 set. 2019.

SEALS, Sara. Intimate Details on Healthcare Workers Exposed as Cloud Security Lags. **Threat Post**, Woburn, out. 2019. Disponível em: <https://threatpost.com/intimate-details-healthcare-workers-exposed-cloud-security/149007/>. Acesso em: 9 out. 2019.

SEALS, Tara. Lenovo Ordered to Pay \$7.3M in Superfish Fiasco. **Threat Post**, 3 Dec. 2018. Disponível em: <https://threatpost.com/lenovo-ordered-to-pay-7-3m-in-superfish-fiasco/139560/>. Acesso em: 24 jun. 2019.

SEQ LEGAL. **SEQ Legal EULA**, [2019?]. Disponível em: <https://seqlegal.com/free-legal-documents/eula>. Acesso em: 24 jun. 2019.

SHAW, Mary. Prospects for an engineering discipline of software. **IEEE Software**, Washington, [s.l.], Nov. 1990, p. 15 – 24, 1990.

SHELLEY, Mary. **Frankenstein or the modern Prometheus**. Adelaide: The University of Adelaide, 2014. Disponível em: <https://ebooks.adelaide.edu.au/s/shelley/mary/s53f/complete.html> . Acesso em: 22 jan. 2019.

SINEVIA. **Kuikie EULA Generator**, [2019?]. Disponível em: <https://kuikie.com/tools/eula-generator/>. Acesso em: 24 jun. 2019.

SIMON, Herbert. A. Designing organizations for an information-rich world.

Computers, communications, and the public interest, Baltimore, John Hopkins Press, 1971.

SINGH, Amit. A question of safety or ethics: The Boeing 737. **The Times of India**, 10 Jan. 2019. Disponível em: <https://timesofindia.indiatimes.com/blogs/mindfly/a-question-of-safety-or-ethics-the-boeing-737/>. Acesso em: 23 jun. 2019.

SILVA, Edna Lúcia da. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. rev. atual. Florianópolis: Laboratório de Ensino à Distância da UFSC, 2001.

SILVA, Maurício Corrêa da *et al.* Procedimentos metodológicos para a elaboração de projetos de pesquisa relacionados a dissertações de mestrado em Ciências Contábeis. **Revista Contabilidade & Finanças – USP**, São Paulo, n. 36, p. 97-104, set./dez. 2004. Disponível em: http://www.eac.fea.usp.br/cadernos/completos/cad36/mauricio_marcia_pg97a104.pdf. Acesso em: 12 mai. 2011.

SINGH, Yogesh Kumar. **Fundamental of research methodology and statistics**. New Dehli: New Age International, 2006.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. **Código de Ética do profissional de Informática**. Porto Alegre: Sociedade Brasileira de Computação, 2013. Disponível em: https://www.sbc.org.br/downloads/02.codigo_de_etica_da_sbc.pdf. Acesso em: 9 set. 2019.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. **Carta aberta**: regulamentação da profissão de TI. Porto Alegre: Sociedade Brasileira de Computação, 2016. Disponível em: <http://www.sbc.org.br/institucional-3/cartas-abertas/send/93-cartas-abertas/1019-regulamentacao-da-profissao>. Acesso em: 9 set. 2019.

SOMMERVILLE, Ian. **Ingengería del software**. 7. ed. Madrid: Pearson Educación, 2005.

SOMMERVILLE, Ian. **Software engineering**. 8th ed. [S.l.]: China Machine Press, [2007?].

SOMMERVILLE, Ian; SAWYER, Pete. **Requirements engineering**: a good practice. West Sussex: John Wiley & Sons, 2003.

SPAMFIGHTER. Foxit Software suffered from data breach impacting more than 328,000 accounts. **Spamfighter**, Copenhagen, set. 2019. Disponível em: <https://www.spamfighter.com/News-22411-Foxit-Software-suffered-from-data-breach-impacting-more-than-328000-accounts.htm>. Acesso em: 19 set. 2019.

STALLINGS, William. **Cryptography and network security**: principles and practice. 5th ed. [Upper Saddle River?]: Prentice Hall/Pearson, 2011.

STALLINGS, William; BROWN, Lawrie. **Computer security**: principles and practice. 3rd ed. [Upper Saddle River?]: Pearson, 2015.

STANFORD UNIVERSITY. The History of Utilitarianism. **Stanford Encyclopedia of Philosophy**. Stanford: Stanford University, 2014. Disponível em: <https://plato.stanford.edu/entries/utilitarianism-history/>. Acesso em: 01 fev. 2019.

STEWART, Emily. Delta's CEO says the Boeing 737 Max 8 scandal has "traumatized" the aviation industry. **Vox**, 11 June 2019. Disponível em: <https://www.vox.com/recode/2019/6/11/18657008/ed-bastian-delta-boeing-737-max-scandal>. Acesso em: 23 jun. 2019.

STOCO, Rui. **Tratado de responsabilidade civil**. 6. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2004.

STUPP, Catherine. Delta sues Chatbot Provider Over 2017 Breach. **The Wall Street Journal**, New York, 16 ago. 2019. Disponível em: <https://www.wsj.com/articles/delta-sues-chatbot-provider-over-2017-breach-11565947801>. Acesso em: 9 set. 2019.

SWETNAM, Derek. **Writing your dissertation**. 3rd ed. Oxford: How To Books, [2007?].

SWIFT, Jonathan. **Gulliver's travels**. [S.l.]: Collector's Library, 2011.

SWINHOE, Dan. The biggest data breach fines, penalties and settlements so far. **CSO**, Framingham, jul. 2019. Disponível em: <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.amp.html>2014. Acesso em: 9 set. 2019.

SWINHOE, Dan. What is the cost of a data breach?. **CSO**, Framingham, ago 2019. Disponível em: <https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.amp.html>. Acesso em: 9 set. 2019.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution**: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: SENAI-SP, 2017.

TARTUCE, Flávio. **Manual de Direito Civil**: volume único. 6. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: Método, 2016.

TERMSFEED. **TermsFeed EULA Generator**, [2019?]. Disponível em: <https://www.termsfeed.com/eula-generator/>. Acesso em: 24 jun. 2019.

THALES eSECURITY. **2018 Thales Data Threat Report**: Trends in encryption and data security. Plantation: **Thales eSecurity**, 2018. Disponível em: <http://go.thalesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf>. Acesso em: 9 set. 2019.

TOWNSEND, Kevin. SamSam Ransomware Attacks Hit Healthcare Firms. **Security Week**, [S.l.], jan. 2018. Disponível em: <https://www.securityweek.com/samsam-ransomware-attacks-hit-healthcare-firms>. Acesso em: 9 set. 2019.

TOP CLASS ACTIONS. ADT Home Security Hacking Vulnerability Class Action Settlement. Top Class Actions, 2018. Disponível em: <https://topclassactions.com/lawsuit-settlements/closed-settlements/826358-adt-home-security-hacking-vulnerability-class-action-settlement/>. Acesso em: 24 jun. 2019.

TRAVIS, Gregory. How the Boeing 737 Max Disaster Looks to a Software Developer.

IEEE Spectrum, 18 Apr. 2019. Disponível em: <https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer>. Acesso em: 23 jun. 2019.

TRAVIS, Gregory. The Case of the 737 MAX. **Medium**, 7 Apr. 2019. Disponível em: <https://medium.com/@gregoryreedtravis/the-case-of-the-737-max-b6b1869839b6>. Acesso em: 23 jun. 2019.

TURINE, Joseliza Alessandra Vanzela; TURINE, Marcelo Augusto Santos; MASIERO, Paulo Cesar. Aspectos jurídicos na formação do profissional em Computação e Informática. **International Conference on Engineering and Computer Education**, São Paulo, ago. 2000. Disponível em: <http://conteudo.icmc.usp.br/pessoas/masiero/direito.htm>. Acesso em: 9 set. 2019.

ULIN, Priscilla R.; ROBINSON, Elizabeth T.; TOLLEY, Elizabeth E. **Qualitative methods in public health: a field guide for applied research**. San Francisco: Jossey-Bass, 2005.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: LVM, 2014.

UNIVERSIDADE FEDERAL DE PERNAMBUCO. Pós-Graduação da Faculdade de Direito do Recife. **Modelo de Tese (Versão PDF)**. Recife: UFPE, 2004. Disponível em: <http://www.ufpe.br/ppgd/download/04MTD.pdf>. Acesso em: 01 ago. 2008.

UNIVERSITY BUSINESS. Higher education's vulnerability to cyber attacks. **University Business**, 6 Sept. 2016. Disponível em: <https://universitybusiness.com/higher-educations-vulnerability-to-cyber-attacks/>. Acesso em: 26 jun. 2019.

VENOSA, Sílvio de Salvo. **Direito Civil: parte geral**. 4. ed. São Paulo: Atlas, 2004. v. I.

VENOSA, Sílvio de Salvo. **Direito Civil**. 9. ed. São Paulo: Atlas, 2009. v. 2, 4.

VILA NOVA, Sebastião. **Introdução à Sociologia**. 6. ed. São Paulo: Atlas, 2004.

VOX MEDIA. What happens when (and if) the Boeing 737 Max returns to the air?. **Vox**, 24 June 2019. Disponível em: <https://www.vox.com/the-goods/2019/6/24/18715751/boeing-737-max-crash-american-airlines-return>. Acesso em: 24 jun. 2019.

WALTON, Jarred. Intel is fighting a battle between performance and security. **PCGamer**, 15 May 2019. Disponível em: <https://www.pcgamer.com/intel-is-fighting-a-battle-between-performance-and-security/>. Acesso em: 24 jun. 2019.

WARREN, Tom. Intel facing 32 lawsuits over Meltdown and Spectre CPU security flaws. **The Verge**, 16 Feb. 2018. Disponível em: <https://www.theverge.com/2018/2/16/17020048/intel-spectre-meltdown-class-action-lawsuits>. Acesso em: 24 jun. 2019.

WATERS, Kelly. Why most IT projects fail and how Agile Principles help. **Agile Software Development Made Easy!**, [s.l.], Aug. 2007. Disponível em:

<http://www.agile-software-development.com/2007/08/why-most-it-projects-fail-and-how-agile.html>. Acesso em: 05 mai. 2010.

WERTH, Laurie. Certification and licensing for software professionals and organizations. **Proceeding of the 11th Conference on Software Engineering Education and Training**, Atlanta, feb. 1998. Disponível em: <https://www.computer.org/csdl/proceedings/cseet/1998/8326/00/83260151.pdf>. Acesso em: 22 jan. 2019.

WHITTAKER, Zack. Laswuits threaten infosec research – just when we need it most. **ZDNet Zero Day**, 19 Fev. 2018. Disponível em: <https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/>. Acesso em: 27 jun. 2019.

WHITTAKER, Zack. Capital One's breach was inevitable, because we did nothing after Equifax. **Tech Crunch**, [S.l.], jul. 2019. Disponível em: <https://techcrunch.com/2019/07/29/capital-one-breach-was-inevitable/amp/>. Acesso em: 9 set. 2019.

WHITTAKER, Zack. FTC slaps Equifax with a fine of up to \$700M for 2017 data breach. **Tech Crunch**, [S.l.], jul. 2019. Disponível em: <https://techcrunch.com/2019/07/22/equifax-fine-ftc/>. Acesso em: 9 set. 2019.

WINDERS, Davey. Top 10 stupid EULAs. **Alphr**, 2009. Disponível em: <https://www.alphr.com/features/247200/top-10-stupid-eulas>. Acesso em: 24 jun. 019.

WIRED. Microsoft sued for weak security. **Wired**, 10 Fev. 2003. Disponível em: <https://www.wired.com/2003/10/microsoft-sued-for-weak-security/>. Acesso em: 24 jun. 2019.

WOODCOCK, Jim; DAVIES, Jim. **Using Z**: specification, refinement, and proof. Oxford: University of Oxford, [s.d.]. Disponível em: <http://www.cs.cmu.edu/~15819/zedbook.pdf>. Acesso em: 20 jun. 2019.

YGLESIAS, Matthew. The emerging 737 MAX scandal, explained. **Vox**, 29 Mar. 2019. Disponível em: <https://www.vox.com/business-and-finance/2019/3/29/18281270/737-max-faa-scandal-explained>. Acesso em: 23 jun. 2019.

YAHOO. 'I'm outraged at Boeing:' Why pilots are suing over the 737 Max. **Yahoo Finance**, 24 June 2019. Disponível em: <https://finance.yahoo.com/news/pilot-lawsuit-747-max-213509346.html>. Acesso em: 24 jun. 2019.

YONG, Lip Eng; WONG, Siew Fan. Software Project Success: a three-legged race. **Symposium on Progress in Information & Communication Tecnology 2009**, Kuala Lumpur, 2009, p. 102-104. Disponível em: http://spict.utar.edu.my/SPICT-09CD/contents/pdf/SPICT09_A-5_2.pdf. Acesso em: 28 abr. 2011.

YOSHIDA, Junko. Boeing 737 Max: Is Automation at Fault? **EET**, 21 Mar. 2019. Disponível em: <https://www.eetindia.co.in/news/article/Boeing-737-Max-Is-Automation-at-Fault>. Acesso em: 23 jun. 2019.

APÊNDICE A – DIRETRIZES PARA O MAPEAMENTO SISTEMÁTICO

1. Identificar, no *ScienceDirect*®²⁰⁴ e no *IEEE Xplore*®²⁰⁵, artigos científicos que apresentem em seu conteúdo palavras compatíveis com o resultado da seguinte expressão regular:

SOFTWARE AND SECURITY AND (LIABILITY OR RESPONSIBILITY OR ETHICS OR ETHICAL) AND (AGREEMENT OR TERMS)

2. Filtrar os artigos identificados, lendo, inicialmente, apenas os títulos e os resumos/*abstracts* e descartando os artigos que, a partir desta leitura mínima, não pareçam se relacionar ao objeto da pesquisa.
3. Dos artigos não descartados no item anterior, ler também as conclusões, descartando, deste subconjunto, os artigos cujas conclusões não se relacionem ao objeto da pesquisa.
4. Dos artigos não descartados no item anterior, efetivar a leitura integral, descartando os que não apresentem em seu bojo informação relevante.
5. Dos artigos não descartados no item anterior, fazer anotações de pontos possivelmente úteis à pesquisa.
6. Avaliar a potencial utilidade das notas obtidas no item anterior, incorporando-as, se for o caso, na pesquisa.

²⁰⁴ Repositório on-line de artigos e capítulos de textos científicos disponível em <http://www.sciencedirect.com>.

²⁰⁵ Biblioteca digital disponível no endereço <http://www.ieeexplore.ieee.org>.

APÊNDICE B – DIRETRIZES PARA O LEVANTAMENTO E A ANÁLISE DE *EULAS/TOSS*

1. Averiguar no computador e no *smartphone* de um usuário comum (“homem médio”), quais os *softwares* instalados e buscar, na Internet, os *EULAs/ToSs* relativos aos principais *softwares*.
2. Partindo dos resultados da aplicação do primeiro questionário, alusivo às percepções acerca da responsabilidade pelo *software*, identificar os *softwares* referidos pelos respondentes e buscar, na *web*, os respectivos *EULAs/ToSs* dos principais *softwares*.
3. Partindo dos resultados da aplicação do primeiro questionário, relativo às percepções acerca da responsabilidade pelo *software*, identificar os principais serviços e aplicativos para *smartphone* mencionados pelos respondentes do citado questionário e buscar, na Internet, os respectivos *EULAs* e *ToSs*.
4. Rastrear, a partir de engenhos de busca (Google, e.g.), listas publicamente divulgadas por sítios *web* referentes a *softwares*, serviços *web* e aplicativos para *smartphone* mais utilizados nos dois últimos anos, buscando, também na Internet, os correspondentes *EULAs* e *ToSs*.
5. Coletados os *EULAs* e *ToSs*, sob a forma de arquivos individuais em *Portable Document Format (PDF)*, a serem utilizados na pesquisa, catalogar suas informações básicas em planilha eletrônica de consolidação de dados (nome do produto/serviço, empresa/ente responsável, ano da licença consultada, origem geográfica da entidade responsável).
6. Ler cada um dos *EULAs* e *ToSs* coletados, buscando identificar em seu corpo as disposições concernentes à responsabilidade por sua produção, ao seu uso e a potenciais falhas, focando-se a atenção na identificação da existência das seguintes espécies de cláusulas:
 - cláusula de integral isenção/exclusão de responsabilidade;
 - cláusula de parcial limitação de responsabilidade;
 - eventual teto limitante de indenização
 - condições de vigência diferenciada em função do ordenamento jurídico da localidade de aquisição/uso do produto/serviço.
7. Interromper a coleta de *EULAs/ToSs* quando, qualitativamente, não se apresentarem inovações nas disposições atinentes à responsabilidade, ou quando atingida a quantidade mínima de 150 (cento e cinquenta) *EULAs/ToSs*.
8. Agrupar todos os *EULAs* e *ToSs* identificados em categorias consoante o segmento do *software/serviço* em *software* (categorização livre e dependente da apuração feita, considerado o escopo da pesquisa).

9. Consolidar os dados registrados na planilha, obtendo indicadores estatísticos, como:

- Quantidade total de *EULAs/ToSs* coletados e utilizados na pesquisa;
- Distribuição dos *softwares/serviços* em *software* identificados em função dos segmentos de livre categorização referidos no item 8 deste conjunto de diretrizes;
- Rol de domínios dos aplicativos e utilitários cujos *EULAs/ToSs* foram considerados no estudo;
- Distribuição de aplicativos e utilitários cujos *EULAs/ToSs* foram analisados na pesquisa em função dos seus domínios;
- Relação de domínios dos serviços *web* cujos *EULAs/ToSs* foram considerados na investigação;
- Distribuição dos serviços *web* considerados na pesquisa em função dos seus domínios;
- Distribuição dos *EULAs/ToSs* analisados em função da localidade geográfica da empresa encarregada do desenvolvimento/fornecimento do *software/serviço* em *software*;
- Quantitativos de *EULAs/ToSs* com cláusula única de exclusão integral de responsabilidade, cláusula única de limitação de responsabilidade, cláusulas duplas de exclusão e de limitação de responsabilidade;
- Distribuição bruta das Razões de Exclusão Integral de Responsabilidade e das Razões de Limitação de Responsabilidade, considerados os segmentos dos *softwares/serviços* em *software*;
- Distribuição normalizada das Razões de Exclusão Integral de Responsabilidade e das Razões de Limitação de Responsabilidade, considerados os segmentos dos *softwares/serviços* em *software*.

10. Elaborar relações relativas aos *EULAs/ToSs* examinados na pesquisa.

APÊNDICE C – MODELO DE QUESTIONÁRIO DE SONDAÇÃO DE PERCEPÇÕES QUANTO AOS REQUISITOS DE SEGURANÇA EM SOFTWARE E À RESPONSABILIDADE GERAL PELO SOFTWARE

PESQUISA PARA COLETA DE DADOS PARA TESE DE DOUTORADO

Questionário de coleta de dados para a Tese em Ciência da Computação da discente Fabiana F. S. Flores, do Centro de Informática da UFPE (CIn/ UFPE).

O preenchimento do questionário não acarreta qualquer risco de dano. Não há identificação pessoal. Todos os dados são coletados e tratados de forma anônima.

Estima-se que o questionário seja preenchido no intervalo entre 10 e 30 minutos.

As suas respostas são essenciais para esta pesquisa. Agradeço muito por sua participação e pelo seu tempo dedicado ao preenchimento do questionário !

* Required

1. Qual o seu gênero? *

Mark only one oval.

- ☐ Masculino
- ☐ Feminino
- ☐ Outro

2. Qual a sua faixa de idade? *

Mark only one oval.

- ☐ menos de 20 anos
- ☐ mais de 20 e menos de 25
- ☐ mais de 25 e menos de 30
- ☐ mais de 30 e menos de 35
- ☐ mais de 35 e menos de 40
- ☐ mais de 40 e menos de 50
- ☐ mais de 50 e menos de 60
- ☐ acima de 60 anos

3. Em que cidade, estado e país você reside atualmente? *

4. Qual a sua titulação acadêmica máxima? *

Mark only one oval.

- ☐ Ensino Médio *Skip to question 5.*
- ☐ Graduação *Skip to question 7.*
- ☐ Especialização *Skip to question 7.*
- ☐ Mestrado *Skip to question 7.*
- ☐ Doutorado *Skip to question 7.*
- ☐ Pós-Doutorado *Skip to question 7.*

5. **Você está fazendo alguma graduação ou curso curso de nível superior no momento?**
Mark only one oval.

☐ Sim *Skip to question 6.*
☐ Não *Skip to question 10.*

6. **Em que Universidade/ Faculdade você estuda no momento?**

Skip to question 10.

7. **Há quanto tempo você concluiu sua graduação? ***
Mark only one oval.

☐ 0 a 1 ano
☐ 1 a 2 anos
☐ 2 a 5 anos
☐ mais de 5 anos

8. Você possui titulações em que segmentos? Por favor, assinale todos os cursos em que você tiver obtido Graduação, Especialização, Mestrado, Doutorado ou Pós-Doutorado.

Check all that apply.

- ☐ Administração
- ☐ Arqueologia
- ☐ Arquitetura e Urbanismo
- ☐ Artes Visuais
- ☐ Biblioteconomia
- ☐ Biomedicina
- ☐ Ciências Atuariais
- ☐ Ciências da Computação
- ☐ Ciências Sociais
- ☐ Ciências Políticas
- ☐ Cinema e Audiovisual
- ☐ Comunicação Social
- ☐ Dança
- ☐ Design
- ☐ Direito
- ☐ Educação Física
- ☐ Enfermagem
- ☐ Engenharia Biomédica
- ☐ Engenharia Cartográfica
- ☐ Engenharia Civil
- ☐ Engenharia da Computação
- ☐ Engenharia de Alimentos
- ☐ Engenharia de Controle e Automação
- ☐ Engenharia de Energia
- ☐ Engenharia de Materiais
- ☐ Engenharia de Minas
- ☐ Engenharia de Produção
- ☐ Engenharia Elétrica
- ☐ Engenharia Eletrônica
- ☐ Engenharia Mecânica
- ☐ Engenharia Naval
- ☐ Engenharia Química
- ☐ Estatística
- ☐ Expressão Gráfica
- ☐ Farmácia
- ☐ Filosofia
- ☐ Física
- ☐ Fisioterapia
- ☐ Fonoaudiologia
- ☐ Geografia
- ☐ Gestão da Informação
- ☐ História
- ☐ Hotelaria
- ☐ Jornalismo
- ☐ Letras
- ☐ Matemática
- ☐ Medicina
- ☐ Museologia

- ☐ Música
- ☐ Oceanografia
- ☐ Odontologia
- ☐ Pedagogia
- ☐ Psicologia
- ☐ Publicidade e Propaganda
- ☐ Química
- ☐ Rádio, TV e Internet
- ☐ Saúde Coletiva
- ☐ Secretariado Executivo
- ☐ Serviço Social
- ☐ Sistemas de Informação
- ☐ Teatro
- ☐ Terapia Ocupacional
- ☐ Turismo

9. Em que Universidade/ Faculdade você obteve a sua maior titulação acadêmica? *

10. O seu trabalho envolve o desenvolvimento de software? *

Mark only one oval.

- ☐ Sim Skip to question 33.
- ☐ Não Skip to question 11.

11. Em que área/ setor você trabalha? *

Mark only one oval.

- ☐ Educação
- ☐ Governo
- ☐ Indústria
- ☐ Comércio
- ☐ Serviços

12. No seu trabalho, você utiliza computador? *

Mark only one oval.

- ☐ Sim Skip to question 13.
- ☐ Não Skip to question 14.

13. **Na lista abaixo, marque, por favor, todos os programas/ serviços que você utiliza no seu trabalho? ***

Check all that apply.

- ☐ Windows
- ☐ Linux
- ☐ Word, Excel e outros aplicativos do Pacote Microsoft Office
- ☐ Outlook
- ☐ Internet Explorer
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Winzip/ Winrar
- ☐ AutoCAD, Revit, etc
- ☐ Serviços de e-mail via Internet
- ☐ Whatsapp, Telegram, Hangout e similares
- ☐ Programas específicos do trabalho

14. **Na sua casa ou na sua vida diária, você utiliza algum dos itens abaixo citados? Por favor, assinale todos os que você utilizar.**

Check all that apply.

- ☐ Computador, laptop, notebook ou netbook
- ☐ Smart TV
- ☐ TV por assinatura
- ☐ Celular
- ☐ iPad, ou Tablet
- ☐ Câmera digital ou filmadora digital
- ☐ Videogame
- ☐ GPS
- ☐ MP3 Player, ou iPod

15. **Na sua vida diária, você utiliza algum dos serviços e programas abaixo? Por favor, marque todos os que você utilizar.**

Check all that apply.

- ☐ Windows
- ☐ Linux
- ☐ Word, Excel e outros aplicativos do pacote Microsoft Office
- ☐ Outlook
- ☐ Internet Explorer
- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Winzip, Winrar ou similar
- ☐ AutoCAD, Revit ou similar
- ☐ Serviço de e-mail pela web (G-Mail, por exemplo)
- ☐ Facebook
- ☐ Instagram
- ☐ Twitter
- ☐ Periscope
- ☐ Youtube
- ☐ Pinterest
- ☐ Messenger
- ☐ Whatsapp, Telegram, Hangout ou similar
- ☐ Internet Banking
- ☐ Rádio on-line
- ☐ Eversnap
- ☐ Jogos
- ☐ Outros apps para celular

16. **Quando você adquire/ instala algum programa no seu computador, ou quando você se cadastra em algum serviço oferecido pela Internet (Facebook e Whatsapp, por exemplo), você lê os avisos/ documentos iniciais chamados "Termos do Serviço" (Terms of Service - ToS) e "Política de Privacidade" (Privacy Policy)?**

Mark only one oval.

- ☐ Não, não leio nenhum deles *Skip to question 17.*
- ☐ Leio apenas os Termos do Serviço *Skip to question 18.*
- ☐ Leio apenas a Política de Privacidade *Skip to question 20.*
- ☐ Leio os dois documentos *Skip to question 22.*

17. **Por que você não lê nenhum dos dois documentos? Por favor, marque todas as opções que você achar que se aplicam.**

Check all that apply.

- ☐ Porque não dá para entender o que está escrito neles.
- ☐ Porque são muito longos.
- ☐ Porque levaria muito tempo para se ler tudo.
- ☐ Porque aquilo não "serve para nada".
- ☐ Porque, para usar o programa/ serviço, sou obrigado(a) mesmo(a) a concordar com tudo. Não tenho, de fato, escolha.

Skip to question 27.

18. Por que você lê apenas os "Termos do Serviço"?

19. O que você acha, em geral, dos "Termos do Serviço"?

Skip to question 24.

20. Por que você lê apenas a "Política de Privacidade"?

21. O que você acha, em geral, da "Política de Privacidade"?

Skip to question 24.

22. Por que você lê os dois documentos?

23. O que você acha, em geral, dos "Termos do Serviço" e das "Políticas de Privacidade"?

24. **Você compreende o que está escrito nesse(s) documento(s)?**
Mark only one oval.
- ☐ Sim, entendo 100% tudo o que está escrito.
- ☐ Mais ou menos. Entendo boa parte, mas não tudo o que está escrito.
- ☐ Não entendo nada. Aquilo "parece grego" para mim.
25. **Quando você passa a usar um programa/ serviço desses, você realmente concorda com os "Termos do Serviço" e com a "Política de Privacidade"?**
Mark only one oval.
- ☐ Sim, só vou adiante se concordo com tudo
- ☐ Em parte eu concordo, mas não concordo, de fato, com tudo.
- ☐ Não, eu aceito as condições impostas porque, na verdade, não tenho escolha. Eu preciso do programa/ serviço.
26. **Você já desistiu de usar algum programa/ serviço desses por não concordar com os "Termos do Serviço", ou com a "Política de Privacidade"?**
Mark only one oval.
- ☐ Sim, sempre desisto quando não concordo com os "Termos do Serviço" ou com a "Política de Privacidade".
- ☐ Às vezes desisto, mas em outras ocasiões não porque eu preciso usar o programa/ serviço.
- ☐ Nunca desisto de usar o programa/ serviço porque eu preciso do programa/ serviço.
27. **Em geral, você está satisfeito com a qualidade desses programas e serviços? Por favor, justifique a sua resposta.**
- _____
- _____
- _____
- _____
28. **Para você, a Segurança (proteção contra roubo de senhas, invasões, etc.) é algo importante nesses programas e serviços?**
Mark only one oval.
- ☐ Sim, sempre
- ☐ Às vezes, dependendo do programa/ serviço
- ☐ Não, não é importante
29. **Você acredita que os programas/ serviços que você usa são seguros e confiáveis?**
Mark only one oval.
- ☐ Sim, sempre
- ☐ Às vezes, dependendo do programa/ serviço
- ☐ Não, nunca
30. **Você já enfrentou ou conhece alguém que já enfrentou algum problema de Segurança nos programas/ serviços que usou?**
Mark only one oval.
- ☐ Sim
- ☐ Não

31. Na sua visão, quando acontece algum problema de segurança (roubo de senha, phishing, invasões, etc.), há alguém ou algo que possa ou deva ser responsabilizado? *
- Mark only one oval.*
- ☐ Sim *Skip to question 32.*
- ☐ Depende *Skip to question 32.*
- ☐ Não, essas coisas são "fatalidades".
32. Quem, na sua percepção, poderia ou deveria vir a ser responsabilizado em caso de problemas de segurança nos programas/ serviços que você usa?
- _____
- _____
- _____
- _____
- Skip to question 80.*
33. Que espécie de software você desenvolve, ou tem ajudado a desenvolver atualmente? *
- Check all that apply.*
- ☐ Sistemas Stand-alone/ isolados
- ☐ Sistemas cliente-servidor
- ☐ Aplicativos web
- ☐ Aplicativos para celular
- ☐ Sistemas embarcados
- ☐ Outros
34. Há quantos anos você trabalha com algo que envolva o desenvolvimento software? *
- Mark only one oval.*
- ☐ 0 a 1 ano
- ☐ 1 a 2 anos
- ☐ 2 a 5 anos
- ☐ Mais de 5 anos
35. A maioria dos seus projetos são desenvolvidos sob filosofias ágeis de desenvolvimento ou sob modelos mais tradicionais? *
- Mark only one oval.*
- ☐ Metodologias ágeis
- ☐ Metodologias tradicionais
36. Você gosta de trabalhar com a metodologia usada na sua empresa/ organização? *
- Mark only one oval.*
- ☐ Sim
- ☐ Não
- ☐ Às vezes, dependendo da espécie de projeto

37. No seu local de trabalho, todos os integrantes da equipe participam da especificação dos requisitos, ou isso é tarefa de um grupo determinado de pessoas? *
- Mark only one oval.*
- ☐ Todos participam ativamente
- ☐ Um grupo determinado define todos os requisitos que são, então, repassados ao time de desenvolvimento
- ☐ Um grupo determinado cuida dos requisitos, mas os demais desenvolvedores podem opinar e fazer sugestões ao longo do processo de desenvolvimento
38. Quando você atua no desenvolvimento de algum tipo de software, você participa da especificação dos requisitos? *
- Mark only one oval.*
- ☐ Sim
- ☐ Não
39. Como é feita a elicitação dos requisitos no seu local de trabalho? Caso você não saiba como isso é feito, marque, por favor, a opção: "Desconheço porque não lido com isso". *
- Mark only one oval.*
- ☐ Existe um conjunto de diretrizes pré-definido pela empresa e seguimos essas diretrizes
- ☐ A sistemática para especificação é dependente do tipo de projeto
- ☐ Na construção de um software, cada equipe trabalha como prefere
- ☐ Desconheço porque não lido com isso
40. Na sua visão, a sua entidade de trabalho dá ênfase a algum tipo de requisito na especificação e no desenvolvimento? Caso você não saiba como isso é feito, marque, por favor, a opção: "Desconheço porque não lido com isso". *
- Mark only one oval.*
- ☐ Não, não existe ênfase. Todos os tipos de requisitos são importantes *Skip to question 44.*
- ☐ Sim, existe ênfase em alguns tipos de requisitos. *Skip to question 41.*
- ☐ Desconheço porque não lido com isso
41. Liste, por favor, os tipos de requisitos que você considera mais importantes.
- _____
- _____
- _____
- _____
- _____

42. Dos requisitos listados abaixo, quais são os considerados mais importantes nos projetos em que você tem trabalhado? Por favor, assinale todos os que têm sido priorizados nos projetos em que você atuou. Caso você não tenha essa informação, marque, por favor, a opção "Não tenho essa informação".

Check all that apply.

- ☐ Funcionalidade
- ☐ Usabilidade
- ☐ Amigabilidade da interface
- ☐ Portabilidade
- ☐ Segurança
- ☐ Acessibilidade
- ☐ Extensibilidade
- ☐ Estabilidade
- ☐ Disponibilidade
- ☐ Interoperabilidade
- ☐ Confiabilidade
- ☐ Integridade
- ☐ Privacidade
- ☐ Tempo de Resposta/ Performance
- ☐ Verificabilidade
- ☐ Manutenibilidade
- ☐ Robustez
- ☐ Estabilidade
- ☐ Tolerância a falhas
- ☐ Conformidade com padrões/ ferramentas/ linguagens de desenvolvimento
- ☐ Compatibilidade com plataformas determinadas
- ☐ Escalabilidade
- ☐ Uso de recursos computacionais
- ☐ Reusabilidade
- ☐ Eficiência
- ☐ Efetividade
- ☐ Adequação à legislação

43. Liste, por favor, em ordem de importância, os cinco tipos de requisitos mais priorizados nos projetos em que você tem atuado.

44. Por favor, indique, dentre os itens abaixo, todos os recursos/ instrumentos que são utilizados na especificação dos requisitos na sua empresa: *

Check all that apply.

- ☐ Conversa com os interessados e usuários
- ☐ Observação do ambiente em que o sistema deverá operar
- ☐ Estudo dos softwares já utilizados pelo cliente
- ☐ Análise de documentos e artefatos do cliente
- ☐ Modelagem de requisitos
- ☐ Elaboração de um documento de requisitos e discussão deste documento com o cliente
- ☐ Não tenho essa informação

45. Para você, qual dos recursos/ instrumentos antes citados é o mais importante para a especificação dos requisitos? *
- Mark only one oval.*
- ☐ Conversa com os interessados e usuários
☐ Observação do ambiente em que o sistema deverá operar
☐ Estudo dos softwares já utilizados pelo cliente
☐ Análise de documentos e artefatos do cliente
☐ Modelagem de requisitos
☐ Elaboração de um documento de requisitos e discussão deste documento com o cliente
46. Além dos itens citados na questão anterior, a sua entidade faz algo mais para a elicitação dos requisitos? *
- Mark only one oval.*
- ☐ Não *Skip to question 48.*
☐ Sim *Skip to question 47.*
47. Liste abaixo, por favor, outras estratégias da sua entidade para a elicitação dos requisitos.
- _____

48. No processo de construção do software no seu local de trabalho, você acredita que seja costume se pensar nas incertezas e nos imprevistos relacionados aos requisitos? *
- Mark only one oval.*
- ☐ Sim
☐ Não
49. É feito, na sua empresa, algo especial em relação às incertezas e aos imprevistos relacionados aos requisitos? *
- Mark only one oval.*
- ☐ Sim *Skip to question 50.*
☐ Não *Skip to question 52.*
☐ Às vezes, a depender do projeto *Skip to question 50.*
50. Liste, por favor, o que costuma ser feito na sua entidade para lidar com incertezas e imprevistos relacionados aos requisitos dos softwares. Por favor, especifique, também, a finalidade do que é feito.
- _____

51. Você acha que as medidas que você listou são, em geral, suficientes para lidar com as incertezas e imprevistos relacionados à especificação de requisitos? *
- Mark only one oval.*
- ☐ Sim
☐ Às vezes, dependendo da natureza do projeto
☐ Não

52. **Você acredita que a especificação dos requisitos tem impacto no desenvolvimento de software? ***
Mark only one oval.
- ☐ Sim *Skip to question 53.*
- ☐ Não *Skip to question 55.*
- ☐ Às vezes, dependendo do projeto *Skip to question 53.*
53. **Na sua opinião, problemas relacionados aos requisitos já resultaram em consequências ruins nos projetos em que você trabalhou? ***
Mark only one oval.
- ☐ Sim, sempre *Skip to question 54.*
- ☐ Sim, às vezes *Skip to question 54.*
- ☐ Não, nunca *Skip to question 55.*
54. **Que espécies de danos foram causados por problemas relacionados à definição dos requisitos? Por favor, marque todos os que você achar aplicáveis. ***
Check all that apply.
- ☐ Atraso no Desenvolvimento
- ☐ Retrabalho
- ☐ Aumento dos Custos do Projeto
- ☐ Falha no Produto
- ☐ Descarte ou Não Utilização do Produto
- ☐ Abandono do Projeto
- ☐ Insatisfação do Cliente
- ☐ Sobrecarga da Equipe de Desenvolvimento
- ☐ Descontentamento da Equipe de Desenvolvimento
- ☐ Reestruturação da Equipe de Desenvolvimento
55. **Você acredita que problemas na especificação de requisitos podem levar a falhas de segurança dos softwares? ***
Mark only one oval.
- ☐ Sim *Skip to question 56.*
- ☐ Não *Skip to question 56.*
- ☐ Talvez, a depender do tipo de software *Skip to question 56.*
56. **Na sua opinião, algo pode ser feito, no processo de desenvolvimento, para lidar com possíveis danos de segurança em software? ***
Mark only one oval.
- ☐ Sim *Skip to question 57.*
- ☐ Não *Skip to question 58.*
57. **Na sua opinião, o que pode ser feito, hoje, no processo de desenvolvimento, para lidar com falhas em segurança de software? Por favor, cite 3 medidas que, na sua visão, podem ser adotadas para minimizar/ evitar problemas de segurança em software.**
- _____
- _____
- _____
- _____
- _____

58. Fora do processo de desenvolvimento, você acredita que poderia haver algo que ajudasse a lidar com eventuais falhas de segurança em softwares?
Mark only one oval.

- ☐ Sim *Skip to question 59.*
- ☐ Não *Skip to question 60.*

59. Fora do processo de desenvolvimento, o que poderia, na sua visão, ser feito para se lidar com eventuais falhas de segurança em softwares?

60. A seguir, são apresentadas várias medidas que, eventualmente, poderiam ser utilizadas ao se lidar com problemas de segurança em software. Por favor, indique, em sua opinião, prioridades para o uso dessas medidas. *
Mark only one oval per row.

	Instalação de firewalls, antivírus e antimalwares	Controle de acesso aos sistemas (senhas, certificação digital, tokens, biometria, etc.)	Adoção de políticas de segurança	Orientação dos usuários	Uso de metodologias específicas de desenvolvimento	Priorização da segurança no desenvolvimento	Treinamento dos desenvolvedores em Segurança Computacional
Prioridade 1	☐	☐	☐	☐	☐	☐	☐
Prioridade 2	☐	☐	☐	☐	☐	☐	☐
Prioridade 3	☐	☐	☐	☐	☐	☐	☐
Prioridade 4	☐	☐	☐	☐	☐	☐	☐
Prioridade 5	☐	☐	☐	☐	☐	☐	☐
Prioridade 6	☐	☐	☐	☐	☐	☐	☐
Prioridade 7	☐	☐	☐	☐	☐	☐	☐

61. Na sua visão, as pessoas que produzem algum tipo de software podem fazer algo a respeito da segurança neles? *
Mark only one oval.

- ☐ Sim
- ☐ Não
- ☐ Talvez

62. Você acredita que, hoje, a entidade em que você trabalha faz tudo o que poderia para lidar com possíveis falhas em segurança nos softwares que vocês desenvolvem? *
Mark only one oval.

- ☐ Sim
- ☐ Não

63. O que você acredita que a sua empresa/ entidade poderia fazer para lidar melhor com possíveis falhas de segurança nos softwares desenvolvidos?

64. O que você acredita que atrapalha ou pode atrapalhar o desenvolvimento de software seguro?

65. Você acredita que a sua equipe de trabalho está capacitada ao desenvolvimento de software seguro? *

Mark only one oval.

- ☐ Sim, totalmente
- ☐ Sim, em parte
- ☐ Não

66. Caso você ache que a sua equipe de trabalho pode estar desenvolvendo software não seguro, assinale, abaixo, todos os fatores que você acredita que contribuem para isso: *

Check all that apply.

- ☐ Prazos muito curtos para o desenvolvimento do produto
- ☐ Peculiaridades da metodologia de desenvolvimento
- ☐ Sobrecarga de trabalho
- ☐ Desconhecimento específico dos domínios/ áreas das aplicações em desenvolvimento
- ☐ Ausência de ferramentas e técnicas adequadas para a especificação dos requisitos
- ☐ Pouca integração e interação entre os membros da equipe de desenvolvimento
- ☐ Pouca receptividade dos tomadores de decisão às sugestões dos membros da equipe de desenvolvimento
- ☐ Desconhecimento técnico sobre gestão de riscos
- ☐ Poucas oportunidades de atualização e reciclagem profissional
- ☐ Falta de treinamento em Segurança Computacional
- ☐ Necessidade de priorização dos requisitos funcionais
- ☐ Baixa remuneração dos profissionais

67. Algum outro fator, além dos já citados, poderia impactar no desenvolvimento de software não seguro? *

Mark only one oval.

- ☐ Sim Skip to question 68.
- ☐ Não Skip to question 69.

68. Que fatores não citados antes poderiam, na sua percepção, impactar no desenvolvimento de software não seguro?

69. Na sua visão, seria bom para a sua empresa capacitar a equipe em Segurança Computacional? *

Mark only one oval.

- ☐ Sim
- ☐ Não

70. Por favor, justifique a sua resposta anterior. *

71. Hoje, você teria interesse pessoal em obter conhecimento formal sobre Segurança Computacional? *

Mark only one oval.

- ☐ Sim
- ☐ Não, pois tenho outras prioridades no momento
- ☐ Não, não há nada que possa ser feito para lidar com incertezas e imprevistos de Segurança. Se algo ocorrer, resolve-se depois
- ☐ Talvez, a depender de como seria possível se obter este conhecimento formal

72. Você acredita que seria útil participar de cursos ou treinamentos em Segurança Computacional? *

Mark only one oval.

- ☐ Sim
- ☐ Não
- ☐ Talvez, dependendo dos custos envolvidos e das disponibilidades de tempo

73. Na sua opinião, qual seria a melhor forma de se capacitar em Segurança? *

Mark only one oval.

- ☐ Lendo um livro ou manual impresso *Skip to question 75.*
- ☐ Seguindo um Tutorial na Internet *Skip to question 75.*
- ☐ Participando de um curso/ treinamento presencial *Skip to question 75.*
- ☐ Participando em uma iniciativa prática de Segurança no desenvolvimento de software *Skip to question 75.*
- ☐ Participando de um curso on-line *Skip to question 75.*
- ☐ Participando de um fórum ou grupo de discussão *Skip to question 75.*
- ☐ Assistindo a palestras *Skip to question 75.*
- ☐ Outros *Skip to question 74.*

74. Que outra forma, para você, seria a melhor para se capacitar em Segurança?

75.

Se você pudesse decidir sobre novos rumos quanto à Segurança no desenvolvimento de software, você: *

Mark only one oval.

- ☐ Acharia melhor deixar tudo como está, pois não se mexe em time que está ganhando Skip to question 77.
- ☐ Acharia melhor deixar tudo como está, pois não são grandes os problemas relacionados à segurança Skip to question 77.
- ☐ Acharia melhor deixar tudo como está, pois os interessados podem instalar firewalls, antivírus e antimalwares Skip to question 77.
- ☐ Acharia melhor deixar tudo como está, pois o usuário é o responsável pelo uso seguro do software Skip to question 77.
- ☐ Acharia melhor deixar tudo como está, pois suas prioridades são outras ou não existem recursos disponíveis para isso no momento Skip to question 77.
- ☐ Estaria aberto à possibilidade de inovar para melhorar o processo produtivo no tocante à Segurança do softwares, desde que fossem demonstrados ou comprovados os resultados positivos potenciais disso Skip to question 77.
- ☐ Gostaria de conhecer mais da área para poder decidir Skip to question 77.
- ☐ Implantaria, de imediato, medidas para maior segurança no software que produz Skip to question 77.
- ☐ Outro Skip to question 76.

76.

Que outra conduta você, pessoalmente, acredita que poderia ser melhor adotar quanto à Segurança no desenvolvimento de software? *

77.

Pessoalmente, você teria interesse em participar de um experimento científico para avaliação de benefícios potenciais do aprendizado sobre Segurança no desenvolvimento de software? *

Mark only one oval.

- ☐ Sim, dependendo de como fosse o experimento
- ☐ Não, não gosto de ser "cobaia"
- ☐ Não, minhas prioridades são outras, ou não disponho de tempo para isso
- ☐ Não, pois não acredito que a responsabilidade pela Segurança seja dos desenvolvedores

78.

Responder este questionário alterou, de alguma forma, a sua percepção pessoal sobre a Segurança no desenvolvimento de software? *

Mark only one oval.

- ☐ Não
- ☐ Sim

79.

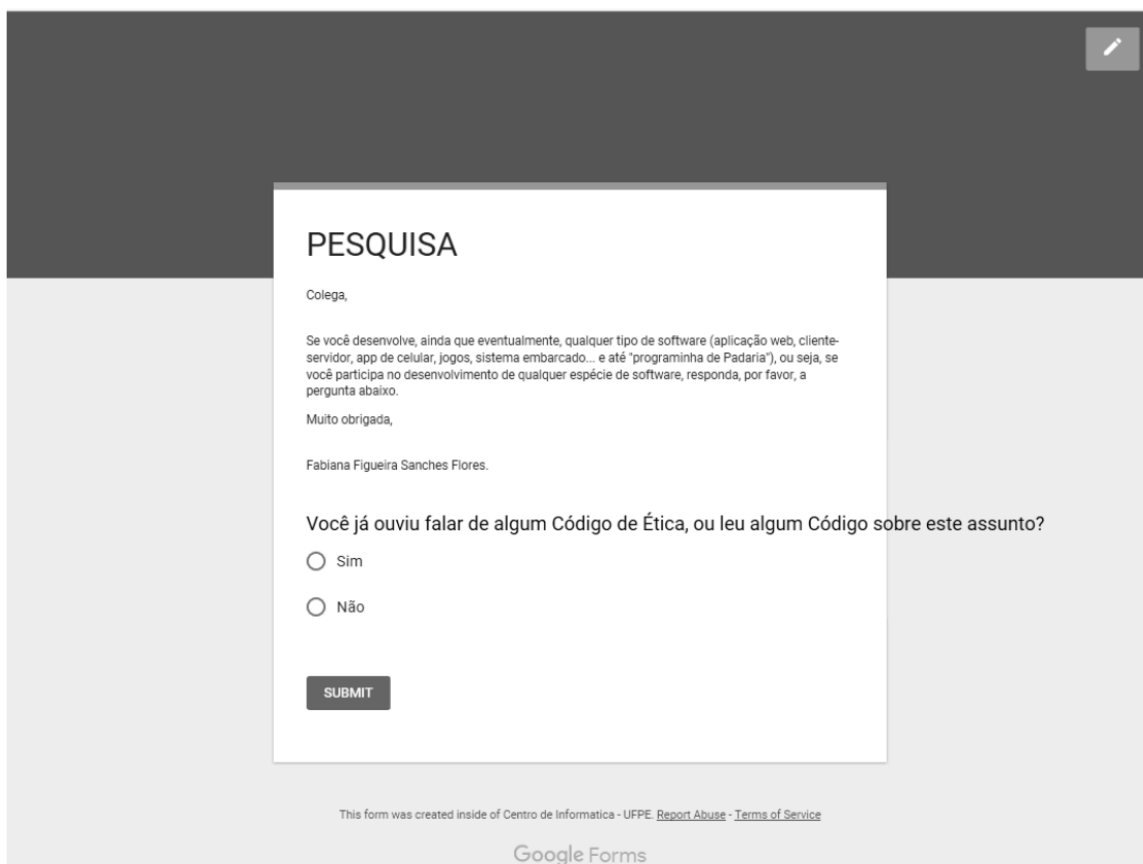
Qual é, hoje, o seu maior interesse em Computação?

80. **Você gostaria de receber feedback sobre o resultado final da pesquisa?**
Mark only one oval.

☐ Sim
☐ Não

81. **Caso você deseje feedback sobre o resultado final da pesquisa, informe, por favor, o seu endereço de e-mail.**

APÊNDICE D – MODELO DE QUESTIONÁRIO DE AVALIAÇÃO DO PRÉVIO CONTATO DE DESENVOLVEDORES DE SOFTWARE COM CÓDIGOS DE ÉTICA



PESQUISA

Colega,

Se você desenvolve, ainda que eventualmente, qualquer tipo de software (aplicação web, cliente-servidor, app de celular, jogos, sistema embarcado... e até "programinha de Padaria"), ou seja, se você participa no desenvolvimento de qualquer espécie de software, responda, por favor, a pergunta abaixo.

Muito obrigada,

Fabiana Figueira Sanches Flores.

Você já ouviu falar de algum Código de Ética, ou leu algum Código sobre este assunto?

☐ Sim

☐ Não

SUBMIT

This form was created inside of Centro de Informatica - UFPE. [Report Abuse](#) - [Terms of Service](#)

Google Forms

APÊNDICE E – PLANO DA PRIMEIRA ENTREVISTA INFORMAL COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO

1. Apresentar-se e esclarecer aos entrevistados o motivo da conversa: a realização de uma pesquisa como discente do CIn/UFPE.
2. Tentar formar, nos entrevistados, um senso de receptividade e confiança, perguntando a eles sob as suas experiências pessoais no CIn/UFPE ou em atividades de pós-graduação.
3. Ouvir atentamente as falas dos entrevistados sobre suas vivências pessoais, tentando identificar nelas pontos de especial interesse para a pesquisa.
4. Caso surja algo de relevante à pesquisa, solicitar mais informações aos entrevistados.
5. Perguntar aos entrevistados suas opiniões pessoais sobre Segurança em *software* e sobre os *EULAs/ToSs*, repetindo-se o item 3 deste plano.
6. Perguntar aos entrevistados se, na percepção deles, há algum outro ponto sobre o qual não foi falado e que seja relevante, ouvindo-os e com repetição do item 3 deste plano.
7. Agradecer aos entrevistados, comprometendo-se a lhes fornecer, ao fim da investigação, *feedback* sobre o que tiver sido apurado no estudo.

APÊNDICE F – PLANO DA SEGUNDA ENTREVISTA INFORMAL COM ESPECIALISTAS EM SEGURANÇA DA INFORMAÇÃO

1. Agradecer, mais uma vez, ao entrevistado, perguntando-lhe generalidades sobre a sua situação profissional atual.
2. Esclarecer ao entrevistado o ponto atual da pesquisa, explicando a necessidade de dados concretos do mundo real para avaliação no estudo.
3. Ouvir o entrevistado acerca do ponto referido no item 2.
4. Observar, na fala do entrevistado, outros possíveis pontos de interesse à pesquisa.
5. Caso identificados pontos de interesse à pesquisa na fala do entrevistado, solicitar mais informações mediante perguntas vagas, que o permitam falar sobre tudo o que julgar pertinente.
6. Enquanto a conversa não se mostrar longa/repetitiva e o entrevistado estiver disposto, proceder de acordo com os itens 4 e 5 deste plano.
7. Agradecer ao entrevistado, comprometendo-se a lhe fornecer, ao fim da investigação, *feedback* sobre os resultados obtidos na pesquisa.

APÊNDICE G – PLANO DE ENTREVISTA TELEFÔNICA INFORMAL COM PESSOA DESENVOLVEDORA DE SOLUÇÕES EM *BUSINESS INTELLIGENCE*

1. Cumprimentar a pessoa entrevistada via telefone, informando necessitar muito de sua ajuda para uma pesquisa acadêmica.
2. Esclarecer à pessoa entrevistada que a pesquisa é anônima e que, caso ela não se sinta à vontade para participar, a entrevista é cancelada a qualquer momento.
3. Explicar que a entrevista é breve e que se destina a obter informações sobre a formação acadêmica de profissional da Indústria de *Software*.
4. Perguntar à entrevistada, qual a sua formação profissional, com ênfase em sua titulação máxima especialmente no tocante à produção de *software*.
5. Perguntar à entrevistada, onde ela concluiu os cursos que eventualmente mencionar.
6. Perguntar à entrevistada se, nos cursos que ela realizou, havia disciplinas relacionadas à Segurança Computacional, Direito, Filosofia, Sociologia, Ética e Moral ou algo similar.
7. Agradecer à pessoa entrevistada por sua colaboração na pesquisa.

**APÊNDICE H – DIRETRIZES PARA O LEVANTAMENTO E A ANÁLISE DA
DOCUMENTAÇÃO RELATIVA ÀS GRADES CURRICULARES DOS CURSOS DE
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, ENGENHARIA DA
COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO DE INSTITUIÇÕES
BRASILEIRAS DE ENSINO**

1. Obter, a partir de engenho de busca na Internet, rol de cursos de graduação em Ciência da Computação, Engenharia da Computação e Sistemas de Informação de instituições brasileiras de ensino que também mantenham, junto à CAPES, programa de pós-graduação estrito senso em atividade (Mestrados e Doutorados, apenas).
2. Partindo da listagem obtida no item 2, buscar na *web*, as grades curriculares e, quando possível/disponível, as ementas/programas das disciplinas dos cursos referidos no tocante à Ética e à Segurança.
3. Analisar as grades, ementas e programas obtidos, para se avaliar se são abordados nelas temas atinentes à Segurança e à Ética, verificando-se, também, se as disciplinas em que tais temas são possivelmente abordados qualificam-se como obrigatórias ou eletivas.
4. Anotar, em planilha eletrônica comercial (Microsoft Excel®, e.g.), os dados da análise do item 3 concernentes a todos os cursos constantes da listagem obtida.
5. Consolidar os dados referidos no item 4, produzindo razões percentuais e gráficos.

APÊNDICE I – DIRETRIZES PARA A ANÁLISE DA AMOSTRA DE DADOS DE PENTESTS OBTIDA JUNTO A EMPRESA DE SEGURANÇA COMPUTACIONAL

1. Avaliar a amostra de dados fornecida pela *Tempest Security Intelligence*, buscando identificar nela possíveis informações/relações úteis à pesquisa.
2. Tabular os dados da amostra com foco na produção de inferências.
3. Normalizar os dados da amostra, para facilitação da produção de inferências.
4. Analisar os dados brutos tabulados e os dados normalizados, buscando produzir inferências.
5. Para as inferências produzidas, construir representações tabulares e gráficas sintéticas que possam ser utilizadas na demonstração/ilustração de pontos/aspectos da tese.

**APÊNDICE J – RELAÇÃO ALFABÉTICA DAS INSTITUIÇÕES DE ENSINO
CUJOS CURSOS DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO,
ENGENHARIA DA COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO FORAM
CONSIDERADOS NO ESTUDO**

- CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA – CEFET/RJ
- CENTRO UNIVERSITÁRIO CAMPO LIMPO PAULISTA (UNIFACCAMP)
- CENTRO DE ESTUDOS E SISTEMAS AVANÇADOS DO RECIFE (CESAR)
- FACULDADE DE FILOSOFIA, CIÊNCIAS E LETRAS DE RIBEIRÃO PRETO DA USP
- FUNDAÇÃO UNIVERSIDADE DE PASSO FUNDO (FUPF)
- FUNDAÇÃO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL (UFMS)
- FUNDAÇÃO UNIVERSIDADE FEDERAL DE SERGIPE (UFS)
- INSTITUTO DE CIÊNCIAS MATEMÁTICAS E COMPUTAÇÃO DA USP/SÃO CARLOS
- INSTITUTO DE MATEMÁTICA E ESTATÍSTICA DA UNIVERSIDADE DE SÃO PAULO
- INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ (IFCE)
- INSTITUTO MILITAR DE ENGENHARIA (IME)
- PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
- PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ (PUC/PR)
- PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO (PUC-RIO)
- PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUC/RS)
- UNIVERSIDADE DE BRASÍLIA (UNB)
- UNIVERSIDADE DE FORTALEZA (UNIFOR)
- UNIVERSIDADE DE PERNAMBUCO (UPE)
- UNIVERSIDADE DE SALVADOR (UNIFACS)
- UNIVERSIDADE DE SÃO PAULO (USP)
- UNIVERSIDADE DO ESTADO DE SANTA CATARINA
- UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE (UERN)
- UNIVERSIDADE DO VALE DO ITAJAÍ
- UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)
- UNIVERSIDADE ESTADUAL DE CAMPINAS (UNICAMP)
- UNIVERSIDADE ESTADUAL DE LONDRINA
- UNIVERSIDADE ESTADUAL DE MARINGÁ
- UNIVERSIDADE ESTADUAL DO CEARÁ (UECE)
- UNIVERSIDADE ESTADUAL DO MARANHÃO
- UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO” (UNESP)
- UNIVERSIDADE FEDERAL DA BAHIA (UFBA)
- UNIVERSIDADE FEDERAL DA PARAÍBA (UFPB)
- UNIVERSIDADE FEDERAL DE ALAGOAS (UFAL)

- UNIVERSIDADE FEDERAL DE CAMPINA GRANDE (UFCG)
- UNIVERSIDADE FEDERAL DE GOIÁS (UFG)
- UNIVERSIDADE FEDERAL DE ITAJUBÁ (UNIFEI)
- UNIVERSIDADE FEDERAL DE JUIZ DE FORA (UFJF)
- UNIVERSIDADE FEDERAL DE LAVRAS (UFLA)
- UNIVERSIDADE FEDERAL DE MINAS GERAIS (UFMG)
- UNIVERSIDADE FEDERAL DE OURO PRETO (UFOP)
- UNIVERSIDADE FEDERAL DE PELOTAS (UFPEL)
- UNIVERSIDADE FEDERAL DE PERNAMBUCO (UFPE)
- UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC)
- UNIVERSIDADE FEDERAL DE SANTA MARIA (UFSM)
- UNIVERSIDADE FEDERAL DE SÃO CARLOS (UFSCAR)
- UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI (UFSJ)
- UNIVERSIDADE FEDERAL DE SÃO PAULO (UNIFESP)
- UNIVERSIDADE FEDERAL DE UBERLÂNDIA (UFU)
- UNIVERSIDADE FEDERAL DE VIÇOSA (UFV)
- UNIVERSIDADE FEDERAL DO ABC
- UNIVERSIDADE FEDERAL DO AMAZONAS (UFAM)
- UNIVERSIDADE FEDERAL DO CEARÁ (UFC)
- UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO (UFES)
- UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO (UNIRIO)
- UNIVERSIDADE FEDERAL DO MARANHÃO (UFMA)
- UNIVERSIDADE FEDERAL DO PARÁ (UFPA)
- UNIVERSIDADE FEDERAL DO PARANÁ (UFPR)
- UNIVERSIDADE FEDERAL DO PIAUÍ
- UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ)
- UNIVERSIDADE FEDERAL DO RIO GRANDE (UFRG)
- UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE (UFRN)
- UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)
- UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (UFRPE)
- UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ (UTFPR)

APÊNDICE K – RELAÇÃO ALFABÉTICA DOS SOFTWARES/SERVIÇOS EM SOFTWARE CUJOS EULAS/TOSS FORAM EXAMINADOS NA PESQUISA²⁰⁶

PRODUTO/SERVIÇO	EMPRESA/ENTIDADE RESPONSÁVEL	ORIGEM GEOGRÁFICA DA EMPRESA PRODUTORA/FORNECEDORA
3DEXPERIENCE R2014X	DASSAULT SYSTEMES	FRANÇA
3DEXPERIENCE R2017X	DASSAULT SYSTEMES	FRANÇA
3DVIA HOME RELEASE 5.0 ONLINE SERVICES	DASSAULT SYSTEMES	FRANÇA
AITAC	DASSAULT SYSTEMES	FRANÇA
ALLOCATE	UNITED STATES BUREAU OF THE CENSUS	ESTADOS UNIDOS
ALTIVUM LLC	ALTIVUM	ESTADOS UNIDOS
AMD CATALYST	ADVANCED MICRO DEVICES	ESTADOS UNIDOS
AMD RADEON	ADVANCED MICRO DEVICES	ESTADOS UNIDOS
APPLE CONFIGURATOR	APPLE	ESTADOS UNIDOS
APPLE MEDIA	APPLE	ESTADOS UNIDOS
ARISTA	ARISTA NETWORKS	ESTADOS UNIDOS
AUTODESK	AUTODESK	ESTADOS UNIDOS
AUTODESK ACCOUNT SERVICES	AUTODESK	ESTADOS UNIDOS
AVAST	PIRIFORM	REINO UNIDO
BLUETOOTH DEVELOPER STUDIO APPLICATION	DELAWARE CORPORATION	ESTADOS UNIDOS
BONJOUR FOR WINDOWS	APPLE	ESTADOS UNIDOS
CCLEANER	PIRIFORM	REINO UNIDO
CISCO SYSTEMS	CISCO	ESTADOS UNIDOS
COINBASE	COINBASE	REINO UNIDO
CONTROL4	DELAWARE CORPORATION	ESTADOS UNIDOS
COPERNIC	COPERNIC	CANADA
CRYPTOBLIZZ	CODEBLIZZ	HOLANDA
DATA MANAGEMENT SOFTWARE CS-S10w	KONICA MINOLTA	JAPÃO
DELL ART SOFTWARE	DELL	HOLANDA
DELL IT MANAGEMENT SaaS	DELL	HOLANDA
DELL WYSE	DELL	HOLANDA
DESKPRO	DESKPRO	REINO UNIDO
DISNEY INTERACTIVE	DISNEY INTERACTIVE	ESTADOS UNIDOS

²⁰⁶ Esclarece-se, em tempo, que os EULAs/ToSs da empresa Adobe aplicavam-se simultaneamente a todos os seus produtos/serviços, razão pela qual, nesta relação, são referidos sob a rubrica “TODOS OS PRODUTOS”.

PRODUTO/SERVIÇO	EMPRESA/ENTIDADE RESPONSÁVEL	ORIGEM GEOGRÁFICA DA EMPRESA PRODUTORA/FORNECEDORA
DUOLINGO	DUOLINGO	ESTADOS UNIDOS
ELCOMSOFT	ELCOMSOFT	RÚSSIA
ELSEVIER MOBILE APPLICATIONS	ELSEVIER	ESTADOS UNIDOS
FACEBOOK	FACEBOOK	ESTADOS UNIDOS
FINAL CUT STUDIO	APPLE	ESTADOS UNIDOS
FITGUARD	FIT	ESTADOS UNIDOS
GMAIL	GOOGLE	ESTADOS UNIDOS
GOOGLE	GOOGLE	ESTADOS UNIDOS
GOOGLE CHROME	GOOGLE	ESTADOS UNIDOS
HD VISUAL COMMUNICATION MOBILE	PANASONIC CORPORATION	JAPÃO
IAME TOKEN	IAME	MAURÍCIA
iBOOKS AUTHOR	APPLE	ESTADOS UNIDOS
iBOOKS FOR IOS	APPLE	ESTADOS UNIDOS
iCLOUD FOR WINDOWS	APPLE	ESTADOS UNIDOS
iLIFE	APPLE	ESTADOS UNIDOS
IMOVIE	APPLE	ESTADOS UNIDOS
INSTAGRAM	FACEBOOK	ESTADOS UNIDOS
INVISION	INVISION POWER SERVICES	ESTADOS UNIDOS
iPHOTO	APPLE	ESTADOS UNIDOS
iTUNES MOVIE THRAILERS	APPLE	ESTADOS UNIDOS
iTUNES U	APPLE	ESTADOS UNIDOS
JAVA	ORACLE	ESTADOS UNIDOS
KASPERSKY	KASPERSKY	RÚSSIA
KEYNOTE FOR IOS	APPLE	ESTADOS UNIDOS
LATISTA	ORACLE	ESTADOS UNIDOS
LEXIA	LEXIA LEARNING	ESTADOS UNIDOS
LINGUEE	DEEPL	ALEMANHA
LUMINEX	LUMINEX CORPORATION	ESTADOS UNIDOS
macOS HIGH SIERRA	APPLE	ESTADOS UNIDOS
macOS MOJAVE	APPLE	ESTADOS UNIDOS
macOS SERVER	APPLE	ESTADOS UNIDOS
macOS SERVER	APPLE	ESTADOS UNIDOS
MARI	FOUNDRY	REINO UNIDO
MASIMO TRACE	MASIMO AMERICAS	ESTADOS UNIDOS
MCAFFEE	MCAFFEE	ESTADOS UNIDOS
MICROSOFT AZURE	MICROSOFT	ESTADOS UNIDOS
MICROSOFT EXCHANGE SERVICE 2010	MICROSOFT	ESTADOS UNIDOS
MICROSOFT EXPRESSION BLEND FOR DEVELOPMENT KIT FOR .NET FRAMEWORK	MICROSOFT	ESTADOS UNIDOS

PRODUTO/SERVIÇO	EMPRESA/ENTIDADE RESPONSÁVEL	ORIGEM GEOGRÁFICA DA EMPRESA PRODUTORA/FORNECEDORA
4.0		
MICROSOFT EXPRESSION STUDIO 4 DESIGN	MICROSOFT	ESTADOS UNIDOS
MICROSOFT FALL OUT: VEGAS	MICROSOFT	ESTADOS UNIDOS
MICROSOFT GARAGE PLUMBAGO	MICROSOFT	ESTADOS UNIDOS
MICROSOFT HYPER V SERVER 2019 RETAIL	MICROSOFT	ESTADOS UNIDOS
MICROSOFT HYPER-V SERVER 2016	MICROSOFT	ESTADOS UNIDOS
MICROSOFT HYPER-V SERVER 2019	MICROSOFT	ESTADOS UNIDOS
MICROSOFT LY NC 2010	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 EXCEL	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2010 ACCESS	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 ACCESS OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 DESKTOP	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 EXCEL OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 HOME AND BUSINESS	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 HOME AND BUSINESS OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 HOME AND STUDENT	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 HOME AND STUDENT OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 OFFICE OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 POWERPOINT	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 POWERPOINT OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 PROFESSIONAL ACADEMIC OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 PROFESSIONAL DESKTOP	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 PROFESSIONAL OEM	MICROSOFT	ESTADOS UNIDOS

PRODUTO/SERVIÇO	EMPRESA/ENTIDADE RESPONSÁVEL	ORIGEM GEOGRÁFICA DA EMPRESA PRODUTORA/FORNECEDORA
MICROSOFT OFFICE 2019 PUBLISHER DESKTOP	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 PUBLISHER OEM	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 2019 WORD DESKTOP	MICROSOFT	ESTADOS UNIDOS
Microsoft Office 365	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 365 PERSONAL	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OFFICE 365 UNIVERSITY	MICROSOFT	ESTADOS UNIDOS
MICROSOFT ONENOTE 2010	MICROSOFT	ESTADOS UNIDOS
Microsoft Online Subscription Agreement	MICROSOFT	ESTADOS UNIDOS
MICROSOFT OUTLOOK 2010	MICROSOFT	ESTADOS UNIDOS
MICROSOFT PROJECT 2010	MICROSOFT	ESTADOS UNIDOS
MICROSOFT SERVICES AGREEMENT	MICROSOFT	ESTADOS UNIDOS
MICROSOFT SHAREPOINT 2010	MICROSOFT	ESTADOS UNIDOS
MICROSOFT SQL SERVER 2012 WEB	MICROSOFT	ESTADOS UNIDOS
MICROSOFT VISUAL STUDIO CODE	MICROSOFT	ESTADOS UNIDOS
MICROSOFT WINDOWS 10	MICROSOFT	ESTADOS UNIDOS
MICROSOFT WINDOWS 8 SECURITY ESSENTIALS	MICROSOFT	ESTADOS UNIDOS
MINECRAFT REALMS	MOJANG	ESTADOS UNIDOS
MOZILLA FIREFOX	MOZILLA	ESTADOS UNIDOS
MOZILLA THUNDERBIRD	MOZILLA	ESTADOS UNIDOS
MY DISNEY EXPERIENCE	WALT DISNEY WORLD	ESTADOS UNIDOS
NERO BURNING ROOM	NERO	ALEMANHA
NVIDIA CUDA TOOLKIT	NVIDIA	ESTADOS UNIDOS
NVIVO 12 FOR WINDOWS	QSR INTERNATIONAL	AUSTRALIA
ORACLE BLACKBERRY APPLICATION	ORACLE	ESTADOS UNIDOS
ORACLE FIELD SERVICE CLOUD APP	ORACLE/APPLE	ESTADOS UNIDOS
OS X YOSEMITE	APPLE	ESTADOS UNIDOS
PINTEREST	COLD BREW LABS	ESTADOS UNIDOS
POKER BTC	ENTERRA HOLDING	CURAÇÃO
QIAGEN	QIGEN'S	HOLANDA
QUICKTIME 7	APPLE	ESTADOS UNIDOS
ROSETTA STONE	ROSETTA STONE	ESTADOS UNIDOS

PRODUTO/SERVIÇO	EMPRESA/ENTIDADE RESPONSÁVEL	ORIGEM GEOGRÁFICA DA EMPRESA PRODUTORA/FORNECEDORA
RUBRIK	RUBRIK	ESTADOS UNIDOS
SAFARI FOR WINDOWS	APPLE	ESTADOS UNIDOS
SAFENET	SAFENET	ESTADOS UNIDOS
SEAGATE CLOUD SYSTEM	SEAGATE TECHNOLOGY	ESTADOS UNIDOS
SEGA GAME	SEGA OF AMERICA	ESTADOS UNIDOS
SIEMENS' TALON BACNET FIELD PANEL FIRMWARE	SIEMENS INDUSTRY	ESTADOS UNIDOS
SKETCH	BOHEMIAN B. V.	HOLANDA
SMITHSONIAN CHANNEL MOBILE APP	SMITHSONIAN NETWORKS	ESTADOS UNIDOS
SOLIDWORKS	DELAWARE CORPORATION	ESTADOS UNIDOS
SONY CREATIVE SOFTWARE	SONY CREATIVE SOFTWARE	ESTADOS UNIDOS
SONY MUSIC CENTER	SONY VIDEO & SONY PRODUCTS	JAPÃO
SPOTIFY	SPOTIFY	SUÉCIA
THE PRINT SHOP 4.0	ENCORE SOFTWARE	ESTADOS UNIDOS
THE SETTLERS VII: HISTORY EDITION	UBISOFT ENTERTAINMENT	REINO UNIDO
TODOS OS PRODUTOS	ADOBE	ESTADOS UNIDOS
TRIMBLE SKETCHUP WEB	DELAWARE CORPORATION	ESTADOS UNIDOS
TROVEMAT	JETCRYPTO	ÁUSTRIA
VIDYO	DELAWARE CORPORATION	ESTADOS UNIDOS
VIZI MODELER FOR MICROSOFT VISIO	ITP COMERCE	SUIÇA
VMWARE	DELAWARE CORPORATION	ESTADOS UNIDOS
VMWARE CLOUD SERVICE	DELAWARE CORPORATION	ESTADOS UNIDOS
WAZE	GOOGLE	ESTADOS UNIDOS
WHATSAPP	FACEBOOK	ESTADOS UNIDOS
WINRAR	WIN.RAR	ALEMANHA
WINSQL	SYNAMETRICS	ESTADOS UNIDOS
WINZIP	COREL CORPORATION	ESTADOS UNIDOS
WORLD OF WARCRAFT	DELAWARE CORPORATION	ESTADOS UNIDOS
XSAN ADMINISTRATION	APPLE	ESTADOS UNIDOS
YAHOO	VERIZON	ESTADOS UNIDOS
YAHOO TOOLBAR	YAHOO	IRLANDA
ZEBRA	ZEBRA TECHNOLOGIES INTERNATIONAL	ESTADOS UNIDOS

**APÊNDICE L – RELAÇÃO ALFABÉTICA DAS EMPRESAS
PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE
CUJOS EULAS/TOSS FORAM EXAMINADOS NA PESQUISA**

- ADOBE
- ADVANCED MICRO DEVICES
- ALTIVM
- APPLE
- ARISTA NETWORKS
- AUTODESK
- BOHEMIAN B. V.
- CISCO
- CODEBLIZZ
- COINBASE
- COLD BREW LABS
- COPERNIC
- COREL CORPORATION
- DASSAULT SYSTEMES
- DEEPL
- DELAWARE CORPORATION
- DELL
- DESKPRO
- DISNEY INTERACTIVE
- DUOLINGO
- ELCOMSOFT
- ELSEVIER
- ENCORE SOFTWARE
- ENTERRA HOLDING
- FACEBOOK
- FIT
- FOUNDRY
- GOOGLE
- IAME
- INVISON POWER SERVICES
- ITP COMERCE
- JETCRYPTO
- KASPERSKY
- KONICA MINOLTA

- LEXIA LEARNING
- LUMINEX CORPORATION
- MASIMO AMERICAS
- MCAFFEE
- MICROSOFT
- MOJANG
- MOZILLA
- NERO
- NVIDIA
- ORACLE
- ORACLE/APPLE
- PANASONIC CORPORATION
- PIRIFORM
- QIGEN'S
- QSR INTERNATIONAL
- ROSETTA STONE
- RUBRIK
- SAFENET
- SEAGATE TECHNOLOGY
- SEGA OF AMERICA
- SIEMENS INDUSTRY
- SMITHSONIAN NETWORKS
- SONY CREATIVE SOFTWARE
- SONY VIDEO & SONY PRODUCTS
- SPOTIFY
- SYNAMETRICS
- UBISOFT ENTERTAINMENT
- UNITED STATES BUREAU OF THE CENSUS
- VERIZON
- WALT DISNEY WORLD
- WIN.RAR
- YAHOO
- ZEBRA TECHNOLOGIES INTERNATIONAL

**APÊNDICE M – RELAÇÃO ALFABÉTICA DAS EMPRESAS
PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE E
DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS EULAS/TOSS
FORAM CONSIDERADOS NA INVESTIGAÇÃO**

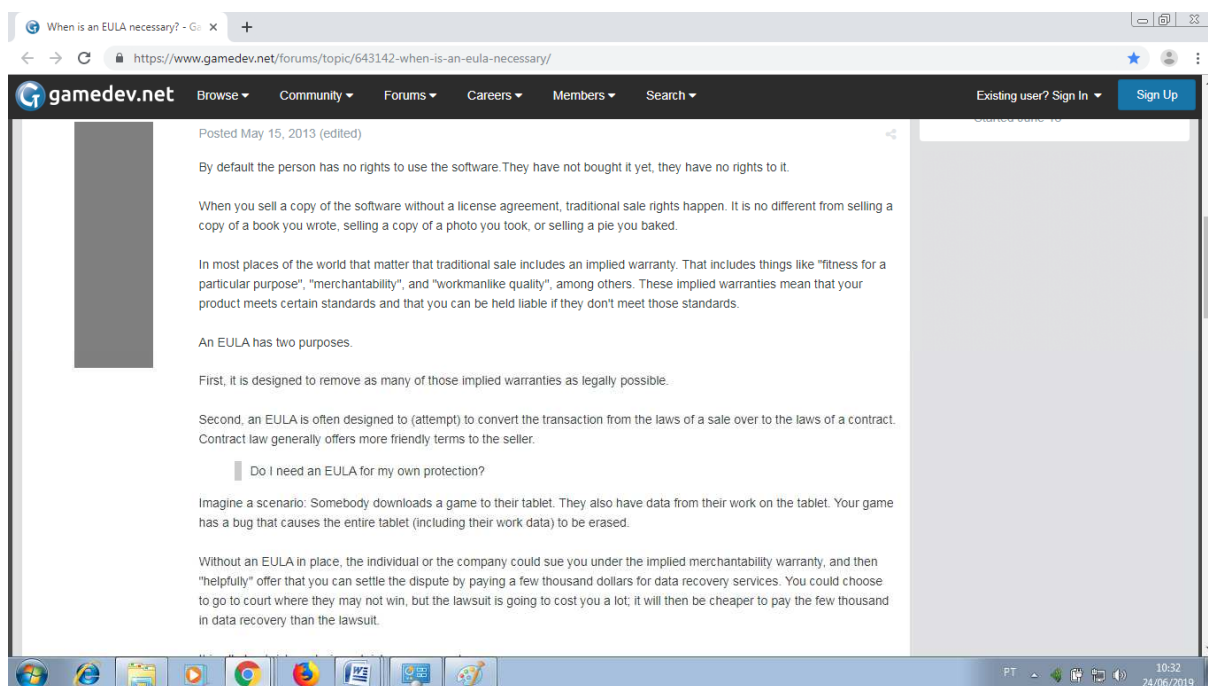
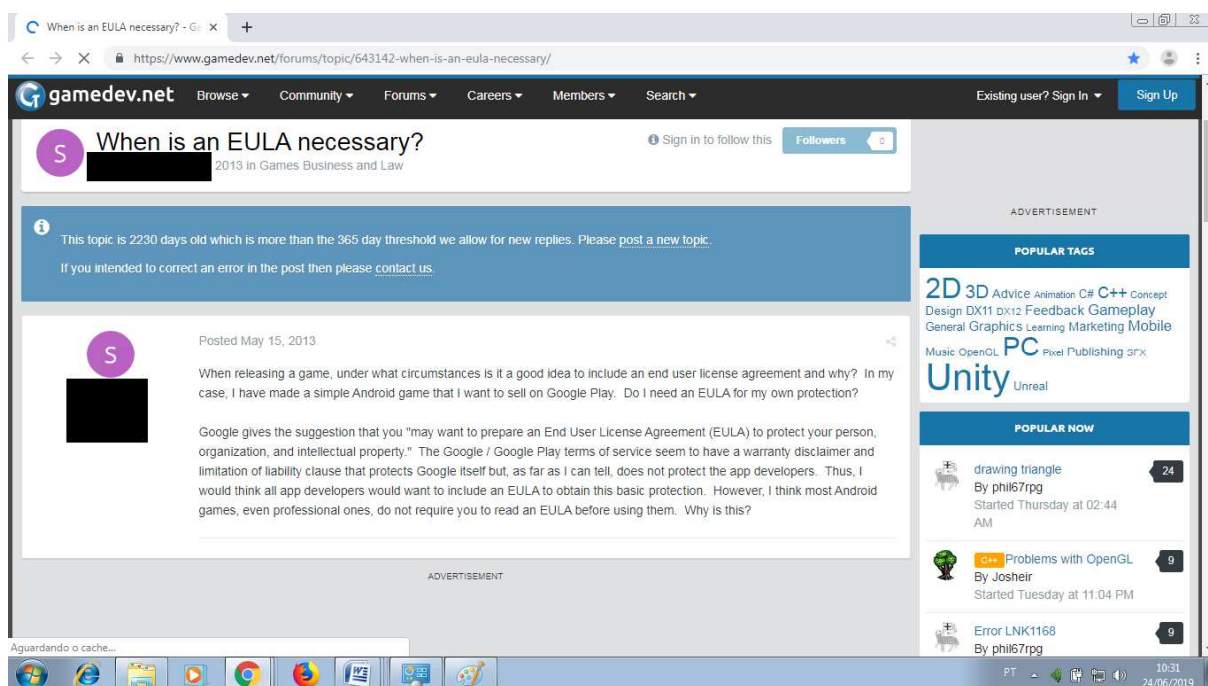
RELAÇÃO DE EMPRESAS PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE E DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS EULAS/TOSS FORAM EXAMINADOS	
EMPRESA/ENTIDADE RESPONSÁVEL	PRODUTO/SERVIÇO
ADOBE	• TODOS OS PRODUTOS
ADVANCED MICRO DEVICES	• AMD CATALYST • AMD RADEON
ALTIVUM	• ALTIVUM LLC
APPLE	• APPLE CONFIGURATOR • APPLE MEDIA • BONJOUR FOR WINDOWS • FINAL CUT STUDIO • IBOOKS AUTHOR • IBOOKS FOR IOS • ICLOUD FOR WINDOWS • ILIFE • IMOVIE • IPHOTO • ITUNES MOVIE THRAILERS • ITUNES U • KEYNOTE FOR IOS • macOS HIGH SIERRA • macOS MOJAVE • macOS SERVER • macOS SERVER • OS X YOSEMITE • QUICKTIME 7 • SAFARI FOR WINDOWS • XSAN ADMINISTRATION
ARISTA NETWORKS	• ARISTA
AUTODESK	• AUTODESK • AUTODESK ACCOUNT SERVICES
BOHEMIAN B. V.	• SKETCH
CISCO	• CISCO SYSTEMS
CODEBLIZZ	• CRYPTOBILIZZ
COINBASE	• COINBASE
COLD BREW LABS	• PINTEREST
COPERNIC	• COPERNIC
COREL CORPORATION	• WINZIP

RELAÇÃO DE EMPRESAS PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE E DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS EULAS/TOSS FORAM EXAMINADOS	
EMPRESA/ENTIDADE RESPONSÁVEL	PRODUTO/SERVIÇO
DASSAULT SYSTEMES	• 3DEXPERIENCE R2014X • 3DEXPERIENCE R2017X • 3DVIA HOME RELEASE 5.0 ONLINE SERVICES • AITAC
DEEPL	• LINGUEE
DELAWARE CORPORATION	• BLUETOOTH DEVELOPER STUDIO APPLICATION • CONTROL4 • SOLIDWORKS • TRIMBLE SKETCHUP WEB • VIDYO • VMWARE • VMWARE CLOUD SERVICE • WORLD OF WARCRAFT
DELL	• DELL ART SOFTWARE • DELL IT MANAGEMENT SaaS • DELL WYSE
DESKPRO	• DESKPRO
DISNEY INTERACTIVE	• DISNEY INTERACTIVE
DUOLINGO	• DUOLINGO
ELCOMSOFT	• ELCOMSOFT
ELSEVIER	• ELSEVIER MOBILE APPLICATIONS
ENCORE SOFTWARE	• THE PRINT SHOP 4.0
ENTERRA HOLDING	• POKER BTC
FACEBOOK	• FACEBOOK • INSTAGRAM • WHATSAPP
FIT	• FITGUARD
FOUNDRY	• MARI
GOOGLE	• GMAIL • GOOGLE • GOOGLE CHROME • WAZE
IAME	• IAME TOKEN
INVISION POWER SERVICES	• INVISION
ITP COMERCE	• VIZI MODELER FOR MICROSOFT VISIO
JETCRYPTO	• TROVEMAT
KASPERSKY	• KASPERSKY
KONICA MINOLTA	• DATA MANAGEMENT SOFTWARE CS-S10w
LEXIA LEARNING	• LEXIA
LUMINEX CORPORATION	• LUMINEX
MASIMO AMERICAS	• MASIMO TRACE
MCAFFEE	• MCAFFEE

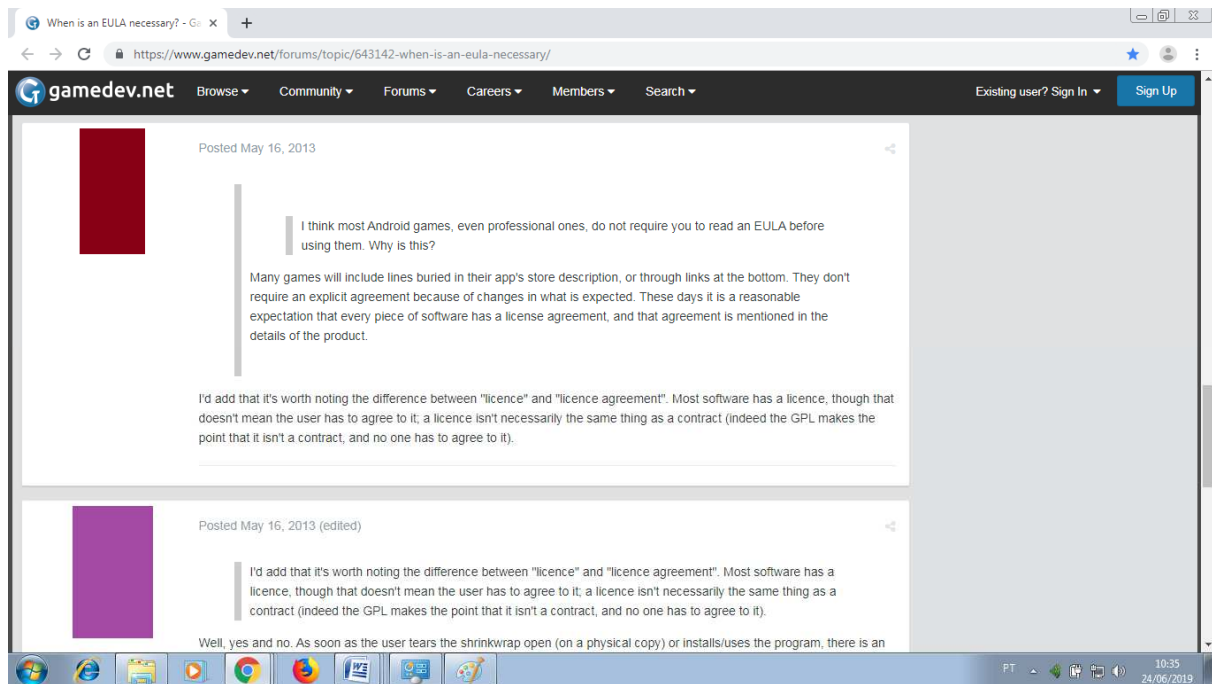
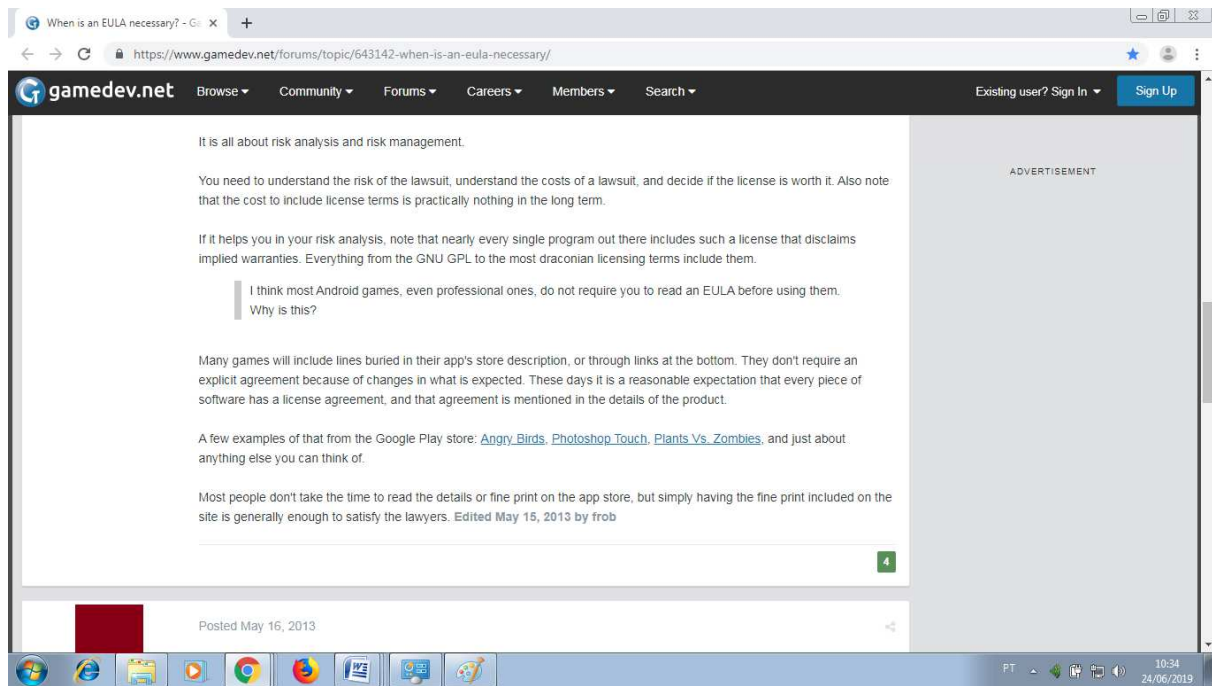
RELAÇÃO DE EMPRESAS PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE E DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS EULAS/TOSS FORAM EXAMINADOS	
EMPRESA/ENTIDADE RESPONSÁVEL	PRODUTO/SERVIÇO
MICROSOFT	• MICROSOFT AZURE • MICROSOFT EXCHANGE SERVICE 2010 • MICROSOFT EXPRESSION BLEND FOR DEVELOPMENT KIT FOR .NET FRAMEWORK 4.0 • MICROSOFT EXPRESSION STUDIO 4 DESIGN • MICROSOFT FALL OUT: VEGAS • MICROSOFT GARAGE PLUMBAGO • MICROSOFT HYPER V SERVER 2019 RETAIL • MICROSOFT HYPER-V SERVER 2016 • MICROSOFT HYPER-V SERVER 2019 • MICROSOFT LY NC 2010 • MICROSOFT OFFICE 2019 EXCEL • MICROSOFT OFFICE 2010 ACCESS • MICROSOFT OFFICE 2019 ACCESS OEM • MICROSOFT OFFICE 2019 DESKTOP • MICROSOFT OFFICE 2019 EXCEL OEM • MICROSOFT OFFICE 2019 HOME AND BUSINESS • MICROSOFT OFFICE 2019 HOME AND BUSINESS OEM • MICROSOFT OFFICE 2019 HOME AND STUDENT • MICROSOFT OFFICE 2019 HOME AND STUDENT OEM • MICROSOFT OFFICE 2019 OFFICE OEM • MICROSOFT OFFICE 2019 POWERPOINT • MICROSOFT OFFICE 2019 POWERPOINT OEM • MICROSOFT OFFICE 2019 PROFESSIONAL ACADEMIC OEM • MICROSOFT OFFICE 2019 PROFESSIONAL DESKTOP • MICROSOFT OFFICE 2019 PROFESSIONAL OEM • MICROSOFT OFFICE 2019 PUBLISHER DESKTOP • MICROSOFT OFFICE 2019 PUBLISHER OEM • MICROSOFT OFFICE 2019 WORD DESKTOP • Microsoft Office 365 • MICROSOFT OFFICE 365 PERSONAL • MICROSOFT OFFICE 365 UNIVERSITY • MICROSOFT ONENOTE 2010 • Microsoft Online Subscription Agreement • MICROSOFT OUTLOOK 2010 • MICROSOFT PROJECT 2010 • MICROSOFT SERVICES AGREEMENT • MICROSOFT SHAREPOINT 2010 • MICROSOFT SQL SERVER 2012 WEB • MICROSOFT VISUAL STUDIO CODE • MICROSOFT WINDOWS 10 • MICROSOFT WINDOWS 8 SECURITY ESSENTIALS

RELAÇÃO DE EMPRESAS PRODUTORAS/FORNECEDORAS DE SOFTWARE/SERVIÇOS EM SOFTWARE E DOS SEUS RESPECTIVOS PRODUTOS/SERVIÇOS CUJOS EULAS/TOSS FORAM EXAMINADOS	
EMPRESA/ENTIDADE RESPONSÁVEL	PRODUTO/SERVIÇO
MOJANG	• MINECRAFT REALMS
MOZILLA	• MOZILLA FIREFOX • MOZILLA THUNDERBIRD
NERO	• NERO BURNING ROOM
NVIDIA	• NVIDIA CUDA TOOLKIT
ORACLE	• JAVA • LATISTA • ORACLE BLACKBERRY APPLICATION
ORACLE/APPLE	• ORACLE FIELD SERVICE CLOUD APP
PANASONIC CORPORATION	• HD VISUAL COMMUNICATION MOBILE
PIRIFORM	• AVAST • CCLEANER
QIGEN'S	• QIAGEN
QSR INTERNATIONAL	• NVIVO 12 FOR WINDOWS
ROSETTA STONE	• ROSETTA STONE
RUBRIK	• RUBRIK
SAFENET	• SAFENET
SEAGATE TECHNOLOGY	• SEAGATE CLOUD SYSTEM
SEGA OF AMERICA	• SEGA GAME
SIEMENS INDUSTRY	• SIEMENS' TALON BACNET FIELD PANEL FIRMWARE
SMITHSONIAN NETWORKS	• SMITHSONIAN CHANNEL MOBILE APP
SONY CREATIVE SOFTWARE	• SONY CREATIVE SOFTWARE
SONY VIDEO & SONY PRODUCTS	• SONY MUSIC CENTER
SPOTIFY	• SPOTIFY
SYNAMETRICS	• WINSQL
UBISOFT ENTERTAINMENT	• THE SETTLERS VII: HISTORY EDITION
UNITED STATES BUREAU OF THE CENSUS	• ALLOCATE
VERIZON	• YAHOO
WALT DISNEY WORLD	• MY DISNEY EXPERIENCE
WIN.RAR	• WINRAR
YAHOO	• YAHOO TOOLBAR
ZEBRA TECHNOLOGIES INTERNATIONAL	• ZEBRA

ANEXO A – REPRODUÇÃO DE DISCUSSÃO ATINENTE A EULAS E TOSS EM FORUM WEB DE USO CORRENTE POR DESENVOLVEDORES DE JOGOS²⁰⁷



²⁰⁷ Apesar de se tratar de fórum de discussões livremente acessível ao público, optou-se, na reprodução feita neste trabalho, por preservar a identidade dos interlocutores, cobrindo-se suas identificações com pequenos retângulos de cores variadas.



When is an EULA necessary? - G... X

https://www.gamedev.net/forums/topic/643142-when-is-an-eula-necessary/

gamedev.net Browse Community Forums Careers Members Search Existing user? Sign In Sign Up

Well, yes and no. As soon as the user tears the shrinkwrap open (on a physical copy) or installs/uses the program, there is an implicit (and sometimes explicit, by clicking the "Yes, I agree" checkbox) agreement.

The user may not respect the agreement or all of its terms, and he may not even have read it (*most people don't read!*) but as far as the lawyer cares, it's certainly an "agreement".

It is not possible to legally use the software otherwise either -- usage of a software is only permitted with a valid license, and a license (usually, except for the Do-WTF-You-Want license) contains a paragraph that states the license is only valid if you agree with the terms. The user can of course *still* use the software illegitimately, but in that case it will be rather hard to press charges against the author.

Though, in the USA, maybe even that is possible. I've heard of a burglar who cut his arm entering a house and sued the house owners for having glass windows that can cut your arm when you break through them. Not sure whether that was a hoax or real...

Edited May 16, 2013 by samoth

GO TO TOPIC LISTING
Games Business and Law

Twitter Facebook Google+ YouTube LinkedIn

Windows taskbar: 10:36 24/06/2019

ANEXO B – CÓDIGO DE ÉTICA IEEE/ACM PARA ENGENHARIA DE SOFTWARE (IEEE COMPUTER SOCIETY; ASSOCIATION FOR COMPUTING MACHINERY, 1999)

The Software Engineering Code of Ethics and Professional Practice

Software Engineering Code of Ethics and Professional Practice (Version 5.2) as recommended by the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices and jointly approved by the ACM and the IEEE-CS as the standard for teaching and practicing software engineering.

Software Engineering Code of Ethics and Professional Practice (Short Version)

PREAMBLE

The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. PUBLIC – Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. PRODUCT – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT – Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7. COLLEAGUES – Software engineers shall be fair to and supportive of their colleagues.

8. SELF – Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Software Engineering Code of Ethics and Professional Practice (Full Version)

PREAMBLE

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their

decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the “Public Interest” is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

PRINCIPLES

Principle 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

Principle 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08. Accept no outside work detrimental to the work they perform for their primary employer.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

Principle 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

- 3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.
- 3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.
- 3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.
- 3.05. Ensure an appropriate method is used for any project on which they work or propose to work.
- 3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.
- 3.07. Strive to fully understand the specifications for software on which they work.
- 3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.
- 3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.
- 3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.
- 3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.
- 3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.
- 3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.
- 3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.
- 3.15. Treat all forms of software maintenance with the same professionalism as new development.

Principle 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

- 4.01. Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

Principle 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance . In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with this Code.

5.12. Not punish anyone for expressing ethical concerns about a project.

Principle 6: PROFESSION

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

Principle 7: COLLEAGUES

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Principle 8: SELF

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06. Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07. Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

This Code was developed by the ACM/IEEE-CS joint task force on Software Engineering Ethics and Professional Practices (SEEPP):

Executive Committee: Donald Gotterbarn (Chair), Keith Miller and Simon Rogerson;

Members: Steve Barber, Peter Barnes, Ilene Burnstein, Michael Davis, Amr El-Kadi, N. Ben Fairweather, Milton Fulghum, N. Jayaram, Tom Jewett, Mark Kanko, Ernie Kallman, Duncan Langford, Joyce Currie Little, Ed Mechler, Manuel J. Norman, Douglas Phillips, Peter Ron Prinzivalli, Patrick Sullivan, John Weckert, Vivian Weil, S. Weisband and Laurie Honour Werth.

This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice.

Copyright (c) 1999 by the Association for Computing Machinery, Inc. and the Institute for Electrical and Electronics Engineers, Inc.