UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE CIÊNCIAS BÁSICAS DA SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO EM CIÊNCIAS:
QUÍMICA DA VIDA E SAÚDE

Antonio João Gonçalves de Azambuja

MODELO DE MATURIDADE DA ARQUITETURA DA INFORMAÇÃO PARA MITIGAR OS IMPACTOS SOCIAIS DOS RISCOS RELACIONADOS COM A PRIVACIDADE, SEGURANÇA E PERDA DE VALOR DAS INFORMAÇÕES DISPONIBILIZADAS NO AMBIENTE DO *BIG DATA*

Porto Alegre

2020

Antonio João Gonçalves de Azambuja

MODELO DE MATURIDADE DA ARQUITETURA DA INFORMAÇÃO PARA MITIGAR OS IMPACTOS SOCIAIS DOS RISCOS RELACIONADOS COM A PRIVACIDADE, SEGURANÇA E PERDA DE VALOR DAS INFORMAÇÕES DISPONIBILIZADAS NO AMBIENTE DO *BIG DATA*

Tese apresentada ao Programa de Pós-Graduação em Educação em Ciências: Química da Vida e Saúde do Instituto de Ciências Básicas da Saúde da Universidade Federal do Rio Grande do Sul como requisito parcial para obtenção do título de doutor em Educação em Ciências.

Orientador:
Prof. Dr. Alexandre Guilherme Motta Sarmento

Co-orientador:
Prof. Dr. Lisandro Zambenedetti Granville

Porto Alegre

2020

CIP - Catalogação na Publicação

Azambuja, Antonio João Gonçalves de
MODELO DE MATURIDADE DA ARQUITETURA DA INFORMAÇÃO PARA MITIGAR OS IMPACTOS SOCIAIS DOS RISCOS RELACIONADOS COM A PRIVACIDADE, SEGURANÇA E PERDA DE VALOR DAS INFORMAÇÕES DISPONIBILIZADAS NO AMBIENTE DO BIG DATA / Antonio João Gonçalves de Azambuja. -- 2020.
175 f.
Orientador: Alexandre Guilherme Motta Sarmento.

Coorientador: Lisandro Zambenedetti Granville.

Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, Instituto de Ciências Básicas da Saúde, Programa de Pós-Graduação em Educação em Ciências: Química da Vida e Saúde, Porto Alegre, BR-RS, 2020.

1. Privacidade das Informações. 2. Segurança da Informação. 3. Risco à Privacidade. 4. Big Data. 5. Lei Geral de Proteção de Dados Pessoais. I. Sarmento, Alexandre Guilherme Motta, orient. II. Granville, Lisandro Zambenedetti, coorient. III. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

ATA AUTENTICADA

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Instituto de Ciências Básicas da Saúde

Programa de Pós-Graduação Educação em Ciências: Química da Vida e Saúde - Associação de IES
QUÍMICA DA VIDA E SAÚDE - Associação de IES - Doutorado
Ata de defesa de Tese

Aluno: Antonio João Gonçalves de Azambuja, com ingresso em 06/03/2018

Título: MODELO DE MATURIDADE DA ARQUITETURA DA INFORMAÇÃO PARA MITIGAR OS IMPACTOS SOCIAIS DOS RISCOS RELACIONADOS COM A PRIVACIDADE, SEGURANÇA E PERDA DE VALOR DAS INFORMAÇÕES DISPONIBILIZADAS NO AMBIENTE DO BIG DATA

Data: 23/04/2020
Horário: 14:30
Local: MConf

Banca Examinadora	Avaliação	Origem
Diogo Losch de Oliveira	Aprovado	UFRGS
Genaina Nunes Rodrigues	Aprovado	UNB
Jackson Max Furtunato Maia	Aprovado	CGEE
Manoel Santana Cardoso	Aprovado	CAPES

Avaliação Geral da Banca: Aprovado
Data da homologação:

Porto Alegre, 13 de maio de 2020

Programa de Pós-Graduação Educação em Ciências: Química da Vida e Saúde - Associação de IES
Rua Ramiro Barcelos, 2600 DBIOQ - Sala 103 - Bairro Santa Cecília - Telefone +555133085538
Porto Alegre - RS

Dedicatória

Dedico a obtenção de meu título de doutor a minha esposa Eliana, meu filho João e aos meus pais Carlos Alberto e Clhoé pelo apoio e exemplo.

AGRADECIMENTOS

Ao Professor Dr. Alexandre Guilherme Motta Sarmento, meu orientador, pelo seu conhecimento, incentivo e a sua paciência na orientação dos caminhos para o desenvolvimento deste trabalho.

Ao Professor Dr. Lisandro Zambenedetti Granville, meu co-orientador, pelo seu conhecimento incentivo e sua paciência na orientação para o desenvolvimento deste trabalho.

Ao meu orientador e co-orientador pelo incentivo, demonstrando que conclusão da Tese não é o fim, e sim outro começo, para outros desafios na vida profissional e acadêmica.

Aos professores membros da banca de qualificação e defesa da Tese, pelas orientações, conhecimento, paciência e sugestões para aperfeiçoar o conhecimento.

Aos colegas do doutorado que durante o período de estudo compartilharam o seu conhecimento nas aulas, trabalhos em grupo e participaram da pesquisa.

Aos professores das disciplinas do doutorado que durante as suas aulas transmitiram todo o seu conhecimento.

Aos funcionários do Programa de Pós-Graduação em Educação em Ciências: Química da Vida e Saúde do Instituto de Ciências Básicas da Saúde da Universidade Federal do Rio Grande do Sul pela colaboração e atendimento.

Ao CNPq e Advocacia-Geral da União, instituições que tive oportunidade de trabalhar agregando conhecimento para o desenvolvimento deste trabalho.

A minha esposa, filho e pais que me apoiaram em todos os momentos do desenvolvimento deste trabalho e pelo seu incentivo para a continuidade da pesquisa e estudos futuros.

RESUMO

O avanço das tecnologias da informação tem possibilitado um crescimento exponencial do volume de dados obtidos, armazenados, processados, transmitidos e publicados no ambiente do *Big Data*. Todo esse crescimento tem gerado desafios para o direito à privacidade, à liberdade de expressão e à segurança das informações tanto as pessoais como as corporativas. As questões do volume de dados, a velocidade com que os dados são processados, a sua variedade e veracidade no ecossistema do *Big Data*, colocam em risco esses direitos e a segurança das informações. Inicialmente este trabalho apresenta uma contextualização sobre o *Big Data*, com definições e suas características. Em seguida aborda questões relacionadas com a ética, a privacidade, a segurança e a organização das informações no *Big Data*. Ao abordar tais questões discorre sobre os riscos e preocupações com a privacidade, riscos com a organização e segurança das informações, conceitos e modelos de maturidade utilizados como base para o Modelo de Maturidade da Arquitetura da Informação proposto. Finalmente apresenta a estrutura do modelo, com seus domínios, objetivos práticas e níveis. O modelo proposto fornece um ponto de referência para as instituições de ensino e pesquisa e de fomento entenderem o nível de suas práticas, processos e métodos para, então, definir metas e prioridades de melhoria, para mitigar os impactos sociais decorrentes de vulnerabilidades de Segurança Cibernética e alinhamento com a Lei Geral de Proteção de Dados Pessoais. A aplicação do modelo foi realizada por meio do questionário *on-line*, que teve a participação de 35 (trinta e cinco) instituições. Os resultados obtidos demonstraram baixa maturidade da Arquitetura da Informação nas instituições pesquisadas. As considerações finais da análise reconhecem que os usuários estão sujeitos aos riscos à privacidade das informações e a sua segurança no universo do *Big Data*.

Palavras-chave: Privacidade das Informações, Segurança da Informação; Risco à Privacidade, Proteção de Dados, *Big Data*, Lei Geral de Proteção de Dados Pessoais

ABSTRACT

The progress of information technologies has enabled an exponential growth in the volume of data collect, stored, processed, transmitted and published in the Big Data environment. All of this growth has created challenges for the right to privacy, freedom of expression and the security of both personal and corporate information. Data volume issues, the speed with which data is processed, its variety and veracity in the Big Data ecosystem, put those rights and the security of information in risk. Initially this paper presents a contextualization about Big Data, with definitions and their characteristics. Then addresses issues related to ethics, privacy, security and the information organization in the Big Data. Addressing such issues related to privacy risks and concerns, information organization and information security risks, concepts and maturity models used as a basis for the proposed Information Architecture Maturity Model. Finally, the thesis presents the structure of the model, the domains, practical objectives and its levels. The proposed model provides a point of reference for education and research and development institutions to understand the level of their practices, processes and methods to then set improvement goals and priorities to mitigate the social impacts of cyber security vulnerabilities and alignment with the Brazilian General Personal Law of Data Protection. The application of the model was done through an on-line questionnaire, which was attended by 35 (thirty-five) institutions. The results demonstrated a low maturity of Information Architecture in the researched institutions. The final considerations in the analysis recognize that users are subject to the risks to information privacy and their security in the Big Data universe.

Keywords: Privacy Information, Information Security, Privacy Risk, Data Protection, Big Data, General Personal Law of Data Protection

LISTA DE FIGURAS

CAPÍTULO 1

Figura 1 – Nuvem de palavras 21
Figura 2 – Nuvem de palavras - combinações 22
Figura 3 – Gerenciador de referências *Mendeley* 23
Figura 4 – Mecanismos da Arquitetura da Informação 24
Figura 5 – Níveis de maturidade do modelo CMM 28
Figura 6 – Níveis de maturidade do modelo CMMI 29
Figura 7 – Níveis de maturidade do modelo C2M2 30
Figura 8 – Objetivos dos níveis do modelo NIST *Cybersecurity Framework* 33
Figura 9 – Níveis de maturidade do modelo CCSMM 35
Figura 10 – Visão em camadas da Segurança da Informação e Comunicações 43
Figura 11 – 5V´s do *Big Data* 45

CAPÍTULO 2

Figura 12 – Fases da análise de conteúdo 57
Figura 13 – Mecanismos da Arquitetura da Informação e princípios da LGPD 60
Figura 14 – Estrutura do modelo proposto 71
Figura 15 – Percentuais 74
Figura 16 – Tela de apresentação do questionário 97
Figura 17 – Tela de cadastro do questionário 97
Figura 18 – Tela do primeiro nível do questionário 98
Figura 19 – Dispositivos 98
Figura 20 – *QR Code* 99
Figura 21 – *Dashboard* das respostas 99
Figura 22 – *Dashboard* dos níveis de maturidade por domínio 100

LISTA DE GRÁFICOS

CAPÍTULO 2

Gráfico 1 – Percentual de investimento em cibersegurança 80
Gráfico 2 – Percentual de confiança do usuário 82
Gráfico 3 – Percentual de confiança do usuário nos serviços *on-line* dos governos 83
Gráfico 4 – Capacidade para atender os requisitos da LGPD 92
Gráfico 5 – Experiência *on-line* 93
Gráfico 6 – Participação dos capítulos da LGPD nos domínios do modelo proposto 94
Gráfico 7 – Percentual de participação na pesquisa 101
Gráfico 8 – Instituições de ensino 103
Gráfico 9 – Percentual das instituições de ensino por nível de maturidade 103
Gráfico 10 – Instituições de pesquisa 104
Gráfico 11 – Percentual das instituições de pesquisa por nível de maturidade 104
Gráfico 12 – Instituições de fomento 105
Gráfico 13 – Percentual das instituições de fomento por nível de maturidade 105
Gráfico 14 – Instituições da APF 106
Gráfico 15 – Percentual das instituições da APF por nível de maturidade 106
Gráfico 16 – Instituições da APE 107
Gráfico 17 – Percentual das instituições da APE por nível de maturidade 107
Gráfico 18 – Instituições privadas 108
Gráfico 19 – Percentual das instituições privadas por nível de maturidade 108
Gráfico 20 – Percentual por nível de maturidade 109
Gráfico 21 – Percentual das práticas por objetivo 110

LISTA DE QUADROS

CAPÍTULO 1

Quadro 1 – Palavras-chave 21
Qaudro 2 – Domínios e objetivos – C2M2 31

CAPÍTULO 2

Quadro 3 – Domínios, elementos, processos, descrição e temas dos modelos 58
Quadro 4 – Níveis de maturidade 61
Quadro 5 – Níveis de maturidade e as características de institucionalização 62
Quadro 6 – Domínios, objetivos e artigos da LGPD 63
Quadro 7 – Domínio: Governança 64
Quadro 8 – Domínio: Proteção de dados 64
Quadro 9 – Domínio: Respostas às vulnerabilidades, ameaças e incidentes 65
Quadro 10 – Domínio: Riscos 66
Quadro 11 – Domínio: Capacitação, conscientização e cultura de proteção dos dados 67
Quadro 12 – Domínio: Tratamento dos dados 68
Quadro 13 – Domínio: Organização da informação 69
Quadro 14 – Domínio: Infraestrutura tecnológica 70
Quadro 15 – Questionário do modelo de maturidade da AI 85
Quadro 16 – Domínios e artigos da LGPD 93

CAPÍTULO 4

Quadro 1 – Competências da BNCC (2018) 145
Quadro 2 – Competências 154
Quadro 3 – Competências da Indústria 4.0 vs Competências da BNCC (2018) 155

LISTA DE TABELAS

CAPÍTULO 2

Tabela 1 – Tipos de instituições participantes..... 100
Tabela 2 – Nível de maturidade das instituições por domínio 101

SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
AI	Arquitetura da Informação
ABRAHOSTING	Associação Brasileira de Empresas de Infraestrutura de Hospedagem na Internet
APF	Administração Pública Federal
APE	Administração Pública Estadual
BNCC	Base Nacional Comum Curricular
CA	*Cambridge Analytica*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CEEI	Centro de Estudos Estratégicos e Internacionais
CGEE	Centro de Gestão e Estudos Estratégicos
CI	Ciência da Informação
CIGI	*Centre for International Governance Innovation*
CMM	*Capability Maturity Model*
CMMI	*Capability Maturity Model Integration*
CCSMM	*The Community Cyber Security Maturity Model*
C2M2	*Cybersecurity Capability Maturity Model*
DPO	*Data Protection Officer*
EUA	Estados Unidos da América
LGPD	Lei Geral de Proteção de Dados Pessoais
GDPR	Regulamento Geral sobre a Proteção de Dados
IBM	*International Business Machines*
IEC	*International Electrotechnical Commission*
IoT	Internet das Coisas – *Internet of Things*

IPC	*Internet Privacy Concern*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
NIST	*National Institute of Standars and Technology*
NISTCyberSecurity	*NIST Cybersecurity Framework*
PwC	*PricewaterhouseCoopers*
RDP	*Random Data Pertubation*
SBC	Sociedade Brasileira da Computação
SBRC	Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos
SegCiber	Segurança Cibernética
SE	Serasa *Experian*
SEI	*Software Engineering Institute*
SI	Segurança da Informação
TI	Tecnologia da informação
TIC	Tecnologia da Informação e Comunicações
UE	União Europeia
USP	Universidade de São Paulo

SUMÁRIO

I INTRODUÇÃO 16
I.I Hipóteses 17
I.II Justificativa 17

CAPÍTULO 1: Modelo de Maturidade da Arquitetura da Informação para mitigar os impactos sociais dos riscos relacionados com a privacidade, segurança e perda de valor das informações disponibilizadas no ambiente do *Big Data* 19
1.1 INTRODUÇÃO 19
1.1.1 Revisão da literatura 21
1.1.2 Problema 23
1.1.3 Pergunta de pesquisa 25
1.2 OBJETIVOS 25
1.2.1 Objetivo geral 25
1.2.2 Objetivos específicos 26
1.3 REFERENCIAL TEÓRICO 26
1.3.1 Modelos de maturidade 26
1.3.1.1 *Capability maturity model* 27
1.3.1.2 *Capability maturity model integration* 28
1.3.1.3 *Cybersecurity capability maturity model* 29
1.3.1.4 *National Institute of Standars and Technology Cybersecurity Framework* 32
1.3.1.5 *The community cyber security maturity model* 34
1.3.2 Ciência da informação 35
1.3.2.1 Sociedade da informação 36
1.3.3 Arquitetura da informação 37
1.3.3.1 Caos informacional 39
1.3.4 Segurança da informação 39
1.3.5 Segurança cibernética 41
1.3.6 *Big Data* 44
1.3.6.1 Características 44
1.3.6.2 Fonte 45
1.3.7 Privacidade 46
1.3.7.1 Normas de privacidade 47
1.3.8 Anonimização de dados 48
1.3.9 Lei Geral de Proteção de Dados Pessoais 50
1.3.9.1 Dados 51
1.3.9.1.1 Dos princípios sobre o tratamento dos dados elencados na LGPD 51
1.3.9.1.2 Do consentimento para o tratamento dos dados estabelecido na LGPD 52
1.3.9.1.3 Dos principais direitos dos titulares dos dados estabelecidos na LGPD 53
1.3.9.1.4 Da transferência internacional dos dados estabelecida na LGPD 53

1.3.9.2 *Data protection officer* 54
1.3.9.3 Da governança da privacidade dos dados 54
1.3.9.4 Das sanções 55
CAPÍTULO 2 56
2.1 METODOLOGIA 56
2.1.1 Descrição da pesquisa 57
2.2 APLICAÇÃO DOS CONHECIMENTOS 60
2.2.1 Níveis de maturidade do modelo proposto 61
2.2.2 Domínios, objetivos e práticas do modelo proposto 62
2.2.2.1 Estrutura do modelo proposto 62
2.2.2.1.1 Domínio: Governança 63
2.2.2.1.2 Domínio: Proteção de dados 64
2.2.2.1.3 Domínio: Respostas às vulnerabilidades, ameaças e incidentes 65
2.2.2.1.4 Domínio: Riscos 66
2.2.2.1.5 Domínio: Capacitação, conscientização e cultura de proteção dos dados 67
2.2.2.1.6 Domínio: Tratamento dos dados 68
2.2.2.1.7 Domínio: Organização da informação 69
2.2.2.1.8 Domínio: Infraestrutura tecnológica 70
2.3 ANÁLISE DOS IMPACTOS SOCIAIS DO *BIG DATA* 71
2.3.1 Riscos à privacidade 71
2.3.2 Preocupação com a privacidade 72
2.3.3 Disposição para fornecer informações *on-line* 73
2.3.4 As contradições dos usuários 74
2.3.5 Ética 75
2.3.6 Organização da informação 76
2.3.7 Riscos à segurança das informações 77
2.3.8 Valor das informações 78
2.4 IMPORTÂNCIA DA PRIVACIDADE, DA ORGANIZAÇÃO, DA SEGURANÇA E DO VALOR DAS INFORMAÇÕES 79
2.4.1 Para as instituições 79
2.4.2 Para os usuários 80
2.5 RESULTADOS 83
2.5.1 Autoavaliação 84
2.5.1.1 Questionário para a autoavaliação 85
2.5.2 Alinhamento com a LGPD 91
2.5.3 Resultados da aplicação do Modelo de Maturidade da AI proposto 95
2.5.3.1 Ferramentas de TIC utilizadas na pesquisa 95
2.5.3.2 Discussão dos resultados 100
CAPÍTULO 3: A privacidade, a segurança da informação e a proteção de dados no *Big Data* (Artigo 1) 111
I APRESENTAÇÃO 111
1 INTRODUÇÃO 113
2 *BIG DATA* 115
2.1 Definição 115

2.2 Características 115
2.3 Fonte 116
3 ÉTICA 116
4 PRIVACIDADE 117
4.1. Disposição para fornecer informações *on-line* 119
4.2. As contradições dos usuários 119
4.3. Riscos à privacidade 119
4.4. Preocupação com a privacidade 120
4.5. Confiança no ambiente *on-line* 121
5 SEGURANÇA DA INFORMAÇÃO 122
5.1. Riscos à segurança das informações 123
6 ORGANIZAÇÃO DA INFORMAÇÃO 123
6.1. Arquitetura da informação 124
6.2. Anonimização de dados 125
6.3. Modelos de anonimização 127
7 PANORAMA DA PROTEÇÃO DE DADOS EM 2018 128
8 CONCLUSÃO 129
REFERÊNCIAS 130
CAPÍTULO 4: As novas competências educacionais no contexto da Indústria 4.0 (Artigo 2) 136
I APRESENTAÇÃO 136
1 INTRODUÇÃO 139
2 REFERENCIAL TEÓRICO 140
2.1 Indústria 4.0 141
2.2 Educação 4.0 143
2.3 Base Nacional Comum Curricular 145
2.4 Aprendizagem 148
3 METODOLOGIA 150
3.1 Fases da pesquisa 151
4 COMPETÊNCIAS PARA INDÚSTRIA 4.0 151
5 RESULTADOS DA PESQUISA 153
6 CONCLUSÃO 156
REFERÊNCIAS 157
CONSIDERAÇÕES FINAIS 161
REFERÊNCIAS 164

I INTRODUÇÃO

Este trabalho está estruturado[1] em 4 (quatro) capítulos: o capítulo 1 (um) apresenta o Modelo de Maturidade da Arquitetura da Informação para mitigar os impactos sociais dos riscos relacionados com a privacidade, segurança e perda de valor das informações disponibilizadas no ambiente do *Big Data,* objeto desta Tese de Doutorado. Neste capítulo está descrita a revisão da literatura, o problema, a pergunta de pesquisa, objetivos e referencial teórico. O capítulo 2 (dois) discorre sobre a metodologia, os impactos sociais do *Big Data* e resultados da aplicação do modelo nas instituições participantes da pesquisa.

A aplicação do Modelo de Maturidade da Arquitetura da Informação proposto no objetivo geral deste trabalho, contou com a participação de 35 (trinta e cinco) instituições. Inicialmente o foco do trabalho foi identificar a maturidade da Arquitetura da Informação (AI) nas instituições de ensino, de pesquisa e de fomento. No entanto, em face da divulgação do trabalho entre profissionais da área de Tecnologia da Informação e Comunicações (TIC), outras organizações demonstraram interesse em participar da pesquisa, tais como: instituições da Administração Pública Federal (APF), da Administração Pública Estadual (APE) e empresas privadas que desenvolvem projetos de pesquisa.

Para coleta dos dados foi encaminhado por *e-mail* um questionário *on-line* para gestores e profissionais envolvidos com as questões de TIC das instituições participantes.

Os capítulos 3 (três) e 4 (quatro) apresentam os 2 (dois) artigos desenvolvidos durante o período do Doutorado e relacionados com o tema da pesquisa.

O artigo 1 (um)[2], apresentado no capítulo 3 (três) discorre sobre a privacidade, a Segurança da Informação (SI) e a proteção de dados no *Big Data*. Foi submetido e publicado na revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos (CGEE), em 2019.

Já o artigo 2 (dois)[3], apresentado no capítulo 4 (quatro) descreve as competências educacionais para atender as demandas relacionadas com o avanço tecnológico presente na 4ª. Revolução Industrial e foi submetido à revista Educação e Pesquisa da Universidade de São Paulo (USP), em 2020.

Os artigos apresentados nos capítulos 3 (três) e 4 (quatro) deste trabalho foram construídos no decurso do doutoramento, com base nas temáticas decorrentes do conhecimento adquirido durante o desenvolvimento do Modelo de Maturidade da AI apresentado no capítulo

[1] Este trabalho está estruturado com base no Modelo de Maturidade da Arquitetura da Informação proposto e nos artigos desenvolvidos.
[2] Artigo 1 (um): *ipsis litteris* como enviado e publicado na revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos.
[3] Artigo 2 (dois): *ipsis litteris* como enviado para a revista Educação e Pesquisa da Universidade de São Paulo.

1 (um) e 2 (dois). No início dos capítulos 3 (três) e 4 (quatro) destaca-se o alinhamento dos artigos desenvolvidos com o tema desta pesquisa.

Sendo assim, os referidos capítulos abordam o tema de estudo, as considerações finais, referências bibliográficas e outros itens apresentados que podem ter repetições de partes do trabalho, já que na estrutura da Tese estão a integra dos artigos desenvolvidos durante o doutorado.

I.I Hipóteses

As hipóteses que orientaram este trabalho foram:

- Que em ambiente tecnológico com o acesso a uma quantidade cada vez maior de dados, a SI e a privacidade das informações pessoais e corporativas estão em risco, segundo os autores Xu *et al*. (2012) e Malhotra *et al*. (2004);
- Que as repetidas ameaças cibernéticas nas organizações de todos os setores, tipos e tamanhos demandam a implementação de práticas, métodos e processos relacionados com a organização da informação armazenada no universo informacional;
- Que com os avanços tecnológicos presentes na 4ª. Revolução Industrial, o tema competências educacionais para atender as demandas das organizações públicas e privadas, está na pauta das discussões acadêmicas, empresariais e governamentais; e
- Que conhecer e compreender o nível de maturidade da AI nas instituições inseridas no ambiente *Big Data* e na forma como as mesmas gerenciam as informações, contribuirá para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a SI e com a perda de valor das informações, bem como o alinhamento com a Lei Geral de Proteção de Dados Pessoais (LGPD).

I.II Justificativa

As instituições estão passando por transformações na forma de lidar com as informações. O avanço das TIC tem permitido o armazenamento de grandes e múltiplas bases de dados, que contém tanto informações pessoais quanto corporativas.

A evolução da capacidade de capturar, analisar e disseminar as informações, que, por vezes, são armazenadas e disponibilizadas sem a concordância dos usuários, gera um aumento das ameaças relacionadas com a privacidade das informações e com a sua segurança.

A organização da sociedade da informação envolve os valores de segurança e privacidade, que fazem parte dos sistemas de informação, os quais precisam ser protegidos

contra os crimes cibernéticos referentes ao uso ilegal de *hardware*, *softwares* ou de dados (LAUDON; LAUDON, 2010). Existem custos sociais e riscos associados ao contínuo vazamento de dados pessoais e corporativos.

O *Big Data* não é uma área de estudo exclusiva da Ciência da Computação pois, como afirmam Boyd e Crawford (2012), físicos, economistas, matemáticos, cientistas políticos, bio-informáticos, sociólogos e outros profissionais poderão fazer uso e reuso da quantidade massiva de informações e das interações produzidas pelas pessoas no meio digital.

Sobre os possíveis problemas éticos levantados, o *Big Data* traz consigo a invasão de privacidade, diminuição das liberdades civis e aumento do controle estatal e corporativo, gerando incerteza e medo quanto aos usos e manipulação dos dados (BOYD; CRAWFORD, 2012).

Com o volume de informações disponíveis, torna-se necessário enfrentar o caos informacional com a utilização da AI. Diante desse contexto, justifica-se conhecer o estado atual da AI das instituições de ensino e pesquisa e de fomento, por meio de um modelo de maturidade, bem como realizar uma análise das competências educacionais para enfrentar as demandas da 4ª. Revolução Industrial.

CAPÍTULO 1

1.1 INTRODUÇÃO

A informatização da sociedade aliada ao avanço das TIC e a sua convergência, evidenciada na era da informação, tem proporcionado um crescimento exponencial do volume de dados no espaço cibernético, o que marca o advento do *Big Data*. A gestão da informação, do conhecimento, a organização da informação, e a proteção dos dados são grandes desafios para as instituições na atualidade.

Vivemos a era do *Big Data* que tem transformado a forma como as instituições estão direcionando o seu processo de tomada de decisão (JANSSEN; VAN DER VOORT; WAHYUDI, 2017). As novas tecnologias permitem que as instituições, a partir da análise dos dados, tenham um ganho de competitividade (EREVELLES; FUKAWA; SWAYNE, 2016).

Nesse cenário, composto pela explosão da quantidade de dados, disponibilidade e potencialidade decorrente do avanço das tecnologias de processamento, coleta e análise dos dados situa-se o fenômeno conhecido como *Big Data*.

Esse fenômeno tem impactado a sociedade, por meio de novos modelos de negócios que fazem rastreamento de dados para analisar padrões de comportamento, consumo e saúde, visando estabelecer uma tomada de decisão baseada em dados.

Ao mesmo tempo que novas formas de comunicação, registro, acesso e recuperação da informação estão sendo viabilizadas, surge a preocupação com a privacidade e segurança das informações (CHEN; YANG; LUO, 2017).

A privacidade e a SI na Internet tem sido uma área que tem despertado interesse de estudo, devido à grande quantidade de informações pessoais e corporativas que são obtidas, armazenadas, transmitidas e publicadas na rede mundial de computadores.

A informação tornou-se um ativo de valor para as instituições, o qual pode ser processado por meio eletrônico usando redes públicas e privadas pela Internet (HONG; THONG, 2013).

Esses ativos que podem ser corporativos e/ou pessoais, compõem o ambiente atual dos negócios das instituições e estão em constante ameaça de vírus, invasões de sistemas, abuso de informações privilegiadas, quebra da privacidade e divulgação não autorizada das informações (JOHNSTON; WARKENTIN, 2010).

Para Zwitter (2014), em um mundo altamente interconectado, lidar com a ética, considerando o consentimento dos usuários, a privacidade, a segurança e a anonimização das informações são desafios do *Big Data*. Já Drinkwater (2016), ressalta que o vazamento de informações *on-line*, aumenta as preocupações dos usuários em relação dos riscos à SI. O direito à privacidade é um princípio constitucional e está intrinsecamente ligado ao direito da personalidade da pessoa humana.

Diante do contexto no qual os direitos à privacidade e proteção de dados foram elevados ao nível dos direitos humanos no cenário internacional, os governos têm dispensado especial atenção para lidar com esses desafios. Nesse cenário, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), publicado em 24 de março de 2018, pela União Europeia (UE), que visa proporcionar aos usuários maior controle sobre seus dados pessoais e aumentar as restrições sobre as empresas que tratam e lidam com esses dados.

Já no cenário nacional o Governo Brasileiro publicou a Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A referida Lei entrará em vigor no primeiro semestre de 2020.

A nova lei terá impactos em como as instituições públicas e privadas deverão lidar com os dados dos seus clientes. As instituições brasileiras terão novas obrigações, e terão vantagem competitiva as que adaptarem seu modelo de negócio às diretrizes da LGPD no prazo estabelecido.

Diante do exposto, este trabalho apresenta um Modelo de Maturidade da Arquitetura da Informação e os resultados da sua aplicação em instituições de ensino, de pesquisa e de fomento para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a organização e a segurança das informações, com a perda de valor das informações, bem como o alinhamento com a LGPD.

O trabalho busca ainda apresentar uma contextualização sobre o *Big Data*, discorre sobre questões relacionadas com a privacidade, com a organização e a SI nesse ambiente, alinhamento com a LGPD e conceitos de AI, Ciência da Informação (CI) e Segurança Cibernética (SegCiber), bem como os modelos de maturidade utilizados como base para o modelo proposto.

1.1.1 Revisão da literatura

Na revisão da literatura, o tema pesquisado foi Modelo de Maturidade da Arquitetura da Informação no ambiente *Big Data*, no período de 2010 a 2019. As buscas foram realizadas no portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), nas seguintes bases de dados: *Web of Science*, *Scopus*, *IEEE Xplore*, *Scielo* e *Google Scholar.*

As palavras-chave, em inglês e português, utilizadas na pesquisa estão apresentadas no Quadro 1.

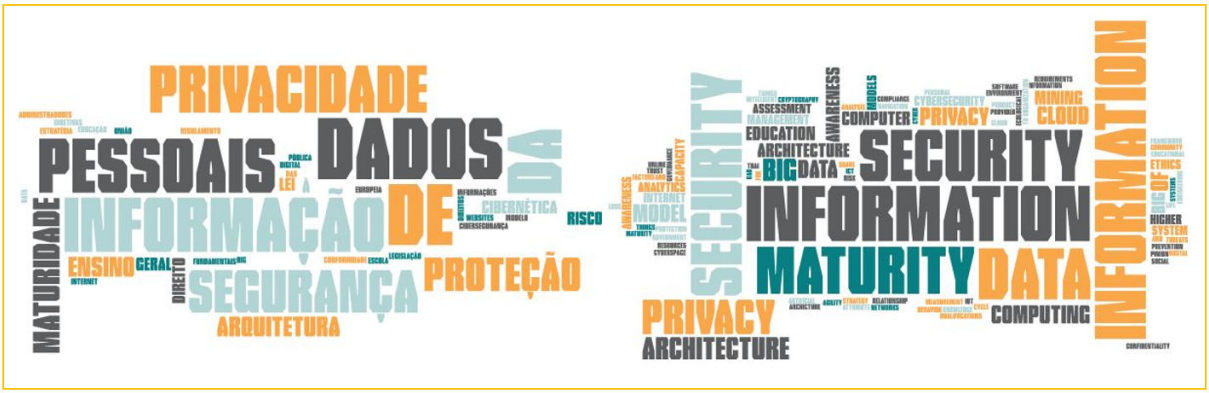
Quadro 1 – Palavras-chave

Português	Inglês
Arquitetura da informação	*Big data*
Comportamento digital	*Cloud computing*
Computação em nuvem	*Cyber security*
Cultura digital	*Digital behavior*
Dados pessoais	*Digital culture*
Modelo de maturidade	*Information architecture*
Privacidade das informações	*Information security*
Proteção de dados	*Maturity model*
Risco à privacidade	*Personal data*
Segurança cibernética	*Privacy of information*
Segurança da informação	*Privacy risk*
	Protection of data

Fonte: O autor

Foi elaborada uma nuvem de palavras com as palavras-chave e *keywords* dos artigos utilizados na pesquisa, que pode ser observada na Figura 1. A nuvem de palavras é um gráfico digital que permite a visualização das palavras em tamanho proporcional à sua frequência no texto pesquisado. As palavras são apresentadas em tamanhos e cores diferentes, conforme sua relevância no conteúdo do artigo.

Figura 1 – Nuvem de palavras



Fonte: O autor

No levantamento bibliográfico, a disponibilidade de artigos é reduzida na combinação dos termos *Information Architecture* AND *Maturity Models*, *Information Architecture* AND *Cyber Security*, *Information Architecture* AND *Privacy of Information* e *Information Architecture* AND *Protection of Data*, apesar da importância da AI para a organização, apresentação e estruturação das informações nas instituições. A Figura 2 apresenta uma nuvem de palavras com as combinações das *keywords*.

Figura 2 – Nuvem de palavras - combinações

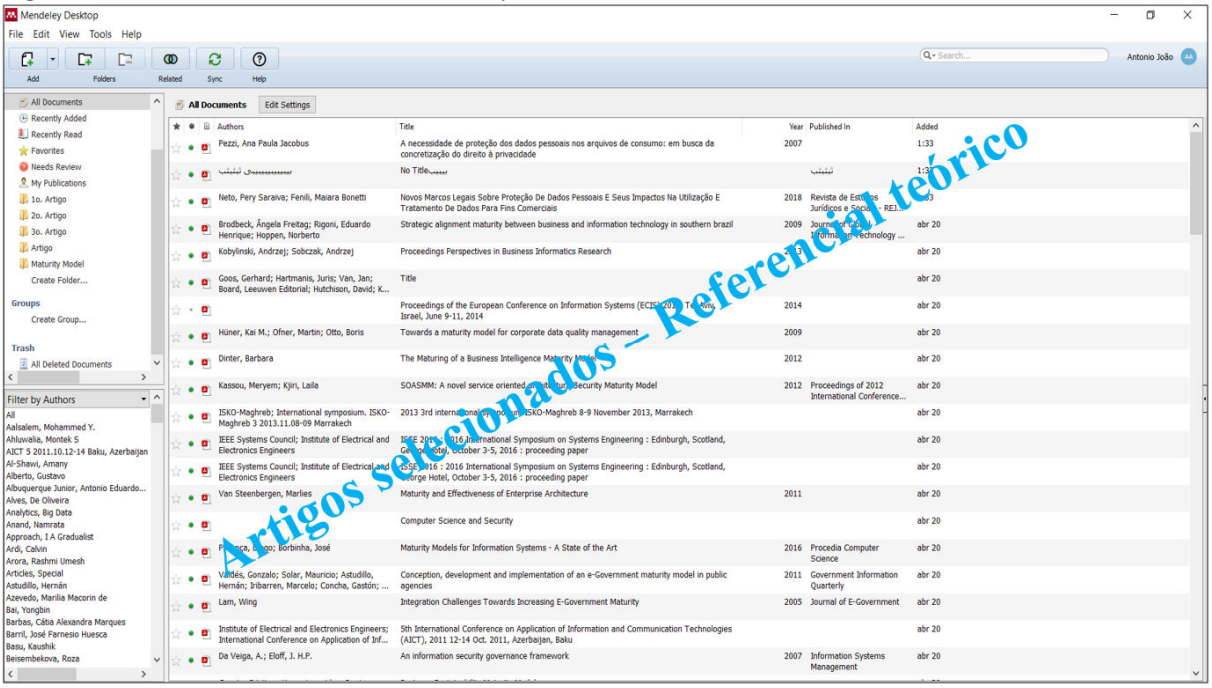
Fonte: O autor

Na pesquisa ficou demonstrado que são poucas as referências teóricas direcionadas à elaboração e aplicação de um Modelo de Maturidade da AI no contexto do *Big Data*, visando as questões relacionadas com os riscos sociais e de TIC presentes no espaço cibernético, confirmando que há uma lacuna de conhecimento nesse tema.

A pesquisa com termos-chave em inglês nas bases de dados disponíveis no Portal de Periódicos da CAPES[4] trouxe um total de 33 (trinta e três) artigos, que tratavam da combinação dos termos pesquisados, apresentados na nuvem de palavras da Figura 2. Os artigos selecionados foram organizados no gerenciador de referências *Mendeley*, conforme um extrato do gerenciador apresentado na Figura 3.

[4] Portal de Periódicos da CAPES: http://www-periodicos-capes-gov-br.ez45.periodicos.capes.gov.br/

Figura 3 – Gerenciador de referências *Mendeley*



Fonte: Mendeley

O estudo encomendado pela *International Business Machines* (IBM), "*Cyber Resilient Organization* 2019", aponta que a colaboração entre privacidade e SegCiber é um requisito para assegurar a proteção dos dados e tomada de decisão, principalmente com a edição das novas regulamentações, como a LGPD no Brasil, a GDPR na União Europeia e o *California Consumer Privacy Act* nos Estados Unidos da América (EUA).

1.1.2 Problema

As repetidas ameaças cibernéticas nas organizações de todos os setores, tipos e tamanhos indicam a necessidade da implementação de práticas, métodos e processos relacionados com a organização da informação armazenada no universo informacional.

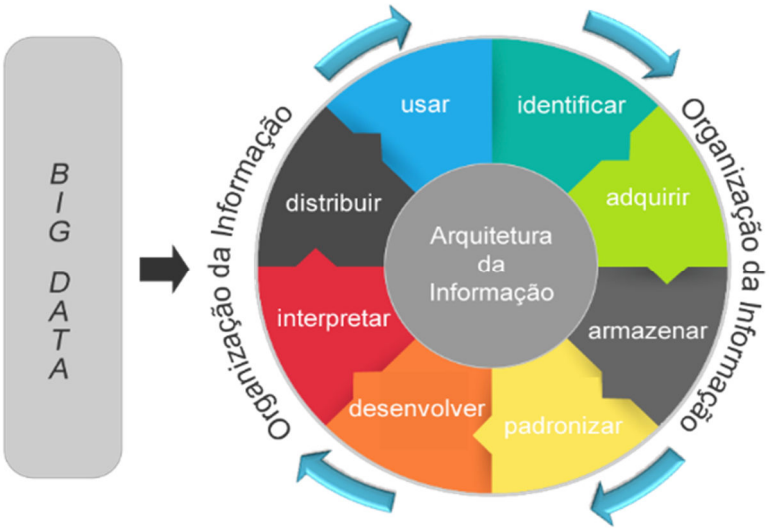
As ameaças continuam a crescer e representam riscos à privacidade e à SI nos ambientes informacionais digitais, que disponibilizam informações a partir dos avanços tecnológicos (GRISOTO *et al*., 2015).

Ao discorrer sobre as questões relativas às necessidades de identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar a informação, no contexto do *Big Data*, esta pesquisa insere-se na temática da AI.

Conforme a definição de Bailey (2003), a AI é a arte e a ciência de estruturar e organizar sistemas de informação com vistas a ajudar os usuários a alcançarem seus objetivos.

A Figura 4 apresenta os mecanismos da AI.

Figura 4 - Mecanismos da Arquitetura da Informação



Fonte: O autor

A avaliação da adequação desses mecanismos pode ser realizada por meio de um modelo de maturidade, que fornecerá um ponto de referência para as instituições de ensino, de pesquisa e de fomento entenderem o nível de maturidade de suas práticas, processos e métodos para, então, definir metas e prioridades de melhoria para mitigar os impactos sociais dos riscos à privacidade e à SI.

Um Modelo de Maturidade da AI se faz necessário para as instituições conhecerem o estado atual dos mecanismos utilizados para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar a informação no ambiente do *Big Data*. O modelo permitirá, ainda, que as organizações avaliem os seus mecanismos com recomendações sobre como conduzir as melhorias necessárias.

O Modelo de Maturidade da AI apoiará na prevenção dos seguintes problemas:

- Falta de conformidade com leis, regulamentos e normas aplicadas à privacidade e à SI dos dados pessoais e das publicações científicas;
- Falta de confidencialidade de informações científicas restritas;
- Falta de integridade das informações científicas coletadas;
- Falta de organização das informações nos repositórios acadêmicos;
- Falta da privacidade das informações pessoais e científicas;
- Perda financeira pelo impacto decorrente da divulgação de informações pessoais e científicas não autorizadas e desorganizadas; e
- Ações de engenharia social no espaço cibernético.

A análise dos modelos de comportamento informacional e uso da informação existentes na literatura apresenta a falta de um arcabouço de maturidade da AI. Nos anos 80 e 90, surgiram modelos ou padrões de comportamento que tratavam apenas da busca e uso da informação, tais como os de Wilson (1981), Dervin (1983) e Ellis (1989) (TABOSA; PINTO, 2015).

A pesquisa proposta fundamenta-se na hipótese de que conhecer e compreender o nível de maturidade da AI nas instituições de ensino, de pesquisa e de fomento, inseridas no ambiente do *Big Data* e na forma como as mesmas gerenciam as informações, contribuirá para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a organização e SI, com a perda de valor das informações, bem como o alinhamento com a LGPD.

1.1.3 Pergunta de pesquisa

As instituições estão passando por transformações na forma de lidar com as informações. O avanço das TIC tem permitido o armazenamento de grandes e múltiplas bases de dados, que contém tanto informações pessoais quanto corporativas.

De acordo com Earp *et al*. (2005), a privacidade das informações tem sido reconhecida como uma importante questão de gestão que vêm crescendo em decorrência do valor da informação para a tomada de decisão das instituições, com o avanço tecnológico. Os autores relatam que o avanço tecnológico cria oportunidades para obter grandes quantidades de informações pessoais e corporativas sobre usuários e organizações e, com isso, violar a privacidade e a SI.

Com o grande volume de informações disponíveis, torna-se necessário enfrentar o caos informacional com a utilização da AI. Nesse contexto, dado o significativo impacto dessas consequências nas instituições de ensino, de pesquisa e de fomento, surge a pergunta: conhecer o estado atual da AI nessas instituições, por meio de um modelo de maturidade poderá apoiar na mitigação dos impactos sociais dos riscos à privacidade, à segurança, à organização e a perda de valor das informações?

1.2 OBJETIVOS

1.2.1 Objetivo geral

O objetivo geral deste estudo é propor um Modelo de Maturidade da Arquitetura da Informação para o aprimoramento do gerenciamento das informações das instituições no *Big Data,* visando mitigar os impactos sociais dos riscos à privacidade, à organização, à segurança,

e perda de valor das informações disponibilizadas pelas instituições de ensino, de pesquisa e de fomento.

1.2.2 Objetivos específicos

- Analisar os impactos sociais do *Big Data* na privacidade, organização, segurança e perda de valor das informações, bem como o alinhamento com a LGPD;
- Identificar o grau de importância da privacidade, da organização, da segurança e do valor das informações para os usuários e as instituições; e
- Definir os domínios, objetivos e práticas para o Modelo de Maturidade da AI proposto, visando identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar a informação no ambiente do *Big Data*.

1.3 REFERENCIAL TEÓRICO

O referencial teórico visa apresentar o suporte necessário para embasar esta pesquisa. Sendo assim, serão abordados a seguir os fundamentos teóricos para o entendimento deste estudo.

1.3.1 Modelos de maturidade

Os modelos de maturidade são baseados na melhoria dos processos, funcionam como um guia para a instituição conhecer o seu estado atual e promover um plano de melhoria.

Segundo Chapin e Akidge (2005), os modelos de maturidade são baseados na melhoria dos processos e na existência de fundamentos para guiar e medir a implementação e a melhoria dos processos.

Para Becker *et al*. (2009), tipicamente um modelo de maturidade tem dois componentes: i) meio de medir e descrever o desenvolvimento de um objeto, mostrando uma progressão hierárquica; e ii) critérios para medir os processos. Esses componentes fornecem uma sucessão de níveis de maturidade para uma classe de objetos.

A importância da aplicação dos modelos de maturidade destacada por Kerzner (2006), refere-se à descoberta de oportunidades de melhoria no gerenciamento de projetos, identificação das mudanças necessárias para a melhoria da maturidade e orientação para o desenvolvimento de um plano de capacitação.

Os modelos de maturidade são organizados em níveis sequenciais de crescimento da maturidade dos processos organizacionais. Os níveis são utilizados para medir a competência

organizacional ou maturidade de um conjunto reconhecido das melhores práticas. As métricas são organizadas em categorias e quantificadas em uma escala de desempenho (ADLER, 2013).

Na sequência são apresentadas a descrição de um conjunto de modelos de maturidade de processos de tecnologia da informação (TI) utilizados como base para o modelo proposto.

1.3.1.1 *Capability maturity model* (CMM)

O CMM é uma marca registrada do *Software Engineering Institute* (SEI) com sede na Universidade *Carnegie Mellon*, em *Pittsburgh*, nos EUA.

O modelo foi desenvolvido nos anos 80, para avaliação de risco na contratação de empresas de *software* pela Força Aérea norte-americana, para avaliar os processos de desenvolvimento utilizados pelas empresas participantes das licitações, referentes a custos, qualidade e prazos nos projetos contratados.

Apesar da aplicação do CMM ter iniciado no ambiente das grandes empresas fornecedoras de soluções tecnológicas para as Forças Armadas dos EUA para projetos militares, os seus princípios são aplicáveis a todo tipo de projeto de *software*. O CMM é utilizado por empresas de diversos setores, tais como: pequenas empresas de desenvolvimento de *software*, fabricantes de *hardware*, empresas de telecomunicações, empresas de consultoria, grandes bancos e seguradoras.

O CMM é um modelo para avaliação da maturidade dos processos de *software* de uma organização. Tem como objetivo a melhoria dos processos de *software* utilizados pelas organizações de desenvolvimento e manutenção de sistemas, para minimizar os erros das organizações em relação ao desenvolvimento, planejamento e aperfeiçoamento dos sistemas informatizados.

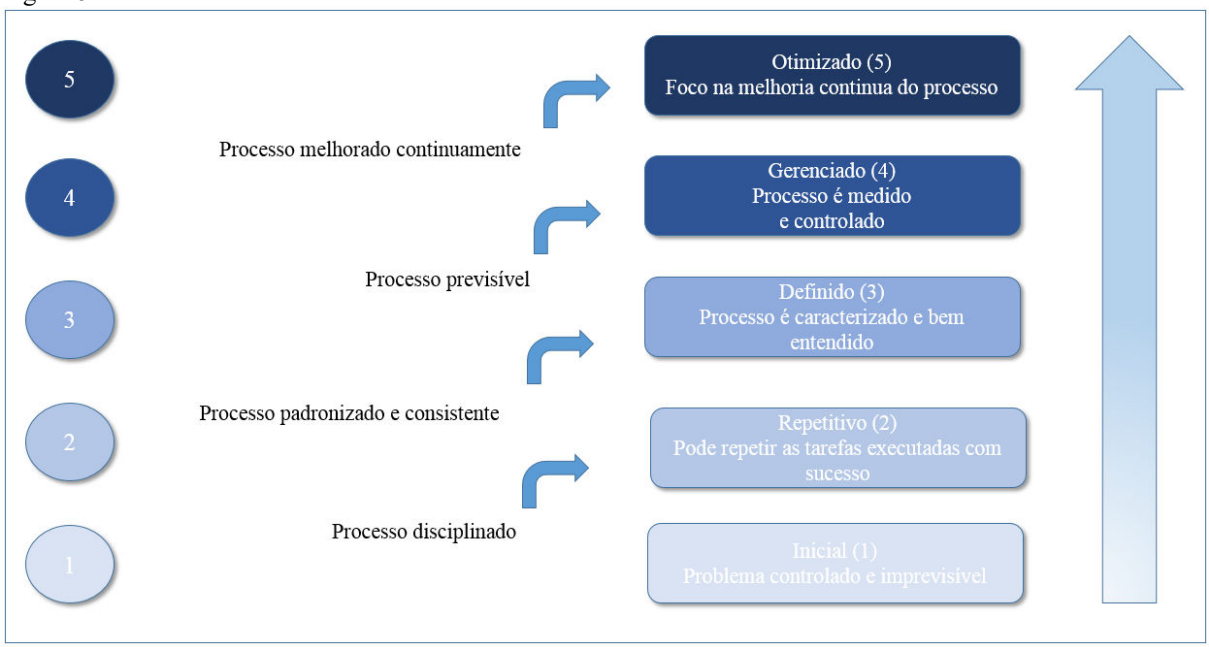
Esse modelo está organizado em 5 (cinco) níveis crescentes de maturidade. Os níveis de maturidade são definidos em áreas-chave de um processo de *software*. As áreas são detalhadas em práticas que devem ser cumpridas na implantação do modelo. As práticas descrevem o que deve ser realizado, exigindo documentos, treinamentos e políticas definidas para as atividades.

As práticas não mencionam o modo como devem ser implementadas. As áreas possuem um conjunto de metas, que se realizadas, possibilitam aumentar a capacitação do processo em criar resultados planejados, garantindo a qualidade.

O CMM direciona o caminho da melhoria contínua para um processo com um nível de maturidade definido. Os níveis são uma forma de priorizar as ações de melhoria.

A Figura 5 apresenta os níveis de maturidade do modelo CMM.

Figura 5 – Níveis de maturidade do modelo CMM



Fonte: O autor

Segundo Royce (2002), o modelo inicial do CMM foi desenvolvido pelo SEI, sendo especificamente destinado à maturidade do processo de *software*. No entanto, com a sua implementação em diferentes domínios, outros modelos no formato CMM foram desenvolvidos para disciplinas e funções particulares como engenharia de sistemas, pessoas, desenvolvimento de produto integrado, aquisição de *software*, entre outros.

Os modelos que fazem parte do CMM são: *Capability Maturity Model Integration* (CMMI), *Capability Maturity Model for Software* (SW-CMM), *People Maturity Model* (P-CMM), *Software Acquisiton Capability Maturity Model* (SA-CMM), *System Enginnering Capability Maturity Model* (SE-CMM), *Integrated Product Development Capability Maturity Model* (IPD-CMM).

1.3.1.2 *Capability maturity model integration* (CMMI)

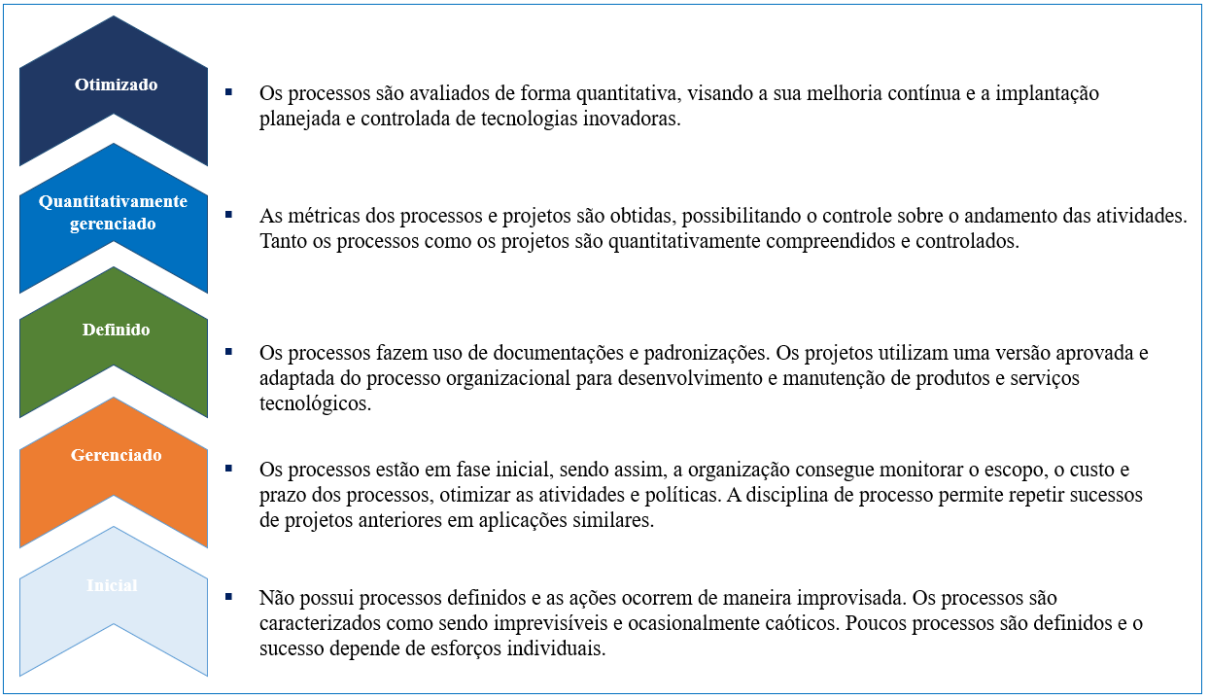
É um modelo evolutivo do CMM, criado pelo SEI, para integrar estruturas de processos de melhorias demandadas pelas organizações. O CMMI estabelece a diferença entre os conceitos de organização e empresa, a valorização, validação e evolução dos processos de verificação. (*U.S. DEPARTMENT OF DEFENSE – The Software Engineering Institute*, 2002).

O modelo está dividido em 5 (cinco) níveis, inicial, gerenciado, definido, quantitativamente gerenciado e otimizado. Os níveis fazem parte das áreas de processos, que possuem um conjunto de metas específicas e/ou genéricas. Entre as suas características destaca-

se o comprometimento com a execução, direcionamento e verificação da implementação das metas estabelecidas.

A Figura 6 apresenta os níveis de maturidade do modelo CMMI.

Figura 6 – Níveis de maturidade do modelo CMMI



Fonte: O autor

1.3.1.3 *Cybersecurity capability maturity model* (C2M2)

O C2M2 (2014) pode ajudar as organizações de todos os setores, tipos e tamanhos a avaliar e fazer melhorias em seus programas de SegCiber. O foco desse modelo está na implementação e gestão de práticas de SegCiber associadas aos ativos de TI, operações de tecnologia e o seu ambiente de operação. Pode ser usado para:

- Fortalecer as capacidades de SegCiber das organizações;
- Permitir que as organizações avaliem de forma eficaz e consistente o estado atual da SegCiber;
- Compartilhar conhecimento, melhores práticas e referências de SegCiber entre as organizações; e
- Permitir que as organizações priorizem as ações e investimentos para melhorar a SegCiber.

O modelo foi desenvolvido para uso de uma metodologia de autoavaliação nas organizações, visando a melhoria do seu programa de SegCiber. Destina-se a uma autoavaliação consistente das suas capacidades de SegCiber para identificação dos seus níveis de maturidade.

O C2M2 fornece uma orientação descritiva e não prescritiva. A autoavaliação concede informações para:

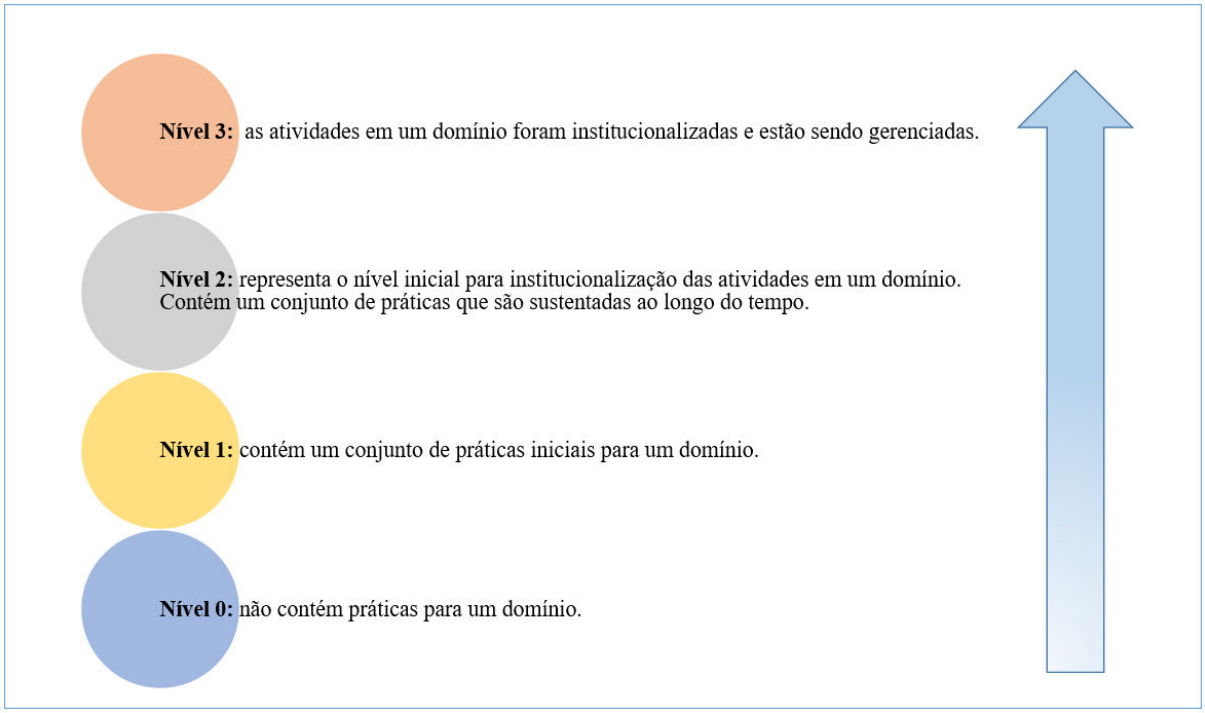
- Os gestores responsáveis pela tomada de decisão;
- Os responsáveis pela gestão de recursos e operações organizacionais;
- Os responsáveis pela aplicação da autoavaliação; e
- Os facilitadores da aplicação da autoavaliação.

Um modelo de maturidade é um conjunto de características, atributos, indicadores ou padrões de capacidade e progressão de uma determinada disciplina. Para medir a progressão, os modelos de maturidade têm tipicamente níveis de maturidade em uma escala numérica. O C2M2 usa uma escala de 0 a 3, que permite a organização definir o seu estado atual de SegCiber, determinar o seu futuro e identificar os recursos necessários para alcançar esse estado futuro.

Os níveis de maturidade são aplicados de forma independente dentro de cada domínio. Como resultado uma organização pode estar em níveis de classificação diferentes para os domínios. Em um domínio, a organização pode estar no nível 1, em outro no nível 3, por exemplo.

A Figura 7 apresenta os 4 (quatro) níveis de maturidade do modelo C2M2.

Figura 7 – Níveis de maturidade do modelo C2M2



Fonte: O autor

O modelo surge de uma combinação de padrões, estruturas, programas e iniciativas de SegCiber. Fornece uma orientação flexível para ajudar as organizações a desenvolver e

melhorar suas capacidades de segurança. As práticas, definidas no modelo podem ser interpretadas por organizações de vários tipos e tamanhos. O modelo está organizado em 10 (dez) domínios, com as práticas agrupadas por objetivo.

As práticas estão organizadas em objetivos, e representam as atividades que uma organização pode realizar para desenvolver e estabelecer a sua maturidade em um domínio.

O Quadro 2 apresenta os domínios e objetivos do modelo.

Quadro 2 – Domínios e objetivos – C2M2

Domínios	**Objetivos**
Gestão de risco	i) estabelecer a estratégia de gestão risco de SegCiber ii) gerenciar o risco cibernético iii) gestão das atividades
Gestão de ativos, mudanças e configurações	i) gerenciar o inventário de ativos ii) gerenciar a configuração de ativos iii) gerenciar as alterações de ativos iv) atividades de gestão
Gestão de identidade e acesso	i) estabelecer e manter identidades ii) controlar o acesso iii) atividades de gestão
Gestão de ameaças e vulnerabilidades	i) identificar e responder as ameaças ii) reduzir as vulnerabilidades de SegCiber iii) atividades de gestão
Consciência situacional	i) realizar registro de *log's* ii) realizar monitoramento iii) estabelecer e manter uma estrutura operacional iv) atividades de gestão
Compartilhamento de informações e comunicações	i) compartilhar informações de SegCiber ii) atividades de gestão
Resposta a eventos, incidentes e continuidade de operações	i) detectar eventos de SegCiber ii) escalar eventos de SegCiber e declarar incidentes iii) responder a incidentes e eventos escalados de SegCiber iv) plano de continuidade v) atividades de gestão
Cadeia de suprimentos e gerenciamento de dependências externas	i) identificar dependências ii) gerenciar o risco da dependência iii) atividades de gestão
Gerenciamento da força de trabalho	i) atribuir responsabilidades de SegCiber ii) controlar o ciclo de vida da força de trabalho iii) desenvolver a força de trabalho de SegCiber iv) aumentar a conscientização da SegCiber v) atividades de gestão
Gestão do programa de SegCiber	i) estabelecer a estratégia do programa de SegCiber ii) patrocinar o programa de SegCiber iii) estabelecer e manter a arquitetura de SegCiber iv) desenvolvimento de *software* seguro v) atividades de gestão

Fonte: O autor

Os objetivos e práticas específicas dos domínios descrevem a progressão da abordagem de SegCiber para cada domínio do modelo. O relatório da autoavaliação identifica as lacunas no desempenho nas práticas do modelo. A etapa inicial da análise dos resultados é determinar se é importante para a organização tratar essas lacunas. Após a análise das lacunas, a

organização deve priorizar as ações necessárias para implementar as práticas que não foram atendidas na primeira avaliação, para com isso, alcançar um nível de maturidade mais elevado para cada domínio.

1.3.1.4 *National Institute of Standars and Technology Cybersecurity Framework* (NISTCyberSecurity)

O modelo foi desenvolvido em resposta a uma ordem do Presidente dos Estados Unidos da América, Barack Obama, em fevereiro de 2013, para reforçar a resiliência da infraestrutura crítica da Nação, e manter um ambiente cibernético que encorajasse a eficiência, inovação e prosperidade econômica (THE PRESIDENT, 2013).

O *National Institute of Standars and Technology Cybersecurity Framework* (2014) permite que as organizações, independentemente do tamanho, do grau de risco da SegCiber ou sofisticação na área, apliquem os princípios e as melhores práticas de gestão de risco para aprimorar a SegCiber e a resiliência das infraestruturas críticas. O modelo fornece uma estrutura de diretrizes e práticas atualizadas para reduzir e melhor gerenciar os riscos de SegCiber.

O *framework*, desenvolvido pelo *National Institute of Standars and Technology* (NIST), tem 5 (cinco) funções que podem ser realizadas simultaneamente e continuamente para formar uma cultura operacional que aborda o risco dinâmico de SegCiber. As funções e seus objetivos são:

- Identificar: desenvolver a compreensão organizacional para gerenciar o risco de sistemas, ativos, dados e recursos;
- Proteger: desenvolver e implementar as salvaguardas adequadas para assegurar os serviços de infraestrutura crítica;
- Detectar: desenvolver e implementar as atividades apropriadas para identificar a ocorrência de eventos de SegCiber;
- Responder: desenvolver e implementar as atividades apropriadas para tomar medidas relativas a eventos de SegCiber detectados; e
- Recuperar: desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido aos eventos de SegCiber.

Os 4 (quatro) níveis utilizados nesse modelo são:

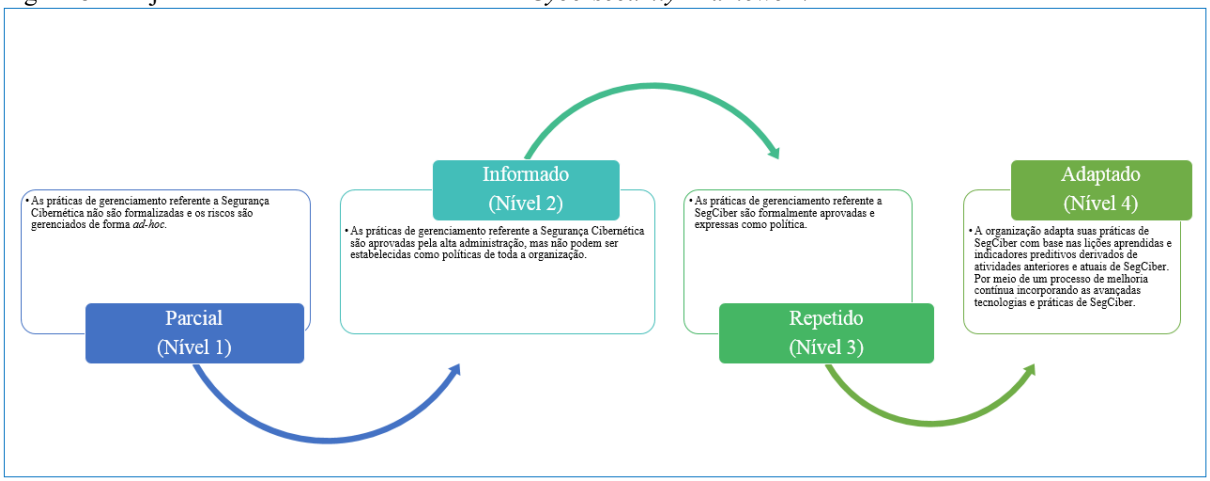
- Parcial;
- Informado;

- Repetido; e
- Adaptado.

Esses níveis descrevem um grau crescente de rigor e sofisticação nas práticas de risco de SegCiber e a sua integração com o risco global da organização e as suas necessidades para o negócio.

Os objetivos dos níveis estão apresentados na Figura 8.

Figura 8 – Objetivos dos níveis do modelo NIST *Cybersecurity Framework*



Fonte: O autor

O modelo apresenta os processos de gerenciamento de risco, programa integrado de gerenciamento de riscos e participação externa, com a seguinte descrição:

- Gerenciamento de risco: processo contínuo de identificação, avaliação e resposta ao risco. Para gerir os riscos, as organizações devem compreender a probabilidade de que um evento ocorra e o seu impacto resultante. Com as informações sobre a probabilidade e o impacto, as organizações tem como determinar o nível aceitável de risco e a tolerância ao risco estabelecida pela organização;
- Programa integrado de gerenciamento de risco: processo de conscientização do risco de SegCiber no nível organizacional com uma abordagem de toda a organização para gerenciar o risco de SegCiber, que permite que as informações de segurança sejam compartilhadas dentro da organização; e
- Participação externa: processo de integração com as organizações do ambiente de atuação, compartilhamento das informações com parceiros para assegurar que informações atuais e precisas são utilizadas para melhorar a SegCiber.

1.3.1.5 *The community cyber security maturity model* (CCSMM)

O CCSMM, proposto por White (2007), fornece uma estrutura que as comunidades e os estados podem usar para determinar seu nível de preparação para criar um plano para melhorar sua postura de SegCiber.

Esse modelo é resultado da necessidade de uma melhoria na definição dos métodos para determinar o estado atual de uma comunidade em sua preparação para o ambiente cibernético.

Com o objetivo de abordar as questões que uma comunidade enfrenta em relação a SegCiber, o autor propõe os seguintes elementos:

- Enfrentar as ameaças;
- Definir métricas;
- Compartilhar informações;
- Usar tecnologias;
- Realizar treinamentos; e
- Realizar testes.

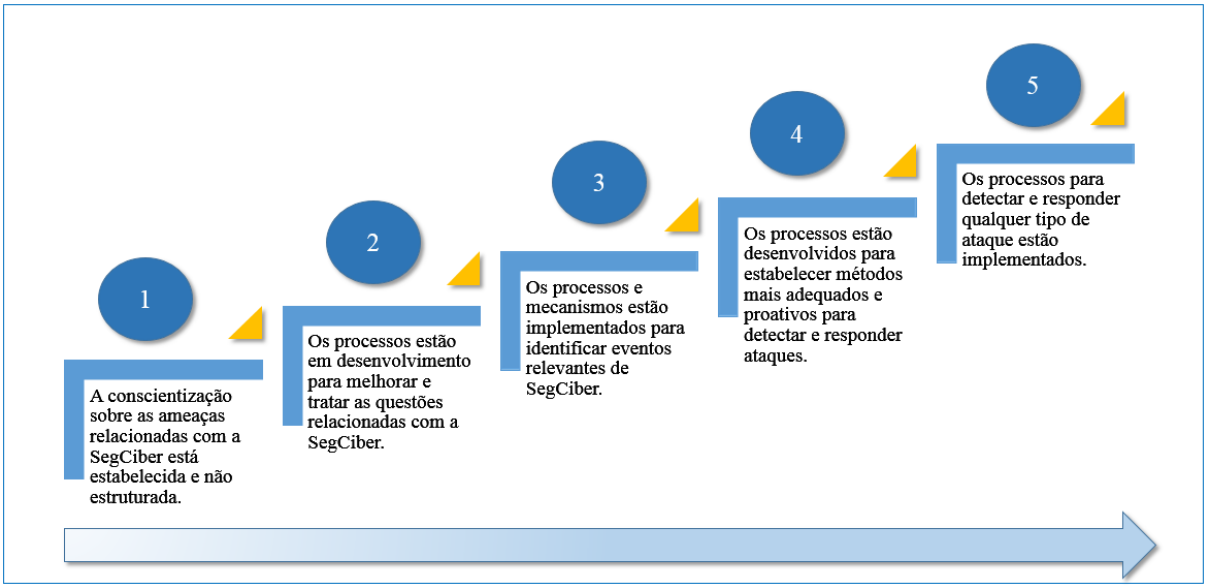
O modelo apresenta 3 (três) tipos de categorias de ataques:

- Ataques não estruturados: são realizados por empregados descontentes, por exemplo;
- Ataques estruturados: são planejados e metódicos para comprometer ou interromper informações ou sistemas para obter vantagens; e
- Ataques altamente estruturados: são multidisciplinares para comprometer, interromper ou destruir informações ou sistemas como parte do esforço coordenado para obter vantagens. Nessa categoria os atacantes são altamente organizados.

O CCSMM reconhece a necessidade que as organizações tenham métricas e tecnologias para desenvolver um programa de SegCiber, como também exercitar testes da capacidade de segurança, implementar atividades de treinamento e compartilhamento das informações relacionadas com a SegCiber (WHITE, 2007).

O modelo usa uma escala de 5 (cinco) níveis. A Figura 9 apresenta a descrição dos níveis do modelo.

Figura 9 – Níveis de maturidade do modelo CCSMM



Fonte: O autor

1.3.2 Ciência da informação

A informação tem se mostrado, atualmente, um ativo de valor e estratégico para as organizações, talvez, o mais precioso devido à sua importância para os negócios. Sendo assim, a CI, que tem foco nas questões de criação, gestão, disseminação, recuperação e uso das informações, apresenta elementos para organizar, estruturar e localizar a informação.

Para Borko (1968), a CI é a disciplina que pesquisa as propriedades e comportamento da informação, as forças que governam o seu fluxo e os meios de processá-la para otimizar sua acessibilidade e uso.

Os conceitos da CI, na década de 60, apresentaram o escopo voltado para a produção, a organização, o armazenamento, a disseminação e o uso da informação. A CI, desde sua concepção, promove uma reflexão afeita à informação. Com o advento das tecnologias, estuda a mediação entre a informação e a criação do conhecimento para o indivíduo (BARRETO, 2000).

A CI, uma ciência, portanto, bastante recente, buscou a partir do seu início constituir-se como uma ciência social e, nesse movimento de aproximação, as ciências sociais e a CI tiveram uma maior identidade, nos conceitos, teorias e metodologias de pesquisa (ARAÚJO, 2004).

Segundo Pinheiro (2005), a CI, como ciência social que é, apresenta singularidades próprias de seu objeto de estudo, por si só, de acentuado grau de abstração e complexidade e pela subjetividade que perpassa o ciclo de transferência da informação.

A CI tem características de interdisciplinaridade, podendo ser considerada uma ciência pura quando investiga seu objeto sem considerar sua aplicação ou ciência aplicada, quando desenvolve serviços e produtos (BORKO, 1968).

Outros autores, como Wersig e Nevelling (1975), afirmam que transmitir o conhecimento para aqueles que dele necessitam é uma responsabilidade social, e essa responsabilidade social parece ser o verdadeiro fundamento da CI.

1.3.2.1 Sociedade da Informação

Segundo Miranda (2000), um dos principais indicadores do desenvolvimento da sociedade da informação é a presença das tecnologias de informação no dia a dia das pessoas, instituições e funcionamento e transformação da sociedade como um todo. Para o autor, na sociedade da informação, a comunicação e a informação tendem a permear as atividades e os processos de tomada de decisão nas diferentes esferas da sociedade.

O avanço tecnológico tem sido um instrumento essencial para o desenvolvimento social, político e econômico dos países. Para Takahashi (2000), o caminho à sociedade da informação é repleto de desafios em todos os países. No entanto, em cada um, o desafio aponta uma combinação de oportunidades e riscos.

Com o avanço tecnológico emergem os riscos relacionados com a privacidade e SI. Utilizar as tecnologias demandam conhecimentos para lidar tanto com as vantagens e desvantagens das ferramentas tecnológicas.

Para Takahashi (2000), educar em uma sociedade da informação significa muito mais que treinar pessoas para o uso das TIC: busca investir na criação de amplas competências que permita que seus integrantes tenham uma atuação afetiva na produção de bens e serviços, para tomar decisões fundamentadas no conhecimento, operar com fluência os novos meios e ferramentas em seu trabalho, bem como aplicar criativamente as novas mídias, seja em usos simples e rotineiros ou em sistemas complexos.

A interconectividade da sociedade por meio dos computadores, presente na sociedade da informação, tem gerado um grande volume de dados produzindo informação e criando conhecimento.

Para Gandelman (2007), a informação e o conhecimento criados pelas novas tecnologias estão acarretando mudanças relevantes na sociedade, com consequências nas relações sociais, econômicas e culturais.

Uma nova era social, econômica e cultural tem sido moldada pela conectividade no ambiente virtual, possibilitando a expansão das fronteiras físicas, alcançado o mercado global com o fluxo da informação, tornando a organização e proteção da informação um requisito básico para os novos modelos de negócios e relações sociais e culturais.

Essa nova era pode ser denominada de Era da Informação segundo Simões (2009); Sociedade do Conhecimento por Hargreaves (2003), na sua obra "O Ensino na Sociedade do Conhecimento – a educação na era da insegurança", Sociedade da Comunicação conforme Ascensão (2002). Já Lévy (2010) utiliza a expressão Cibercultura, na sua obra de mesmo nome, na qual o autor aborda suas percepções sobre o crescimento do ciberespaço e a interconexão de computadores. E o autor, Castells (2005), utiliza o termo Sociedade em Rede, como uma estrutura social baseada em redes operadas por TIC.

1.3.3 Arquitetura da informação

Com base na importância para a organização e apresentação da informação, Richard Saul Wurman, utilizou pela primeira vez o termo AI, em 1976. O criador do termo, afirma que o arquiteto da informação dá clareza ao que é complexo, fazendo com que a informação possa ser compreendida (WURMAN, 2005).

Para Rosenfeld e Morville (2006), a AI pode ser representada pela convergência entre usuários, conteúdos e contextos que se relacionam de maneira independente. Os autores mencionam que a AI é composta por 4 (quatro) componentes elementares: i) os sistemas de organização; ii) sistemas de rotulagem; iii) sistemas de busca; e iv) os sistemas de navegação.

Já McGee e Prusak (1994), destacam que a AI define qual informação é mais importante para a organização. Davenport (1998) define AI como um guia para estruturar e localizar a informação dentro de uma organização.

A AI deve conter mecanismos para obtenção e utilização de recursos tecnológicos, financeiros, humanos, materiais e físicos para o gerenciamento da informação e, com isso, a informação torna-se um insumo estratégico para indivíduos e organizações (DOS SANTOS, 2013).

Segundo Lima-Marques e Macedo (2006), a AI permite a organização da informação para suporte às ações de gestão do conhecimento, à medida que visa promover a acessibilidade à informação para a tomada de decisões.

A informação é um recurso valorizado no nível operacional, tático e estratégico para a tomada de decisões, para o desenvolvimento de competências e para a execução das atividades humanas. As tecnologias da informação contribuem para a transmissão da informação e para a criação de ambientes propícios para a construção do conhecimento.

Diante do volume de dados disponível, que pode ser utilizado para a tomada de decisões e melhoria da qualidade de vida, os usuários estão dispostos a trocarem informações por serviços melhores, sem a devida atenção sobre as condições de privacidade oferecidas por esses serviços.

Com a frequente evolução de novas ferramentas tecnológicas, a cada dia, o usuário passa a ter mais e mais informação. A informação gerada de forma excessiva, sem critérios de seleção, organização e disseminação fez surgir, como define Reis (2007), a síndrome da fadiga da informação, caracterizada pela tensão, irritabilidade e sentimento de abandono causado pela sobrecarga de informação imposta ao ser humano.

Wurman (1991), afirma que uma edição do *The New York Times* em um dia publica mais informações do que um cidadão inglês normal poderia receber durante toda a sua vida no século XVII.

Toda essa quantidade de informações, para Wurman (1991), leva à síndrome de ansiedade da informação, que o autor define como o resultado da distância cada vez maior entre o que compreendemos e o que achamos que deveríamos compreender.

O desenvolvimento e aperfeiçoamento das tecnologias da informação encurtam o caminho do usuário tanto para obter como para fornecer informações. Todo esse avanço tem as suas vantagens, como também as suas desvantagens, sobretudo no que se refere à privacidade, à segurança, ao valor e à confiabilidade das informações.

Atualmente, novos produtos especializados para assegurar a SegCiber são desenvolvidos, implantados e atualizados frequentemente para o melhor desempenho dos sistemas no espaço cibernético.

Entretanto, tais medidas não garantem total segurança uma vez que o fator humano é suscetível a falhas. Para Furnell e Thompson (2009), os usuários são um dos problemas e uma das ameaças relatadas na implementação de práticas e procedimentos de segurança.

A AI pode ser usada como uma estratégia para a organização da grande massa de informações disponível, para mitigar os riscos relacionados com a privacidade, a organização,

a segurança, a confiabilidade e a perda de valor das informações. Com o grande volume de informações publicadas no espaço cibernético, a utilização da AI é um requisito para enfrentar o caos informacional na era da informação.

1.3.3.1 Caos informacional

O fluxo das informações por meio de novas formas de acesso e produção de conteúdo, produz diariamente uma grande quantidade de informações, de forma que as pessoas e instituições parecem não ter condições de interpretar, refletir e usar a carga informacional disponibilizada.

Ao fato da explosão informacional, que eleva o volume de informações a um nível mais complexo de interpretação, soma-se uma combinação de informações verdadeiras e informações resultantes de dados falsos, por vezes divulgadas de forma intencional.

A velocidade de transmissão das mensagens, tem possibilitado o consumo e disseminação de informações falsas, distorcidas, manipuladas, popularmente conhecidas como *fakenews*, servindo às mais variadas utilidades pessoais e institucionais.

Para os autores, Aragão e Vilicic (2016), o número de interações nas redes sociais com as notícias falsas excedeu o de interações com as notícias que, de fato, eram verdadeiras. As redes sociais potencializaram a disseminação da criatividade de comunicação da sociedade.

O caos informacional característico do ciberespaço, segundo Lévy (2010), é um espaço aberto para a prática de toda a sorte de atos ilícitos e disseminação de *fakenews*. Diante desse cenário, implementar ações de SI poderá mitigar os riscos decorrentes da disseminação de informações falsas, distorcidas e manipuladas.

1.3.4 Segurança da informação

A definição do termo SI pode ser encontrada na norma ABNT NBR ISO/IEC 27002:2013 que diz: a SI é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos.

Entre os decretos, normas e regulamentos publicados pela APF que são aplicados à SI, estão o Decreto nº. 9.637/2018 (BRASIL, 2018) e o Decreto nº. 7.485/2012 (BRASIL, 2012), que tratam das questões de proteção, sigilo e classificação das informações.

O Decreto nº 9.637/2018 (BRASIL, 2018), institui uma política de SI nos órgãos e entidades da APF, definindo os seguintes requisitos básicos para uma política de SI: i) assegurar o sigilo da correspondência e das comunicações, nos termos previstos na Constituição; ii)

proteger os assuntos que mereçam tratamento especial; iii) prover mecanismos de SI, a partir de tecnologias e processos; iv) criar, desenvolver e manter uma cultura de SI; e v) prover capacitação científico-tecnológica para uso de criptografia na segurança e defesa do Estado.

O Decreto nº 7.845/2012 (BRASIL, 2012), regulamenta os procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito da APF, que dispõe sobre o Núcleo de Segurança e Credenciamento. A seção VII do Capítulo III, Art. 38, que trata dos Sistemas de Informação, estabelece que no tratamento da informação classificada, devam ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pela APF, para assegurar a autenticidade, sigilo, controle e registro de acesso, uso de recursos criptográficos e de segurança para a proteção da informação.

A Instrução Normativa (IN) nº 1 do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) (BRASIL, 2008), define SI como ações que objetivam viabilizar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Para a *Information Systems Audit and Control Association* (ISACA, 2012), a SI deve proteger as informações contra divulgação não autorizada, alterações em seu estado original e manter a disponibilidade das informações quando for solicitada, com isso, assegurar a confidencialidade, integridade e disponibilidade.

No glossário das Forças Armadas Brasileiras (BRASIL, 2007) a SI é definida da seguinte forma:

> "[...]
>
> Conjunto de conceitos, técnicas e atividades que visem a proporcionar confidencialidade, integridade e disponibilidade às informações, protegendo recursos de informação contra ações deliberadas ou não-autorizadas de aquisição, dano, manipulação, modificação, perda, revelação ou uso desses recursos.
>
> [...]"

Os conceitos de SI apresentados direcionam o seu foco para a proteção da informação de uma forma global, já que a informação é um ativo essencial para os negócios da organização e deve ser protegida (ABNT ISO/IEC 27002:2013).

Segundo Killmeyer (2006), para assegurar a eficácia da gestão da segurança, a SI baseia-se nos seguintes atributos:

- Confidencialidade: proteção das informações contra acesso não autorizado, independente da forma como ela é armazenada ou local de armazenamento;

- Integridade: é a proteção de informações, aplicações, sistemas e redes contra mudanças intencionais, não autorizadas ou acidentais; e
- Disponibilidade: é a garantia de que as informações e os recursos estão acessíveis pelos usuários autorizados conforme a necessidade.

1.3.5 Segurança cibernética

A Estratégia de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética da APF (BRASIL, 2015), define a SegCiber como a arte de assegurar a existência da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas.

Para a norma ABNT NBR ISO/IEC 27032:2015, as práticas básicas de segurança para as partes interessadas no espaço cibernético fornecem as diretrizes para melhorar o estado de SegCiber, determinando os aspectos comuns dessa atividade e suas ramificações em outros domínios de segurança, tais como: as redes computadores e a proteção de infraestruturas críticas de informação (ABNT, 2015).

Segundo a Estratégia de SIC e de SegCiber, os ativos de informação são os meios de armazenamento, transmissão e processamento dos sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Já as infraestruturas críticas, para Mandarino Júnior (2010), são as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político à segurança do Estado e da sociedade.

Em maio de 2000, o então Presidente da França, Jacques Chirac, durante uma palestra sobre crimes cibernéticos, citou que:

> "[...]
>
> Alguns qualificam o espaço cibernético como um novo mundo, um mundo virtual, mas podemos nos equivocar. Não há dois mundos diferentes, um real e outro virtual, mas apenas um, no qual se devem aplicar e respeitar os mesmos valores de liberdade, igualdade e dignidade da pessoa.[5]"
>
> [...]"

Segundo Carvalho (2010), o espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas e/ou organizacionais, constituindo novo território, por vezes conhecido e desconhecido, a ser desbravado pelos bandeirantes do século XXI.

[5] http://egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf

Para Mandarino Júnior (2010), na medida em que a sociedade da informação vai se estabelecendo em um país, começa um processo de construção de uma verdadeira nação virtual que o autor denomina como espaço cibernético. Para o autor, o conjunto de pessoas, empresas, equipamentos e suas interconexões, dos sistemas de informação e das informações que por eles trafegam também pode ser denominado espaço cibernético. Todo esse espaço cibernético faz uso de uma infraestrutura crítica de informações.

O GSI/PR na Norma Complementar nº 10 da IN nº 1, de 2012, no uso de suas atribuições, define como infraestruturas críticas os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

Para a Secretaria de Assuntos Estratégicos da Presidência da República (BRASIL, 2011), com o aparecimento da sociedade da informação, em que as tecnologias têm papel preponderante nas infraestruturas de uma nação e na interação entre elas, constata-se que as infraestruturas de informação são consideradas críticas porque não podem parar, para evitar descontinuidade no uso das informações por parte da sociedade. Os sistemas de gestão e controle de infraestruturas críticas, sistemas do mercado financeiro e controle militar estão cada vez mais sofisticados demandando o uso dos ativos do espaço cibernético.

A falta de práticas, processos e métodos para assegurar a proteção do espaço cibernético, seus ativos e suas infraestruturas críticas podem impactar a segurança do Estado e da sociedade, mudando a percepção da SegCiber no mundo, direcionando a uma reflexão de como estão evoluindo as atividades de guerra cibernética no século XXI.

O relatório publicado pelo Centro de Estudos Estratégicos e Internacionais (CEEI) dos EUA para a 44ª. Presidência, estabelece que a SegCiber é um grande problema nacional para o Governo e que uma compreensão estratégica do que é SegCiber tornará o País mais seguro (BARROS, GOMES E FREITAS, 2011).

Não é simples determinar o que deve ser protegido, contra quem e com que meios. O pensamento tradicional da segurança e defesa muitas vezes pode resultar na SegCiber sendo entendida como algo em que a intrusão vem de fora, que é feito por eles contra nós (BRASIL, 2011).

A Secretaria de Assuntos Estratégicos da Presidência da República (BRASIL, 2011), define que a SegCiber visa a proteção e garantia da utilização de ativos de informação

estratégicos, principalmente ligados às infraestruturas críticas de informação (redes de comunicação e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Já o Ministério da Defesa estabelece que a Defesa Cibernética é um conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação (BRASIL, 2010).

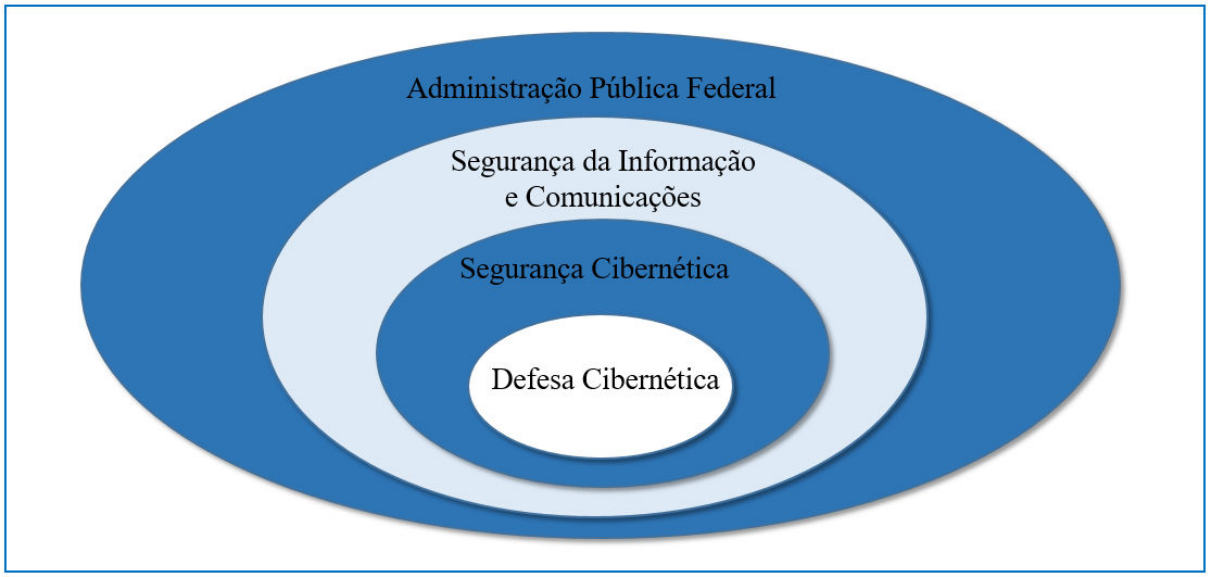
De fato, os conceitos de segurança são complementares. Fazem referência à proteção dos ativos de informação, das infraestruturas críticas e sistemas de informação. Buscam assegurar a confidencialidade, a integridade e a disponibilidade dos ativos de informação.

Para Dutra (2008), a segurança no ambiente de negócios e nos serviços de infraestrutura básica de uma sociedade deve ser encarada com a devida importância em virtude da crescente interconexão dos sistemas.

Segundo Clarke *et al*. (2011), existe o receio de que a modernização tecnológica, principalmente das infraestruturas críticas, seja uma porta de entrada para os ataques cibernéticos.

A Figura 10 apresenta a visão em camadas da SI, Segurança e Defesa Cibernética, que visam assegurar o uso adequado do espaço cibernético, contra as ações prejudiciais aos interesses da Nação e sociedade (BRASIL, 2015).

Figura 10 – Visão em camadas da Segurança da Informação e Comunicações



Fonte: Estratégia de SIC e de SegCiber (BRASIL, 2015) - Adaptado pelo autor

1.3.6 *Big Data*

O *Big Data* é um fenômeno que se refere à explosão da disponibilidade de dados relevantes, como resultado recente e sem precedente do avanço das tecnologias de armazenamento e registro de dados. Fenômeno do processamento de grandes volumes de dados, com os quais as ferramentas tradicionais não são capazes de lidar na velocidade requerida (GOLDMAN *et al.*, 2012).

Brynjolfsson *et al.* (2012), afirmam ainda que soluções de *Big Data* possuem um potencial maior do que as soluções analíticas tradicionais para trazer benefícios e aumentar a competitividade das empresas.

O termo *Big Data* surgiu para definir arquiteturas de sistemas capazes de lidar com as novas dimensões dos dados: velocidade, variedade e volume (AZEVEDO; NEVES; NOVO, 2014).

Nesse cenário de crescimento exponencial da informação publicada na Internet, com a presença de base de dados que contém um grande volume de dados situa-se o *Big Data* (SHINATAKU; DUQUE; SUAIDEN, 2014).

O *Big Data* não é uma área de estudo exclusiva da Ciência da Computação pois, como afirmam Boyd e Crawford (2012), físicos, economistas, matemáticos, cientistas políticos, bioinformáticos, sociólogos e outros profissionais poderão fazer uso e reuso da massivo de informações e das interações produzidas pelas pessoas no meio digital.

1.3.6.1 Características

O fenômeno *Big Data* está associado ao grande volume de dados, mas essa não é sua única característica. Inicialmente, foi caracterizado pelo volume, velocidade e variedade (3V´s) dos dados. Os atributos veracidade e valor foram considerados posteriormente como relevantes. Essas características são conhecidas como os 5V´s do *Big Data*, apresentados na Figura 11:

- Volume: refere-se ao tamanho dos dados. Os dados são coletados de uma grande variedade de fontes, incluindo transações comerciais, redes sociais e informações de sensores ou dados transmitidos de máquina a máquina;
- Velocidade: refere-se à velocidade de transmissão dos dados. Os dados fluem em uma velocidade sem precedentes e devem ser armazenados, tratados e analisados com agilidade;

- Variedade: refere-se ao formato no qual os dados são gerados, isto é, estruturados e não estruturados. Os dados estruturados são organizados em linhas e colunas e geralmente são armazenados em banco de dados relacionais, os quais facilitam a atualização e a recuperação de dados em menor granularidade. Os dados não estruturados não possuem uma organização pré-definida. Em decorrência disso, há maior dificuldade para sua recuperação e seu processamento, a exemplo dos vídeos, dos comentários em redes sociais, dos *e-mails*, entre outros;
- Veracidade: tem relação com a confiabilidade dos dados. Durante a análise dos dados é necessário conhecer o contexto em que os dados foram gerados, se eles são autênticos e de fontes confiáveis; e
- Valor: os dados devem agregar valor ao negócio. Sem valor, a informação não tem utilidade.

Figura 11 – 5V´s do *Big Data*

Fonte: O autor

1.3.6.2 Fonte

As fontes de dados do *Big Data* são: os usuários e a tecnologia. Dados, informações e conhecimento são gerados diariamente. A complexidade do *Big Data* não está no volume, como disse Davenport (2014), mas na falta de estrutura que dificulta a análise para geração de conhecimento, inovação ou valor.

O autor destaca a relevância de se resumir os dados e encontrar seus significados e seus padrões para o contexto no qual ele foi resumido. Reforça a importância da definição adequada do problema e da pertinência da formulação correta da pergunta, os quais devem orientar a coleta e a posterior síntese dos dados, na busca da organização da informação.

1.3.7 Privacidade

A palavra privacidade do latim (*privates*) tem o significado de separado do resto, portanto, indicando que uma pessoa pode ficar afastada ou isolada em relação às demais. A preocupação com a privacidade antecede a era da Internet.

O artigo publicado, em 1873, pelo Juiz Americano, Tomas Cooley, define a privacidade como a limitação do acesso às informações de uma determinada pessoa, ao acesso à própria pessoa, à sua intimidade, envolvendo as questões de anonimato, sigilo, afastamento e o direito de ser deixado em paz.

No mundo atual, no qual cada vez mais está presente o uso dos computadores e mecanismos tecnológicos de comunicação, emerge, segundo Lévy (1998), a questão do fim da privacidade e da preservação das informações, decorrente do fluxo informacional produzido e disponibilizado em grande escala na rede mundial de computadores.

A privacidade no ambiente digital, surge como um desafio, onde as informações e os dados são gerados, sendo essencial o estudo do tema por parte da CI durante todo o ciclo de vida da informação. A privacidade das informações, de acordo com Smith, Milberg e Burke (1996), é uma das questões éticas da sociedade da informação na era da informação.

O avanço das tecnologias da informação, os serviços da Internet e os *softwares* de *business intelligence* que realizam a coleta e mineração de grandes quantidades de dados, são canais de vulnerabilidade para o acesso às informações (HONG; THONG, 2013).

Sendo assim, as redes de computadores, a Internet e os avanços das ferramentas tecnológicas tanto de *hardware* e *software*, permitem a criação de novos ambientes informacionais, tornando relevante as questões para a preservação e privacidade das informações e os dados.

A era do *Big* Data demanda novos modelos de privacidade. Um novo modelo deve ser considerado: o modelo de identificação, no qual novas informações pessoais são deduzidas por meio de análise preditiva dos dados coletados. Destaca-se a necessidade de inserir a privacidade no contexto do *Big Data*, no qual os indivíduos não só se preocupam com a coleta de dados, mas também com a forma como esses dados serão analisados e usados (MAI, 2016).

Um fator importante de privacidade é opção de consentimento dada pelo consumidor, opção de decidir se o sistema pode ou não usar seus dados. Quando os sistemas de segurança

que preservam a privacidade estão funcionando adequadamente, o usuário demonstra confiança para compartilhar as suas informações.

As organizações devem considerar o fato de que a confiança do usuário é mais lucrativa, com resultados positivos a longo prazo, e a quebra dessa confiança terá um impacto negativo. Tratar das preocupações dos usuários em relação à privacidade gera valor para as organizações (MANDIĆ, 2009).

1.3.7.1 Normas de privacidade

A *International Organization for Standardization* (ISO) e o NIST tem um conjunto de normas relacionadas à privacidade e proteção de informações pessoais, a saber:

- ISO/IEC 29100:2011 - *Information technology - Security technique - Privacy framework*: fornece uma diretriz específica para a privacidade, define os atores no processamento de dados pessoais, descreve as considerações de proteção de privacidade e as referências aos princípios de privacidade no ambiente de TIC. A norma se aplica às pessoas físicas e instituições envolvidas na especificação, aquisição, arquitetura, projeto, desenvolvimento, teste, manutenção, administração e operação de sistemas de TIC;
- ISO/IEC 29101:2013 - *Information technology - Security technique - Privacy architecture framework*: fornece uma estrutura da arquitetura de privacidade, a qual estabelece as preocupações com os sistemas de TIC que processam informações pessoais. É aplicável às entidades envolvidas na especificação, aquisição, arquitetura, projeto, teste, manutenção, administração e operação de sistemas de TIC;
- ISO/IEC 29151:2017 - *Information technology - Security technique – Code of practice for personally identifiable information protection*: estabelece os objetivos de controle e diretrizes para implementar controles para atender aos requisitos identificados por uma avaliação de riscos e impacto relacionado à proteção de informações de identificação pessoal;
- ISO/IEC 29190:2015 - *Information technology - Security technique - Privacy capability assessment model*: fornece uma orientação de alto nível às instituições para uma avaliação da capacidade de gerenciar processos relacionados à privacidade e como integrar a avaliação de capacidade de gerenciar processos relacionados à privacidade nas operações organizacionais;

- ISO/IEC 27018:2014 - *Information technology - Security technique - Code of practice for protection of personally identifiable information in public clouds acting as personally identifiable information processors*: fornece um conjunto de práticas para proteção de informações pessoais publicadas em uma estrutura de computação em nuvem (*cloud computing*), segundo os princípios da norma ISO/IEC 29100. Estabelece os requisitos de risco de SI de um provedor de serviços de computação em nuvem;
- ISO/IEC 27701:2019 - *Security techniques for privacy information management*: estabelece os requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade.
- ISO/IEC 29134 - *Information technology - Security technique - Privacy impact assessment - Guidelines*: fornece uma metodologia para direcionar as avaliações sobre o impacto da privacidade. É aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas, empresas privadas, entidades governamentais e organizações sem fins lucrativos; e
- NISTIR 8062 - *Privacy Risk Management for Federal Information Systems*: descreve uma estrutura de gerenciamento de risco de privacidade focada em objetivos de engenharia de privacidade e um modelo de risco de privacidade para sistemas federais. O documento apresenta uma gestão da privacidade e um modelo de risco de privacidade.

As políticas globais de governança e regulamentação da privacidade no ambiente cibernético tem despertado interesse para publicação de diretrizes, normas ou regulamentos para proteger informações pessoais e instituições, como por exemplo: a LGPD no Brasil, a GDPR na União Europeia e o *California Consumer Privacy Act* nos EUA.

1.3.8 Anonimização de dados

A anonimização de dados tem um vasto campo de aplicação, podendo ser adotada como medida de segurança. O termo anonimato representa o fato de o sujeito não ser unicamente caracterizado dentro de um conjunto de sujeitos. O conceito de sujeito refere-se a uma entidade ativa, como uma pessoa ou computador (MONTEIRO; MACHADO; BRANCO JR, 2014).

O anonimato representa o fato de um registro não ser unicamente identificado em um conjunto de registros. Conjunto de registros pode ser um grupo de pessoas ou rede de computadores (PFITZMANN; KÖHNTOPP, 2005).

Para Camenisch, Fischer-Hübner e Rannenberg (2011), uma transação é considerada anônima quando os seus dados, individuais ou combinados, não possibilitam a associação para identificação de um registro em particular.

Os dados de indivíduos podem ser classificados como:

- Identificadores: atributos que identificam individualmente as pessoas (CPF, nome, identidade);
- Semi-identificadores: atributos que podem ser combinados com informações para reduzir a incerteza sobre a identificação das pessoas (data de nascimento, CEP, profissão, cargo, local de trabalho); e
- Atributos sensíveis: atributos que contêm informações sensíveis sobre as pessoas (salário, informações de saúde, despesas de cartão de crédito, hábitos de consumo).

As técnicas que podem ser utilizadas e/ou combinadas para a anonimização dos dados são as seguintes (MONTEIRO; MACHADO; BRANCO JR, 2014):

- Generalização: substitui os valores de atributos semi-identificadores por valores menos específicos com semântica consistente;
- Supressão: exclui valores de atributos identificadores e/ou semi-identificadores da tabela anonimizada;
- Encriptação: utiliza esquemas criptográficos normalmente baseados em chave pública ou chave simétrica para substituir dados sensíveis por dados encriptados; e
- Perturbação: é utilizada para a substituição de valores dos dados reais por dados fictícios para mascaramento de banco de dados de testes ou treinamento.

A técnica de perturbação procura alterar randomicamente os dados para preservar as características dos dados sensíveis para o modelo de dados, utilizando as seguintes abordagens (CHEN; LIU, 2011):

- Condensação de dados: condensa os dados em múltiplos grupos e tamanhos predefinidos. Dentro de um grupo não é possível distinguir diferenças entre os

registros. Cada grupo tem um tamanho *k*, que é o nível de privacidade decorrente da condensação; e

- *Random Data Pertubation* (RDP): adiciona ruídos, de forma randômica, aos dados sensíveis. A maioria dos métodos utilizados para adicionar ruído randômico são casos especiais de mascaramento de matriz.

O mascaramento é utilizado para disponibilizar bases de dados para teste ou treinamento, com informações que não identificam os usuários, porém com informações que pareçam ser reais. As técnicas de mascaramento de dados são:

- Substituir (*Replace*): substituição randômica de conteúdo por informações sem relação com o dado real;
- Embaralhar (*Shuffing*): substituição randômica do dado real por um dado derivado da própria coluna da tabela;
- Desfocar (*Blurring*): técnica aplicada a números e datas. Muda o valor do dado por uma percentagem do seu valor original; e
- Anular (*Null)*: substitui os dados sensíveis por valor nulos.

1.3.9 Lei Geral de Proteção de Dados Pessoais

No dia 14 de agosto de 2018, foi sancionada a Lei No. 13.709, Lei Geral de Proteção de Dados Pessoais. A referida Lei dispõe no primeiro artigo seu objetivo geral:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Com a entrada da LGPD, as empresas terão impactos nas questões relacionadas com a gestão da informação. Na era da informação, que segundo os autores Castells (2016) e Mattelart (2002), é uma consequência do crescimento das interações entre os usuários e a tecnologia, surgiram vários modelos de negócios, nos quais a informação é um ativo de valor estratégico.

A informação tem se mostrado, atualmente, um ativo de valor para as empresas, talvez o mais precioso, dada a sua importância para os negócios, portanto, a informação deve ser protegida. A importância de uma legislação adequada sobre o armazenamento e proteção de dados pessoais na Internet, visando garantir o direito à privacidade, que é assegurado pela Constituição Federal, também no ambiente virtual, tem sido uma demanda da sociedade.

Segundo o princípio da confidencialidade das comunicações, assegurado pela Constituição Federal, as informações privadas que trafegam pelo espaço cibernético requerem uma proteção. Segundo Tomizawa (2008), pelo fato do espaço cibernético ser público emerge a dificuldade de obtenção de proteção jurídica e sigilo das informações.

A LGPD pretende criar um arcabouço normativo para colocar o Brasil no seleto rol de países ou organismos que realizam um grau de proteção de dados pessoais adequado. A Lei cria uma série de obrigações para a empresas sobre a coleta, o uso e as garantias da integridade dos dados pessoais a serem observadas, sob pena de pesadas sanções.

Submetem-se à LGPD as entidades públicas ou privadas que efetuam o tratamento de dados pessoais no Brasil, coletam dados no País, ou que ofertam bens ou serviços no território nacional. No Artigo 3º, a matéria dispõe sobre a quem a Lei deve ser aplicada:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - A operação de tratamento seja realizada no território nacional;
>
> II - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e
>
> III - Os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2018).

1.3.9.1 Dados

O Artigo 5º, inciso I da LGPD apresenta a seguinte definição:

> "I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

O inciso II menciona:

> II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

O grande desafio que se coloca diante dos cidadãos é o controle dos dados pessoais que pode ser feito por empresas ou, até mesmo, pelos governos. As TIC permitem que uma infinidade de informações e dados sejam publicados e/ou coletados no ambiente do *Big Data*.

1.3.9.1.1 Dos princípios sobre o tratamento dos dados elencados na LGPD

- Finalidade: os dados devem ser tratados para os fins específicos informados ao titular, sem possibilidade de tratamento posterior de forma incompatível;

- Adequação: o tratamento dos dados deve ser compatível com a finalidade que foi informada para o usuário;
- Necessidade (ou minimização): só devem ser coletados dados pertinentes, proporcionais e não excessivos em relação às finalidades pretendidas;
- Livre acesso: os titulares dos dados devem poder consultar gratuitamente a forma e a duração do tratamento dos seus dados;
- Qualidade dos dados: garante aos titulares que seus dados serão exatos, terão informações claras, relevantes e atualizadas para o tratamento;
- Transparência: garante aos usuários informações claras e de fácil acesso sobre o tratamento dos seus dados e sobre os responsáveis pela sua gestão;
- Segurança: os agentes de tratamento dos dados têm obrigação de adotar medidas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: as empresas que tratam de dados devem adotar medidas para prevenir a ocorrência de danos no tratamento dessas informações;
- Não discriminação: os dados não podem ser utilizados para fins discriminatórios ilícitos ou abusivos; e
- Responsabilização e prestação de contas: os agentes de tratamento dos dados devem demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais.

1.3.9.1.2 Do consentimento para o tratamento dos dados estabelecido na LGPD

O consentimento passa a ser a melhor forma para legitimar o tratamento dos dados pessoais. O usuário tem o direito de escolher quais dados irá ou não fornecer e poderá retirar seu consentimento a qualquer momento. Em outras palavras, não pode o usuário ser induzido a consentir com o tratamento de seus dados pessoais para ter acesso a determinada aplicação na Internet.

No seu Artigo 5º inciso XII a LGPD dispõe que:

> XII: Consentimento: é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (BRASIL, 2018).

- Consentimento livre: o usuário deve ter o direito pleno de controle de seus dados pessoais;
- Consentimento informado: o usuário deve ter informações suficientes sobre a empresa, os serviços e o tratamento de seus dados, para que possa entender o

propósito do contrato ao qual está aderindo e tomar uma decisão adequada e consciente;

- Consentimento inequívoco: o usuário deve se manifestar por meio de um ato positivo. O usuário deve ainda realizar uma ação indicando sua aceitação, seja por envio de um *e-mail*, assinatura eletrônica, ou por um clique em um determinado local visível; e
- Consentimento para finalidade específica: a coleta de dados deve ser sempre vinculada a uma ou mais finalidades específicas e informadas na respectiva Política de Privacidade, sendo coibido o uso de dados para fins não previstos, sem prévio consentimento do usuário.

1.3.9.1.3 Dos principais direitos dos titulares dos dados estabelecidos na LGPD

- Direito de acesso e correção de dados incompletos, sem exatidão ou desatualizados;
- Direito à anonimização dos seus dados ou eliminação de dados desnecessários;
- Direito à portabilidade dos dados a outro fornecedor de serviço ou produto;
- Direito à eliminação dos dados pessoais tratados com o consentimento do titular;
- Direito à informação das entidades públicas e privadas com as quais teve os seus dados compartilhados; e
- Direito à revogação do consentimento.

1.3.9.1.4 Da transferência internacional dos dados estabelecida na LGPD

A transferência internacional dos dados somente poderá ser realizada para os países que forneçam um grau de proteção dos dados adequados ao previsto na Lei, ou quando tiver comprovadas garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos no mesmo texto normativo.

A transferência internacional de dados também é controlada no capítulo V, artigos 33 ao 36, exigindo garantia por parte do controlador do devido cumprimento dos princípios desta Lei para proteção de dados previsto.

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei [...] (BRASIL, 2018); e

> Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional (BRASIL, 2018).

1.3.9.2 *Data protection officer* (DPO)

O DPO ou o encarregado de proteção de dados é o responsável por disseminar a cultura de proteção de dados na instituição, estabelecer um canal de comunicação com a alta direção sobre o assunto e apoiar na criação de políticas e normas adequadas à LGPD.

O Artigo 42 no § 2º estabelece as seguintes atividades para o DPO:

> § 2º As atividades do encarregado consistem em:
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018).

1.3.9.3 Da governança da privacidade dos dados

A LGPD fomenta a criação de boas práticas, políticas, ações educativas, organização, supervisão, mitigação de riscos e implantação da governança da privacidade de dados.

A estrutura de governança da privacidade de dados deve:

- Demonstrar o comprometimento do controlador dos dados em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais e corporativos;
- Aplicar as políticas e processos estabelecidos sob todos os dados pessoais e corporativos controlados pela instituição, independente da forma de coleta do dado, *on-line* ou *off-line*. A aplicação se estende por todo o ciclo de vida do dado, da entrada ao seu descarte;
- Adaptar as políticas e processos conforme o tamanho da instituição. Quanto maior e mais complexa a instituição, maior deve ser a segurança dos dados;
- Estabelecer políticas, processos e salvaguardas adequadas sustentada nos processos de avaliação sistemática de impactos e riscos à privacidade;
- Estabelecer uma relação de confiança com o titular do dado, por meio de uma atuação transparente que assegura a participação do titular nas questões de consentimento do uso dos dados;

- Integrar a governança da privacidade dos dados na governança da instituição, assegurando foco na privacidade dos dados pessoais e corporativos;
- Estabelecer políticas e processos de auditoria para realizar ações de análises de vulnerabilidades, ameaças e incidentes de SegCiber dos dados pessoais e corporativos;
- Criar planos de resposta ao vazamento de dados pessoais e corporativos decorrentes das vulnerabilidades, ameaças e incidentes de SegCiber; e
- Revisar e atualizar as políticas e processos que compõem a governança da privacidade dos dados com periodicidade estabelecida no programa de governança institucional.

1.3.9.4 Das sanções

Para efetiva aplicação da Lei, é necessário a aplicação de sanções administrativas, que estão identificadas no capítulo VII, que trata da fiscalização:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; e
>
> III - Multa diária, observado o limite total a que se refere o inciso II.

As aplicações das sanções devem seguir critérios como a gravidade, a boa fé ou vantagem pretendida pelo infrator, a sua condição econômica, a reincidência, o grau do dano, entre outros dispostos na Lei. Para o cálculo do valor da multa serão disponibilizadas as metodologias estabelecidas pela autoridade nacional, conforme o artigo 53º:

> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (BRASIL, 2018)
>
> IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e
>
> VI - Eliminação dos dados pessoais a que se refere a infração (BRASIL, 2018).

CAPÍTULO 2

Este capítulo incialmente apresenta a metodologia, os níveis de maturidade, domínios, objetivos e práticas do modelo proposto. A seguir discorre sobre os impactos sociais do *Big Data* relacionados com a privacidade, ética, organização da informação, riscos à SI e valor da informação para as instituições e usuários. Por fim, apresenta o questionário da autoavaliação, alinhamento com a LGPD e os resultados da aplicação do modelo.

2.1 METODOLOGIA

Esta pesquisa classifica-se como Pesquisa Aplicada, quanto à sua natureza. Este tipo de pesquisa tem como objetivo possibilitar maior familiaridade com o problema, visando torná-lo mais explícito ou construir hipóteses.

Com relação à forma de abordagem do problema, foi realizada uma pesquisa qualitativa para analisar, compreender e interpretar as referências bibliográficas.

Do ponto de vista dos objetivos, a pesquisa é descritiva, já que foi efetuada uma análise dos riscos referentes à privacidade, à organização, à segurança e a perda de valor das informações no ambiente do *Big Data*.

Para analisar, compreender e interpretar o material qualitativo foi realizada uma análise de conteúdo, que representa um conjunto de técnicas de análise de comunicações que visaram obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores que permitam a inferência de conhecimentos relativos às condições de produção/recepção destas mensagens (BARDIN, 2016).

A análise de conteúdo, conforme Bardin (2016) prevê 3 (três) fases. As diferentes fases, assim como o inquérito sociológico ou a experimentação, organizam-se da seguinte forma:

- 1ª. Fase: pré-análise;
- 2ª. Fase: exploração do material; e
- 3ª. Fase: tratamento dos resultados, inferência e a interpretação.

A fase de pré-análise visa organizar o material da pesquisa, sistematizar as ideias iniciais e desenvolver um plano de análise. Esta fase tem 3 (três) subfases: i) a escolha dos documentos que serão analisados; ii) a formulação das hipóteses e dos objetivos; e iii) a elaboração de indicadores para fundamentar a interpretação final (BARDIN, 2016).

A fase de exploração do material consiste na definição das categorias, identificação das unidades de registro visando à categorização e à contagem de frequência, e das unidades de

contexto nos documentos. Para BARDIN (2016), essa fase possibilita ou não a riqueza das interpretações e inferências, sendo assim, a codificação, a classificação e a categorização são requisitos básicos para a exploração do material.

Na 3ª. fase os resultados são condensados para uma análise crítica. O pesquisador, tendo à sua disposição resultados significativos, pode então apresentar inferências e adiantar interpretações relacionadas com os objetivos previstos ou a outras descobertas (BARDIN, 2016).

A metodologia descrita nesta seção foi replicada na elaboração dos artigos integrantes deste trabalho.

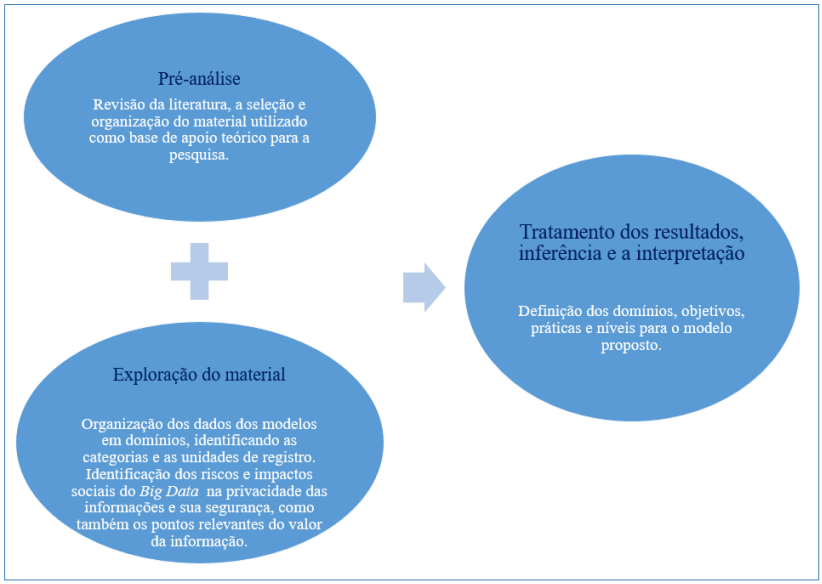
2.1.1 Descrição da pesquisa

Na 1a. fase, chamada de pré-análise, foi realizada a revisão da literatura, a seleção e organização do material utilizado como base de apoio teórico para a pesquisa.

Já na 2ª. fase, foram organizados os dados dos modelos em domínios, identificando as categorias e as unidades de registro. Identificação dos riscos e impactos sociais do *Big Data* na privacidade das informações e sua segurança, como também os pontos relevantes do valor da informação.

A definição dos domínios, objetivos, práticas e níveis para o modelo proposto, bem como a discussão dos resultados foram estabelecidos na 3ª. fase da pesquisa. Para Bardin (2016), esta fase compreende a inferência e a interpretação dos resultados. A Figura 12 apresenta as fases da análise de conteúdo.

Figura 12 – Fases da análise de conteúdo



Fonte: O autor

A interpretação dos temas e domínios comuns entre os modelos e conceitos apresentados no referencial teórico são a base para o modelo proposto. Os modelos selecionados na pesquisa, estão apresentados no Quadro 3, com os seus respectivos domínios e temas.

Quadro 3 – Domínios, elementos, processos, descrição e temas dos modelos

Modelo *Cybersecurity capability maturity model (C2M2)*	
Domínio: gestão de risco	
Descrição	Tema
Estabelecer, operar e manter o programa de gerenciamento de riscos de SegCiber para identificar, analisar e reduzir os riscos. A gestão do risco da SegCiber envolve o enquadramento, a identificação, a avaliação, a resposta (aceitar, evitar, mitigar, transferir) e o monitoramento dos riscos de uma maneira que exista um alinhamento com as necessidades da organização.	A gestão do risco de SegCiber
Domínio: gestão de ativos, mudanças e configurações	
Descrição	Tema
Um ativo de informação é algo de valor para a organização. Os ativos considerados para este modelo são os ativos de tecnologia da informação e organizacionais.	Gestão de ativos
Domínio: gestão de identidade e acesso	
Descrição	Tema
Criar e gerenciar identidades de acesso físico e lógico aos recursos e ativos da organização. O controle de acesso deve ser limitado às necessidades do usuário.	Gestão de acesso
Domínio: gestão de ameaças e vulnerabilidades	
Descrição	Tema
Manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder a ameaças e vulnerabilidades de SegCiber.	Gestão de ameaças, vulnerabilidades
Domínio: consciência situacional	
Descrição	Tema
Desenvolvimento do conhecimento organizacional, com o registro e monitoramento das atividades de TI. Deve-se estabelecer e manter atividades e tecnologias para manter, analisar, alertar, apresentar e utilizar informações operacionais sobre a SegCiber.	Gestão de ativos, estrutura tecnológica, consciência situacional
Domínio: compartilhamento de informações e comunicações	
Descrição	Tema
Manter relações com organizações do ambiente do negócio para compartilhar informações de SegCiber.	Compartilhamento de informações
Domínio: respostas a eventos, incidentes e continuidade de operações	
Descrição	Tema
Manter planos, procedimentos e tecnologias para detectar, analisar e responder aos eventos de SegCiber.	Resposta a eventos, gestão de continuidade
Domínio: cadeia de suprimentos e gerenciamento de dependências externas	
Descrição	Tema
Manter controles para gerenciar os riscos de SegCiber relacionados a serviços e ativos de entidades externas.	A gestão dos riscos da SegCiber associados a partes interessadas externas
Domínio: gerenciamento da força de trabalho	
Descrição	Tema
Manter planos, procedimentos e tecnologias para criar uma cultura de SegCiber. Adequar as competências da força de trabalho conforme a tecnologia utilizada pela organização. Aumentar a consciência da força de trabalho sobre a SegCiber é tão importante quanto a implementação de novas tecnologias para melhorar a SegCiber.	Cultura de SegCiber, papéis e responsabilidades, treinamento, conscientização
Domínio: gestão do programa de SegCiber	
Descrição	Tema

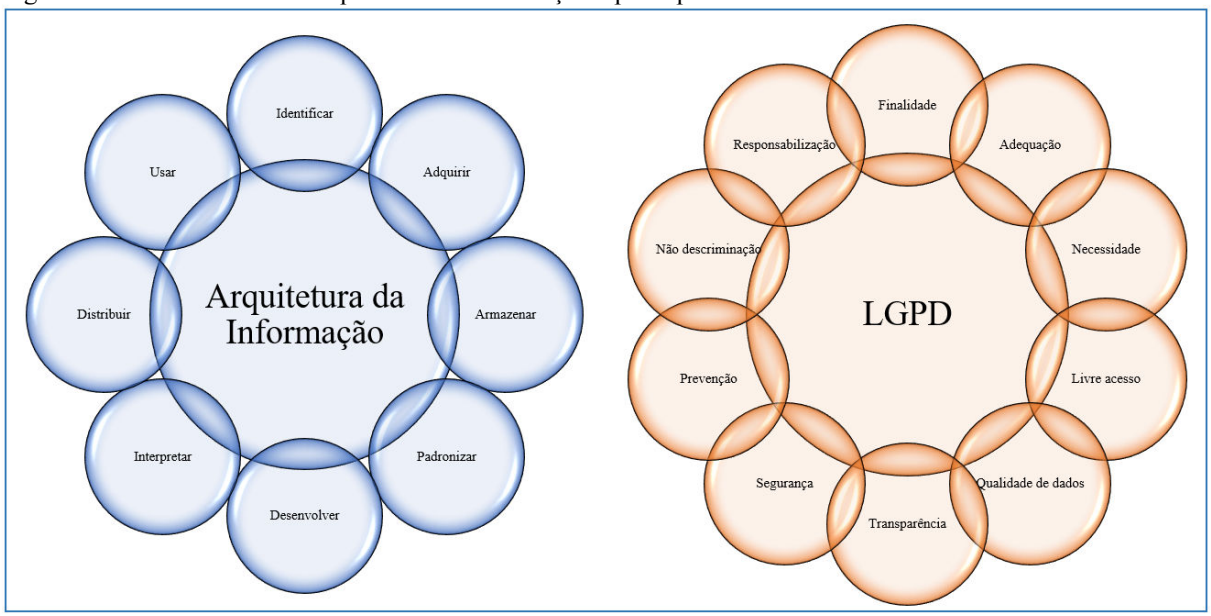
Manter um programa de SegCiber que forneça governança, planejamento estratégico e patrocínio para as atividades. O patrocínio da alta administração é importante para a implementação do programa.	Governança de SegCiber
Modelo *NIST Cybersecurity Framework*	
Processo: gerenciamento de risco	
Descrição	Tema
É um processo contínuo de identificação, avaliação e resposta ao risco. Com as informações sobre a probabilidade e o impacto, as organizações têm como determinar o nível aceitável de risco e a tolerância ao risco estabelecida pela organização.	A gestão dos riscos da SegCiber
Processo: programa integrado de gerenciamento de risco	
Descrição	Tema
Conscientização do risco de SegCiber no nível organizacional com uma abordagem de toda a organização para gerenciar o risco. Processos que permitem que as informações de SegCiber sejam compartilhadas dentro da organização.	Conscientização, gestão de riscos de SegCiber, compartilhamento
Processo: participação externa	
Descrição	Tema
Integração com as organizações do ambiente de atuação, compartilhamento das informações com parceiros para assegurar que informações atuais e precisas são utilizadas para melhorar a SegCiber.	Compartilhamento de informações
Modelo *The community cyber security maturity model (CSMM)*	
Elemento: enfrentar ameaças	
Descrição	Tema
Categorias de ameaças: i) ameaças não estruturadas: exploram a falta de estrutura da organização; ii) ameaças estruturadas: estas ameaças são caracterizadas por ataques planejados e sistemáticos para comprometer, interromper os sistemas de informações e afetar as operações para conseguir vantagem com as informações acessadas; iii) ameaças altamente planejadas: consistem em ataques planejados, multidisciplinares.	Ameaças
Elemento: métricas	
Descrição	Tema
As métricas podem ser classificadas como técnicas e não técnicas. As técnicas incluem, por exemplo: tentativas de *login*, tempo médio de uso da rede, número de *e-mails* enviados e recebidos e tráfego de rede. As não técnicas incluem a formação dos funcionários em SI, número de funcionários da organização, programa de SI e conscientização dos funcionários sobre o assunto.	Métrica de segurança, ameaças
Elemento: compartilhamento de informações	
Descrição	Tema
Compartilhar as informações é uma premissa básica do modelo, para enfrentar os ataques de SegCiber em uma comunidade. As informações compartilhadas dentro da comunidade são instrumento para aumentar o nível de conhecimento para enfrentar as ameaças.	Compartilhamento, informações
Elemento: tecnologias	
Descrição	Tema
Um programa de SegCiber eficaz para abordar as questões de ameaças cibernéticas requer uma estrutura tecnológica adequada. As vulnerabilidades e ameaças têm que ser integradas com o ambiente tecnológico e organizacional, para a organização ter um programa global que atenda os objetivos estratégicos da organização.	Estrutura tecnológica
Elemento: treinamento	
Descrição	Tema
O treinamento é um componente essencial para o modelo. As organizações implementam somente um treinamento básico de SI para os funcionários. O treinamento deve atender os diversos níveis de funcionários da organização.	Treinamento

Elemento: testes	
Descrição	Tema
Com a implantação do programa, é necessário estabelecer um processo para testar as capacidades do modelo e avaliar o progresso da implementação.	Testar modelo, avaliar implementação

Fonte: O autor

A análise dos temas em conjunto com os mecanismos da AI e os princípios da LGPD permitiu a definição dos domínios, objetivos e práticas do modelo proposto. A Figura 13 apresenta os mecanismos da AI e os princípios da LGPD.

Figura 13 – Mecanismos da Arquitetura da Informação e princípios da LGPD



Fonte: O autor

O material selecionado, que faz parte do *corpus* da pesquisa, foi exportado para o gerenciador de referências *Mendeley*. A pesquisa realizada nas bases de dados mencionadas no item 1.1.1, Revisão da Literatura, trouxe um total de 33 (trinta e três) artigos, que tratam das combinações dos termos pesquisados.

2.2 APLICAÇÃO DOS CONHECIMENTOS

Este trabalho propõe um Modelo de Maturidade da AI para mitigar os impactos sociais dos riscos à privacidade, à organização, à segurança e perda de valor das informações nas instituições inseridas no ambiente do *Big Data*.

O modelo adota uma abordagem holística da AI, que engloba pessoas, processos e tecnologias. Ele propõe um conjunto estruturado de domínios, objetivos e práticas alinhados com a LGPD, com os níveis de maturidade estabelecidos.

2.2.1 Níveis de maturidade do modelo proposto

Segundo Adler (2013), os níveis de maturidade são utilizados para medir a competência organizacional ou maturidade de um conjunto reconhecido das melhores práticas. As métricas são organizadas em categorias e quantificadas em uma escala de desempenho.

O Quadro 4 apresenta a escala para os níveis de maturidade do modelo proposto com a descrição das práticas, considerando os modelos apresentados no referencial teórico deste trabalho.

Quadro 4 – Níveis de maturidade

Nível de maturidade	Descrição
Nível 0 - Não contém práticas para o domínio	
As práticas não são realizadas	-
Nível 1 - Contém um conjunto de práticas iniciais para o domínio	
As práticas iniciais são realizadas, mas podem ser *ad hoc*	A realização da prática depende da iniciativa ou experiência de um colaborador, sem a formalidade de um plano documentado. As lições aprendidas não são documentadas tornando difícil a repetição da melhoria na instituição.
Nível 2 - Representa um nível de institucionalização das atividades para o domínio	
As práticas são documentadas	As práticas de um domínio estão em fase inicial de documentação, visando o planejamento para atender as necessidades dos objetivos da instituição.
As partes interessadas são identificadas e envolvidas	As partes interessadas são identificadas e envolvidas no desempenho das práticas. Pode incluir partes interessadas internas e externas da instituição.
Os recursos para apoiar os processos são fornecidos	Os recursos são fornecidos na forma de pessoas, financiamento e ferramentas para que as práticas sejam realizadas conforme o planejamento. A implementação de uma prática está relacionada com a disponibilidade ou escassez de recurso.
Os padrões e/ou diretrizes são utilizados e identificados para implementar as práticas	A instituição identifica padrões e/ou diretrizes para implementação de práticas de um domínio.
Nível 3 - As atividades do domínio são institucionalizadas e estão sendo gerenciadas	
As práticas são orientadas por políticas, diretrizes e governança	As atividades gerenciadas de um domínio recebem orientação organizacional seguindo as políticas, diretrizes e governança.
As políticas incluem requisitos de conformidade para padrões e/ou diretrizes específicas	As práticas seguem requisitos de conformidade com os padrões e/ou diretrizes estabelecidas.
As atividades são revisadas periodicamente para assegurar a conformidade com a política da instituição e legislação em vigor	A organização realiza periodicamente a revisão das atividades para manter o alinhamento da conformidade com a política da instituição e legislação em vigor.
As responsabilidades são atribuídas para os colaboradores e equipe	São estabelecidas as responsabilidades e autoridade para realizar as práticas definidas.
A equipe possui habilidades e conhecimento para as atividades	A equipe possui qualificação para realizar as práticas definidas para um domínio.

Fonte: C2M2 – *NISTCyberSecurity* – CCSMM – Adaptado pelo autor

O Quadro 5 apresenta os níveis com as suas respectivas características que devem ser atendidas para a progressão dos níveis de maturidade. A institucionalização descreve até que ponto uma prática está implantada nas operações da instituição. A progressão é descrita por um

conjunto de práticas que podem ser realizadas para certificar as práticas específicas de um domínio.

Quadro 5 – Níveis de maturidade e as características de institucionalização

Nível	Características de institucionalização
Nível 0	- As práticas não são realizadas
Nível 1	- As práticas iniciais são realizadas, mas podem ser *ad hoc*;
Nível 2	- As práticas são documentadas - As partes interessadas são identificadas e envolvidas - Os recursos para apoiar os processos são fornecidos - Os padrões e/ou diretrizes são utilizados para implementar as práticas - Os padrões e/ou diretrizes utilizados para implementar as práticas estão identificadas - As práticas são mais completas ou avançadas do que no Nível 1
Nível 3	- As práticas são orientadas por políticas, diretrizes e governança - As políticas incluem requisitos de conformidade para padrões e/ou diretrizes específicas - As atividades são revisadas periodicamente para assegurar a conformidade com a política da instituição e legislação em vigor - As responsabilidades são atribuídas para os colaboradores e equipe - A equipe possui habilidades e conhecimento para as atividades - As práticas são mais completas ou avançadas do que no Nível 2

Fonte: C2M2 – *NISTCyberSecurity* – CCSMM – Adaptado pelo autor

2.2.2 Domínios, objetivos e práticas do modelo proposto

Os objetivos dos domínios compreendem um conjunto de práticas que são ordenadas por nível de maturidade. Um conjunto de práticas representa as atividades que uma organização pode realizar para implementar e desenvolver a capacidade de maturidade em um domínio. As práticas estão organizadas em objetivos que apóiam as atividades dentro de um domínio.

O modelo proposto fornece um ponto de referência para as instituições de ensino e pesquisa e de fomento entenderem o nível de suas práticas, processos e métodos para, então, definir metas e prioridades de melhoria, para mitigar os impactos sociais decorrentes de vulnerabilidades de SegCiber e para facilitar o alinhamento com a LGPD.

2.2.2.1 Estrutura do modelo proposto

O modelo é composto por práticas, para cada um dos 8 (oito) domínios, agrupadas por objetivos que apóiam a estrutura do modelo. Os objetivos e as práticas são ordenados por nível de maturidade.

Com a análise de conteúdo foi possível estabelecer os domínios, objetivos e práticas que compõe o modelo proposto com base nos modelos de maturidade: *Cybersecurity Capability Maturity Model*, *NIST Cybersecurity Framework* e *The Community Cyber Security Maturity Model*, com as normas ISO/IEC, mecanismos de AI e com os conceitos estudados e apresentados no referencial teórico.

O Quadro 6 apresenta o relacionamento do modelo proposto, seus domínios e objetivos, com os artigos da LGPD.

Quadro 6 – Domínios, objetivos e artigos da LGPD

Domínios	Objetivos	Artigos da LGPD
Governança	Definir e implementar uma estratégia e estrutura de governança da privacidade dos dados, integrada à governança corporativa.	Art. 3º, 7º, 8º, 9º, 10º, 12º, 14º, 15º, 23º, 41º, 42º, 46º, 49º e 50º
Proteção de dados	Assegurar a proteção de dados contra acessos não autorizados. Gerenciar as ações de destruição acidental ou ilícita dos dados. Comunicação inadequada com o uso dos dados.	Art. 8º, 9º, 11º, 12º, 33º, 34º, 35º e 36º
Resposta às vulnerabilidades, ameaças e incidentes	Gerenciar e responder às vulnerabilidades, ameaças e incidentes relacionados aos ativos de informação. Estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder às vulnerabilidades, ameaças e incidentes.	Art. 42º, 43º, 44º, 45º, 46º e 47º
Riscos	Analisar os riscos e impactos à privacidade dos dados.	Art. 10º, 11º, 52º, 53º e 54º
Capacitação, conscientização e cultura	Disseminar e implementar a cultura de proteção de dados na instituição.	Art. 18º, 19º, 21º, 41º e 51º
Tratamento dos dados	Atender as solicitações do titular dos dados e instituição competente quanto às informações referentes ao tratamento dos dados, consentimento realizado pelo titular dos dados e assegurar que os dados são bloqueados e/ou excluídos a pedido do usuário ou encerramento do contrato.	Art. 11º, 12º , 16º, 18º, 19º, 21º, 22º, 37º, 38º, 39º, 40º, 41º, 46º, 47º e 48º
Organização da informação	Identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações.	Art. 5º, 7º, 8º, 9º, 11º, 12º, 14º, 17º, 23º, 25º, 31º, 32º, 33º, 46º e 47º
Infraestrutura tecnológica	Realizar e monitorar as atividades operacionais.	Art. 46º, 47º, 48º, 49º e 50º

Fonte: O autor

2.2.2.1.1 Domínio “Governança”

O domínio governança tem como objetivos definir e implementar uma estratégia e estrutura de governança de privacidade dos dados, integrada à governança corporativa da instituição.

A instituição posicionada no nível 3 atende todas as práticas estabelecidas para o referido domínio, demonstra alinhamento com os artigos 7º, 8º, 9º, 10º, 12º, 14º, 15º, 23º, 41º, 42º, 46º, 49º e 50º da LGPD, que abordam questões relacionadas com o tratamento dos dados pessoais, com o tratamento de dados pessoais pelo poder público, com as atribuições do encarregado pelo tratamento dos dados pessoais, com a responsabilidade e o resarcimento de danos, com a segurança, com o sigilo dos dados e com as boas práticas de governança.

No Quadro 7 estão apresentadas as práticas, do domínio governança, para cada um dos níveis do modelo.

Quadro 7 – Domínio: Governança

Domínio: Governança	
Objetivos: definir e implementar uma estratégia e estrutura de governança da privacidade dos dados, integrada à governança corporativa.	
Nível	Práticas
Nível 0	Não tem práticas
Nível 1	1.1 A instituição tem uma estratégia de alinhamento da governança de privacidade dos dados com a governança corporativa 1.2 A instituição fornece os recursos necessários para implementar a governança de privacidade dos dados
Nível 2	2.1 A instituição tem uma estratégia documentada do alinhamento da governança de privacidade dos dados com a governança corporativa 2.2 A estratégia e as prioridades para as atividades de governança de privacidade dos dados são documentadas e alinhadas com os objetivos estratégicos e de risco da instituição 2.3 A instituição tem planos de respostas a incidentes para continuidade do negócio alinhados com as atividades de SegCiber 2.4 A instituição tem uma estrutura organizacional de SegCiber, com políticas e salvaguardas adequadas para mitigar os impactos e riscos à privacidade
Nível 3	3.1 A estratégia e estrutura são atualizadas para refletir as mudanças do setor de atuação, as mudanças no ambiente operacional e as mudanças no perfil de ameaças 3.2 As atividades de SegCiber são orientadas por políticas e diretrizes organizacionais 3.3 A instituição implementa e documenta os mecanismos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações 3.4 A alta administração patrocina o desenvolvimento e manutenção de políticas de proteção dos dados

Fonte: O autor

2.2.2.1.2 Domínio “Proteção de dados”

Os objetivos do domínio proteção de dados são assegurar a proteção dos dados contra acessos não autorizados e gerenciar as ações de destruição acidental ou ilícita dos dados e comunicação inadequada com o uso dos dados.

O atendimento das práticas dos níveis 1, 2 e 3 para esse domínio, demonstra um alinhamento com os artigos 8º, 9º, 11º, 12º, 33º, 34º, 35º e 36º da LGPD, que abordam questões relacionadas com o tratamento dos dados pessoais, com o tratamento de dados pessoais sensíveis e com a transferência internacional dos dados.

No Quadro 8 estão apresentadas as práticas, do domínio proteção de dados, para cada um dos níveis do modelo.

Quadro 8 – Domínio: Proteção de dados

Domínio: Proteção dos dados	
Objetivos: assegurar a proteção de dados contra acessos não autorizados. Gerenciar as ações de destruição acidental ou ilícita dos dados. Comunicação inadequada com o uso dos dados.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As identidades são provisionadas para pessoas e outras entidades que necessitam de acesso 1.2 As credenciais de acesso são emitidas para pessoas e outras entidades que necessitam de acesso 1.3 As credenciais de acesso que não são mais necessárias são revogadas
Nível 2	2.1 Os repositórios de identidades são periodicamente revisados e atualizados para assegurar a validade do acesso

Domínio: Proteção dos dados	
Objetivos: assegurar a proteção de dados contra acessos não autorizados. Gerenciar as ações de destruição acidental ou ilícita dos dados. Comunicação inadequada com o uso dos dados.	
Nível	**Práticas**
	2.2 As credenciais de acesso são revisadas periodicamente para assegurar que estão associadas a pessoas ou entidades corretas 2.3 As credenciais de acesso são revogadas dentro de limites de tempo definidos pela instituição e legislação vigente 2.4 As ações de destruição acidental ou ilícita dos dados são documentadas 2.5 As solicitações de acesso são revisadas e aprovadas pelo proprietário do recurso
Nível 3	3.1 Os requisitos das credenciais de acesso são estabelecidos considerando os critérios de risco da instituição 3.2 Os privilégios de acesso são revisados e atualizados periodicamente para assegurar sua validade 3.3 O acesso aos ativos é concedido pelo proprietário do ativo com base nos critérios de risco estabelecidos para realizar a atividade 3.4 As tentativas irregulares de acesso são monitoradas por meio dos indicadores de eventos de SegCiber 3.5 Os requisitos de acesso incorporam princípios de privilégios mínimos e de separação de funções 3.6 Os privilégios de acesso administrativo, acesso de emergência e contas compartilhadas têm controle e monitoramento adicionais 3.7 A instituição implementa e documenta os mecanismos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações classificadas como sensíveis

Fonte: O autor

2.2.2.1.3 Domínio “Resposta às vulnerabilidades, ameaças e incidentes”

A gestão de vulnerabilidades, ameaças e incidentes visa estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder a incidentes relacionados aos ativos de informação.

A maturidade para o referido domínio demonstra um alinhamento com os artigos 42º, 43º, 44º, 45º e 46º da LGPD. Esses artigos abordam questões sobre a responsabilidade e resarcimento de danos, a segurança e o sigilo dos dados.

No Quadro 9 estão apresentadas as práticas, do domínio resposta às vulnerabilidades, ameaças e incidentes, para cada um dos níveis do modelo.

Quadro 9 – Domínio: Respostas às vulnerabilidades, ameaças e incidentes

Domínio: Resposta às vulnerabilidades, ameaças e incidentes	
Objetivos: gerenciar e responder às vulnerabilidades, ameaças e incidentes relacionados aos ativos de informação. Estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder às vulnerabilidades, ameaças e incidentes.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As fontes de informação para apoiar as atividades de gestão de vulnerabilidades, ameaças e incidentes são identificadas 1.2 As informações sobre vulnerabilidades, ameaças e incidentes são internalizadas e interpretadas 1.3 As vulnerabilidades, ameaças e incidentes são controladas e monitoradas
Nível 2	2.1 As vulnerabilidades, ameaças e incidentes são identificadas, analisadas e tratadas conforme prioridade estabelecida

Domínio: Resposta às vulnerabilidades, ameaças e incidentes	
Objetivos: gerenciar e responder às vulnerabilidades, ameaças e incidentes relacionados aos ativos de informação. Estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder às vulnerabilidades, ameaças e incidentes.	
Nível	**Práticas**
	2.2 O impacto operacional para implementação de uma correção de SegCiber é avaliado antes da sua implementação 2.3 As vulnerabilidades, ameaças e incidentes são adicionadas ao registro de riscos da instituição 2.4 As características das vulnerabilidades, ameaças e incidentes são registradas e documentadas
Nível 3	3.1 As avaliações das vulnerabilidades, ameaças e incidentes são realizadas com uma periodicidade estabelecida pela organização 3.2 As avaliações das vulnerabilidades, ameaças e incidentes seguem os critérios de risco da organização 3.3 As avaliações das vulnerabilidades, ameaças e incidentes são realizadas por equipes independentes da atividade de operação 3.4 A análise e priorização das vulnerabilidades, ameaças e incidentes seguem os critérios de risco da organização 3.5 As informações sobre vulnerabilidades, ameaças e incidentes são adicionadas ao registro de riscos da organização 3.6 As atividades de monitoramento de risco validam as respostas às vulnerabilidades, ameaças e incidentes

Fonte: O autor

2.2.2.1.4 Domínio “Riscos”

O risco no espaço cibernético é um dos componentes do ambiente que alimenta o risco organizacional. Para o NIST (2014), o gerenciamento de risco é um processo contínuo de identificação, avaliação e resposta ao risco, visando obter informações para compreender a probabilidade de que um evento de SegCiber ocorra e o seu impacto resultante.

Os objetivos do domínio são analisar os riscos e impactos à privacidade dos dados. Conquistar a maturidade do nível 3 para esse domínio, demonstra um alinhamento com os artigos 10º, 11º , 52º, 53º e 54º da LGPD, que abordam questões relacionadas com os requisitos para o tratamento de dados pessoais, com o tratamento de dados pessoais sensíveis, com as boas práticas de governança e com as sanções administrativas.

No Quadro 10 estão apresentadas as práticas, do domínio riscos, para cada um dos níveis do modelo.

Quadro 10 – Domínio: Riscos

Domínio: Riscos	
Objetivos: analisar os riscos e impactos à privacidade dos dados.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As práticas de gestão de risco são aprovadas pela alta administração 1.2 As práticas de gestão de risco são estabelecidas como políticas da instituição 1.3 Os riscos de SegCiber são identificados
Nível 2	2.1 Os riscos e impactos à privacidade dos dados identificados são documentados 2.2 Os riscos e impactos à privacidade dos dados identificados são analisados para priorizar as atividades de resposta conforme a estratégia e estrutura de governança de privacidade de dados 2.3 Os riscos identificados são monitorados conforme a estratégia de gestão de riscos 2.4 A análise de risco é realizada na arquitetura de rede

Domínio: Riscos	
Objetivos: analisar os riscos e impactos à privacidade dos dados.	
Nível	**Práticas**
Nível 3	3.1 As avaliações dos riscos são realizadas com uma periodicidade estabelecida pela organização 3.2 As avaliações dos riscos são realizadas por equipes independentes da atividade de operação 3.3 A análise e priorização dos riscos seguem os critérios de gestão de riscos da instituição 3.4 As informações sobre os riscos são adicionadas ao registro de riscos da instituição

Fonte: O autor

2.2.2.1.5 Domínio "Capacitação, conscientização e cultura de proteção dos dados"

São atividades que procuram criar uma cultura de proteção dos dados na instituição e assegurar as competências atualizadas para a força de trabalho. À medida que as instituições adotam novas tecnologias, aumenta o desafio para melhorar as competências dos usuários do ambiente tecnológico.

Implementar e realizar as práticas de todos os níveis para o referido domínio possibilita aumentar a cultura de proteção dos dados na instituição e direcionar o alinhamento com os artigos 18º, 19º, 21º, 41º e 51º da LGPD, que abordam questões relacionadas com o treinamento, com os direitos do titular, com as atribuições do encarregado pelo tratamento dos dados pessoais e com as boas práticas de governança.

No Quadro 11 estão apresentadas as práticas, do domínio capacitação, conscientização e cultura de proteção dos dados, para cada um dos níveis do modelo.

Quadro 11 – Domínio: Capacitação, conscientização e cultura de proteção dos dados

Domínio: Capacitação, conscientização e cultura de proteção dos dados	
Objetivos: disseminar e implementar a cultura de proteção de dados na instituição.	
Nível	Práticas
Nível 0	Não tem práticas
Nível 1	1.1 As responsabilidades para as atividades de proteção dos dados são identificadas 1.2 As atividades de capacitação e conscientização para disseminar a cultura de proteção dos dados são realizadas
Nível 2	2.1 Os objetivos das atividades de capacitação e conscientização para disseminar a cultura de proteção dos dados são estabelecidos e mantidos 2.2 As atividades de capacitação e conscientização para disseminar a cultura de proteção dos dados incluem oportunidades de educação permanente de desenvolvimento profissional dos colaboradores 2.3 O treinamento nas atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção de dados é um requisito para concessão de acesso aos ativos sensíveis da instituição 2.4 O conteúdo das atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção de dados é baseado no perfil das vulnerabilidades, ameaças e incidentes
Nível 3	3.1 A instituição tem formalmente um *Data Protection Officer* (DPO) 3.2 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados estão alinhadas com as atividades operacionais da organização 3.3 A eficácia das atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados é avaliada com uma periodicidade estabelecida pela instituição e melhorias são implementadas, conforme a necessidade 3.4 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados e os requisitos de trabalho são revisados e atualizados conforme a necessidade

Domínio: Capacitação, conscientização e cultura de proteção dos dados	
Objetivos: disseminar e implementar a cultura de proteção de dados na instituição.	
Nível	Práticas
	3.5 A cultura de proteção dos dados faz parte dos critérios de avaliação de desempenho profissional

Fonte: O autor

2.2.2.1.6 Domínio "Tratamento dos dados"

O tratamento dos dados deve estar presente nas operações realizadas com dados pessoais e corporativos, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, comunicação, transferência e difusão ou extração.

O atendimento das práticas do referido domínio, demonstram o alinhamento com os artigos 11º, 12º , 16º, 18º, 19º, 21º, 22º, 37º, 38º, 39º, 40º, 41º, 47º e 48º da LGPD, que abordam questões relacionadas com os requisitos para o tratamento de dados pessoais, com o tratamento de dados pessoais sensíveis, com o término do tratamento dos dados, com as atribuições do encarregado pelo tratamento dos dados pessoais, com a segurança e com o sigilo dos dados.

No Quadro 12 estão apresentadas as práticas, do domínio tratamento dos dados, para cada um dos níveis do modelo.

Quadro 12 – Domínio: Tratamento dos dados

Domínio: Tratamento dos dados	
Objetivos: atender as solicitações do titular dos dados e instituição competente quanto às informações referentes ao tratamento dos dados, consentimento realizado pelo titular dos dados e assegurar que os dados são bloqueados e/ou excluídos a pedido do usuário ou encerramento do contrato.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As atividades realizadas com os dados pessoais são monitoradas 1.2 As atividades realizadas com os dados corporativos são monitoradas 1.3 A instituição implementa políticas para o tratamento, consentimento e exclusão dos dados
Nível 2	2.1 As atividades para o tratamento, consentimento e exclusão dos dados são monitoradas e documentadas 2.2 As credenciais de acesso para o tratamento, consentimento e exclusão são emitidas para as pessoas e outras entidades que necessitam de acesso 2.3 As cláusulas para o consentimento do uso dos dados estão formalmente divulgadas e documentadas na instituição 2.4 As cláusulas para a exclusão do uso dos dados estão formalmente divulgadas e documentadas na instituição 2.5 As cláusulas para a finalidade do uso dos dados estão formalmente divulgadas e documentadas na instituição
Nível 3	3.1 Os processos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações fazem parte da gestão dos dados na instituição 3.2 As práticas seguras de desenvolvimento de *software* com o uso de dados pessoais e corporativos são patrocinadas pela alta direção 3.3. A alta administração fortalece a privacidade e a confiança no uso dos dados pessoais e corporativos 3.4 Os privilégios de acesso para o tratamento, consentimento e exclusão dos dados são revisados e atualizados periodicamente para assegurar sua validade

Domínio: Tratamento dos dados	
Objetivos: atender as solicitações do titular dos dados e instituição competente quanto às informações referentes ao tratamento dos dados, consentimento realizado pelo titular dos dados e assegurar que os dados são bloqueados e/ou excluídos a pedido do usuário ou encerramento do contrato.	
Nível	**Práticas**
	3.5 As tentativas irregulares de acesso para o tratamento, consentimento e exclusão dos dados são monitoradas por meio dos indicadores de eventos de SegCiber 3.6 Os requisitos de acesso incorporam princípios de privilégios mínimos e de separação de funções 3.7 A instituição implementa e documenta os mecanismos para o tratamento, consentimento e exclusão dos dados e informações classificadas como sensíveis

Fonte: O autor

2.2.2.1.7 Domínio "Organização da informação"

A informação é um recurso valorizado no nível operacional, tático e estratégico para a tomada de decisões, que deve ser protegida. Os objetivos do domínio são identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações.

Implementar e realizar as práticas de todos os níveis para o referido domínio demonstra um alinhamento com os artigos 5º, 7º, 8º, 9º, 11º, 12º, 14º, 17º, 23º, 25º, 31º, 32º, 33º, 46º e 47º da LGPD que versam sobre os requisitos para o tratamento de dados pessoais, o tratamento de dados pessoais sensíveis, os direitos do titular, as regras, a responsabilidade, a transferência internacional de dados, a segurança e o sigilo dos dados.

No Quadro 13 estão apresentadas as práticas, do domínio organização da informação, para cada um dos níveis do modelo.

Quadro 13 – Domínio: Organização da informação

Domínio: Organização da informação	
Objetivos: identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As fontes dos dados e informações são verificadas quanto à sua veracidade 1.2 A instituição implementa políticas para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações
Nível 2	2.1 As atividades para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são monitoradas 2.2 As atividades para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são documentadas 2.3 As partes interessadas para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são conhecidas formalmente
Nível 3	3.1 Os processos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações fazem parte da gestão dos dados na instituição 3.2 Os dados são identificados e classificados como estruturados e não estruturados 3.3 As práticas seguras para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são patrocinadas pela alta direção

Domínio: Organização da informação	
Objetivos: identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações.	
Nível	**Práticas**
	3.4 Os privilégios de acesso identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são revisados e atualizados periodicamente para assegurar sua validade 3.5 As partes interessadas que compartilham as informações são identificadas com base no interesse comum e no risco que podem apresentar para a instituição

Fonte: O autor

2.2.2.1.8 Domínio "Infraestrutura tecnológica"

Um aspecto importante para a SegCiber é reconhecer que a tecnologia deve tratar as ameaças e vulnerabilidades de forma integrada. Para o C2M2 (2014), é necessário o registro e monitoramento das atividades de TI para o desenvolvimento do conhecimento organizacional. O registro e monitoramento visa manter, analisar, alertar, apresentar e utilizar informações operacionais sobre a SegCiber.

Atender o objetivo e as práticas do domínio demonstra um alinhamento com os artigos 46º, 47º, 48º, 49º e 50º da LGPD, que abordam as questões relacionadas com a segurança, com o sigilo dos dados e com as boas prática de governança.

No Quadro 14 estão apresentadas as práticas, do domínio infraestrutura tecnológica, para cada um dos níveis do modelo.

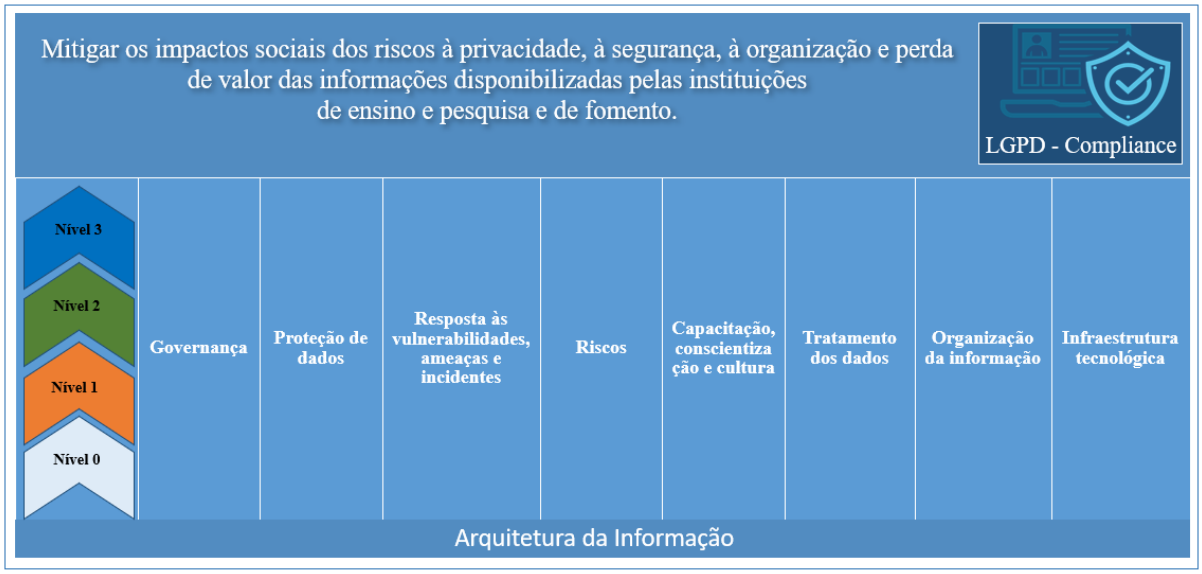
Quadro 14 – Domínio: Infraestrutura tecnológica

Domínio: Infraestrutura tecnológica	
Objetivos: realizar e monitorar as atividades operacionais.	
Nível	**Práticas**
Nível 0	Não tem práticas
Nível 1	1.1 As atividades de monitoramento da SegCiber são realizadas 1.2 Os ambientes operacionais são monitorados quanto ao comportamento irregular que pode indicar vulnerabilidades, ameaças e incidentes
Nível 2	2.1 Requisitos de monitoramento e análise dos eventos das vulnerabilidades, ameaças e incidentes são definidos 2.2 Alarmes e alertas são configurados para ajudar na identificação das vulnerabilidades, ameaças e incidentes 2.3 Indicadores de atividade irregular são definidos e monitorados em todo o ambiente operacional 2.4 As atividades de monitoramento estão alinhadas com o perfil da instituição
Nível 3	3.1 Os requisitos de monitoramento baseiam-se no risco da atividade 3.2 O monitoramento permanente é realizado em todo o ambiente operacional para identificar uma atividade irregular 3.3 Os indicadores de riscos são utilizados para identificar uma atividade irregular 3.4 Os alarmes e alertas são configurados com base nos indicadores de atividade irregular

Fonte: O autor

A Figura 14 apresenta a representação gráfica da estrutura do modelo proposto.

Figura 14 – Estrutura do modelo proposto



Fonte: O autor

2.3 ANÁLISE DOS IMPACTOS SOCIAIS DO *BIG DATA*

Esta seção apresenta uma análise dos impactos sociais do *Big Data* na privacidade, organização, segurança e perda de valor das informações.

A AI, definida como a arte e a ciência de estruturar e organizar sistemas de informação, segundo Bailey (2003), demanda a necessidade de identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar a informação no contexto do *Big Data*.

As instituições procuram tirar proveito do fenômeno do *Big Data*, no entanto, estão experimentando um novo paradigma no qual todos devem levar em consideração as questões relacionadas com proteção dos dados e informações disponíveis na era da informação.

A busca constante para mitigar as vulnerabilidades, ameaças e incidentes de SegCiber tem sido um desafio para a inovação e competitividade das instituições. O *Big Data* é uma realidade. A grande quantidade de dados e informações, provenientes das mais diversas fontes, gera uma preocupação com a privacidade, organização, segurança e valor da informação.

2.3.1 Riscos à privacidade

As potenciais perdas das informações confidenciais e de identificação pessoal, bem como o seu uso e divulgação não autorizada direcionam para uma avaliação subjetiva dos riscos à privacidade (FEATHERMAN; MIYAZAKI; SPROTT, 2010).

Nas transações *on-line*, tanto as realizadas no comércio eletrônico como as financeiras, os usuários identificam a falta de informações sobre a privacidade e a potencial perda de controle das informações confidenciais, como uma desvantagem para o uso desses serviços (BELANGER; HILLER; SMITH, 2002).

As empresas que fornecem serviços *on-line* têm a capacidade de coletar dados pessoais confidenciais de alto valor para explorá-los comercialmente (BELANGER; CROSSLER, 2011). Os autores afirmam que ocorrem perdas financeiras e de privacidade dos dados decorrentes do uso indevido das informações durante as transações *on-line*.

Segundo Milne e Culnan (2004), as vulnerabilidades que podem ser geradas nas transações *on-line* são as seguintes: i) os dados do seu computador podem ser comprometidos; ii) as transferências de dados *on-line* podem ser comprometidas; e iii) os dados coletados durante a transação podem ser comprometidos e divulgados sem autorização do usuário.

Para os autores, o risco à privacidade ocorre tanto durante a transação *on-line*, como também durante o armazenamento das informações do usuário, pelo fato das empresas não garantirem que os dados não serão compartilhados ou utilizados no ambiente do *Big Data* para a tomada de decisão.

A falta da privacidade das informações e a sua segurança não está restrita às empresas que realizam negócios *on-line*. Os dados obtidos pelos governos também estão sujeitos a esses riscos, tanto pela infraestrutura tecnológica desatualizada, como pela pouca cultura de SI nas instituições públicas.

2.3.2 Preocupação com a privacidade

No ambiente do *Big Data*, a informação trafega com velocidade. Moor (1997) afirma que a informação quando digitalizada trafega facilmente e rapidamente no ciberespaço, que é um ambiente resultante da interação de pessoas, *software* e serviços da Internet por meio de dispositivos tecnológicos e redes conectadas.

De acordo com o autor, as preocupações com a privacidade emergem quando a velocidade e conveniência fazem com que as informações pessoais tenham uma divulgação não autorizada.

As preocupações dos usuários não ficam restritas somente ao fato de ter uma divulgação não autorizada, mas o uso das informações pessoais e corporativas de forma inadequada e não autorizada também é uma preocupação.

O avanço das TIC, de acordo com Belanger e Crossler (2011), elevou o nível de preocupações com a privacidade das informações, motivando os pesquisadores de sistemas de informação a estudar soluções técnicas para tratar a informação.

Segundo Hong e Thong (2013), tem crescido a área de estudo da *Internet Privacy Concern* (Preocupação com a privacidade na Internet – tradução livre), em decorrência do grande volume de informações que estão sendo coletadas, armazenadas, transmitidas e publicadas na Internet, fomentando o ambiente do *Big Data*.

Nesse ambiente os usuários não ficam restritos à preocupação com a coleta dos dados realizadas pelas instituições, mas também pela forma de como os seus dados estão sendo utilizados.

As instituições devem adotar estratégias de coleta e uso dos dados dos usuários alinhadas com a LGPD. Diante da pesquisa realizada pelo Serasa *Experian*[6] (SE), realizada entre os meses de fevereiro e março de 2019, os usuários reconhecem que embora não se sintam seguros no espaço cibernético, tem intenção de continuar ou passar a disponibilizar seus dados pessoais e corporativos nas plataformas *on-line*.

No contexto da personalização das plataformas *on-line* observa-se, segundo Taylor *et al.* (2009) que quanto menor o nível de controle informacional, maior é o nível de preocupação com a privacidade, que leva a um cenário de falta de confiança nos serviços *on-line*.

2.3.3 Disposição para fornecer informações *on-line*

O processo para descobrir padrões de consumo e conhecimento tem tornado a mineração de dados um instrumento de destaque para que as empresas obtenham maior entendimento dos negócios e mercado a partir da análise dos dados minerados no *Big Data*, proporcionando o desenvolvimento de produtos alinhados às necessidades dos usuários. (PROVOST; FAWCETT, 2013).

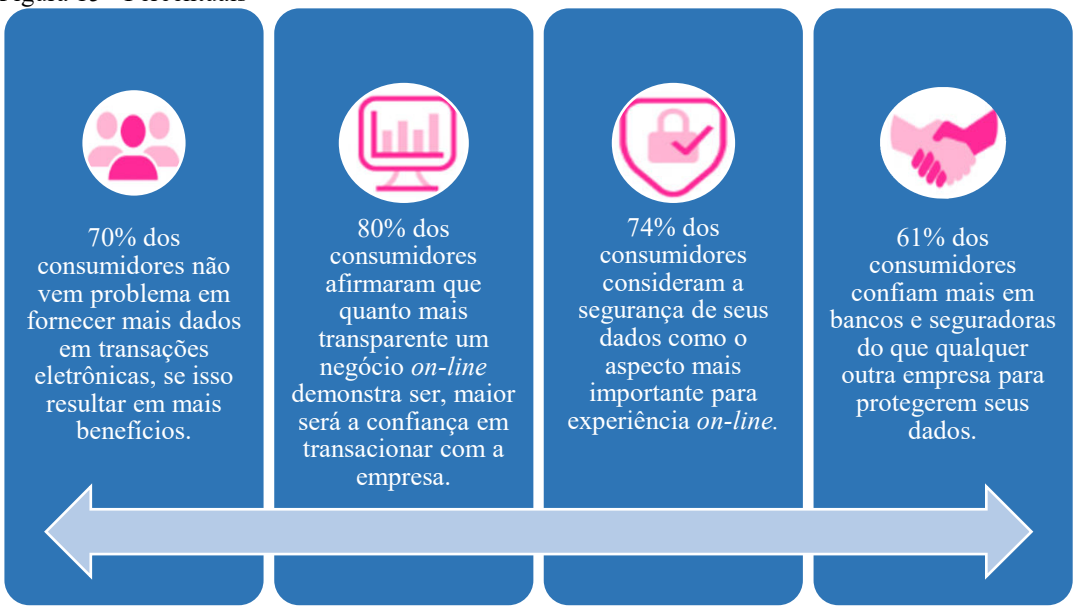
Porém, na visão do usuário, fornecer informações com base nas suas necessidades e desejos específicos, poderá levar a uma possível perda de privacidade (CHELLAPPA; SIN, 2005). A preocupação com a privacidade afeta negativamente a confiança dos usuários nos serviços tecnológicos *on-line* e, consequentemente, a disposição de fornecer suas informações pela Internet (MARTINS, 2016).

[6] Serasa *Experian*: empresa líder em serviços de informações. No Brasil, é sinônimo de solução para todas as etapas do ciclo de negócios e oferece os relatórios mais precisos e eficazes do mercado. https://www.serasaexperian.com.br

Os usuários desejam segurança e conveniência nos serviços *on-line* disponibilizados no espaço cibernético. Quanto maior a confiança que os usuários têm em uma marca e/ou instituição, mais predispostas estarão para compartilhar informações pessoais e corporativas.

A Figura 15 apresenta percentuais relacionados com: i) disponibilidade do usuário em fornecer dados nas transações eletrônicas; ii) relação de confiança e transparência nos negócios *on-line*; iii) segurança dos dados; e iv) empresas mais confiáveis com modelos de negócios *on-line*.

Figura 15 - Percentuais



Fonte: Serasa *Experian* - Pesquisa de Fraude e Identidade - (2019)

2.3.4 As contradições dos usuários

Martins (2016), na discussão dos resultados da sua pesquisa sobre privacidade e confiança, ressalta que apesar dos usuários acreditarem que fornecer informações pessoais na Internet gera riscos, eles encaram que os benefícios compensam. Apesar das profundas preocupações dos usuários com questões de privacidade e segurança, diariamente os usuários publicam dados nas suas redes sociais.

Segundo Schoenbachler e Gordon (2002), a possibilidade de os usuários fornecerem informações pessoais *on-line* depende do tipo da informação. Os usuários têm mais restrição para informar dados financeiros em comparação com os seus dados demográficos ou de consumo.

A perspectiva de perdas de privacidade e uso indevido de informações no ambiente do *Big Data*, que contempla, por exemplo, o comércio eletrônico, redes sociais, *Internet Banking*, dados do cidadão de posse dos governos, provedores de Internet e seguradoras podem

influenciar a disposição do usuário em fornecer seus dados (FEATHERMAN; MIYAZAKI; SPROTT, 2010).

Para ter acesso aos serviços *on-line* gratuitos e revolucionários, os usuários concordam em fornecer suas informações sem uma avaliação dos riscos. Os usuários pagam por esses serviços com o que tem de mais precioso: dados pessoais e o seu comportamento no universo *on-line*.

A monetização de dados pessoais e corporativos é um novo modelo de negócio presente na era da informação. Os efeitos da TI estão no dia a dia da sociedade, dominando as suas vidas e instituições de formas que elas não imaginam.

2.3.5 Ética

Questões éticas devem ser consideradas no atual cenário do *Big Data*, tais como: Qual a fronteira para o uso dos dados produzidos pelas pessoas no seu dia a dia, com as novas tecnologias? Eles podem ser acessados em tempo real? Por quem? Para que finalidade?

O volume de dados cresce de forma exponencial com a evolução e sofisticação da rede mundial de computadores e de suas aplicações. Todo o potencial de conhecimento obtido com a coleta, processamento, armazenamento e análise dos dados pode ser utilizado a favor da sociedade.

Por outro lado, os dados podem ser utilizados pelos governos para o controle do cidadão com objetivos políticos, ou pelas empresas privadas para direcionar um determinado padrão de consumo.

Um caso clássico do uso de *Big Data* que teve repercussão na mídia sobre a conduta ética da empresa envolvida no episódio foi a iniciativa da rede varejista norte americana *Target*, que tentou alterar os hábitos de consumo de consumidoras de sua rede, por meio de técnicas estatísticas que identificavam a possibilidade de determinada consumidora estar grávida (DAVIS, 2012). Tal fato representa a aplicação de técnicas associadas ao *Big Data* com implicações éticas e jurídicas.

Azevedo *et al*. (2014), destacam que é necessário que o usuário tenha maior controle sobre quem pode acessar seus dados e qual o uso que as empresas estão fazendo desses dados. No entanto, o tema demanda regulamentações que estabeleçam padrões de identificação e de segurança dos dados pessoais.

Um antídoto para condutas antiéticas no ambiente do *Big Data* pode estar disponível no próprio conjunto de normas e regulamentos das empresas, os quais estabelecem um conjunto de valores, e esclarecem que os colaboradores devem ter confiança e responsabilidade pessoal no processo de análise dos dados (DIAS; VIEIRA, 2013).

As empresas estão experimentando um novo paradigma no qual todos devem levar em consideração questões como a privacidade, a transparência, o rastreamento e como estão sendo utilizados os dados pessoais e corporativos.

Sendo assim, emerge a necessidade crescente de implementar proteções éticas que assegurem a privacidade e segurança dos dados.

2.3.6 Organização da informação

Segundo Menezes (2006), a organização da informação surgiu como uma subárea da CI, dedicada para o estudo das formas de organização da informação, utilizando os mecanismos AI para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os conteúdos informacionais.

A organização da informação surge para propor soluções práticas para o acesso à informação relevante com as demandas e necessidades informacionais dos usuários, por meio de técnicas, métodos e práticas para assegurar a eficácia e segurança nos processos que envolvam a gestão, produção, acesso e uso da informação.

A falta de métodos, ferramentas e mecanismos para organizar a informação impactam negativamente nos processos de recuperação de informações. O fenômeno da recuperação da informação teve início com a escrita. Quando o usuário passou a utilizar registro em suportes documentais passou a desenvolver processos de armazenamento, organização e recuperação futura.

As repetidas ameaças cibernéticas nas instituições de todos os setores, tipos e tamanhos indicam a necessidade da implementação de práticas, métodos e processos relacionados com a organização da informação armazenada no *Big Data*.

Na perspectiva da CI a gestão da informação relaciona-se com o fluxo dos ativos de informação, os quais tem um ciclo contínuo de coleta, tratamento, armazenamento, distribuição e uso para tomada de decisão (BEAL, 2005).

Os processos que envolvem o fluxo dos ativos de informação devem modelar os sistemas de informação pautados nos princípios da SI para assegurar a confidencialidade, integridade e disponibilidade.

2.3.7 Riscos à segurança das informações

A preocupação com a gestão adequada da informação no ambiente do *Big Data* envolve o espaço cibernético, que para o autor Killmeyer (2006), é um ambiente propício para a exposição ao risco, no qual estão os ativos de informação, os meios de armazenamento, transmissão e processamento dos sistemas de informação.

Os projetos de *Big Data* trabalham com um grande volume de dados provenientes de diversas fontes, que demandam cuidados com a segurança. O armazenamento de um grande volume de dados pode se transformar em alvo de ataques e vazamento de informações sigilosas, o que pode gerar perdas de credibilidade para a instituição.

Para se proteger as instituições devem implementar soluções e boas práticas de SI, adequar-se às normas e leis, definir políticas, controlar o acesso às informações críticas, e capacitar as equipes de TI.

Em uma época que os usuários estão mais informados sobre os riscos de oferecer seus dados a uma instituição com serviços *on-line*, uma política de SI representa um diferencial de competitividade. A SI deve ser encarada como um valor agregado para produtos e serviços.

Os métodos tradicionais usados para proteger os sistemas de informações contra ameaças de segurança incluem a implementação de *firewalls*[7], regras de autenticação e o uso de redes privadas virtuais (AL-SHAWI, 2011). Para o autor, cada uma dessas técnicas tem suas próprias vulnerabilidades e limitações e podem não ter capacidade de proteger os recursos de ataques cibernéticos.

Os atacantes coletam e monitoram continuamente os dados dos usuários e as redes governamentais e privadas para tirar vantagem de fraquezas do sistema resultantes de falhas no *design*, na implementação de medidas de segurança e baixo nível de maturidade para a organização da informação.

O risco de fraude é uma ameaça crescente. Segundo a pesquisa *2019 – Global Identy and Fraud Report* realizada pelo SE, 2 (dois) de 5 (cinco) usuários que fazem uso de serviços *on-line* relatam que experimentaram um evento fraudulento no espaço cibernético. Já para as

[7] *Firewall*: é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída. Implementa regras para autorizar ou bloquear tráfegos específicos com base em um conjunto de regras de SI.

instituições pesquisadas, 55% delas relatam um aumento das perdas relacionadas a fraudes *on-line* em 2018.

Dada a centralidade do tema de cibersegurança na era da informação, é notório que o referido assunto tem impactos diretos na sociedade. Entre os impactos relacionados com o vazamento de dados ou ataques cibernéticos destacam-se as perdas financeiras, crise na imagem da instituição e/ou marca, insatisfação dos usuários e desengajamento dos colaboradores.

2.3.8 Valor das informações

No ano de 2018 aumentou o foco para a proteção de dados quando se descobriu que os dados de 87 milhões de usuários do *Facebook* foram utilizados para traçar perfis de comportamento e influenciar politicamente os usuários na eleição americana, e o plebiscito que separou o Reino Unido da União Europeia.

Em setembro de 2018, o *Facebook* descobriu um ataque *hacker* que alcançou 50 milhões de usuários em todo o mundo. Diante do fato, vários usuários tiveram os perfis desconectados. Uma nova falha aconteceu em dezembro, a qual possibilitou a exposição das imagens postadas por 6,8 milhões de usuários.

O *The New York Times* revelou na sua edição do mês de dezembro de 2018, que o *Facebook* forneceu, sem autorização, dados de usuários a empresas como *Microsoft*, *Netflix*, *Spotify*, *Amazon* e *Yahoo*. As autorizações davam acesso às mensagens privadas. Segundo a reportagem, as empresas podiam ler, escrever e apagar as mensagens, além de ver todos os participantes em um tópico. A reportagem não detalha como isso era feito.

Onde meus dados foram parar? No caso da *Cambridge Analytica*[8] (CA), 300 mil pessoas foram pagas para participar de um teste de personalidade e fornecer seus dados. Porém elas foram usadas para coletar dados de outros, com isso foi possível criar um banco de dados com 87 milhões de pessoas, que não tinham ideia de que estariam envolvidas em campanhas políticas e outras atividades.

No ambiente do *Big Data* existe uma fatia considerável de usuários que não se importa em fornecer seus dados nas redes sociais, mas não aceita que seus dados sejam usados como produtos para vender mensagens com as quais não concordam.

“ Você é o produto: preocupe-se com o que fazem com seus dados! “

[8]*Cambridge Analytica*: criada em 2013 como parte da *Strategic Communication Laboratories Group* (SCL) e atua como um serviço de análise de dados para fins comerciais ou políticos.

O GDPR regulamenta os direitos dos usuários no que diz respeito à proteção e controle de seus dados pessoais. Com isso, as pessoas têm direito de saber se seus dados serão usados para gerar propagandas, se as informações serão geradas para criar perfis ou se as empresas que coletam dados vendem ou venderão esses dados a terceiros.

A LGPD estabelece uma série de regras que empresas e outras instituições atuantes no Brasil devem seguir para permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

A perda de informações tem impactos financeiros tangíveis e intangíveis para a instituição. Os custos intangíveis incluem: perda de credibilidade, impactos na imagem da empresa perante o mercado, transgressões regulatórias que afetam a competitividade e valor das informações.

2.4 IMPORTÂNCIA DA PRIVACIDADE, DA ORGANIZAÇÃO, DA SEGURANÇA E DO VALOR DAS INFORMAÇÕES

Esta seção identifica as questões relacionadas com a importância da privacidade, da organização, da segurança e do valor das informações para as instituições e os usuários.

2.4.1 Para as instituições

A pesquisa global da *PricewaterhouseCoopers* (PwC, 2018)[9] entrevistou líderes de instituições, que apontaram que são claros os riscos de ataques cibernéticos às tecnologias emergentes. O foco da pesquisa analisou como as instituições estão atuando nas questões relacionadas com os seguintes itens:

- Riscos de cibersegurança associados às novas tecnologias; e
- Privacidade e proteção de dados na era da informação.

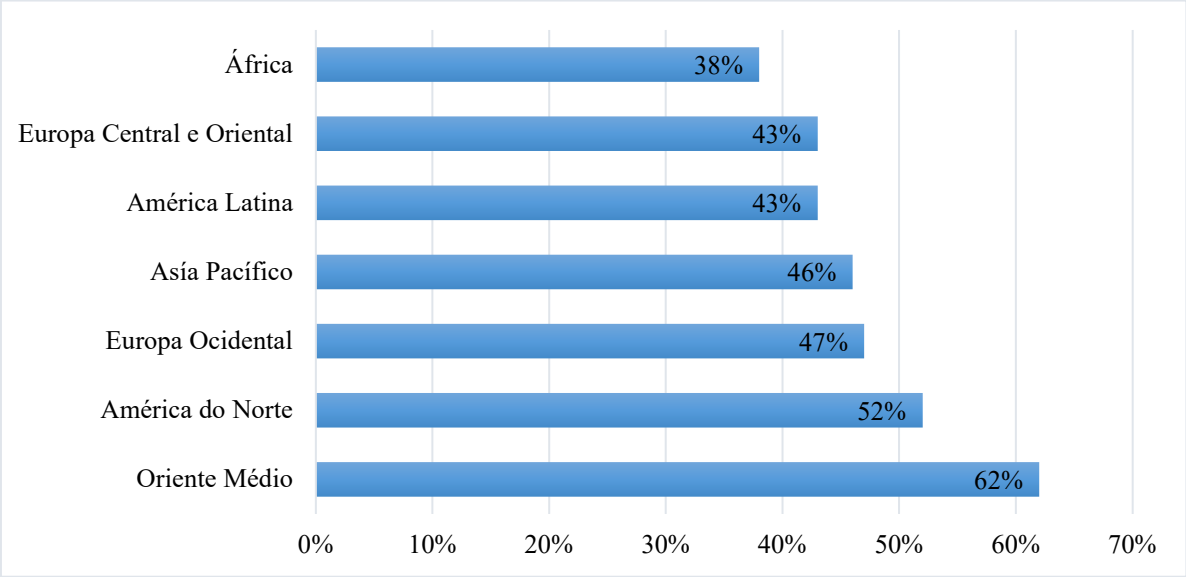
Os entrevistados reconhecem que um ciberataque de sucesso aos sistemas automatizados ou robotizados pode ter consequências como: perda de operações, perda de dados, perda da qualidade da produção e danos à propriedade física.

Na pesquisa, os entrevistados afirmaram que, entre as maiores ameaças à proteção da privacidade, estão os *hackers* e novas tecnologias como inteligência artificial, a aprendizagem de máquina e a Internet das Coisas (IoT).

[9]*PricewaterhouseCoopers*: empresa especializada em consultoria, trabalha com tecnologias que permitem a análise de dados para reconstruir fatos em processos de auditoria para tomada de decisão. *Cybersecurity and Privacy*. *Revitalizing privacy and trust in a data-driven world*. https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

Segundo a pesquisa, os gestores estão desenvolvendo a confiança na relação com seus usuários com base nos investimentos de larga escala em cibersegurança. O Gráfico 1 apresenta o percentual de investimento em TIC realizado pelas instituições nas questões de cibersegurança por região.

Gráfico 1 – Percentual de investimento em cibersegurança



Fonte: *PwC* – Pesquisa Anual com CEO´s (2018)

Para os líderes globais, participantes da pesquisa, priorizar a governança de dados é essencial para a competitividade. O uso de dados das formas mais inovadoras leva a mais oportunidades de negócio, no entanto, aumenta os riscos.

As instituições devem ter capacidade de equilibrar o uso de dados com controles de proteção e detecção que minimizem os riscos. Um ponto de partida para desenvolver uma estrutura de governança de dados é uma conscientização dos colaboradores sobre as atividades de coleta e retenção de dados em conformidade com a legislação.

A pesquisa aponta que 70% das empresas com valor de mercado superior a 25 bilhões de dólares têm uma estratégia de SI, 69% tem programas de treinamento para os colaboradores em políticas e práticas de privacidade e 68% limitam a coleta, a retenção e o acesso a dados pessoais ao mínimo necessário.

2.4.2 Para os usuários

A pesquisa realizada pelo *Centre for International Governance Innovation* (CIGI), entre dezembro de 2018 e fevereiro de 2019[10], apresenta os seguintes pontos relevantes:

[10] *Centre for International Governance Innovation*. Pesquisa realizada em 23 (vinte e três) países: África do Sul, Alemanha, Austrália, Brasil, Canadá, Estados Unidos da América, França, Grã-Bretanha, Hong Kong (China), Índia, Indonésia, Itália, Japão, México, Nigéria, Paquistão,

- Oito em de cada dez usuários estão preocupados com a sua privacidade *on-line*;
- A preocupação maior está entre os usuários dos países em desenvolvimento;
- Um em cada cinco usuários menciona que está com menos confiança para navegar na Internet, em virtude de um possível vazamento dos seus dados e monitoramento do seu comportamento digital; e
- Aumento do paradoxo do uso de serviços *on-line* gratuitos em troca do cadastro dos dados pessoais e corporativos.

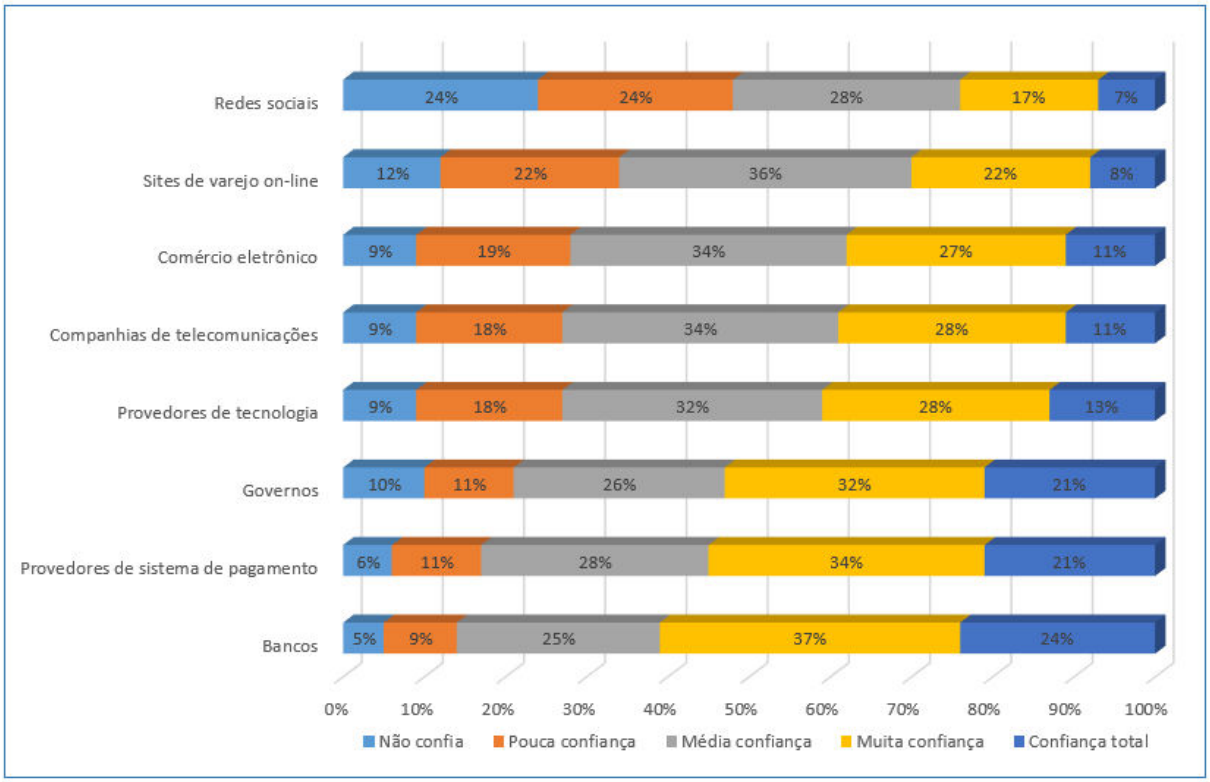
Os usuários afirmam que os criminosos cibernéticos são o principal fator para o aumento da preocupação com a sua privacidade *on-line* no ambiente do *Big Data*. Entre os usuários participantes da pesquisa os de *Hong Kong* (China) são os com maior percentual de preocupação com a privacidade *on-line*. No Brasil, 40% dos usuários estão relativamente preocupados, 42% estão muito preocupados e 82% estão totalmente preocupados.

No que pese o elevado percentual de preocupação dos usuários brasileiros, o levantamento do SE (2019) aponta que 75% dos brasileiros desconhecem a LGPD, que entrará em vigor em 2020, e transformará a forma como as instituições terão que atuar na condução do tratamento de dados pessoais no ciberespaço, visando um grau de proteção de dados pessoais adequado.

Os usuários esperam uma experiência cibernética segura e conveniente. O Gráfico 2 apresenta a percepção de confiança do usuário referente à coleta, uso e armazenamento dos dados pessoais por instituições com serviços *on-line*.

Peru, Polônia, Quênia, República da Coreia, Rússia, Suécia e Tunísia, com a participação de 25.229 usuários da Internet. https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf

Gráfico 2 – Percentual de confiança do usuário



Fonte: Serasa *Experian* - Pesquisa de Fraude e Identidade - (2019)

Já o Gráfico 3 apresenta os percentuas de confiança dos usuários participantes da pesquisa do CIGI (2019) em relação à confiança nos serviços *on-line* disponibilizados pelos governos dos seus países.

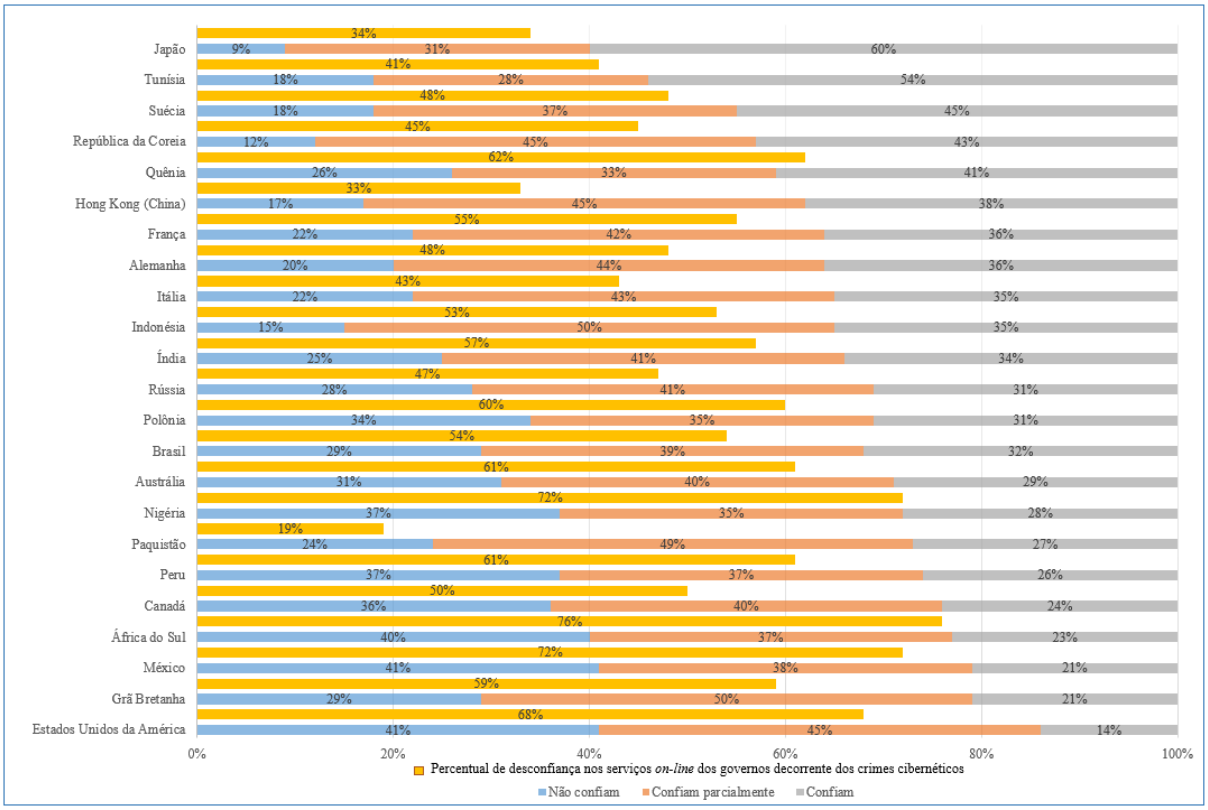
Segundo a pesquisa, entre os usuários dos EUA, 41% não confiam nos serviços *on-line* do governo do seu país. No Brasil, 29% não confiam, 39% confiam parcialmente e 32% confiam nos serviços *on-line* do governo. O Japão é o país com maior percentual de confiança dos usuários nos serviços *on-line* disponibilizados pelo governo, com um percentual de 60% de confiança.

O referido gráfico também apresenta o percentual de desconfiança dos usuários nos serviços *on-line* dos governos decorrente dos crimes cibernéticos. O fato dos americanos terem pouca confiança nos serviços *on-line* do governo tem relação com o elevado percentual de desconfiança decorrente dos crimes cibernéticos no país, conforme apresentado na pesquisa: 68%.

No Brasil o percentual de desconfiança decorrente dos crimes cibernéticos é de 54%, estando na mesma faixa percentual que a França, Grã-Bretanha, Indonésia, Índia e Canadá. A pesquisa aponta que do total de países pesquisados 14 (quatorze) estão com grau de

desconfiança decorrentes dos crimes cibernéticos acima de 50%, ou seja, 61% dos países tem elevado grau de desconfiança.

Gráfico 3 – Percentual de confiança do usuário nos serviços *on-line* dos governos



Fonte: CIGI (2019) – Adaptado pelo autor

2.5 RESULTADOS

Os modelos de maturidade são úteis para orientar uma organização no desenvolvimento de processos a um estado de maturidade na área para a qual o modelo foi desenvolvido (WEBER *et al*., 1993).

Um modelo de maturidade funciona como um guia para a organização conhecer o seu estado atual e realizar um plano de melhoria, na busca da excelência (OLIVEIRA, 2006).

Este trabalho fundamenta-se na hipótese de que as instituições de ensino, de pesquisa e de fomento, inseridas no ambiente do *Big Data*, devem conhecer o seu nível de maturidade da AI, para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a organização e segurança das informações, com a perda de valor das informações, bem como o alinhamento com a LGPD.

A cada dia o virtual está mais presente na sociedade da informação. Nas instituições de ensino, de pesquisa e de fomento, não é diferente. Diante disso, fica claro que a aplicação de

mecanismos para assegurar a privacidade, a organização, a SI e fortalecer o seu valor, reduzindo sua exposição ao risco, possibilita a criação de uma vantagem competitiva.

A aplicação do modelo proposto, nas instituições, como um instrumento de autoavaliação irá:

- Preservar as informações científicas das propostas submetidas à instituição;
- Manter a privacidade das informações pessoais nas instituições de ensino, de pesquisa e de fomento;
- Garantir a confidencialidade, integridade e disponibilidade das informações dos projetos e práticas científicas;
- Preservar a propriedade intelectual das pesquisas científicas;
- Organizar as informações da instituição visando a sua integridade;
- Facilitar o acesso e o uso às informações;
- Proporcionar comunicação mais efetiva;
- Ter processos bem definidos e controlados para a produção de informações científicas; e
- Incorporar cibersegurança e privacidade nas decisões e nos processos organizacionais.

O modelo visa fortalecer os fundamentos para:

- Avaliar e priorizar os componentes fundamentais em cibersegurança e privacidade;
- Desenvolver uma estratégia, capacidades e processos para combater as vulnerabilidades, ameaças e incidentes de SegCiber;
- Monitorar e responder a vulnerabilidades, ameaças e incidentes de SegCiber;
- Incorporar a segurança e proteção de dados nas operações da instituição; e
- Assegurar o alinhamento com a LGPD.

2.5.1 Autoavaliação

O nível de maturidade da AI das instituições de ensino, de pesquisa e de fomento pode ser realizado por meio de um questionário, estruturado com base nos domínios, objetivos e práticas estabelecidas no modelo proposto.

As perguntas que fazem parte do questionário estão separadas por níveis. A instituição terá alcançado determinado nível se atender todas as práticas estabelecidas para aquele nível.

2.5.1.1 Questionário para a autoavaliação

A aplicação do questionário tem como escopo realizar a aplicação do modelo e colher sugestões dos participantes para melhoria do modelo proposto. Para Fonseca (2002), o questionário, como instrumento de pesquisa, permite a obtenção de dados ou informações sobre as características ou as opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo.

O Quadro 15 apresenta estrutura do questionário para a autoavaliação.

Quadro 15 – Questionário do modelo de maturidade da AI

Questionário do Modelo de Maturidade da Arquitetura da Informação

O questionário visa avaliar a maturidade da Arquitetura da Informação da instituição. Um modelo de maturidade fornece um ponto de referência para uma organização conhecer o nível de maturidade de suas práticas, processos e métodos para, então, definir metas e prioridades de melhoria.

Este questionário, que é parte da minha Tese de Doutorado, permite que os gestores da instituição realizem uma autoavaliação, tendo como base os domínios, objetivos e práticas do Modelo de Maturidade da Arquitetura da Informação que desenvolvi para mitigar os impactos sociais dos riscos à privacidade, à organização, à segurança, e perda de valor das informações disponibilizadas pelas instituições de ensino, de pesquisa, de fomento, da Administração Pública Federal, da Administração Pública Estadual e privadas.

O autor compromete-se a manter a privacidade, confidencialidade e sigilo em relação à identificação das organizações e dos gestores que participarem da pesquisa.

Dados iniciais (Marque mais de uma se for necessário)

Sua instituição é:

( ) De ensino ( ) Administração Pública Federal

( ) De pesquisa ( ) Administração Pública Estadual

( ) De Fomento ( ) Empresa Privada

Este espaço é opcional:

Nome da sua organização: _____

Seu nome: _____E-mail: _____

1 - Domínio: Governança

Objetivos: definir e implementar uma estratégia e estrutura de governança de privacidade dos dados, integrada à governança corporativa.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 A instituição tem uma estratégia de alinhamento da governança de privacidade dos dados com a governança corporativa?	☐	☐	☐

1.2. A instituição fornece os recursos necessários para implementar a governança de privacidade dos dados?	☐	☐	☐
2.1 A instituição tem uma estratégia documentada do alinhamento da governança de privacidade dos dados com a governança corporativa?	☐	☐	☐
2.2 A estratégia e as prioridades para as atividades de governança de privacidade dos dados são documentadas e alinhadas com os objetivos estratégicos e de risco da instituição?	☐	☐	☐
2.3 A instituição tem planos de respostas a incidentes para continuidade do negócio alinhados com as atividades de SegCiber?	☐	☐	☐
2.4 A instituição tem uma estrutura organizacional de SegCiber, com políticas e salvaguardas adequadas para mitigar os impactos e riscos à privacidade?	☐	☐	☐
3.1 A estratégia e estrutura são atualizadas para refletir as mudanças do setor de atuação, as mudanças no ambiente operacional e as mudanças no perfil de ameaças?	☐	☐	☐
3.2 As atividades de SegCiber são orientadas por políticas e diretrizes organizacionais?	☐	☐	☐
3.3 A instituição implementa e documenta os mecanismos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações?	☐	☐	☐
3.4 A alta administração patrocina o desenvolvimento e manutenção de políticas de proteção dos dados?	☐	☐	☐

2 - Domínio: Proteção de dados

Objetivos: assegurar a proteção dos dados contra acessos não autorizados. Gerenciar as ações de destruição acidental ou ilícita dos dados e comunicação inadequada com o uso dos dados.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As identidades são provisionadas para pessoas e outras entidades que necessitam de acesso?	☐	☐	☐
1.2 As credenciais de acesso são emitidas para pessoas e outras entidades que necessitam de acesso?	☐	☐	☐
1.3 As credenciais de acesso que não são mais necessárias são revogadas?	☐	☐	☐
2.1 Os repositórios de identidades são periodicamente revisados e atualizados para assegurar a validade do acesso?	☐	☐	☐
2.2 As credenciais de acesso são revisadas periodicamente para assegurar que estão associadas a pessoas ou entidades corretas?	☐	☐	☐
2.3 As credenciais de acesso são revogadas dentro de limites de tempo definidos pela instituição e legislação vigente?	☐	☐	☐
2.4 As ações de destruição acidental ou ilícita dos dados são documentadas?	☐	☐	☐
2.5 As solicitações de acesso são revisadas e aprovadas pelo proprietário do recurso?	☐	☐	☐
3.1 Os requisitos das credenciais de acesso são estabelecidos considerando os critérios de risco da instituição?	☐	☐	☐

3.2 Os privilégios de acesso são revisados e atualizados periodicamente para assegurar sua validade?	☐	☐	☐
3.3 O acesso aos ativos é concedido pelo proprietário do ativo com base nos critérios de risco estabelecidos para realizar a atividade?	☐	☐	☐
3.4 As tentativas irregulares de acesso são monitoradas por meio dos indicadores de eventos de SegCiber?	☐	☐	☐
3.5 Os requisitos de acesso incorporam princípios de privilégios mínimos e de separação de funções?	☐	☐	☐
3.6 Os privilégios de acesso administrativo, acesso de emergência e contas compartilhadas têm controle e monitoramento adicionais?	☐	☐	☐
3.7 A instituição implementa e documenta os mecanismos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações classificadas como sensíveis?	☐	☐	☐

3 - Domínio: Resposta às vulnerabilidades, ameaças e incidentes

Objetivos: gerenciar e responder às vulnerabilidades, ameaças e incidentes relacionados aos ativos de informação.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As fontes de informação para apoiar as atividades de gestão de vulnerabilidades, ameaças e incidentes são identificadas?	☐	☐	☐
1.2 As informações sobre vulnerabilidades, ameaças e incidentes são internalizadas e interpretadas?	☐	☐	☐
1.3 As vulnerabilidades, ameaças e incidentes são controladas e monitoradas?	☐	☐	☐
2.1 As vulnerabilidades, ameaças e incidentes são identificadas, analisadas e tratadas conforme prioridade estabelecida?	☐	☐	☐
2.2 O impacto operacional para implementação de uma correção de SegCiber é avaliado antes da sua implementação?	☐	☐	☐
2.3 As vulnerabilidades, ameaças e incidentes são adicionadas ao registro de riscos da instituição?	☐	☐	☐
2.4 As características das vulnerabilidades, ameaças e incidentes são registradas e documentadas?	☐	☐	☐
3.1 As avaliações das vulnerabilidades, ameaças e incidentes são realizadas com uma periodicidade estabelecida pela organização?	☐	☐	☐
3.2 As avaliações das vulnerabilidades, ameaças e incidentes seguem os critérios de risco da organização?	☐	☐	☐
3.3 As avaliações das vulnerabilidades, ameaças e incidentes são realizadas por equipes independentes da atividade de operação?	☐	☐	☐
3.4 A análise e priorização das vulnerabilidades, ameaças e incidentes seguem os critérios de risco da organização?	☐	☐	☐
3.5 As informações sobre vulnerabilidades, ameaças e incidentes são adicionadas ao registro de riscos da organização?	☐	☐	☐

3.6 As atividades de monitoramento de risco validam as respostas às vulnerabilidades, ameaças e incidentes?	☐	☐	☐

4 - Domínio: Riscos

Objetivos: analisar os riscos e impactos à privacidade dos dados.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As práticas de gestão de risco são aprovadas pela alta administração?	☐	☐	☐
1.2 As práticas de gestão de risco são estabelecidas como políticas da instituição?	☐	☐	☐
1.3 Os riscos de SegCiber são identificados?	☐	☐	☐
2.1 Os riscos e impactos à privacidade dos dados identificados são documentados?	☐	☐	☐
2.2 Os riscos e impactos à privacidade dos dados identificados são analisados para priorizar as atividades de resposta conforme a estratégia e estrutura de governança de privacidade de dados?	☐	☐	☐
2.3 Os riscos identificados são monitorados conforme a estratégia de gestão de riscos?	☐	☐	☐
2.4 A análise de risco é realizada na arquitetura de rede?	☐	☐	☐
3.1 As avaliações dos riscos são realizadas com uma periodicidade estabelecida pela organização?	☐	☐	☐
3.2 As avaliações dos riscos são realizadas por equipes independentes da atividade de operação?	☐	☐	☐
3.3 A análise e priorização dos riscos seguem os critérios de gestão de riscos da instituição?	☐	☐	☐
3.4 As informações sobre os riscos são adicionadas ao registro de riscos da instituição?	☐	☐	☐

5 - Domínio: Capacitação, conscientização e cultura de proteção de dados

Objetivos: disseminar e implementar a cultura de proteção dos dados na instituição.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As responsabilidades para as atividades de proteção dos dados são identificadas?	☐	☐	☐
1.2 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados são realizadas?	☐	☐	☐
2.1 Os objetivos das atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados são estabelecidos e mantidos?	☐	☐	☐
2.2 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados incluem oportunidades de educação permanente de desenvolvimento profissional dos colaboradores?	☐	☐	☐
2.3 O treinamento nas atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção de dados é um requisito para concessão de acesso aos ativos sensíveis da instituição?	☐	☐	☐
2.4 O conteúdo das atividades de capacitação e conscientização para disseminar e implementar a	☐	☐	☐

cultura de proteção de dados é baseado no perfil das vulnerabilidades, ameaças e incidentes?			
3.1 A instituição tem formalmente um *Data Protection Officer* (DPO)?	☐	☐	☐
3.2 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados estão alinhadas com as atividades operacionais da organização?	☐	☐	☐
3.3 A eficácia das atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados é avaliada com uma periodicidade estabelecida pela instituição e melhorias são implementadas, conforme a necessidade?	☐	☐	☐
3.4 As atividades de capacitação e conscientização para disseminar e implementar a cultura de proteção dos dados e os requisitos de trabalho são revisados e atualizados conforme a necessidade?	☐	☐	☐
3.5 A cultura de proteção dos dados faz parte dos critérios de avaliação de desempenho profissional?	☐	☐	☐

6 - Domínio: Tratamento dos dados

Objetivos: atender as solicitações do titular dos dados e instituição competente quanto às informações referentes ao tratamento dos dados, consentimento realizado pelo titular dos dados e assegurar que os dados são bloqueados e/ou excluídos a pedido do usuário ou encerramento do contrato.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As atividades realizadas com os dados pessoais são monitoradas?	☐	☐	☐
1.2 As atividades realizadas com os dados corporativos são monitoradas?	☐	☐	☐
1.3 A instituição implementa políticas para o tratamento, consentimento e exclusão dos dados?	☐	☐	☐
2.1 As atividades para o tratamento, consentimento e exclusão dos dados são monitoradas e documentadas?	☐	☐	☐
2.2 As credenciais de acesso para o tratamento, consentimento e exclusão são emitidas para as pessoas e outras entidades que necessitam de acesso?	☐	☐	☐
2.3 As cláusulas para o consentimento do uso dos dados estão formalmente divulgadas e documentadas na instituição?	☐	☐	☐
2.4 As cláusulas para a exclusão do uso dos dados estão formalmente divulgadas e documentadas na instituição?	☐	☐	☐
2.5 As cláusulas para a finalidade do uso dos dados estão formalmente divulgadas e documentadas na instituição?	☐	☐	☐
3.1 Os processos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, distribuir e usar os dados e informações fazem parte da gestão dos dados na instituição?	☐	☐	☐

3.2 As práticas seguras de desenvolvimento de *software* com o uso de dados pessoais e corporativos são patrocinadas pela alta direção?	☐	☐	☐
3.3. A alta administração fortalece a privacidade e a confiança no uso dos dados pessoais e corporativos?	☐	☐	☐
3.4 Os privilégios de acesso para o tratamento, consentimento e exclusão dos dados são revisados e atualizados periodicamente para assegurar sua validade?	☐	☐	☐
3.5 As tentativas irregulares de acesso para o tratamento, consentimento e exclusão dos dados são monitoradas por meio dos indicadores de eventos de SegCiber?	☐	☐	☐
3.6 Os requisitos de acesso incorporam princípios de privilégios mínimos e de separação de funções?	☐	☐	☐
3.7 A instituição implementa e documenta os mecanismos para o tratamento, consentimento e exclusão dos dados e informações classificadas como sensíveis?	☐	☐	☐

7 - Domínio: Organização da informação

Objetivos: identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As fontes dos dados e informações são verificadas quanto à sua veracidade?	☐	☐	☐
1.2 A instituição implementa políticas para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações?	☐	☐	☐
2.1 As atividades para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são monitoradas?	☐	☐	☐
2.2 As atividades para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são documentadas?	☐	☐	☐
2.3 As partes interessadas para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são conhecidas formalmente?	☐	☐	☐
2.4 A instituição tem uma estrutura organizacional de SegCiber, com políticas e salvaguardas adequadas para mitigar os impactos e riscos à privacidade?	☐	☐	☐
3.1 Os processos para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações fazem parte da gestão dos dados na instituição?	☐	☐	☐
3.2 Os dados são identificados e classificados como estruturados e não estruturados?	☐	☐	☐
3.3 As práticas seguras para identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são patrocinadas pela alta direção?	☐	☐	☐

3.4 Os privilégios de acesso identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar os dados e informações são revisados e atualizados periodicamente para assegurar sua validade?	☐	☐	☐
3.5 As partes interessadas que compartilham as informações são identificadas com base no interesse comum e no risco que podem apresentar para a instituição?	☐	☐	☐

8 - Domínio: Infraestrutura tecnológica

Objetivos: realizar e monitorar as atividades operacionais.	**Sim**	**Não**	**Não tenho informações suficientes para responder**
1.1 As atividades de monitoramento da SegCiber são realizadas?	☐	☐	☐
1.2 Os ambientes operacionais são monitorados quanto ao comportamento irregular que pode indicar vulnerabilidades, ameaças e incidentes?	☐	☐	☐
2.1 Requisitos de monitoramento e análise dos eventos das vulnerabilidades, ameaças e incidentes são definidos?	☐	☐	☐
2.2 Alarmes e alertas são configurados para ajudar na identificação das vulnerabilidades, ameaças e incidentes?	☐	☐	☐
2.3 Indicadores de atividade irregular são definidos e monitorados em todo o ambiente operacional?	☐	☐	☐
2.4 As atividades de monitoramento estão alinhadas com o perfil da instituição?	☐	☐	☐
3.1 Os requisitos de monitoramento baseiam-se no risco da atividade?	☐	☐	☐
3.2 O monitoramento permanente é realizado em todo o ambiente operacional para identificar uma atividade irregular?	☐	☐	☐
3.3 Os indicadores de riscos são utilizados para identificar uma atividade irregular?	☐	☐	☐
3.4 Os alarmes e alertas são configurados com base nos indicadores de atividade irregular?	☐	☐	☐

Fonte: O autor

2.5.2 Alinhamento com a LGPD

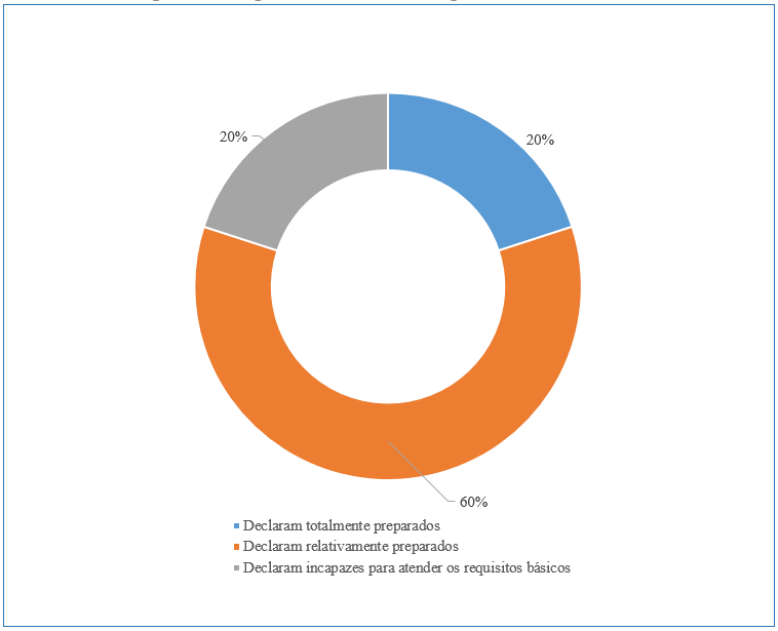
A LGPD estabelece uma série de regras que empresas e outras instituições atuantes no Brasil devem seguir para permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

A Associação Brasileira de Empresas de Infraestrutura de Hospedagem na Internet (ABRAHOSTING)[11] realizou em 2018 uma pesquisa sobre os impactos da LGPD sobre os negócios do setor.

[11] Associação Brasileira de Empresas de Infraestrutura de Hospedagem na Internet: é uma associação sem fins lucrativos que tem como objetivo apoiar o desenvolvimento das atividades relacionadas à *hosting* e infraestrutura.

Pelos dados da pesquisa, 60% dos associados se declaram relativamente preparados para responder às exigências da LGPD, enquanto 20% se declaram totalmente preparados, e os 20% restantes, se declaram incapazes para atender os requisitos básicos da Lei. O Gráfico 4 apresenta os percentuais da capacidade das instituições atenderem aos requisitos da LGPD.

Gráfico 4 - Capacidade para atender os requisitos da LGPD



Fonte: ABRAHOSTING

Já o item que exige que a empresa tenha um profissional de dados, responsável por desenvolver relatórios com validade forense, sobre segurança e violação de dados na sua infraestrutura, não é atendido por 70% das empresas pesquisadas.

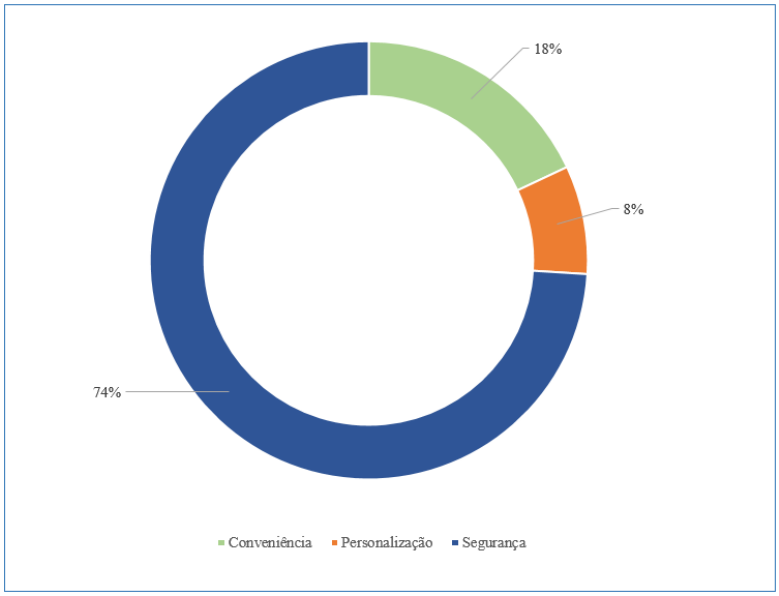
O estudo identificou também que 53% das empresas programam investimentos em governança de bancos de dados como medida prioritária em face da LGPD.

Segundo o *Gartner*[12], o investimento global com produtos e serviços de SI somou a marca de US$ 114 bilhões em 2018, com um crescimento de 12,4% em relação ao ano de 2017. Já para 2019 o total de investimento foi US$ 124 bilhões, apresentando um indicador de recursos 8,7% maior do que ano de 2018.

O Gráfico 5 apresenta a segurança como o item mais importante para a experiência dos usuários nos serviços *on-line*.

[12] *Gartner*: empresa que atua no ramo de pesquisas, consultorias, eventos e prospecções sobre o mercado de tecnologia da informação. https://www.gartner.com/en/information-technology/insights/cybersecurity

Gráfico 5 – Experiência *on-line*



Fonte: Serasa *Experian*

Adequar-se à LGPD é um grande desafio para as instituições, pois envolve diversos departamentos, bem como etapas que exigem um conhecimento da maturidade da proteção de dados, conhecimento conceitual, técnico e tecnológico para enfrentar o desafio.

No modelo proposto neste trabalho as instituições que apresentam o nível 3 de maturidade da AI asseguram o alinhamento de cada um dos domínios com os seguintes artigos da LGPD, conforme apresentado no Quadro 16.

Quadro 16 – Domínios e artigos da LGPD

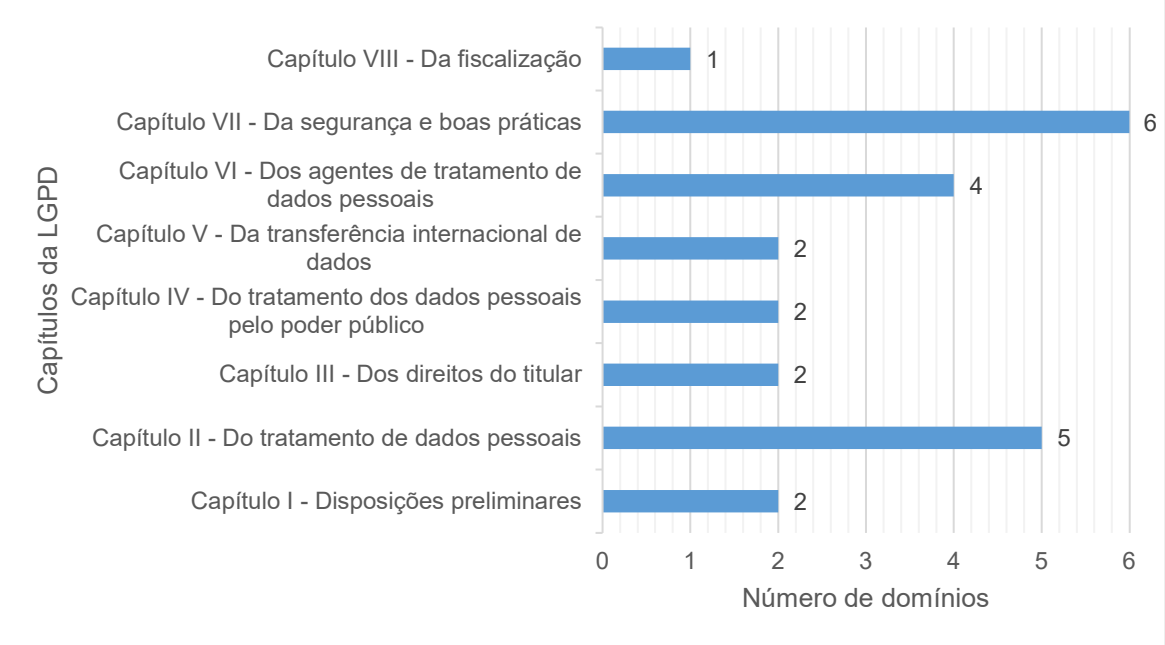
Domínios	Artigos da LGPD	Capítulos
Governança	Art. 3º, 7º, 8º, 9º, 10º, 12º, 14º, 15º, 23º, 41º, 42º, 46º, 49º e 50º	Capítulo I – Disposições preliminares Capítulo II – Do tratamento de dados pessoais Capítulo IV – Do tratamento dos dados pessoais pelo poder público Capítulo VI – Dos agentes de tratamento de dados pessoais Capítulo VII – Da segurança e boas práticas
Proteção de dados	Art. 8º, 9º, 11º, 12º, 33º, 34º, 35º e 36º	Capítulo II – Do tratamento de dados pessoais Capítulo V – Da transferência internacional de dados
Resposta às vulnerabilidades, ameaças e incidentes	Art. 42º, 43º, 44º, 45º, 46º e 47º	Capítulo VI – Dos agentes de tratamento de dados pessoais Capítulo VII – Da segurança e boas práticas
Riscos	Art. 10º, 11º, 52º, 53º e 54º	Capítulo II – Do tratamento de dados pessoais Capítulo VIII – Da fiscalização
Capacitação, conscientização e cultura	Art. 18º, 19º, 21º, 41º e 51º	Capítulo III – Dos direitos do titular Capítulo VI – Dos agentes de tratamento de dados pessoais

Domínios	Artigos da LGPD	Capítulos
		Capítulo VII – Da segurança e boas práticas
Tratamento dos dados	Art. 11º, 12º , 16º, 18º, 19º, 21º, 22º, 37º, 38º, 39º, 40º, 41º, 46º, 47º e 48º	Capítulo II – Do tratamento de dados pessoais Capítulo III – Do direito do titular Capítulo VI – Dos agentes de tratamento de dados pessoais Capítulo VII – Da segurança e boas práticas
Organização da informação	Art. 5º, 7º, 8º, 9º, 11º, 12º, 14º, 17º, 23º, 25º, 31º, 32º, 33º, 46º e 47º	Capítulo I – Disposições preliminares Capítulo II – Do tratamento de dados pessoais Capítulo IV – Do tratamento de dados pessoais pelo poder público Capítulo V – Da transferência internacional de dados Capítulo VII – Da segurança e boas práticas
Infraestrutura tecnológica	Art. 46º, 47º, 48º, 49º e 50º	Capítulo VII – Da segurança e boas práticas

Fonte: O autor

O Gráfico 6 apresenta a necessidade de atendimento das questões de segurança e boas práticas para a organização situar-se no nível 3 de maturidade do modelo proposto, já que os artigos do capítulo VII da LGPD que abordam a segurança e boas práticas são requisitos para o alinhamento com a referida Lei em 6 (seis) domínios do modelo.

Gráfico 6 – Participação dos capítulos da LGPD nos domínios do modelo proposto



Fonte: O autor

2.5.3 Resultados da aplicação do Modelo de Maturidade da AI proposto

Este item apresenta os resultados da aplicação do Modelo de Maturidade da AI proposto no objetivo geral deste trabalho. Para analisar, compreender e interpretar o material qualitativo foi realizada uma análise de conteúdo, segundo BARDIN (2016).

Os procedimentos de coleta de dados em uma pesquisa qualitativa, são realizados no ambiente do participante. A análise e interpretações sobre o significado dos dados são feitas pelo pesquisador (CRESWELL, 2010).

A pesquisa qualitativa tem um estilo indutivo, envolve sobretudo métodos de coleta de dados não estruturados. Entre os métodos de coleta de dados utilizados na pesquisa qualitativa destacam-se entrevistas, grupos focais e questionários. Os questionários, método utilizado neste trabalho, caracterizam-se como uma série organizada de perguntas a serem respondidas pelo participante, sem a necessidade de mediação (SILVA; MENEZES, 2005).

Sendo assim, o uso de ferramentas de TIC para apoio à etapa de coleta, análise, recuperação e gerenciamento dos dados é um instrumento de apoio ao pesquisador (COFFEY *et al.*, 1996).

Para aplicação do modelo, foram selecionadas 35 (trinta e cinco) instituições de ensino, de pesquisa, de fomento, da APF, da APE e privadas inseridas no ambiente do *Big Data*. O *link* de acesso ao questionário *on-line* foi encaminhado por *e-mail* para gestores e profissionais envolvidos com as questões de TIC das instituições participantes.

2.5.3.1 Ferramentas de TIC utilizadas na pesquisa

Para construção do questionário *on-line* foi utilizada a ferramenta de construção de formulários do *Google*[13] que permite coletar e organizar informações *on-line*. Os dados coletados foram organizados em tabelas e gráficos. Os resultados estão apresentados por meio dos *dashboards on-line* e gráficos desenvolvidos como parte integrante deste trabalho.

Os *dashboards* foram construídos com a ferramenta *Data Studio*[14] que transforma os dados coletados em relatórios e painéis informativos. É uma ferramenta de análise de dados da empresa *Google*. Com o *Data Studio* é possível: i) visualizar os dados por meio de gráficos e tabelas personalizadas; ii) integrar-se com as seguintes fontes de dados: *Google Ads*, *Google*

[13] Formulários *Google*: https://www.google.com/intl/pt-BR/forms/about/
[14] *Data Studio*: https://datastudio.google.com/u/0/

Analytics, *Google Sheets*, banco de dados *MySQL*, *PostgreSQL* e *Excel*; e iii) inserir dados e extrair informações para a tomada de decisão.

Os gráficos foram desenvolvidos utilizando o *Google Chart*[15] e o *MS Excel*[16]. Os gráficos são modelos visuais utilizados para representar os dados, possibilitando demonstrar um padrão ou tendência.

O *Google Chart* é uma ferramenta que permite a criação de gráficos com os dados coletados pela ferramenta de formulários do *Google*. O *MS Excel* possui recursos utilizados pelos usuários para a criação de gráficos que permitem que os dados sejam analisados de forma visual.

Na análise e tabulação dos dados foi utilizado tanto o *MS Excel* quanto o *Google Sheets*. Durante essa fase os dados foram exportados do *Google Sheets* para planilhas automatizadas no *MS Excel*.

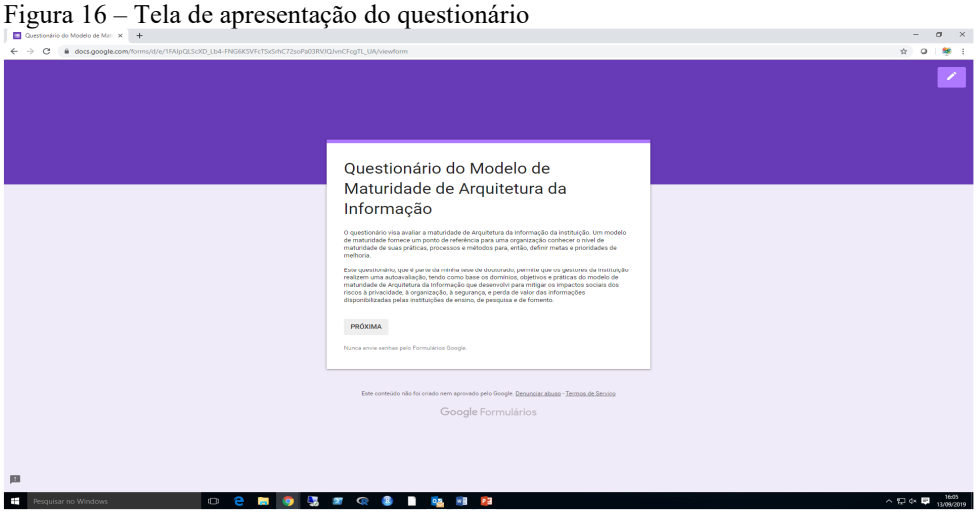
Para automatizar as planilhas fez-se uso da funcionalidade de Macros do *MS Excel*. Uma macro é uma sequência de comandos e funções armazenadas em um módulo *Visual Basic for Application*[17] (VBA).

Com o volume de dados coletados na aplicação do questionário foi necessário o uso de tabelas dinâmicas e filtros avançados. As tabelas dinâmicas permitem resumir uma grande quantidade de dados, elaborar cálculos e fórmulas personalizadas, agilizar o acesso e integrar os dados por categorias e subcategorias.

Já os filtros avançados possibilitam pesquisa e tabulação dos dados segundo critérios básicos e avançados de complexidade. As figuras a seguir apresentam de forma gráfica as telas do questionário, *dashboards* e o *QR Code*[18] para acesso *on-line* ao questionário.

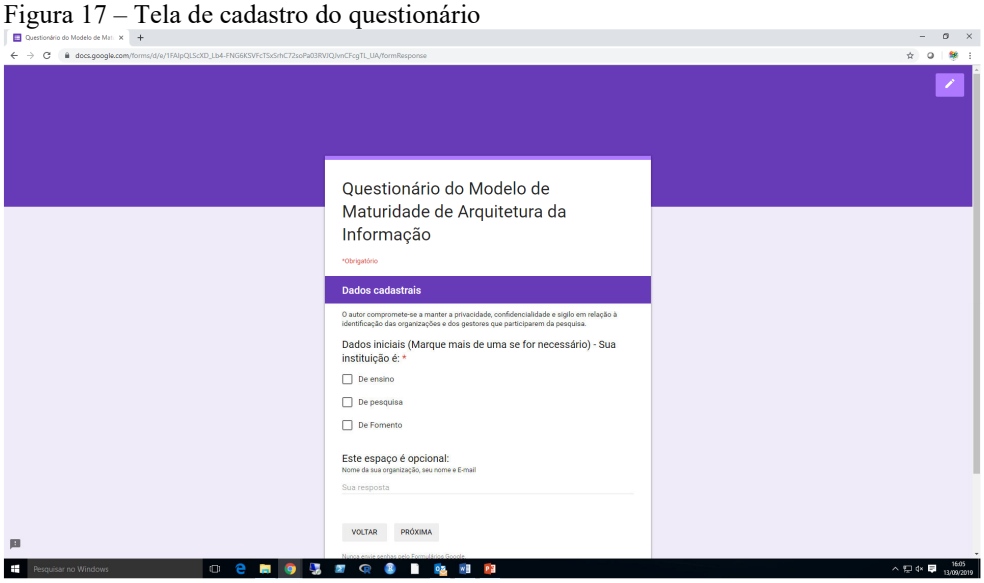
[15] *Google Chart*: https://developers.google.com/chart/interactive/docs
[16] *MS Excel*: https://products.office.com/pt-br/excel
[17] *Visual Basic Application*: permite que o usuário utilize recursos de programação nos aplicativos do *Microsoft Office*, por exemplo *MS Excel*.
[18] *QR Code Quick Response*, uma das vantagens do *QR Code* é que ele dispensa a necessidade da digitação de endereço de uma *URL* na Internet. Iniciando o aplicado é só aproximar o celular da imagem para ter acesso ao conteúdo disponibilizado na imagem.

Figura 16 – Tela de apresentação do questionário



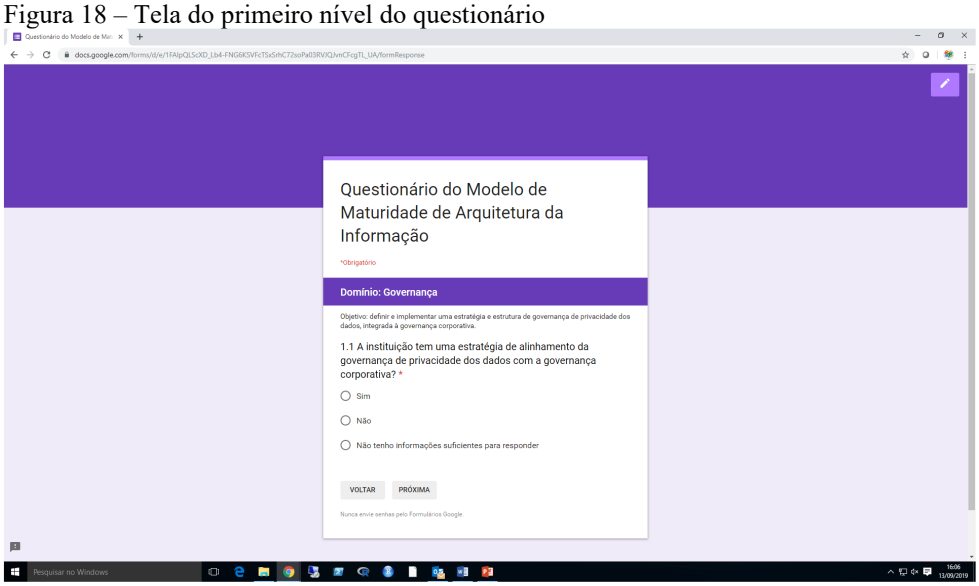
Fonte: O autor

Figura 17 – Tela de cadastro do questionário



Fonte: O autor

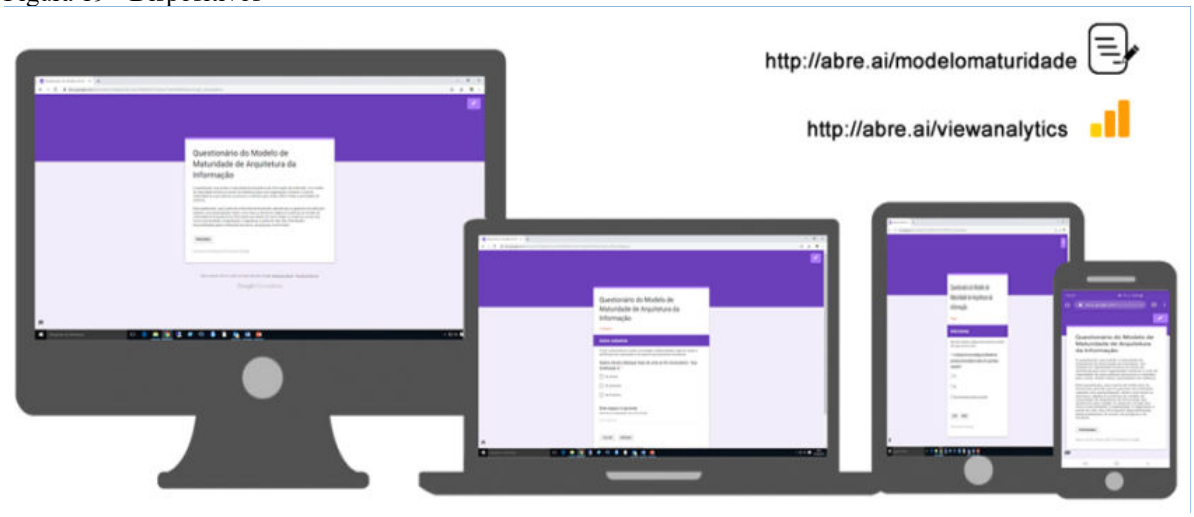
Figura 18 – Tela do primeiro nível do questionário



Fonte: O autor

Na Figura 19 é possível visualizar o *layout* do questionário em diversos dispositivos: *desktop*, *notebook*, *tablet* e *smartphone*.

Figura 19 - Dispositivos



Fonte: O autor

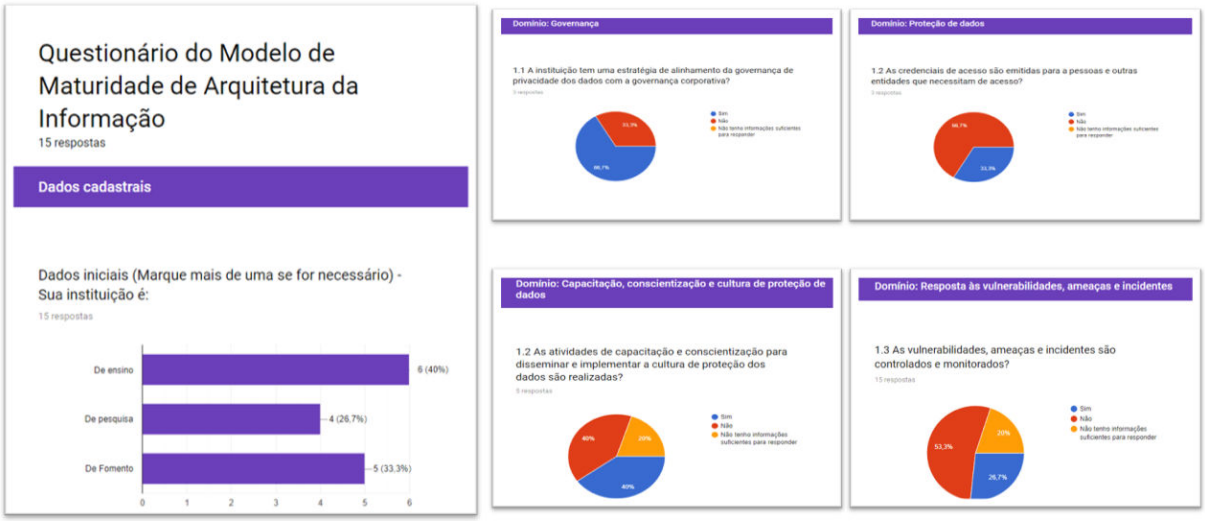
A Figura 20 apresenta o *QR Code* para acesso ao questionário e ao *dashboard* dos níveis de maturidade das instituições por domínio.

Figura 20 – *QR Code*

Fonte: O autor

A Figura 21 apresenta o *dashboard* das respostas do questionário. Na referida figura é possível identificar a quantidade de instituições participantes, bem como os percentuais das respostas para cada uma das perguntas do questionário.

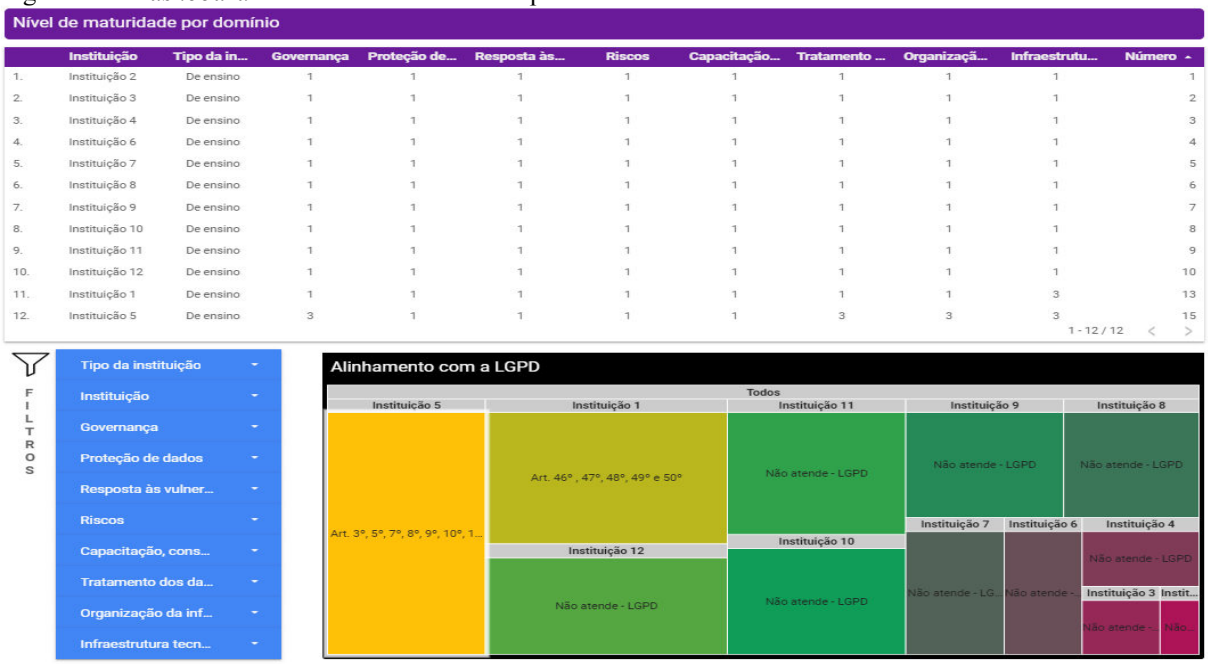
Figura 21 – *Dashboard* das respostas



Fonte: O autor

Na Figura 22 é possível visualizar o *dashboard* com os níveis de maturidade de cada uma das instituições participantes por domínio. Entre as funcionalidades desenvolvidas é possível realizar uma pesquisa por tipo de instituição, nível de maturidade por domínio e visualizar o alinhamento das práticas da AI das instituições participantes da pesquisa com a LGPD.

Figura 22 – *Dashboard* dos níveis de maturidade por domínio



Fonte: O autor

2.5.3.2 Discussão dos resultados

Os dados foram analisados mediante a interpretação das respostas coletadas por meio do questionário *on-line*. Na proposta inicial do trabalho o foco foi identificar a maturidade da AI nas instituições de ensino, de pesquisa e de fomento. No entanto, em face da divulgação do trabalho entre profissionais da área de TIC outras organizações demonstraram interesse em participar da pesquisa, tais como: instituições da APF, da APE e empresas privadas que desenvolvem projetos de pesquisa.

Como se pode conferir na Tabela 1, de um total de 35 (trinta e cinco) instituições participantes, 12 foram instituições de ensino, 5 de pesquisa e 2 de fomento.

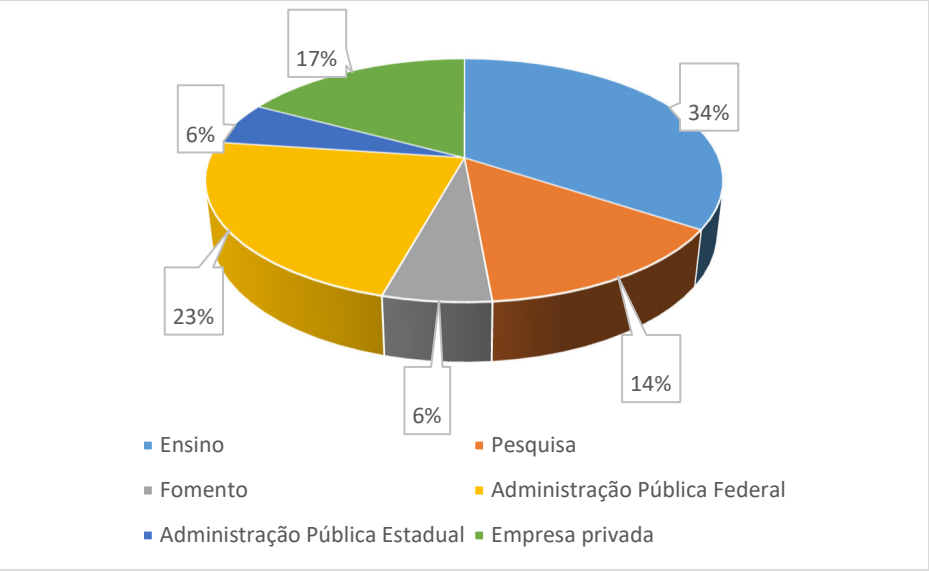
Tabela 1 – Tipos das instituições participantes

Tipo da instituição	Quantidade	% de participação
De ensino	12	34%
De pesquisa	5	14%
De fomento	2	6%
Administração Pública Federal	8	23%
Administração Pública Estadual	2	6%
Empresa privada	6	17%
Total	35	

Fonte: O autor

O Gráfico 7 apresenta os percentuais de participação na pesquisa por instituição. A maioria dos participantes da pesquisa foi do tipo “Instituição de Ensino”.

Gráfico 7 – Percentual de participação na pesquisa



Fonte: O autor

A Tabela 2 apresenta o número de instituições por nível para cada um dos domínios do modelo do proposto.

Tabela 2 – Nível de maturidade das instituições por domínio

Domínios	Número de instituições por nível			
	Nível 0	Nível 1	Nível 2	Nível 3
Ensino				
Governança	5	5	1	1
Proteção de dados	10	2	0	0
Resposta à Vulnerabilidades, Ameaças e Incidentes	11	1	0	0
Riscos	10	2	0	0
Capacitação, Conscientização e Cultura	10	1	1	0
Tratamento dos Dados	10	1	1	0
Organização da Informação	9	1	1	1
Infraestrutura Tecnológica	6	2	2	2
Pesquisa				
Governança	4	1	0	0
Proteção de dados	2	3	0	0
Resposta à Vulnerabilidades, Ameaças e Incidentes	3	1	1	0
Riscos	3	1	1	0
Capacitação, Conscientização e Cultura	4	1	0	0
Tratamento dos Dados	5	0	0	0
Organização da Informação	5	0	0	0
Infraestrutura Tecnológica	1	2	2	0

Domínios	Número de instituições por nível			
	Nível 0	Nível 1	Nível 2	Nível 3
Fomento				
Governança	2	0	0	0
Proteção de dados	2	0	0	0
Resposta à Vulnerabilidades, Ameaças e Incidentes	2	0	0	0
Riscos	2	0	0	0
Capacitação, Conscientização e Cultura	2	0	0	0
Tratamento dos Dados	2	0	0	0
Organização da Informação	2	0	0	0
Infraestrutura Tecnológica	2	0	0	0
Administração Pública Federal				
Governança	4	2	1	1
Proteção de dados	6	2	0	0
Resposta à Vulnerabilidades, Ameaças e Incidentes	4	2	1	1
Riscos	2	4	1	1
Capacitação, Conscientização e Cultura	5	2	1	0
Tratamento dos Dados	4	2	1	1
Organização da Informação	5	1	1	1
Infraestrutura Tecnológica	2	4	1	1
Administração Pública Estadual				
Governança	2	0	0	0
Proteção de dados	1	1	0	0
Resposta à Vulnerabilidades, Ameaças e Incidentes	1	1	0	0
Riscos	1	1	0	0
Capacitação, Conscientização e Cultura	2	0	0	0
Tratamento dos Dados	1	1	0	0
Organização da Informação	2	0	0	0
Infraestrutura Tecnológica	2	0	0	0
Empresa Privada				
Governança	3	1	1	1
Proteção de dados	3	1	1	1
Resposta à Vulnerabilidades, Ameaças e Incidentes	3	1	1	1
Riscos	4	1	1	0
Capacitação, Conscientização e Cultura	3	2	1	0
Tratamento dos Dados	4	1	1	0
Organização da Informação	3	2	1	0
Infraestrutura Tecnológica	1	3	1	1

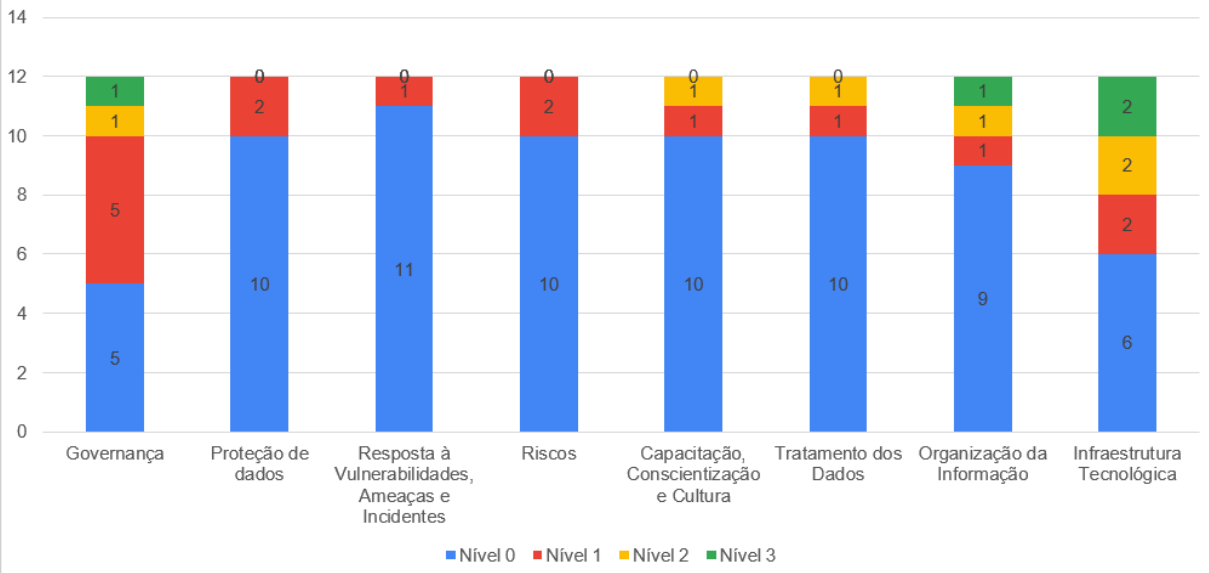
Fonte: O autor

O Gráfico 8 apresenta o número de instituições de ensino por níveis de maturidade para cada um dos domínios do modelo proposto. As referidas instituições estão no nível 3 de

maturidade somente para os domínios Governança, Organização da Informação e Infraestrutura Tecnológica.

As instituições de ensino participantes da pesquisa apresentam alinhamento com os seguintes artigos da LGPD: Art. 3º, 5º, 7º, 8º, 9º, 10º, 11º, 12º, 14º, 15º, 17º, 23º, 25º, 31º, 32º, 33º, 41º, 42º, 46º, 47º, 48º, 49º e 50º.

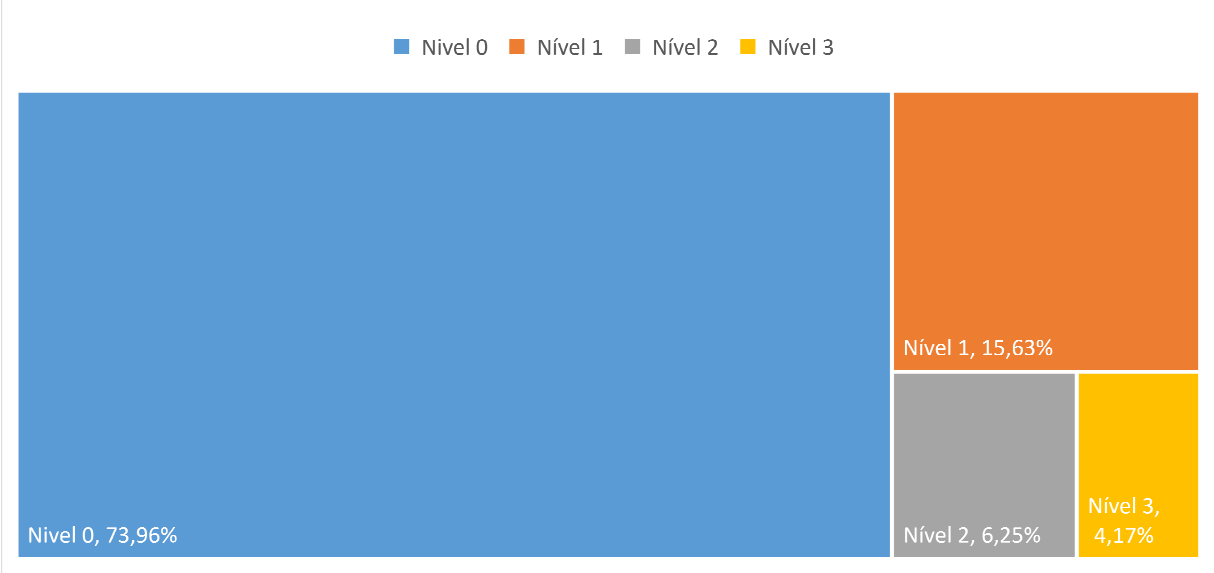
Gráfico 8 – Instituições de ensino



Fonte: O autor

O Gráfico 9 apresenta os percentuais de instituições de ensino para cada um dos níveis do modelo: 73, 96% estão no nível 0, 15,63% estão no nível 1, 6,25% estão no nível 2 e 4,17% estão no nível 3.

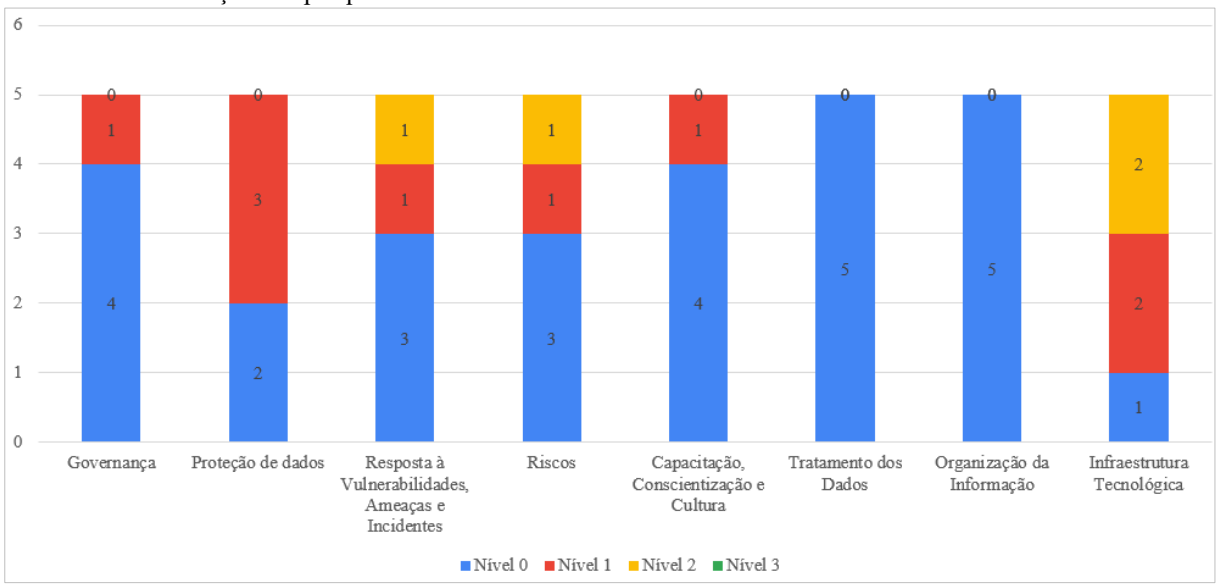
Gráfico 9 – Percentual das instituições de ensino por nível de maturidade



Fonte: O autor

As instituições de pesquisa estão no nível 0, 1 e 2 de maturidade, desta forma não apresentam alinhamento com a LGPD para os domínios do modelo proposto. O Gráfico 10 apresenta o número de instituições de pesquisa por níveis de maturidade para cada um dos domínios do modelo proposto.

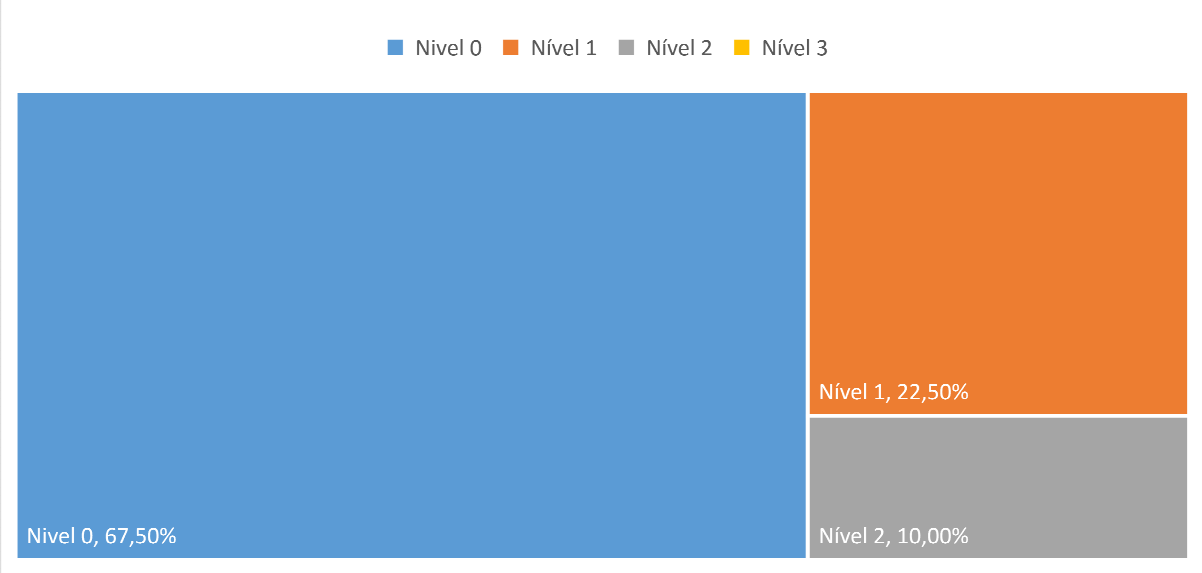
Gráfico 10 – Instituições de pesquisa



Fonte: O autor

Essas instituições apresentam os seguintes percentuais por nível: 67,50% estão no nível 0, 22,50% estão no nível 1 e 10% estão no nível 2. O Gráfico 11 apresenta os percentuais das instituições de pesquisa.

Gráfico 11 – Percentual das instituições de pesquisa por nível de maturidade

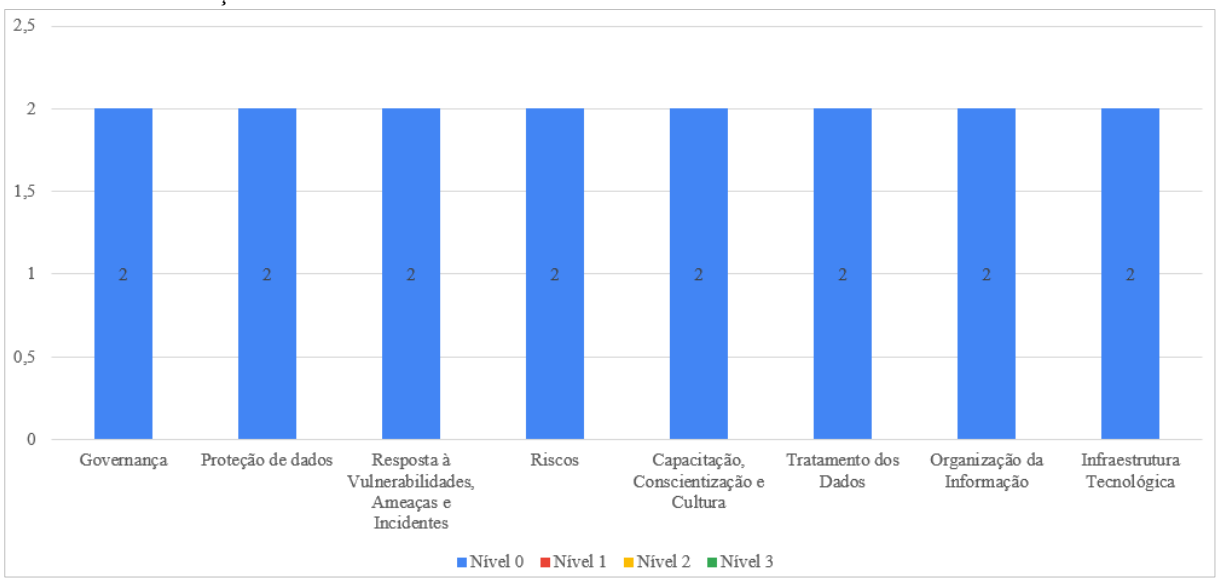


Fonte: O autor

Os resultados da aplicação do Modelo de Maturidade da AI nas instituições de fomento apresentam a totalidade dos participantes no nível 0. Esses resultados podem ser visualizados no Gráfico 12.

A baixa maturidade das referidas instituições reforça a necessidade de implementar a AI para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a SI e com a perda de valor das informações, bem como o alinhamento com a LGPD.

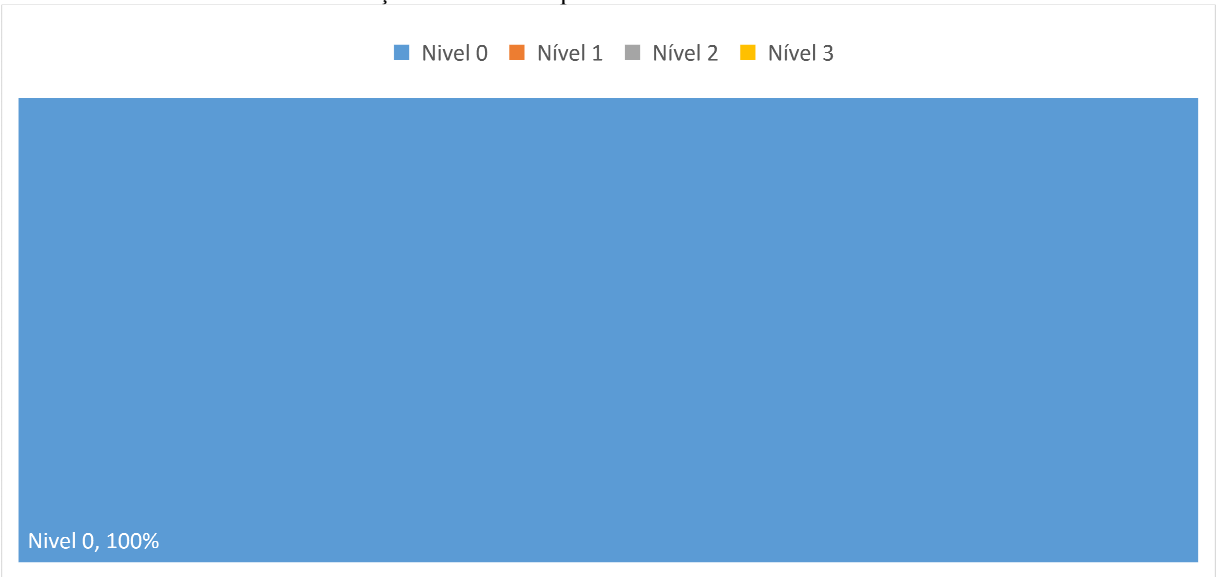
Gráfico 12 – Instituições de fomento



Fonte: O autor

O Gráfico 13 apresenta o percentual das instituições de pesquisa no nível 0.

Gráfico 13 – Percentual das instituições de fomento por nível de maturidade



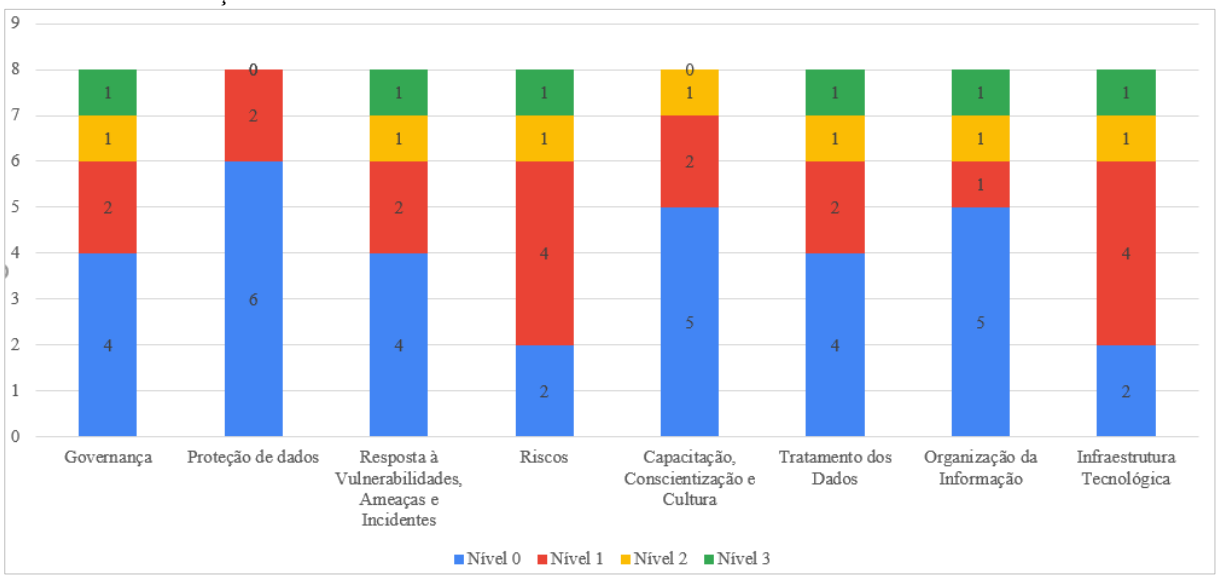
Fonte: O autor

Entre as instituições da APF que participaram da pesquisa 9,38 % estão no nível 3, apresentando um alinhamento com a LGPD nos domínios Governança, Resposta à Vulnerabilidades, Ameaças e Incidentes, Riscos, Tratamento dos Dados, Organização da Informação e Infraestrutura Tecnológica.

As instituições da APF foram as que apresentaram o maior alinhamento com os artigos da LGPD: Art. 3º, 5º, 7º, 8º, 9º, 10º, 11º, 12º, 14º, 15º, 16º, 17º, 18º, 19º, 21º, 22º, 23º, 31º, 32º, 33º, 37º, 38º, 39º, 40º, 41º, 42º, 43º, 46º, 47º, 48º, 49º, 50º, 52º, 53º, 54º.

No Gráfico 14 é possível visualizar o número de instituições da APF por níveis de maturidade para cada um dos domínios do modelo proposto.

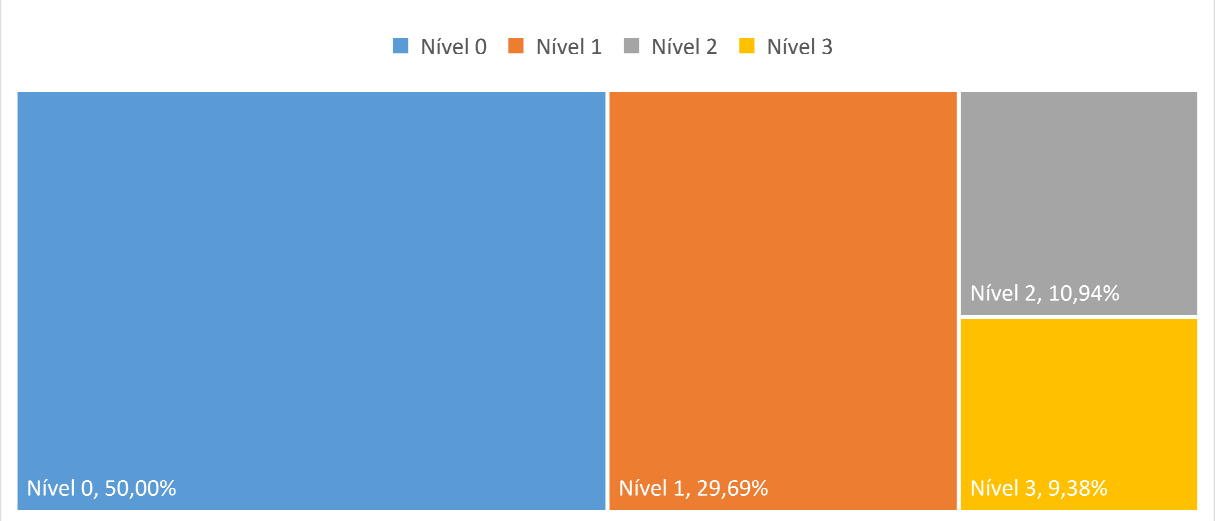
Gráfico 14 – Instituições da APF



Fonte: O autor

O Gráfico 15 apresenta os percentuais dessas instituições para os níveis de maturidade.

Gráfico 15 – Percentual das instituições da APF por nível de maturidade

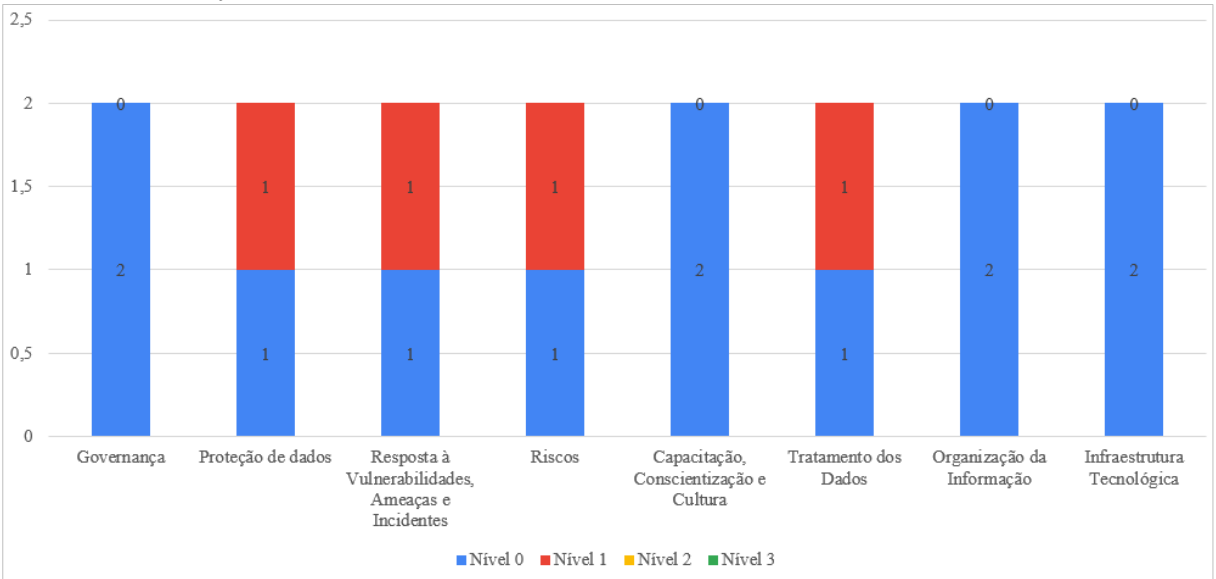


Fonte: O autor

Diferente das instituições da APF, 75% das instituições da APE estão no nível 0 e 25% das instituições estão no nível 1. Com esses resultados, as instituições estaduais não demonstram alinhamento com a LGPD. Os resultados demandam dessas instituições a implementação das práticas do modelo proposto para os níveis de maturidade 2 e 3.

O Gráfico 16 apresenta o número de instituições da APE por níveis de maturidade para cada um dos domínios do modelo proposto.

Gráfico 16 – Instituições da APE



Fonte: O autor

Os percentuais dessas instituições para os níveis de maturidade estão apresentados no Gráfico 17.

Gráfico 17 – Percentual das instituições da APE por nível de maturidade

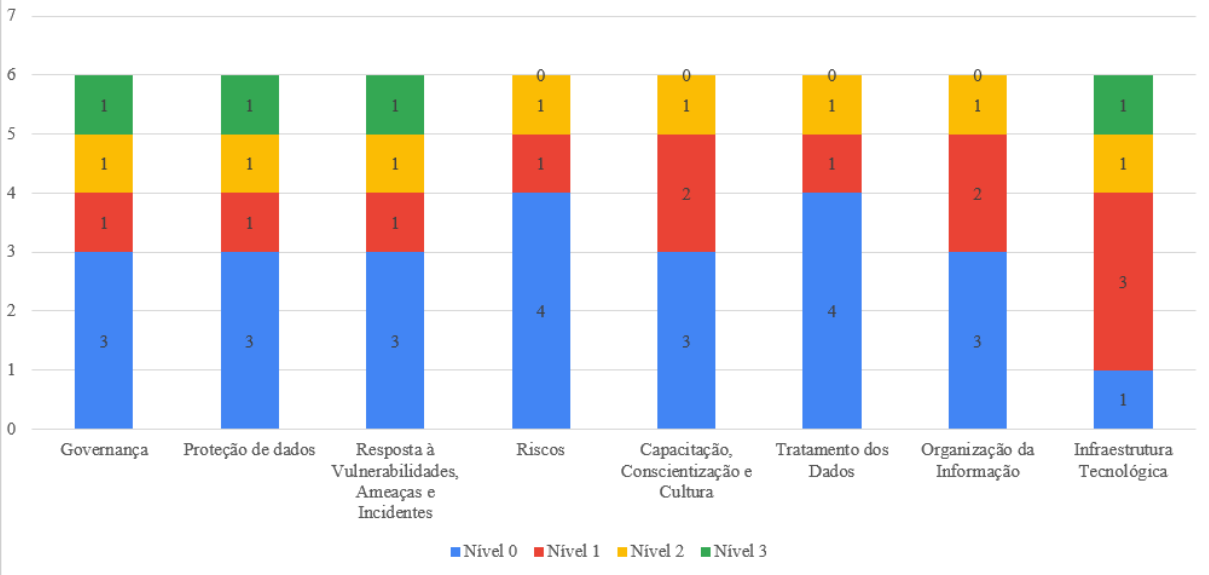
Fonte: O autor

As instituições do setor privado participantes da pesquisa apresentaram os seguintes percentuais: 50% estão no nível 0, 25% estão no nível 1, 16,67% estão no nível 2 e 8,33% estão no nível 3.

As empresas privadas que estão no nível 3 de maturidade demonstram o alinhamento com a LGPD nos domínios Governança, Proteção de Dados, Resposta à Vulnerabilidades, Ameaças e Incidentes e Infraestrutura Tecnológica. A maturidade dessas instituições apresenta um alinhamento com os seguintes artigos da LGPD: Art. 3º, 7º, 8º, 9º, 10º, 11º, 12º, 14º, 15º, 23º, 33º, 34º, 35º, 36º, 41º, 42º, 43º, 44º, 45º, 46º, 47º, 48º, 49º e 50º.

O número de instituições privadas por níveis de maturidade para cada um dos domínios do modelo proposto pode ser visualizado no Gráfico 18.

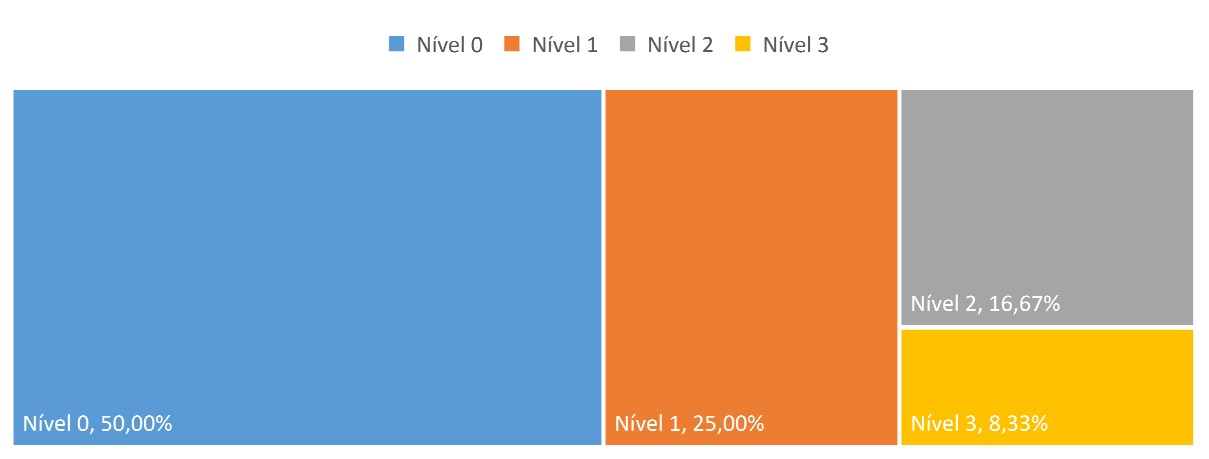
Gráfico 18 – Instituições privadas



Fonte: O autor

O Gráfico 19 apresenta os percentuais dessas instituições para os níveis de maturidade.

Gráfico 19 – Percentual das instituições privadas por nível de maturidade

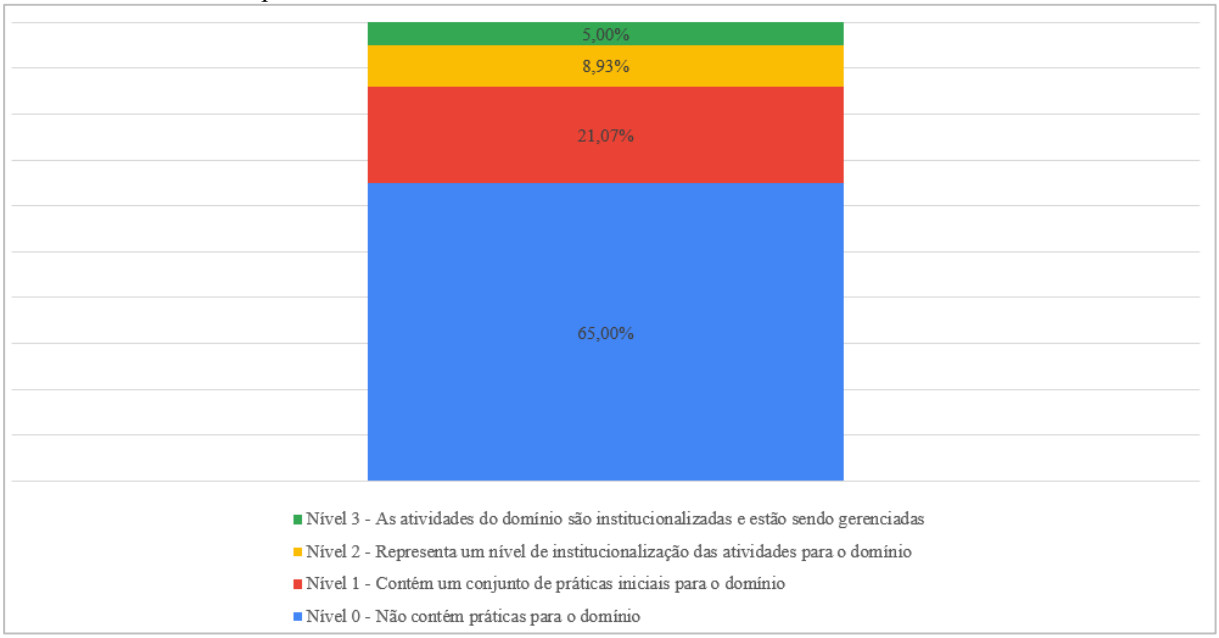


Fonte: O autor

Com base nos resultados da pesquisa, foi possível identificar que as instituições têm um caminho pela frente para aumentar o seu nível de maturidade da AI e alinhar seus processos às exigências da LGPD.

O Gráfico 20 apresenta que 65 % dos participantes da pesquisa estão no nível 0, 21,07% estão no nível 1, 8,93 % no nível 2 e 5 % no nível 3.

Gráfico 20 – Percentual por nível de maturidade



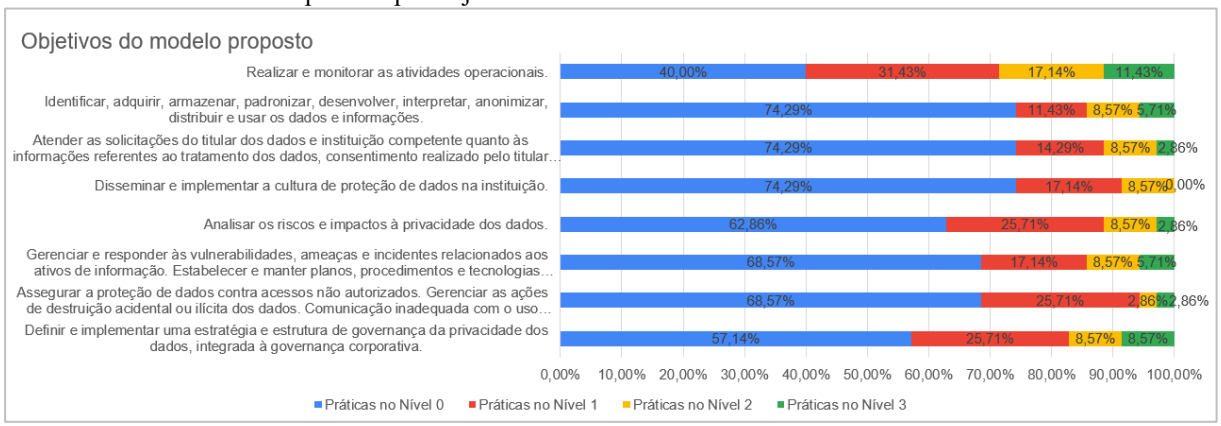
Fonte: O autor

No que pese a importância na proteção de dados para as instituições pesquisadas, os resultados demonstram um baixo percentual de maturidade para atendimento dos objetivos do modelo proposto.

Já nas práticas para assegurar a proteção de dados contra acessos não autorizados, gerenciar as ações de destruição acidental ou ilícita dos dados e comunicação inadequada com o uso dos dados, 68,57% das instituições estão no nível 0.

Nas práticas que visam identificar, adquirir, armazenar, padronizar, desenvolver, interpretar, anonimizar, distribuir e usar dados e informações, o percentual de instituições no nível 0 é maior, com um índice de 74,29%. O Gráfico 21 apresenta o percentual das práticas por nível para os objetivos do modelo proposto.

Gráfico 21 – Percentual das práticas por objetivos



Fonte: O autor

Apesar da evolução das novas tecnologias de SegCiber, o treinamento da força de trabalho é requisito importante para a proteção dos dados pessoais e corporativos. O resultado identificado com a pesquisa para disseminar e implementar a cultura de proteção de dados na instituição está entre os 3 (três) objetivos com maior percentual de organizações no nível 0. Desta forma, essas instituições apresentam maior vulnerabilidade para ações de engenharia social que tem como missão atacar o elo fraco de uma organização, o ser humano (HADNAGY, 2011).

A engenharia social é a ciência de utilizar a interação social como uma forma de motivar uma pessoa ou uma organização a atender a uma solicitação de um invasor, tendo como ferramenta recursos de TIC com impactos nos princípios da SI: confidencialidade, integridade e disponibilidade (MOUTON *et al.*; SÊMOLA, 2014).

À medida que as organizações adotam novas tecnologias, cresce o desafio para melhorar as competências dos usuários do ambiente tecnológico. O desenvolvimento dessas competências inclui conscientização e treinamento da força de trabalho.

A revisão dos processos e obrigações para aderência à LGPD terá impacto tecnológico nas instituições participantes desta pesquisa. O planejamento para realizar essa adequação à Lei exige das instituições treinamento da equipe para o desenvolvimento das competências para atender as demandas do avanço tecnológico.

CAPÍTULO 3

I APRESENTAÇÃO

O artigo 1 (um)[19] apresentado neste capítulo discorre sobre a privacidade, a SI e a proteção de dados no ambiente do *Big Data*. Diante de um cenário composto pela explosão da quantidade e disponibilidade de dados decorrentes dos avanços tecnológicos, situa-se o fenômeno do *Big Data*, que tem impactado a sociedade por meio de novos modelos de negócios que realizam o rastreamento de dados para analisar padrões de comportamento, consumo e saúde, visando a estabelecer uma tomada de decisão baseada em dados.

No contexto do *Big Data* os direitos à privacidade e à proteção de dados tem sido um desafio para as instituições públicas e privadas. Sendo assim, os governos têm dispensado especial atenção para lidar com esses desafios. A UE, publicou em 2018, o GDPR, que visa proporcionar aos usuários maior controle sobre seus dados pessoais e a aumentar as restrições sobre as organizações que tratam e lidam com esses dados.

No Brasil, por sua vez, o Governo publicou a LGPD, n. º 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A referida Lei entrará em vigor em 2020.

O artigo busca apresentar uma contextualização sobre o *Big Data*, discorrer sobre as questões relacionadas com a ética, a privacidade, a segurança e a organização das informações nesse ambiente, abordar os conceitos e modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários e mencionar o panorama sobre a proteção de dados em 2018.

Conhecer o estado atual da AI nas instituições e estar alinhado com a LGPD, por meio de um modelo de maturidade conforme descrito no capítulo 1 (um), permite enfrentar as questões relacionadas com a ética, a privacidade, a segurança e a organização das informações no ambiente do *Big Data*, temas abordados neste artigo.

[19] Artigo 1 (um): o *layout* apresentado é o publicado pela revista Parcerias Estratégicas do CGEE.

A privacidade, a segurança da informação e a proteção de dados no *Big Data*

Antonio João Gonçalves de Azambuja[1], *Lisandro Zambenedetti Granville*[2] *e Alexandre Guilherme Motta Sarmento*[3]

Resumo

O avanço das tecnologias da informação tem possibilitado um crescimento exponencial do volume de dados obtidos, armazenados, processados, transmitidos e publicados no ambiente do *Big Data*. Todo esse crescimento tem gerado desafios para o direito à privacidade, à liberdade de expressão e a segurança das informações, tanto pessoais como as corporativas. As questões do volume de dados, a velocidade com que os dados são processados, a sua variedade e veracidade no ecossistema do *Big Data* colocam em risco esses direitos e a segurança das informações. Inicialmente, este trabalho apresenta

Abstract

The progress of information technologies has enabled an exponential growth in the volume of data collect, stored, processed, transmitted and published in the Big Data environment. All of this growth has created challenges for the right to privacy, freedom of expression and the security of both personal and corporate information. Data volume issues, the speed with which data is processed, its variety and veracity in the Big Data ecosystem, put those rights and the security of information in risk. Initially this paper presents a contextualization about Big Data, with definitions and their characteristics. Then

1 Chefe do Serviço de Segurança da Informação e Comunicações da Advocacia-Geral da União. Mestre em Gestão do Conhecimento e Tecnologia da Informação pela Universidade Católica de Brasília (UCB).

2 Professor do Programa de Educação em Ciências Universidade Federal do Rio Grande do Sul (UFRGS). Doutor em Computação pela UFRGS.

3 Coordenador técnico de apoio a pesquisa, desenvolvimento e aplicações do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Doutor em Educação em Ciências pela UFRGS.

uma contextualização sobre o *Big Data*, com definições e suas características. Em seguida aborda questões relacionadas com a ética, a privacidade, a segurança e a organização das informações no *Big Data*. Ao abordar tais questões, discorre sobre os riscos à privacidade, segurança da informação, organização da informação, conceitos e modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários. Finalmente, apresenta um panorama da proteção de dados em 2018, com os eventos de divulgação e manipulação de dados sem autorização dos usuários, fato que direciona para maior cuidado com os nossos dados. As considerações finais da análise reconhecem que os usuários estão sujeitos aos riscos à privacidade das informações e a sua segurança no universo do *Big Data*.

Palavras-chave: Privacidade das informações. Segurança da informação. Risco à Privacidade. Proteção de dados. *Big Data*.

addresses issues related to ethics, privacy, security and the organization of information in Big Data. Addressing such issues related to privacy risks, information security, information organization, anonymization concepts and models that can be used to preserve users' privacy. Finally presents a panorama of data protection in 2018, the events of disclosure and manipulation of data without users authorization. That fact leads to a greater care with our data. The final considerations in the analysis recognize that users are subject to the risks to information privacy and their security in the Big Data universe.

Keywords: *Privacy information. Information Security. Privacy risk. Data protection. Big Data.*

1. Introdução

A informatização da sociedade, aliada ao avanço tecnológico e a sua convergência, tem proporcionado um crescimento exponencial do volume de dados no espaço cibernético, o que marca o advento do *Big Data*.

Vivemos a era do *Big Data*, que tem transformado a forma como as organizações estão direcionando o seu processo de tomada de decisão (JANSSEN *et al.*, 2017). As novas tecnologias permitem que as organizações, a partir da análise dos dados, tenham um ganho de competitividade (EREVELLES; FUKAWA; SWAYNE, 2016).

Nesse cenário, composto pela explosão da quantidade e disponibilidade de dados decorrente do avanço das tecnologias de processamento, coleta e análise dos dados, situa-se o fenômeno conhecido como *Big Data*.

Esse fenômeno tem impactado a sociedade, por meio de novos modelos de negócios que fazem rastreamento de dados para analisar padrões de comportamento, consumo e saúde, visando a estabelecer uma tomada de decisão baseada em dados.

Ao mesmo tempo que novas formas de comunicação, registro, acesso e recuperação da informação estão sendo viabilizadas, surge a preocupação com a privacidade e segurança das informações (CHEN; YANG; LUO, 2017).

A privacidade e a segurança da informação (SI) na internet têm correspondido a uma área que desperta interesse de estudo, devido à grande quantidade de informações pessoais e corporativas que são obtidas, armazenadas, transmitidas e publicadas na rede mundial de computadores.

A informação tornou-se um ativo de valor para as organizações, que pode ser processada por meio eletrônico e com a utilização de redes públicas e privadas de internet (HONG; THONG, 2013).

Esses ativos que podem ser corporativos e/ou pessoais compõem o ambiente atual dos negócios das organizações e estão em constante ameaça de vírus, invasões de sistema, abuso de informações privilegiadas, quebra da privacidade e divulgação não autorizada das informações (JOHNSTON; WARKENTIN, 2010).

Para Zwitter (2014), em um mundo altamente interconectado, lidar com a ética, considerando o consentimento dos usuários, a privacidade, a segurança e a anonimização das informações, é um desafio do *Big Data*. Já Drinkwater (2016), ressalta que o vazamento de informações *on-line*, aumenta as preocupações dos usuários em relação ao risco da informação.

Diante do contexto no qual os direitos à privacidade e proteção de dados foram elevados ao nível dos direitos humanos no cenário internacional, os governos têm dispensado especial atenção para lidar com esses desafios. Nesse cenário, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), publicado em 2018, pela União Europeia (EU), que visa a proporcionar aos usuários maior controle sobre seus dados pessoais e a aumentar as restrições sobre as organizações que tratam e lidam com esses dados.

No cenário nacional, por sua vez, o Governo Brasileiro publicou a Lei Geral de Proteção de Dados Pessoais (LGPD), n.º 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A referida Lei entrará em vigor no primeiro semestre de 2020.

Diante do exposto, este artigo busca apresentar uma contextualização sobre o *Big Data*, discorrer sobre questões relacionadas com a ética, a privacidade, a segurança e a organização das informações nesse ambiente, apresentar conceitos e modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários, além de um panorama sobre a proteção de dados em 2018.

2. *Big Data*

2.1. Definição

O *Big Data* é um fenômeno que se refere à explosão da disponibilidade de dados relevantes, como resultado recente e sem precedente do avanço das tecnologias de armazenamento e registro de dados. Fenômeno do processamento de grandes volumes de dados, com os quais as ferramentas tradicionais não são capazes de lidar na velocidade requerida (GOLDMAN *et al.*, 2012).

Brynjolfsson *et al.* (2012) afirmam, ainda, que soluções de *Big Data* possuem um potencial maior que as soluções analíticas tradicionais, no sentido de trazer benefícios e aumentar a competitividade das empresas.

O termo *Big Data* surgiu para definir arquiteturas de sistemas capazes de lidar com as novas dimensões dos dados: velocidade, variedade e volume (AZEVEDO; NEVES; NOVO, 2014).

Nesse cenário de crescimento exponencial da informação publicada na internet, com a presença de base de dados que contém um grande volume de dados, situa-se o *Big Data* (SHINATAKU; DUQUE; SUAIDEN, 2014).

2.2. Características

O fenômeno *Big Data* está associado ao grande volume de dados, mas essa não é sua única característica. Inicialmente, foi caracterizado pelo volume, pela velocidade e variedade (3V's) dos dados. Os atributos veracidade e valor foram considerados posteriormente como relevantes. Essas características são conhecidas como os 5V's do *Big Data*:

- *Volume:* refere-se ao tamanho dos dados. Os dados são coletados de uma grande variedade de fontes, incluindo transações comerciais, redes sociais e informações de sensores ou dados transmitidos de máquina a máquina;

- *Velocidade:* refere-se à velocidade de transmissão dos dados. Os dados fluem em uma velocidade sem precedentes e devem ser armazenados, tratados e analisados com agilidade;

- *Variedade:* refere-se ao formato no qual os dados são gerados, isto é, estruturados e não estruturados. Os dados estruturados são organizados em linhas e colunas e geralmente são armazenados em banco de dados relacionais, os quais facilitam a atualização e a recuperação de dados em menor granularidade. Os dados não estruturados não possuem uma organização predefinida. Em decorrência disso, há maior dificuldade para a sua recuperação e o seu processamento, a exemplo dos vídeos, dos comentários em redes sociais, dos e-mails, entre outros;

- *Veracidade:* tem relação com a confiabilidade dos dados. Durante a análise dos dados, é necessário conhecer o contexto em que os dados foram gerados, se eles são autênticos e de fontes confiáveis; e

- *Valor:* os dados devem agregar valor ao negócio. Sem valor, a informação não tem utilidade.

2.3. Fonte

As fontes de dados do *Big Data* são: os usuários e a tecnologia. Dados, informações e conhecimento são gerados diariamente. A complexidade do *Big Data* não está no volume, como apontou Davenport (2014), mas na falta de estrutura que dificulta a análise para a geração de conhecimento, inovação ou valor.

O autor destaca a relevância de se resumir os dados e encontrar seus significados e seus padrões para o contexto no qual ele foi resumido. Reforça a importância da definição adequada do problema e da pertinência da formulação correta da pergunta, os quais devem orientar a coleta e o posterior resumo dos dados, na busca da organização da informação.

3. Ética

Questões éticas devem ser consideradas no atual cenário do *Big Data*, tais como: Qual a fronteira para o uso dos dados produzidos pelas pessoas no seu dia a dia, com as novas tecnologias? Esses dados podem ser acessados em tempo real? Por quem? Para que finalidade?

O volume de dados cresce de forma exponencial com a evolução e sofisticação da rede mundial de computadores e de suas aplicações. Todo o potencial de conhecimento obtido com a coleta, o processamento, o armazenamento e a análise dos dados pode ser utilizado a favor da sociedade.

Por outro lado, os dados podem ser utilizados: pelos governos, para o controle do cidadão e com objetivos políticos; ou pelas organizações privadas, para direcionar um determinado padrão de consumo.

Um caso clássico do uso do *Big Data*, que teve repercussão na mídia em razão da conduta da organização envolvida no episódio, foi a atitude tomada pela rede varejista norte americana *Target* de tentar alterar os hábitos de consumo de suas clientes, por meio de técnicas estatísticas que identificavam a possibilidade de determinada consumidora estar grávida (DAVIS, 2012). Tal fato representa a aplicação de técnicas associadas ao *Big Data*, com implicações éticas e jurídicas.

Azevedo, Neves e Novo (2014) destacam ser necessário que o usuário tenha maior controle sobre quem pode acessar seus dados e o uso que as organizações estão dando a esses dados, no entanto, o tema demanda regulamentações para estabelecer padrões de identificação e de segurança dos dados pessoais.

Um antídoto para condutas antiéticas no ambiente do *Big Data* pode estar disponível no próprio conjunto de normas e regulamentos das organizações, que estabelecem uma série de valores e esclarecem que os colaboradores devem ter confiança e responsabilidade pessoal no processo de análise dos dados (DIAS; VIEIRA, 2013).

As organizações estão experimentando um novo paradigma no qual todos devem levar em consideração questões como a privacidade, a transparência, o rastreamento e como estão sendo utilizados os dados pessoais e corporativos.

Sendo assim, emerge a necessidade crescente de implementar proteções éticas que assegurem a privacidade dos dados.

4. Privacidade

A palavra privacidade, do latim (*privates*), tem o significado de separado do resto, portanto, que uma pessoa pode ficar afastada ou isolada em relação aos demais.

A preocupação com a privacidade antecede a era da internet. O artigo publicado em 1873, pelo juiz americano Tomas Cooley, define a privacidade como a limitação do acesso às informações de uma determinada pessoa, à própria pessoa e à sua intimidade, envolvendo as questões de anonimato, sigilo, afastamento e o direito de ser deixado em paz.

No mundo atual, no qual cada vez mais está presente o uso dos computadores e de mecanismos tecnológicos de comunicação, emerge, segundo Levy (1998), a questão do fim da privacidade e da preservação das informações, decorrente do fluxo informacional produzido e disponibilizado em grande escala na rede mundial de computadores.

A privacidade surge como um desafio no ambiente digital, onde as informações e os dados são gerados, sendo essencial o estudo do tema por parte da Ciência da Informação durante todo o ciclo de vida da informação. A privacidade das informações, de acordo com Smith, Milberg e Burke (1996), é uma das questões éticas da era da informação.

O avanço das tecnologias da informação, os serviços da internet e os *softwares de business intelligence* que realizam a coleta e mineração de grandes quantidades de dados são canais de vulnerabilidade para o acesso às informações (HONG e THONG, 2013).

A era do *Big Data* demanda novos modelos de privacidade. As atividades de identificação das novas informações pessoais são deduzidas por meio de análise preditiva dos dados coletados. Destaca-se a necessidade de inserir a privacidade no contexto do *Big Data*, no qual os indivíduos não só se preocupam com a coleta de dados, mas também com a forma como esses dados serão analisados e usados (MAI, 2016).

Um fator importante de privacidade é a opção de consentimento dada ao consumidor, ou seja, a oportunidade de decidir se o sistema pode ou não usar seus dados. Quando os sistemas de segurança que preservam a privacidade estão funcionando adequadamente, o usuário demonstra confiança para compartilhar as suas informações.

As organizações devem considerar o fato de que a confiança do usuário é mais lucrativa, com resultados positivos a longo prazo, e a quebra dessa confiança terá um impacto negativo. Tratar das preocupações dos usuários em relação à privacidade gera valor para as organizações (MANDIĆ, 2009).

4.1. Disposição para fornecer informações *on-line*

O processo para descobrir padrões de consumo e conhecimento tem tornado a mineração de dados um instrumento de destaque para que as organizações obtenham maior entendimento a respeito dos negócios e do mercado, a partir da análise dos dados minerados no *Big Data*, proporcionando o desenvolvimento de produtos alinhados às necessidades dos usuários. (PROVOST; FAWCETT, 2013).

Na visão do usuário, porém, fornecer informações com base nas suas necessidades e desejos específicos poderá levar a uma possível perda de privacidade (CHELLAPPA; SIN, 2005). A preocupação com a privacidade afeta negativamente a confiança dos usuários nos serviços tecnológicos *on-line* e, consequentemente, a disposição em fornecer suas informações pela internet (MARTINS, 2016).

4.2. As contradições dos usuários

Martins (2016), na discussão dos resultados da sua pesquisa sobre privacidade e confiança, ressalta que, apesar dos usuários acreditarem que fornecer informações pessoais na internet gera riscos, eles encaram que os benefícios trazem compensação. A despeito das profundas preocupações dos usuários com questões de privacidade e segurança, diariamente, os usuários publicam dados nas suas redes sociais.

Segundo Schoenbachler e Gordon (2002), a possibilidade dos usuários fornecerem informações pessoais *on-line* depende do tipo da informação. Os usuários têm mais restrição para informar dados financeiros em comparação com os seus dados demográficos ou de consumo.

A perspectiva de perdas de privacidade e uso indevido de informações no ambiente do *Big Data*, que contempla, por exemplo, o comércio eletrônico, as redes sociais, o *Internet Banking*, os dados do cidadão de posse dos governos, os provedores de internet e as seguradoras, podem influenciar a disposição do usuário em fornecer seus dados (FEATHERMAN; MIYAZAKI; SPROTT, 2010).

Para ter acesso aos serviços *on-line* gratuitos e revolucionários, os usuários concordam em fornecer suas informações sem uma avaliação dos riscos. Os usuários pagam por esses serviços com o que tem de mais precioso: dados pessoais e o seu comportamento no universo *on-line*.

4.3. Riscos à privacidade

A análise dos *Riscos à privacidade* corresponde à avaliação subjetiva: das potenciais perdas de controle sobre a confidencialidade das informações, incluindo as de identificação pessoal;

bem como do uso e da divulgação não autorizados desses dados (FEATHERMAN; MIYAZAKI; SPROTT, 2010).

Nas transações *on-line*, tanto as realizadas no comércio eletrônico como as financeiras, os usuários identificam a falta de informações sobre a privacidade e a potencial perda de controle das informações confidenciais como desvantagens para o uso desses serviços (BELANGER; HILLER; SMITH, 2002).

As organizações que fornecem serviços *on-line* têm a capacidade de coletar dados pessoais confidenciais de alto valor para explorá-los comercialmente (BELANGER; CROSSLER, 2011). Os autores afirmam que ocorrem perdas financeiras e de privacidade dos dados, em razão do uso indevido das informações durante as transações *on-line*.

Entre os fatores que geram vulnerabilidades no ambiente virtual, podem ser destacados os seguintes: i) nas transações *on-line*, os dados do seu computador podem ser comprometidos; ii) a transferência de dados *on-line* pode ser comprometida; iii) transações *on-line* por meio de redes públicas podem trazer riscos; e iv) os dados coletados durante a transação podem ser comprometidos e divulgados sem autorização do usuário (MILNE; CULNAN, 2004).

Para os autores, o risco à privacidade ocorre tanto durante a transação *on-line* como durante o armazenamento das informações do usuário, em razão do fato de as organizações não garantirem que os dados não serão compartilhados ou utilizados no ambiente do *Big Data* para a tomada de decisão.

A falta da privacidade das informações e a sua segurança não estão restritas às empresas que realizam negócios *on-line*. Os dados obtidos pelos governos também estão sujeitos a esses riscos, tanto pela infraestrutura tecnológica desatualizada como pela pouca cultura de Segurança da Informação (SI) nas instituições públicas.

4.4. Preocupação com a privacidade

No ambiente do *Big Data*, a informação trafega com velocidade. Moor (1997) afirma que a informação, quando digitalizada, trafega facilmente e rapidamente no ciberespaço, que é um ambiente resultante da interação de pessoas, *softwares* e serviços da internet, por meio de dispositivos tecnológicos e redes conectadas.

De acordo com o autor, as preocupações com a privacidade emergem quando a velocidade e conveniência fazem com que as informações pessoais tenham uma divulgação não autorizada.

As preocupações dos usuários não ficam restritas somente ao fato de ter uma divulgação não autorizada, mas também ao uso das informações pessoais de forma inadequada e sem permissão.

O avanço das tecnologias da informação, de acordo com Belanger e Crossler (2011), elevou o nível de preocupações com a privacidade das informações, motivando os pesquisadores de sistemas de informação a estudar soluções técnicas para tratar a informação.

A *Internet Privacy Concern* (IPC) é uma área de estudo que, segundo Hong e Thong (2013), tem crescido em decorrência do grande volume de informações que estão sendo coletadas, armazenadas, transmitidas e publicadas na internet, fomentando o ambiente do *Big Data*.

O IPC corresponde ao grau em que o usuário da internet está preocupado com as práticas realizadas pelos *sites* para a obtenção e o uso das informações pessoais (MALHOTRA; KIM; AGARWAL, 2004).

4.5. Confiança no ambiente *on-line*

A confiança se configura como um dos principais fatores que afetam o comportamento dos indivíduos diante de riscos e incertezas. Assim como a privacidade, a confiança é situacional e depende do contexto (LEE TURBAN, 2001).

A forma mais comum de fornecer aos usuários informações para estabelecer uma confiança nos serviços *on-line* diz respeito às declarações e políticas de privacidade. Dessa maneira, as organizações informam aos usuários sobre: serviços disponíveis na internet referentes a sua política de proteção de dados; quem está coletando os dados; e os limites de utilização.

No entanto, os usuários não dispensam seu tempo para ler essas políticas, uma vez que são dispostas em textos longos e escritos com termos jurídicos e técnicos.

Para Mandić (2009), uma forma de aumentar a confiança na privacidade de um serviço *on-line* é usar verificações de selo de privacidade, também conhecido como selo de segurança para site.

O selo de segurança indica que o site tomou medidas de proteção, seja para corrigir vulnerabilidades de segurança ou mesmo para criptografar informações que são trocadas entre o site e os usuários.

5. Segurança da informação

A Associação Brasileira de Normas Técnicas (ABNT), por meio da norma ABNT NBR ISO/IEC 27002:2013, define o termo Segurança da Informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos. Definição similar é apresentada por Manoel (2014).

Os princípios básicos da SI - a confidencialidade, a integridade e a disponibilidade - orientam a análise, o planejamento, a implantação e o controle de segurança para as informações das organizações.

As definições desses princípios são: i) *confidencialidade:* proteção das informações contra acesso não autorizado, independente da forma ou do local de armazenamento desses dados; ii) *integridade:* é a proteção de informações, aplicações, sistemas e redes contra mudanças intencionais, não autorizadas ou acidentais; e iii) *disponibilidade:* é a garantia de que as informações e os recursos estão acessíveis aos usuários autorizados, conforme a necessidade (KILLMEYER, 2006).

A gestão da SI envolve as seguintes atividades: i) elaborar uma Política de Segurança da Informação; ii) definir papéis e responsabilidades relacionados com a SI na organização; iii) desenvolver uma estrutura de controle com normas, práticas e procedimentos de SI; iv) estabelecer procedimentos de monitoramento para detectar e assegurar a correção de falhas de segurança; e v) promover a conscientização sobre a necessidade de proteger as informações (WILLIAMS, 2001).

As organizações enfrentam uma revolução nas práticas de gestão da informação, com o foco cada vez maior no valor global das informações protegidas e entregues (*Information Security Governance* – ITGI, 2006).

A segurança, como podemos ver, está relacionada com a capacidade da organização de proteger os dados dos usuários e evitar fraudes *on-line*, por meio de medidas de segurança.

5.1. Riscos à segurança das informações

A preocupação com a gestão adequada da informação no ambiente do *Big Data* envolve o espaço cibernético, que, segundo o autor Killmeyer (2006), é um ambiente propício para a exposição ao risco e no qual estão os ativos de informação, além dos meios de armazenamento, transmissão e processamento dos sistemas de informação.

Segundo Carvalho (2010), o espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas e/ou organizacionais, constituindo novo território, por vezes conhecido e desconhecido, a ser desbravado pelos bandeirantes do século 21.

Os projetos de *Big Data* trabalham com um grande volume de dados provenientes de diversas fontes, que demandam cuidados com a segurança. O armazenamento de um grande volume de dados pode se transformar em alvo de ataques e vazamento de informações sigilosas, o que pode gerar perdas de credibilidade para a organização.

As organizações devem adotar soluções e boas práticas de SI, adequação às normas e leis, definição de políticas, controle de acesso às informações críticas e de capacitação de equipes de TI, entre outras.

Os métodos tradicionais usados para proteger os sistemas de informações contra ameaças de segurança incluem a implementação de *firewalls*, regras de autenticação e o uso de redes privadas virtuais. (AL-SHAWI, 2011). Para o autor, cada uma dessas técnicas tem suas próprias vulnerabilidades e limitações e pode não ser capaz de proteger os recursos de ataques cibernéticos.

Os atacantes coletam e monitoram continuamente os dados dos usuários e das redes governamentais e privadas para tirar vantagem de fraquezas do sistema resultantes de falhas no *design* e na implementação de medidas de segurança, além das falhas ocasionadas em função do baixo nível de maturidade para a organização da informação.

6. Organização da informação

As repetidas ameaças cibernéticas nas organizações de todos os setores, tipos e tamanhos indicam a necessidade da implementação de práticas, métodos e processos relacionados com a organização da informação armazenada.

As instituições estão passando por transformações na forma de lidar com as informações. Considerando o volume de dados disponíveis no *Big Data*, torna-se necessário enfrentar o caos informacional com a utilização da Arquitetura da Informação (AI).

6.1. Arquitetura da informação

A Arquitetura da Informação permite a organização da informação para suporte às ações de gestão do conhecimento, ao mesmo tempo que visa a promover a acessibilidade à informação para a tomada de decisões (LIMA-MARQUES; MACEDO, 2006).

Com base na importância para a organização e apresentação da informação, Richard Saul Wurman utilizou pela primeira vez o termo Arquitetura da Informação em 1976. O criador do termo afirma que o arquiteto da informação dá clareza ao que é complexo, fazendo com que a informação possa ser compreendida (WURMAN, 2005).

Diante de todo esse volume de dados disponível, que pode ser utilizado para a tomada de decisões e melhoria da qualidade de vida, os usuários estão dispostos a trocar informações por serviços melhores, sem a devida atenção sobre as condições de privacidade oferecidas por esses serviços.

Com a frequente evolução de novas ferramentas tecnológicas, a cada dia, o usuário passa a ter mais e mais informação. A informação gerada de forma excessiva, sem critérios de seleção, organização e disseminação, fez surgir, como define Reis (2007), a síndrome da fadiga da informação, caracterizada por tensão, irritabilidade e sentimento de abandono causados pela sobrecarga de informação imposta ao ser humano.

Wurman (1991) afirma que uma edição do *The New York Times* publica, em um dia, mais informações do que um cidadão inglês normal poderia ter recebido durante toda a sua vida, no século 17. O autor adverte que mais dados não significam melhor compreensão, identificando a explosão da não informação.

Toda essa quantidade de informações, para Wurman (1991), leva à síndrome de ansiedade da informação, definida pelo autor como o resultado da distância cada vez maior entre o que compreendemos e o que achamos que deveríamos compreender.

O desenvolvimento e aperfeiçoamento das tecnologias da informação encurtam o caminho do usuário, tanto para obter como para fornecer informações. Todo esse avanço tem as suas vantagens, como também as desvantagens, sobretudo no que se refere à privacidade, à segurança, ao valor e a confiabilidade das informações.

A AI pode ser usada como uma estratégia para a organização da grande massa de informações disponível, para mitigar os riscos relacionados à privacidade, segurança, confiabilidade e perda de valor das informações.

As organizações públicas e privadas têm sido, cada vez mais, cobradas para publicar seus dados brutos em formato eletrônico. No entanto, antes dessa divulgação, visando a mitigar os riscos desse processo, os dados devem ser sanitizados, de modo a haver a remoção de identificadores pessoais. Para isso, podem ser utilizadas técnicas de anonimização (MONTEIRO; MACHADO; BRANCO JR, 2014).

6.2. Anonimização de dados

A anonimização de dados tem um vasto campo de aplicação, podendo ser adotada como medida de segurança. O termo anonimato representa o fato do sujeito não ser unicamente caracterizado dentro de um conjunto de sujeitos. O conceito de sujeito refere-se a uma entidade ativa, como uma pessoa ou computador (MONTEIRO, MACHADO, BRANCO JR, 2014).

O anonimato representa o fato de um registro não ser unicamente identificado em um conjunto de registros. Conjunto de registros pode ser um grupo de pessoas ou rede de computadores (PFITZMANN e KÖHNTOPP, 2005).

Para Camenisch, Fischer-Hübner e Rannenberg (2011), uma transação é considerada anônima quando os seus dados, individuais ou combinados, não possibilitam a associação para identificação de um registro em particular.

Os dados de indivíduos podem ser classificados como:

- Identificadores: atributos que identificam individualmente as pessoas (CPF, nome, identidade);

- Semi-identificadores: atributos que podem ser combinados com informações para reduzir a incerteza sobre a identificação das pessoas (data de nascimento, CEP, profissão, cargo, local de trabalho); e

- Atributos sensíveis: contêm informações sensíveis sobre as pessoas (salário, informações de saúde, despesas de cartão de crédito, hábitos de consumo).

As técnicas que podem ser utilizadas e/ou combinadas para a anonimização dos dados são as seguintes (MONTEIRO; MACHADO; BRANCO JR, 2014):

- Generalização: substitui os valores de atributos semi-identificadores por valores menos específicos e com semântica consistente;

- Supressão: exclui valores de atributos identificadores e/ou semi-identificadores da tabela anonimizada;

- Encriptação: utiliza esquemas criptográficos normalmente baseados em chave pública ou chave simétrica para substituir dados sensíveis por dados encriptados; e

- Perturbação: é utilizada para a substituição de valores dos dados reais por dados fictícios, para mascaramento de banco de dados de testes ou treinamento.

A técnica de perturbação procura alterar randomicamente os dados, com vistas a preservar as características dos dados sensíveis para o modelo de dados, utilizando as seguintes abordagens (CHEN; LIU, 2011):

- Condensação de dados: condensa os dados em múltiplos grupos e tamanhos predefinidos. Dentro de um grupo, não é possível distinguir diferenças entre os registros. Cada grupo tem um tamanho *k*, que é o nível de privacidade decorrente da condensação; e

- *Random Data Pertubation* (RDP): adiciona ruídos, de forma randômica, aos dados sensíveis. A maioria dos métodos utilizados para adicionar ruído randômico corresponde a casos especiais de mascaramento de matriz.

O mascaramento é utilizado na disponibilização de bases de dados para teste ou treinamento, com informações que não identificam os usuários, mas que pareçam ser reais. As técnicas de mascaramento de dados são (LANE, 2012):

- Substituição: substituição randômica de conteúdo por informações sem relação com o dado real;

- Embaralhamento (*Shuffing*): substituição randômica do dado real por um dado derivado da própria coluna da tabela;

- *Blurring*: técnica aplicada a números e datas. Muda o valor do dado por uma percentagem do seu valor original; e

- Anulação/Truncagem: substitui os dados sensíveis por valor nulos (*null*).

6.3. Modelos de anonimização

Diante da necessidade de se manter a privacidade dos dados e a segurança das informações, são apresentados, a seguir, os principais modelos de anonimização encontrados na literatura: *k-anonymity, l-divesity, t-closeness e b-likeness*.

- *k-anonymity*: demanda que qualquer combinação de atributos semi-identificadores seja compartilhada por pelo menos *k* registros, em um banco de dados anonimizado. Este modelo assume o pressuposto de que cada registro representa apenas uma pessoa;

- *l-diversity*: captura o risco da descoberta de atributos sensíveis em um banco de dados anonimizado;

- *t-closeness*: propõe a proteção contra a divulgação de atributo sensíveis; e

- *b-likeness*: apresenta-se como uma solução ao problema, que ocorre com menor frequência, de exposição de privacidade de valores de atributos sensíveis.

Visando a alcançar elevado nível de segurança, podem ser utilizadas ferramentas de segurança para: limitar o acesso aos dados; preservar a privacidade dos usuários; liberar dados úteis para mineradores de dados, sem divulgar as identidades dos usuários; desenvolver modelos de privacidade adequados para quantificar a possível perda de privacidade, em razão de diferentes ataques; e aplicar técnicas de anonimização (LEI XU; WANG; YUAN; REN, 2014).

7. Panorama da proteção de dados em 2018

No ano de 2018, aumentou o foco para a proteção das informações, quando se descobriu que os dados de 87 milhões de usuários do *Facebook* foram utilizados para traçar perfis de comportamento e influenciar politicamente a eleição americana, além do plebiscito que separou o Reino Unido da União Europeia.

Em setembro de 2018, o *Facebook* descobriu um ataque *hacker* que alcançou 50 milhões de usuários em todo o mundo. Em razão desse fato, vários perfis foram desconectados. Uma nova falha, ocorrida em dezembro, possibilitou a exposição das imagens postadas por 6,8 milhões de usuários.

O *The New York Times* revelou, em dezembro do mesmo ano, que o *Facebook* forneceu, sem autorização, dados de usuários a empresas como *Microsoft*, *Netflix*, *Spotify*, *Amazon* e *Yahoo*. As autorizações davam acesso às mensagens privadas. Segundo a reportagem, as empresas podiam ler, escrever e apagar as mensagens, além de ver todos os participantes em um tópico. A reportagem não detalha como isso era feito.

Onde meus dados foram parar? No caso da *Cambridge Analytica*, 300 mil pessoas foram pagas para participar de um teste de personalidade e fornecer seus dados. Elas, porém, foram usadas para coletar dados de outros. Com isso, foi possível criar um banco de dados com 87 milhões de pessoas, que não tinham ideia de que seriam envolvidas em campanhas políticas e outras atividades.

No ambiente do *Big Data*, existe uma fatia considerável de usuários que não se importa em fornecer seus dados nas redes sociais, mas não aceita que suas informações sejam usadas para vender mensagens com as quais não concorda.

Você é o produto: preocupe-se com o que fazem com seus dados.

O *General Data Protection Regulation* (GDPR)[4] regulamenta os direitos dos usuários europeus no que diz respeito à proteção e ao controle de seus dados pessoais. Por meio desse instrumento legal, as pessoas têm direito de saber se seus dados serão usados para gerar propagandas, se as informações serão geradas para criar perfis ou se as empresas que coletam dados vendem ou venderão esses dados a terceiros.

4 Acesse informações sobre o GDPR em https://eugdpr.org/.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), de n.º 13.709/2018, estabelece uma série de regras que empresas e outras organizações atuantes no País devem seguir para permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais.

8. Conclusão

A análise realizada neste artigo permite abordar a problemática acerca dos riscos à privacidade, segurança e organização da informação no ambiente do *Big Data*. Para discutir o tema, este estudo também apresentou questões que possibilitam identificar esses riscos e a preocupação gerada em função deles.

Fica evidente, no contexto do trabalho, o paradoxo dos benefícios que a coleta dos dados apresenta aos usuários, tendo em vista que os avanços tecnológicos estão promovendo: maior facilidade na busca por serviços; e o aumento da exposição dos usuários no espaço cibernético, com risco à privacidade.

No entanto, não é uma tarefa simples, para organizações que utilizam todo o potencial do volume de dados produzidos diariamente pelos usuários no ambiente do *Big Data*, manter um nível de segurança da informação adequado. Organizações de qualquer setor estão sujeitas às ameaças cibernéticas que são disseminadas pelos *hackers*.

Para que todo o potencial do *Big Data* possa ser explorado pelas organizações, é fundamental assegurar a privacidade, segurança e organização das informações. Vários modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários são propostos na literatura.

O avanço tecnológico não garante uma eficaz segurança da informação, sem uma conscientização do ser humano em relação à segurança. O acesso não autorizado a informações, lugares, objetos, entre outros tipos de dados, na organização, torna a segurança vulnerável, uma vez que as pessoas e as empresas interessadas nesses dados têm acesso indevido a essas informações.

As políticas de privacidade dos serviços *on-line* oferecidos pelas organizações devem estar em conformidade com a LGDP e GDPR. As referidas leis podem aplicar penalidades para as organizações que não se prepararem corretamente para a coleta, a gestão e o uso dos dados privados dos usuários.

Estar *compliance* com a LGDP e GDPR será não só uma oportunidade para melhorar e aumentar o nível de privacidade, segurança e gerenciamento de dados, como um diferencial para os novos modelos de negócio baseados em dados.

Em 2018, emerge o conceito de que somos o produto do espaço cibernético. Grande quantidade de informação é publicada no ciberespaço e os sistemas que recebem esses dados ficam cada vez mais inteligentes, ou seja, são capazes de fazer cruzamentos que nem imaginamos.

O *Big Data* é uma realidade. Os efeitos da tecnologia da informação estão no dia a dia das pessoas, dominando as suas vidas de formas que elas não imaginam.

Referências

AL-SHAWI, A. **Data mining techniques for information security applications.** John Wiley & Sons, Inc., v. 3, May/June 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO/IEC 27002:2013:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: 2013.

AZEVEDO, M.M.; NEVES, J.M.S.; NOVO, R.F. **O crescimento do *Big Data* e as possíveis implicações éticas do seu uso na análise das redes sociais.** *In*: WORKSHOP DE PÓS-GRADUAÇÃO E PESQUISA DO CENTRO PAULA SOUZA, 9., Estratégias Globais e Sistemas Produtivos Brasileiros, 2014.

BELANGER, F.; HILLER, J.S.; SMITH, W.J. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. **Journal of Strategic Information Systems.** v. 11 n. 3/4, p. 245–70, 2002.

BELANGER, F.; CROSSLER, R.E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. **Mis Quarterly**, v. 35, n. 4, p. 1017–1041, 2011.

BRASIL. Presidência da República. **Lei n.º 13.709, de 14 de agosto de 2018. Lei geral de proteção de dados.** Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014(Marco Civil da Internet). Disponível em: *http://www.planalto.gov.br/ccivil_03/_ Ato2015-2018/2018/Lei/L13709.htm.* Acesso em: 20 dez. 2018.

BRYNJOLFSSON, E; MCAFEE, A. *Big Data* - **a revolução da gestão.** Harvard Business Review, 2012.

CAMENISCH, J.; FISCHER-HÜBNER, S.; RANNENBERG, K. **Privacy and identity management for life.** Springer. 2011.

CARVALHO, P.S.M. **A Defesa cibernética e as infraestruturas críticas nacionais.** Núcleo de Estudos Estratégicos, Comando Militar do Sul, 2010.

CHELLAPPA, R.K.; SIN, R.G. Personalization versus Privacy: an empirical examination of the online consumer's dilemma. **Information Technology and Management**, v. 6, p. 181-202, 2005.

CHEN, K.; LIU, L. Privacy preserving data classification with rotation perturbation. In: IEEE International Conference on Data Mining, 5. IEEE Computer Society, 2011. **Proceedings...** 2011.

CHEN X.S.; YANG L.; LUO Y.G. Large data security protection technology. **Engineering Science and technology,** v. 49, n. 05, p. 1-12, 2017.

COMISSÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados.** Disponível em: *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt*. Acesso em: 20 dez. 2018.

DAVENPORT, THOMAS. *Big Data* **at work, uncovering the opportunities**, 2014.

DAVENPORT, THOMAS. **Dados demais! como desenvolver habilidades analíticas para resolver problemas complexos, reduzir riscos e decidir melhor**. 1. ed. Rio de Janeiro: Elsevier, 2014.

DAVIS, K. **Ethics of** *Big Data*. Sebastopol: O`Reilly Media, 2012.

DIAS, G.A; VIEIRA, A.N. *Big Data*: questões éticas e legais emergentes. **Revista Ciência da Informação,** Brasília, DF, v. 42 n. 2, p.174-184, 2013.

DRINKWATER, D. **Does a data breach really affect your firm's reputation.** Disponível em: *http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-reallyaffect-your-firm-s-reputation.html*, 2016. Acesso em: 20 dez. 2018.

EREVELLES, S.; FUKAWA, N.; SWAYNE, L. *Big Data* **consumer analytics and the transformation of marketing**. Journal of Business Research, 69(2), 897–904, 2016.

FEATHERMAN, M.S.; MIYAZAKI, A.D.; SPROTT, D.E. Reducing *online* privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. **The Journal of Services Marketing**, v. 24, n. 3, p. 219-229, 2010.

GOLDMAN, A., *et al.* Apache hadoop: conceitos teóricos e práticos, evolução e novas possibilidades. *In*: JORNADAS DE ATUALIZAÇÕES EM INFORMÁTICA, 31., 2012. **Anais...** 2012.

HONG, W.Y.; THONG, J.Y.L. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. MIS Quarterly, v. 37, n. 1, p. 275, 2013.

INFORMATION SECURITY GOVERNANCE – ITGI. **Guidance for information security managers**. EUA: 2006.

JANSSEN, M.; VAN DER VOORT, H.; WAHYUDI, A. Factors influencing *Big Data* decision-making quality. **Journal of Business Research**, v. 70, n. 1, p. 338–345, 2017.

JOHNSTON, A.C.; WARKENTIN, M. Fear appeals and information security behaviors: An empirical study. **MIS Quarterly**, v. 34, n. 3, p. 549 – 566, 2010.

KILLMEYER, J. **Information security architecture: an integrated approach to security in organization.** Florida: Auerbach Publications, 2006.

LANE, A. **Understanding and selecting data masking solutions: Creating secure and useful data**, 2012.

LEE, M.K.O.; TURBAN, E. A trust model for consumer Internet shopping. **International Journal of Electronic Commerce**, v. 6, n. 1, p. 75-91, 2001.

LEI XU, C.J.; WANG, J.; YUAN J.; REN, Y. **Information Security in *Big Data*: Privacy and Data Mining.** IEEE, v. 2, 2014

LEVY, P. A **Inteligência Coletiva: por uma antropologia do ciberespaço**. Rio de Janeiro: Loyola, 214 p. 1998.

LIMA-MARQUES, M.; MACEDO, F.L.O. Arquitetura da informação: base para a gestão do conhecimento. In: TARAPANOFF, K. (Org.). **Inteligência, informação e conhecimento em corporações**. IBICT, UNESCO, Brasília, 2006.

MAI, J-E. *Big Data* privacy: The datafication of personal information. **The Information Society**, 2016.

MALHOTRA, N.K.; KIM, S.S.; AGARWAL, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. **Information Systems Research**. v. 15, n. 4, p. 336–355, 2004.

MANDIĆ, M. Privacy and Security in E-Commerce. Art Design and Internet Technologies. **Privatnost I Sigurnost**, v. XXI, br. 2, str. 247–260, 2009.

MANOEL, S.S. **Governança de Segurança da Informação: como criar oportunidades para o seu negócio**. Rio de Janeiro: Brasport, 2014.

MARTINS, R. M. **Preocupação com a privacidade, confiança e disposição dos consumidores a fornecer informações** *on-line* **no contexto do** *Big Data*. Universidade Federal de Uberlândia, 2016.

MILNE, G.R.; CULNAN, M.J. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. **Journal of Interactive Marketing**, v. 18, n. 3, p. 15-29, 2004.

MONTEIRO, J.M.; BRANCO, E.C. JR; MACHADO, J.C. **Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem**. Tópicos em Gerenciamento de Dados e Informações, 2014.

MOOR, J. H. Towards a Theory of Privacy in the Information Age. **Computers and Society**, Sep., 1997.

PFITZMANN A; KÖHNTOPP, M. **Anonymity, unobservability, and pseudonymity – a proposal for terminology**. In Designing privacy enhancing technologies, Springer, 2005.

PROVOST, F.; FAWCETT, T. Data science and its relationship to *Big Data* and data-driven decision making. *Big Data*, v. 1, n. 1, p. 51-59, 2013.

REIS, G.A.D. **Centrando a Arquitetura de Informação no usuário.** Escola de Comunicação e Artes, Universidade de São Paulo. São Paulo, 2007.

SCHOENBACHLER, D.D.; GORDON, G.L. Trust and customer willingness to provide information in database-driven relationship marketing. **Journal of Interactive Marketing**, v. 16, n. 3, p. 2-16, 2002.

SHINATAKU, M; DUQUE, C.G.; SUAIDEN, E.J. Análise sobre o uso das tendências tecnológicas nos repositórios brasileiros. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**. João Pessoa, v. 9, n. 2, p. 001-012, 2014.

SMITH, H.J.; MILBERG, S.J.; BURKE, S.J. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. **MIS Quarterly**, v. 20, n. 2, p. 167-196, 1996.

WILLIAMS, P.A. Information Security Governance. **Information Security Technical Report**. v. 6, n. 3 p. 60–70, 2001.

WURMAN, R.S. **Information Architects**. Zurich, Schweiz: Gingko Press, 240 p., 1997.

WURMAN, R.S. **Ansiedade de Informação: como transformar informação em compreensão.** São Paulo: Cultura Editores Associados. 1991.

WURMAN, R S. **Ansiedade de Informação 2**. São Paulo: Editora de Cultura, 2005. 298 p. Tradução de Information Anxiety 2, Indianapolis, IN: QUE, 2001. 350 p.

ZWITTER, A. *Big Data* **ethics**. *Big Data* & Society, 2014.

CAPÍTULO 4

I APRESENTAÇÃO

Este capítulo apresenta o artigo 2 (dois) que descreve as competências educacionais para atender as demandas advindas do avanço tecnológico presente na 4ª. Revolução Industrial.

Destaca que a transformação digital presente tanto para as instituições públicas e privadas requerem novas competências para o desenvolvimento técnico e profissional das atividades com o uso das tecnologias presentes na 4ª. Revolução Industrial.

Para tanto, é necessário um conjunto de conhecimentos, competências educacionais, controles, políticas, processos, procedimentos, estruturas organizacionais, normas e regulamentos que, uma vez estabelecidos, precisam ser monitorados, avaliados, analisados e melhorados conforme a necessidade.

As exigências das novas competências para atender às demandas da Indústria 4.0, conhecida como a 4ª Revolução Industrial, tem impactos no processo de aprendizagem, o qual deve acompanhar o novo mercado, destacando a aplicação de novas tecnologias da Educação 4.0 e a revisão dos componentes curriculares.

A pesquisa realizada apresenta um relacionamento das competências com maior impacto para a Indústria 4.0 com as competências gerais estabelecidas pela Base Nacional Comum Curricular (2018) e as principais competências necessárias para o novo profissional. As competências requeridas foram classificadas como:

- Competências funcionais;
- Competências comportamentais; e
- Competências sociais.

Na aplicação do Modelo de Maturidade da AI foi identificado um baixo nível de maturidade nas atividades educacionais para treinar, disseminar e implementar a cultura de proteção de dados nas instituições. Sendo assim, diante dos desafios econômicos, ambientais e sociais, a educação é requisito necessário para o futuro das nações.

No que pese o modelo proposto ter como foco inicial as instituições de ensino, pesquisa e fomento, sua aplicação transborda para instituições que fazem uso de tecnologias para o seu modelo de negócio, entre elas as inseridas na Indústria 4.0.

A gestão da informação, a interoperabilidade dos sistemas, a internet das coisas, a inteligência artificial, a digitalização, os sistemas ciberfísicos, o *Big Data*, a computação em

nuvem, a logística da indústria conectada com o cliente, e a automação com sensores são grandes desafios para essas instituições.

Essas tecnologias combinadas geram um conjunto de oportunidades de produção competitiva, redução de custos de investimentos, centros de distribuição mais inteligentes, visão integrada da cadeia de suprimentos, tomadas de decisão mais eficientes e a evolução e maturação dos sistemas produtivos.

Diante desse contexto, de sistemas integrados, máquinas inteligentes e novos modelos de negócios baseados em dados publicados no ambiente do *Big Data*, a maturidade das estratégias de SegCiber combinadas com os mecanismos da AI deve ser sólida, estável, resiliente e madura, para assegurar a segurança dos dados em todos os elos da cadeia de valor da Indústria 4.0. Para tanto torna-se necessário para as organizações ter profissionais capacitados nas novas tecnologias.

AS NOVAS COMPETÊNCIAS EDUCACIONAIS NO CONTEXTO DA INDÚSTRIA 4.0[20]

Resumo

Com os avanços tecnológicos, o tema competências para atender as demandas da Indústria 4.0, conhecida como 4ª Revolução Industrial, entrou na pauta das discussões acadêmicas, empresariais e governamentais. As tendências para o aprendizado do profissional do futuro, envolvem o papel das instituições de ensino na produção de conhecimento e da multidisciplinaridade curricular para formação de competências no ecossistema da Indústria 4.0. Este trabalho discorre sobre as competências requeridas pela Indústria 4.0 e o seu relacionamento com as competências que a Base Nacional Comum Curricular traz para a Educação 4.0 e o processo de aprendizagem. A metodologia utilizada para analisar, compreender e interpretar o material qualitativo foi a análise de conteúdo. A pesquisa classifica-se como pesquisa aplicada quanto à sua natureza, com o objetivo de possibilitar maior familiaridade com o problema. Do ponto de vista dos objetivos, a pesquisa é descritiva, já que foi realizada uma análise das competências requeridas para o profissional da Indústria 4.0. Como resultado a pesquisa apresenta as principais competências identificadas como necessárias para o profissional da Indústria 4.0 e aponta para a necessidade de mudanças no processo de aprendizagem com uma revisão das matrizes curriculares. Nesse sentido, a aplicação de novas metodologias de ensino, as quais focam na criatividade, inovação, comunicação, resolução de problemas e conhecimentos técnicos fazem parte do motor da competitividade da indústria.

Palavras-chave: Educação 4.0, Competências, Indústria 4.0, Qualificação Profissional, Tecnologias

Abstract

Due to technological advances, the theme "competences to help the demands of Industry 4.0", known as the 4th industrial revolution, entered the academic, business and governmental agenda discussions. Emerging trends for future professional learning involve the role of educational institutions in knowledge production and curricular multidisciplinarity for skill building in the Industry 4.0 ecosystem. Thus, the present work discusses the competences required by Industry 4.0 and their relationship with the competences that the Brazilian´s Common National Curriculum Base brings to Education 4.0 and its learning process. The methodology employed to analyze, understand and interpret the qualitative material was content analysis. The research is classified as applied according to its nature, with the objective of allowing greater familiarity with the problem. From the point of view of the objectives, the research is descriptive, since an analysis of the competences required of the professionals for the Industry 4.0 was performed. As a result, the research presents the main competences identified as necessary for professional of Industry 4.0, and points to the need for changes in the learning process with a review of the curriculum matrices. In this sense, the application of new teaching methodologies, which focus on creativity, innovation, communication, problem solving, and technical knowledge are part of the engine of industry competitiveness.

Keywords: Education 4.0, Skills, Industry 4.0, Professional Qualification, Technologies

[20] Artigo *ipsis litteris* como enviado para a revista Educação e Pesquisa da Universidade de São Paulo.

1 INTRODUÇÃO

No contexto da Indústria 4.0, caracterizada pela combinação de diferentes tecnologias, em diversos graus de maturidade, aplicáveis a produtos e processos produtivos de forma híbrida, encontra-se uma esteira de grandes mudanças voltadas à transição da experiência de aprendizagem linear para a cultura de aprender a aprender e desenvolver competências para lidar com tecnologias de ponta.

Os processos de aprendizagem educacionais devem estar conectados com o cenário da indústria, da tecnologia e da inovação para capacitar futuros profissionais e requalificar os atuais, devido às novas demandas decorrentes dos avanços tecnológicos.

A informatização da sociedade aliada ao avanço das Tecnologias da Informação e Comunicações (TIC) e a sua convergência, evidenciada na era da informação, tem impactado a construção de novos cenários educacionais para o século XXI, os quais devem contemplar ambientes para estimular a criatividade, a inovação, o compartilhamento, a investigação, a interação, a educação e a cultura *maker*[21].

Na educação o movimento *maker* dialoga com as teorias construtivistas que partem de Jean Piaget[22], as quais compartilham o foco na construção de conhecimento multidisciplinar partindo da interação e participação ativa do aprendiz com o meio.

O matemático sul africano Seymour Papert, seguidor do construtivismo de Piaget, é um dos maiores visionários do uso da tecnologia na educação. Na década de 60, Papert já dizia que toda criança deveria ter um computador em sala de aula. Segundo o matemático, o aluno desenvolve o conhecimento conforme seus interesses. Dessa forma, é enfatizada a construção de objetos reais na produção do conhecimento por meio do uso de recursos tecnológicos.

A utilização de tecnologias e sistemas inteligentes, que são capazes de agregar valor aos processos e proporcionar uma maior competitividade e flexibilidade para as indústrias de manufatura e de serviços, demandam novas competências dos profissionais que irão se inserir no mercado de trabalho.

---

[21] Educação e Cultura *Maker*: Barack Obama, afirmou que "apoiar o movimento *maker* é essencial para uma nova revolução industrial". A proposta *maker* é que as pessoas tornem realidade suas próprias ideias, desenvolvam as próprias tecnologias, dispositivos e ferramentas, em projetos que reforcem suas leituras da sociedade (REVISTA GALILEU, 2014).

[22] Jean Piaget: suíço que revolucionou a forma de encarar a educação de crianças ao mostrar que elas não pensam como os adultos e constroem o próprio aprendizado.

Durante o processo de formação das competências requeridas, faz-se necessária uma análise do processo de aprendizagem visando seu alinhamento com o novo cenário e as novas perspectivas da Indústria 4.0.

Para Schwab (2016), diante desse novo cenário, preparar o profissional do futuro para interagir com os sistemas ciberfísicos[23] é um desafio para os envolvidos na formação de competências. A educação deve estar conectada com o cenário da indústria, da tecnologia e da inovação já que estamos em uma sociedade em rede[24] (CASTELLS, 2016).

A transformação em direção à digitalização das fábricas inteligentes, é uma realidade. A incorporação da digitalização à atividade industrial, integrando componentes físicos e virtuais é uma característica da Indústria 4.0.

Segundo Carlucci e Schiuma (2018), o desenvolvimento tecnológico na Indústria 4.0 é exponencial e sua integração com a revolução digital está transformando o ecossistema industrial. A digitalização passa a ocupar um papel central nas organizações.

Diante do referido cenário, será exigido que os trabalhadores do futuro estejam capacitados a desenvolver o seu papel em uma sociedade digitalizada e integrada, potencializada pelas tecnologias habilitadoras dessa indústria.

Este trabalho aborda as competências requeridas pela Indústria 4.0. Ele foi construído em 6 (seis) seções, sendo que, na seção 2 (dois), são apresentados os conceitos essenciais relacionados à Indústria 4.0, Educação 4.0, Base Nacional Comum Curricular e Aprendizagem.

Na seção 3 (três), são abordados os procedimentos metodológicos utilizados na pesquisa. Na seção 4 (quatro), consta uma análise das competências da Indústria 4.0. Por fim, na seção 5 (cinco), o estudo apresenta os resultados da pesquisa, e, na seção 6 (seis) a conclusão do trabalho.

2 REFERENCIAL TEÓRICO

O referencial teórico visa apresentar o suporte necessário para apoiar esta pesquisa na qual serão abordados os fundamentos teóricos para o entendimento do seu conteúdo.

[23] Sistemas ciberfísicos: permitem a fusão dos mundos físico e virtual, por meio de computadores embarcados que controlam os processos físicos gerando respostas instantâneas (KAGERMAN *et al*., 2013).
[24] Sociedade em rede: consiste que a base de todas as relações se estabelece por meio da informação e da sua capacidade de processamento e geração de conhecimentos (CASTELLS, 2016).

2.1 Indústria 4.0

A Indústria 4.0 ou Manufatura Avançada, conhecida como a 4ª Revolução Industrial, é consequência da era da tecnologia da informação e comunicações, a qual tem sua estrutura fundamentada na integração e no controle remoto de produção, por meio de sensores e equipamentos conectados em rede, associados a sistemas ciberfísicos, dados e serviços inteligentes de Internet – Plano de CT&I para Manufatura Avançada no Brasil, ProFuturo, Ministério da Ciência, Tecnologia, Inovações e Comunicações – (MCTIC, 2017).

A evolução tecnológica presente nesta revolução diferencia esse período dos movimentos industriais anteriores, pela possibilidade da convergência e a combinação de diversas tecnologias, em vários níveis de maturidade, serem aplicáveis a produtos e processos de produção. Entre esses processos, situa-se a incorporação da digitalização à atividade industrial, integrando componentes físicos e virtuais.

A referida integração possibilita maior captação, transporte, armazenamento e análise de dados em um ambiente de máquinas e equipamentos conectados, os quais emergem como fontes de dados e informações para auxiliar o processo de tomada de decisão.

A Estratégia Nacional de Ciência, Tecnologia e Inovação (ENCTI 2016-2022), indica como prioritárias as seguintes áreas tecnológicas para o desenvolvimento e soberania nacional relevantes para a Indústria 4.0: dispositivos eletroeletrônicos; tecnologias da informação e comunicações; *Big Data*; computação em nuvem; novos materiais; nanotecnologia; fotônica; impressoras 3D; sistemas ciberfísicos; internet das coisas; automação; energias renováveis; simulação e modelagem; interoperabilidade; segurança cibernética e propriedade intelectual.

O relatório do *Boston Consulting Group* (BCG, 2015), estabelece 9 (nove) tecnologias habilitadoras para a Indústria 4.0, determinantes para a produtividade e crescimento do setor produtivo, a saber:

- Robôs autônomos: realizam de forma precisa e segura uma série de atividades no ambiente industrial. Trabalham sem supervisão ou intervenção humana, interagindo de forma inteligente com outras máquinas;
- Manufatura aditiva: possibilita, com o uso de impressoras 3D, produzir itens personalizados, realizando a produção de peças, sem a necessidade de um molde físico, sendo uma de suas vantagens estratégicas a maior flexibilidade e capacidade de impressão de desenhos complexos;
- Simulação: permite propor soluções, testar hipóteses, aplicar mudanças, otimizar

processos e produtos durante a fase de desenvolvimento em um ambiente virtual, reduzindo os custos e tempo de criação;

- Integração horizontal e vertical de sistemas: visa uma operação industrial, por meio de um processo de transformação digital. Permite a unificação de toda a cadeia produtiva de forma automatizada, integrando sistemas das empresas, fornecedores, distribuidores e clientes. A integração horizontal relaciona-se com a opção de terceirização do desenvolvimento dos seus produtos. A vertical se refere à capacidade de integrar, reconfigurar e flexibilizar seus processos produtivos, visando a internalização da fabricação dos seus produtos;
- *Big Data*: busca coletar dados de diversas fontes com foco em gerar informações para acompanhamento e tomada de decisões em tempo instantâneo, visando melhorar o desempenho da Indústria 4.0;
- Computação em Nuvem: virtualiza estruturas, simplifica soluções e reduz custos de infraestrutura tecnológica. Permite o acesso, integração e suporte dos dados de qualquer localidade, aumentando a flexibilidade da gestão dos recursos tecnológicos;
- Segurança Cibernética: visa a proteção dos dados dos sistemas integrados, das máquinas inteligentes e novos modelos de negócios baseados em dados. As estratégias de segurança cibernética devem ser sólidas, estáveis, resilientes e maduras, bem como integradas à estratégia organizacional, para assegurar a segurança dos dados em todos os elos da cadeia de valor da Indústria 4.0; e
- Realidade Aumentada: realiza a integração do mundo virtual ao mundo real. Permite a sobreposição de objetivos gerados virtualmente em um ambiente real, por meio de dispositivos de visualização, como *smartphones, tablets* ou óculos especiais.

Entre as novas tecnologias apresentadas, a elevada conectividade, a capacidade de processamento e comunicação autônoma das máquinas, produtos e sistemas, aumentam de forma exponencial o fluxo de dados e informações trafegando por diversas redes, dentro e fora da indústria.

Nesse contexto, que tem impactos nos novos modos de produção, como na vida das pessoas, torna-se necessário estabelecer novas estratégias empresariais e políticas públicas.

Segundo o ProFuturo, do MCTIC (2017), a capacitação e competência em áreas tecnológicas aplicáveis à Indústria 4.0 são uma das principais referências para as políticas dos países sobre este tema. É preciso “aplicar esforços em inovação de produtos e processos

integrados e em educação para manufatura avançada" como a principal forma de alavancar a produtividade das empresas brasileiras.

Os avanços tecnológicos e o uso cada vez maior das tecnologias habilitadoras da Indústria 4.0, demandam atualização dos conhecimentos, habilidades e competências profissionais. Segundo Aires *et al.* (2017), um novo perfil de competências profissionais se faz necessário para dominar as novas tecnologias.

Diante dos avanços tecnológicos as instituições de ensino estão passando por mudanças de uma experiência de aprendizagem verticalizada para uma cultura do aprender a aprender onde a informação está disponível no ciberespaço[25], no qual desperta a Educação 4.0.

2.2 Educação 4.0

O termo Educação 4.0 é uma menção à 4ª Revolução Industrial, caracterizada pela convergência e possibilidades de combinação de diferentes tecnologias, em diversos graus de maturidade, aplicáveis tanto na forma de pensar, quanto de se relacionar e de agir do ser humano. O avanço tecnológico tem impactado o processo educacional na busca de um profissional inserido nesse ambiente, que surge para suprir uma lacuna do novo cenário laboral, redesenhado pela tecnologia.

Na era digital, dos serviços inteligentes, da integração dos sistemas, dos sensores e dos equipamentos de tecnologia da informação e comunicações conectados, manifestou-se o fenômeno do *Big Data*, composto pela explosão da quantidade de dados, disponibilidade e potencialidade decorrente do avanço das tecnologias de processamento, coleta e análise.

Sendo assim, surge o conceito *learning by doing* (aprender fazendo. Tradução livre), no qual a vivência e a experimentação são valorizadas, bem como o desenvolvimento de competências socioemocionais criativas. Esse conceito traz a ideia do aprendizado por meio de experiências, projetos, testes e mão na massa.

O novo modelo de educação deve considerar as questões relacionadas com a era da Indústria 4.0, tanto no que diz respeito à conectividade dos sistemas, facilidade de acesso ao conhecimento, novas mídias, velocidade da inovação, como também em relação ao desenvolvimento de novas habilidades e conhecimentos constantes.

[25] Ciberespaço: é um ambiente resultante da interação de pessoas, *software* e serviços da Internet por meio de dispositivos tecnológicos e redes conectadas (MOOR, 1997).

Com o objetivo de atender tais questões, os recursos tecnológicos devem facilitar e promover o processo de aprendizagem de forma autônoma para garantir a privacidade e segurança das informações.

Na Educação 4.0 os recursos tecnológicos disponíveis devem estar alinhados a um planejamento pedagógico estratégico, eficaz e com os objetivos de aprendizagem definidos, para que o aluno desenvolva competências para responder com rapidez às inovações tecnológicas, contribuindo com criatividade e colaboração na solução de problemas, objetivando ter um nível de reflexão sistêmica, assim, deixando de lado a simples replicação de conteúdo.

Em um cenário em constante evolução, segundo Aires *et al.* (2017), as competências mais requisitadas são: criatividade, inovação, comunicação, solução de problemas e conhecimentos técnicos.

Já para Resnick *et al.* (1991) aprender a aprender na era digital está relacionada com o desenvolvimento de um pensamento crítico, uma dimensão ética e responsável sobre o rigor e a orientação na busca e aplicação do conhecimento.

Os ambientes de construção de aprendizagem no ciberespaço devem oferecer aos alunos possibilidades para gerenciar, elaborar, planejar, compartilhar as informações e atuar em grupos para compartilhar o conhecimento, dentro do conceito aprender fazendo.

A revolução tecnológica está provocando mudanças efetivas na forma de como se constitui a dinâmica do ensino, assim, o uso das TIC passa a ser um recurso didático pedagógico interativo, utilizado por alunos e professores. Cada vez mais será necessário adequar o ambiente educacional às expectativas da sociedade conectada em redes.

Para Souza (2015), a educação conectada é integral, holística e complexa, que envolve a utilização digital da Internet, como espaço de diálogo, de interatividade, de compartilhamento de informações, desse modo, transformando o conhecimento em instrumento de cibercidadania.

Na Educação 4.0, realidade do século XXI, as instituições de ensino deixarão de ter o monopólio do conhecimento, pois haverá um novo modelo pedagógico inovador, por meio de um currículo multidisciplinar e da transferência de conhecimento de forma integrada na rede, devido às exigências do mercado para o desenvolvimento dos trabalhadores que enfrentarão os desafios da Indústria 4.0.

2.3 Base Nacional Comum Curricular

O caminho rumo à Educação 4.0 tem na Base Nacional Comum Curricular (BNCC)[26] um instrumento de partida para o desenvolvimento de competências que os alunos devem desenvolver ao longo da educação básica, de modo que tenham assegurados seus direitos de aprendizagem e desenvolvimento, em conformidade com os preceitos do Plano Nacional de Educação (PNE)[27].

O principal objetivo da BNCC é ser um balizador da qualidade da educação no país por meio do estabelecimento de um patamar de aprendizagem e desenvolvimento a que todos os alunos têm direito (BNCC, 2018).

O Quadro 1 apresenta as 10 (dez) competências gerais exigidas pela BNCC (2018). O conteúdo tem como base o documento oficial publicado no site do Ministério da Educação.

Quadro 1 – Competências da BNCC (2018)

<table>
<tr><th colspan="2">Competência</th><th>Dimensão</th><th>Subdimensões</th></tr>
<tr><td colspan="4">Conhecimento</td></tr>
<tr><td>Para: valorizar os conhecimentos sobre o mundo físico, social, cultural e digital</td><td>Visa: entender e explicar a realidade, continuar aprendendo e colaborar com a sociedade</td><td>Aprendizagem e Conhecimento</td><td>- Busca de informação
- Aplicação do conhecimento, aprendizagem ao longo da vida
- Consciência sobre o que, como e por que aprende
- Contextualização sociocultural do conhecimento</td></tr>
<tr><td colspan="4">Pensamento científico, crítico e criativo</td></tr>
<tr><td rowspan="2">Para: exercitar a curiosidade intelectual e utilizar as ciências com criticidade e criatividade</td><td rowspan="2">Visa: investigar causas, formular hipóteses, formular e resolver problemas e criar soluções</td><td>Criatividade</td><td>- Exploração de ideias
- Conexões
- Criação de processos de investigação
- Soluções
- Execução</td></tr>
<tr><td>Pensamento científico e crítico</td><td>- Formulação de perguntas
- Interpretação de dados
- Lógica e raciocínio
- Desenvolvimento de hipóteses
- Avaliação do raciocínio e explicação de evidências
- Síntese</td></tr>
</table>

[26] Base Nacional Comum Curricular: documento de caráter normativo que define o conjunto orgânico e progressivo de aprendizagens essenciais que todos os alunos devem desenvolver ao longo das etapas e modalidades da Educação Básica. Fonte: Ministério da Educação.
[27] Plano Nacional de Educação: determina diretrizes, metas e estratégias para a política educacional no período de 2014 a 2024. Fonte: Ministério da Educação.

Repertório cultural			
Para: valorizar diversas manifestações artísticas e culturais	Visa: desfrutar e participar de práticas diversificadas de produção artístico-cultural	Repertório cultural	- Desfrute - Expressão
		Identidade e diversidade cultural	- Investigação e identidade cultural - Consciência multicultural - Respeito à diversidade cultural - Mediação da diversidade cultural
Comunicação			
Para: utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital	Visa: expressar-se e compartilhar informações, experiências, ideias, sentimentos e, assim, produzir sentidos que levem ao entendimento recíproco	Comunicação	- Escuta - Expressão - Discussão - Comunicação por meio de plataformas analógicas e digitais
Cultura digital			
Para: compreender, utilizar e criar tecnologias digitais de forma crítica, significativa e ética	Visa: comunicar, acessar e produzir informações e conhecimentos, resolver problemas e exercer protagonismo e autoria	Computação e programação	- Utilização de ferramentas digitais - Produção de multimídia - Linguagem de programação
		Pensamento computacional	- Domínio de algoritmos - Visualização e análise de dados
		Cultura e mundo digital	- Mundo digital - Uso ético
Trabalho e projeto de vida			
Para: valorizar e apropriar-se de conhecimentos e experiências	Visa: entender o mundo do trabalho e fazer escolhas alinhadas à cidadania e ao seu projeto de vida com liberdade, autonomia, criticidade e responsabilidade	Projeto de vida	- Determinação - Esforço - Auto eficácia - Perseverança - Autoavaliação
		Trabalho	- Compreensão sobre o mundo do trabalho - Preparação para o trabalho
Argumentação			
Para: argumentar com base em fatos, dados e informações confiáveis	Visa: formular, negociar e defender ideias, pontos de vista e decisões comuns, com base em direitos humanos, consciência socioambiental, consumo responsável e ética	Argumentação	- Afirmação argumentativa - Inferências - Confronto de pontos de vista
		Consciência global	- Perspectiva global - Consciência socioambiental
Autoconhecimento e autocuidado			
Para: conhecer-se, compreender-se na diversidade humana e apreciar-se	Visa: cuidar de sua saúde física e emocional, reconhecendo suas emoções e as dos outros, com autocrítica e	Autoconhecimento e autocuidado	- Autoconsciência - Autoestima - Autoconfiança - Equilíbrio emocional - Saúde e desenvolvimento físico - Atenção plena e capacidade de reflexão

	capacidade para lidar com elas		
Empatia e cooperação			
Para: exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação	Visa: respeitar e promover o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade, sem preconceitos de qualquer natureza	Empatia	- Valorização da diversidade - Reconhecimento do outro - Acolhimento das perspectivas do outro
		Diálogo e cooperação	- Diálogo e convivência - Colaboração - Mediação de conflitos
Responsabilidade e cidadania			
Para: agir pessoal e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação	Visa: tomar decisões com base em princípios éticos, democráticos, inclusivos, sustentáveis e solidários	Responsabilidade	- Incorporação de diretos e responsabilidades - Tomada de decisão - Ponderação sobre consequências
		Valores	- Análise e incorporação de valores próprios - Postura ética
		Cidadania	- Participação social e liderança - Solução de problemas ambíguos e complexos

Fonte: Ministério da Educação – Adaptado pelo autor

Tais exigências demandam das instituições de ensino desafios relacionados com a sua missão de formação do profissional. A BNCC, referência nacional para formulação dos currículos dos sistemas e das redes escolares dos Estados, do Distrito Federal e dos Munícipios, bem como das propostas pedagógicas das instituições escolares, integra a política nacional de Educação Básica e tem potencial para contribuir com o alinhamento de outras políticas e ações, em âmbito federal, estadual e municipal, referentes à formação de professores, à avaliação, à elaboração de conteúdos educacionais e aos critérios para oferta de infraestrutura adequada para o pleno desenvolvimento da educação (BNCC, 2018).

Segundo a BNCC (2018), competência é definida como a mobilização de conhecimentos (conceitos e procedimentos), habilidade (práticas, cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas de vida cotidiana, do pleno exercício da cidadania e do mundo do trabalho.

Com isso, os gestores educacionais da rede pública e privada devem criar metodologias próprias na busca do desenvolvimento de espaços estruturados equipados com ferramentas, matérias-primas básicas, componentes e mecanismos, que possibilitam ao aluno assimilar conceitos teóricos por meio de projetos funcionais. Esses espaços são chamados de “espaços *maker”*, cujo objetivo é inserir o estudante na “educação *maker*” e “cultura *maker*”.

Nesse cenário, composto pela explosão da quantidade de dados e grandes inovações tecnológicas, a construção de contextos educacionais deve contemplar ambientes que estimulem a autonomia, a criatividade, o empreendedorismo, a colaboração e a investigação em forma de pesquisa e inovação, assim como está posta a cultura *maker*, a qual apresenta a ideia de que o aluno é estimulado a "pôr a mão na massa" e encontrar soluções criativas para seus problemas.

As instituições de ensino devem ter foco no seu compromisso de fomentar a reflexão e a análise crítica em relação ao conteúdo, bem como a oferta, de modo multidisciplinar dos recursos educacionais digitais disponíveis. A BNCC propõe levar o aluno para o centro do processo de aprendizagem, por meio das novas tecnologias. A educação deve formar um profissional questionador e motivado para aprender a aprender.

Para o ProFuturo (MCTIC, 2017), faz-se necessário um novo modelo acadêmico, objetivando alinhar os currículos de educação profissional e de nível superior, de modo que formem profissionais colaborativos, com capacidade sistêmica de executar projetos reais e capacidade analítica para tomada de decisão.

Na Indústria 4.0, o desenvolvimento profissional deve ser contínuo, já que os avanços tecnológicos são rápidos e demandam novas dinâmicas em relação aos perfis profissionais e às competências. Nesse sentido, é fundamental implementar treinamento e estratégias organizacionais para um aprendizado ao longo da vida profissional de uma pessoa. (KAGERMANN; WAHLSTER; HELBIG, 2013).

2.4 Aprendizagem

Segundo Veiga (2010), a aprendizagem é concebida como um processo de assimilação de determinados conhecimentos, habilidades intelectuais e psicomotoras, atitudes e valores, organizados e orientados no processo de ensino.

O processo de aprendizagem demanda que o professor tenha uma preparação didático-pedagógica com capacidade de identificar a forma de ensino e aprendizagem adequada para o aluno, de modo a fornecer aos envolvidos no processo de aprendizado um ambiente convidativo para exercer uma efetiva relação entre ensino e aprendizagem.

Para Gil (2011), um espaço de aprendizagem, deve compreender significados para: i) adquirir conhecimentos pela experiência ou atividade intelectual; ii) adquirir capacidade para fazer, praticar ou empreender uma ação; e iii) desenvolver a capacidade para exercer uma profissão.

A demanda da Indústria 4.0 por competências e sua multidisciplinaridade, muda o modelo do processo de aprendizagem. Bueno *et al*. (2017), destacam as seguintes metodologias de ensino e aprendizagem: i) metodologias ativas que forçam o aluno a sair da zona de conforto; ii) *lean education* focada na melhoria contínua; e iii) aprendizagem baseada em projetos, que explora projetos para focar em obter novas habilidades e competências.

A criação de um currículo baseado em competências é um direcionamento para o desenvolvimento de competências socioemocionais (BANCO MUNDIAL, 2018). O currículo multidisciplinar integra diferentes conhecimentos e fortalece o desenvolvimento de multicompetências.

As instituições de ensino necessitam ter capacidade de gerir o conhecimento aberto que ultrapassa as fronteiras da universidade, indústria e governo, conhecida como tríplice hélice, objetivando à inovação e ao empreendedorismo para gerar valor social (ETZKOWITZI; ZHOU, 2017).

Zen (2011), por sua vez, estabelece que para traçar novos planos para assegurar o processo de aprendizagem deve-se definir o papel do professor e do aluno, os quais são variáveis essenciais para o sucesso no processo de aprendizagem.

Na Educação 4.0 e para alcançar as competências requeridas pela 4ª Revolução Industrial, os professores devem estar aptos a trabalhar de maneira a integrar o meio virtual com o real, de modo a estabelecer metodologias inovadoras no processo de aprendizado.

O aprendizado torna-se baseado em problemas, em trabalho de equipes, sala de aula invertida e projetos que facilitam a integração entre o virtual e o real. As metodologias amparadas no ensino híbrido[28], qualificadas como práticas pedagógicas progressistas[29] no âmbito educacional, têm impacto no desenvolvimento da autonomia e de estímulo das competências requeridas pela Indústria 4.0 (RIOS; CÉSAR, 2019).

O aluno é parte responsável durante o processo de aprendizagem. É essencial que tenha um perfil participativo. Nas escolas progressistas os alunos desempenham atividades para ajudar a projetar currículos, formular perguntas, buscar respostas, pensar em possibilidades e avaliar o sucesso delas (KOHN, 2015).

[28] Ensino Híbrido: combina aprendizado *online* e *offline*. Integra a educação com a tecnologia. Fonte: Inovações em Educação – Porvir.org
[29] Práticas Pedagógicas Progressistas: os modelos propostos por Waldorf, Maria Montessori e Reggio Emilia, abordam visões para melhorar a sociedade humana, ajudando os alunos a desenvolverem seu potencial como pessoas inteligentes, criativas, dinâmicas a autoras ativas do seu próprio desenvolvimento (RIOS; CÉSAR, 2019).

Em meados dos anos 50, Albert Einstein foi questionado pelo Departamento de Educação do Estado de Nova York sobre o que a escola deveria enfatizar. Disse ele:

> "*A acumulação de material não deve sufocar a independência do estudante. A vantagem competitiva de uma sociedade não virá da eficiência com que a escola ensina multiplicação e tabela periódica, mas de modo como estimula a imaginação e criatividade (ISAACSON, 2007).*"

3 METODOLOGIA

A metodologia utilizada para o desenvolvimento deste trabalho classifica-se como Pesquisa Aplicada, quanto à sua natureza. A pesquisa tem como objetivo possibilitar maior familiaridade com o problema, para torná-lo mais explícito ou construir hipóteses. Com relação à forma de abordagem do problema, foi realizada uma pesquisa qualitativa para analisar, compreender e interpretar as referências bibliográficas.

Do ponto de vista dos objetivos, a pesquisa é descritiva, já que foi realizada uma análise das competências requeridas para o profissional da Indústria 4.0. Para analisar, compreender e interpretar o material qualitativo foi utilizada a "análise de conteúdo", segundo Bardin (2016), a qual representa um conjunto de técnicas de análise de comunicações que visam obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores que permitam a inferência de conhecimentos relativos às condições de produção/recepção destas mensagens.

A análise de conteúdo, conforme Bardin (2016) estabelece , apresenta 3 (três) fases: 1ª) pré-análise; 2ª) exploração do material; e 3ª) tratamento dos resultados, inferência e a interpretação. A fase de pré-análise visa organizar o material da pesquisa, sistematizar as ideias iniciais e desenvolver um plano de análise. Esta fase tem 3 (três) subfases: i) a escolha dos documentos que serão analisados; ii) a formulação das hipóteses e dos objetivos; e iii) a elaboração de indicadores para fundamentar a interpretação final (BARDIN, 2016).

Já a fase de exploração do material consiste na definição das categorias, identificação das unidades de registro visando à categorização e à contagem de frequência, e das unidades de contexto nos documentos. Para Bardin (2016), a referida fase possibilita ou não a riqueza das interpretações e inferências, sendo assim, a codificação, a classificação e a categorização são requisitos básicos na exploração do material.

Na 3ª. fase, os resultados são condensados para uma análise crítica. O pesquisador, tendo à sua disposição resultados significativos, pode então apresentar inferências e adiantar

interpretações relacionadas com os objetivos previstos ou a outras descobertas (BARDIN, 2016).

3.1 Fases da pesquisa

A pesquisa foi dividida nas seguintes fases. A 1a. fase, pré-análise, constituiu-se na realização da revisão da literatura, leitura crítica, seleção e organização do material para apoio teórico do estudo.

Na 2ª. fase, foram organizadas as fontes dos dados, análise dos títulos, resumos e palavras-chave. As referências selecionadas têm aderência ao tema de estudo, resultando em um conjunto de artigos analisados.

O material foi exportado para o gerenciador de referências *Mendeley*[30]. Com a organização do material no referido *software* foi aplicada a técnica de codificação. Vale ressaltar que organizar uma codificação consiste na escolha, recorte, enumeração, classificação e agregação das categorias (BARDIN, 2016).

Na 3ª. fase foi realizada interpretação dos resultados, por meio de processos de descrição, inferência e interpretação dos dados, a qual refere-se à análise dos resultados. Nesta fase foi possível identificar as competências com maior relevância para o profissional da Indústria 4.0.

4 COMPETÊNCIAS PARA INDÚSTRIA 4.0

McClelland (1973) foi um dos primeiros a definir competência. Segundo ele, o conceito apresenta traços de personalidade ou conjunto de hábitos que levam a um desempenho de trabalho mais eficaz.

Competência é um tema em pauta nas discussões acadêmicas e organizacionais. Estudiosos do tema, como Boyatzis, Fleury e Fleury, Zarifia, Bartram e Dutra apresentam diferentes perspectivas sobre competência.

Para Boyatzis (2008), as competências são definidas como uma capacidade e habilidade. O autor relaciona competência ao desempenho efetivo de alta performance no trabalho. O desempenho efetivo ocorre quando a capacidade é consistente com as necessidades do trabalho e do ambiente organizacional.

[30] *Mendeley*: https://www.mendeley.com/download-desktop/

Já Fleury e Fleury (2001), definem competências como um saber agir responsável e reconhecido, para mobilizar, integrar, transferir conhecimentos, recursos e habilidades, que geram valor econômico à organização e valor social ao indivíduo.

Conforme Zarifia (1999), as competências não ficam limitadas a um estoque de conhecimentos teóricos e empíricos obtidos pelo indivíduo, isto é, elas não se reduzem a um conhecimento específico.

Bartram (2012), por sua vez, argumenta que competências consistem em repositórios comportamentais, relacionados à forma como o conhecimento e as habilidades são utilizadas para o desempenho da atividade de trabalho. Já Dutra (2011), considera que as competências do indivíduo estão relacionadas com as entregas realizadas.

Segundo Fleury e Fleury (2001), a concepção de competência está relacionada aos seguintes termos: saber agir, mobilizar recursos, integrar saberes multidisciplinares e complexos, aprender a aprender, aderir a uma causa, assumir responsabilidades e ter uma visão estratégica

Para McClelland o conjunto de conhecimento, habilidades e atitudes constitui a competência. As competências, nessa perspectiva, são direcionadas a processos e tecnologias, bem como à interação, e podem variar de cargo para cargo (FRANÇA, 2014).

Para um melhor entendimento sobre conhecimento, habilidades e atitudes, seguem as perspectivas dos autores Durand, Chiavenato, Fleury e Fleury, Robbins, Decenzo e Wolter sobre os temas:

- Conhecimento: conjunto estruturado de informação que permite entender e interpretar o mundo (DURAND, 1998). Para Chiavenato (2014), o conhecimento constitui-se no acervo de conceitos, ideias, informações, experiências e aprendizagem sobre uma especialização profissional. O autor afirma que, na era da informação, esse é o recurso mais importante. No entanto, o conhecimento sem habilidade significativa e atitude torna-se improdutivo (DURAND, 1998);
- Habilidades: capacidade de transformar o conhecimento em ação (CHIAVENATO, 2014). Capacidade de aplicar o conhecimento na prática (FLEURY; FLEURY, 2001). Capacidade de utilizar e aplicar o conhecimento para solucionar problemas, criar e inovar (FRANÇA, 2014). Segundo os autores, Robbins, Decenzo e Wolter (2014), são três os tipos de habilidades: i) habilidades técnicas: saber como utilizar métodos e tecnologias para realizar o trabalho; ii) habilidades humanas: capacidade

para trabalhar com as pessoas, compreender atitudes e liderar equipes; e iii) habilidades conceituais: capacidade para lidar e trabalhar com as ideias e conceitos complexos, teorias e abstrações na organização; e

- Atitudes: é o saber fazer acontecer, responsável pela auto realização pessoal. Representa o estilo pessoal de fazer as coisas na prática, envolve a maneira de liderar, motivar, comunicar. Permite atingir as metas, assumir os riscos, ser agente de mudança e agregar valor (CHIAVENATO, 2014).

As competências dos profissionais inseridos na 4ª. Revolução Industrial demandam desafios alinhados aos movimentos que se caracterizam pela educação do aprender a aprender, aprender fazendo, colocar a mão na massa, características presentes na cultura *maker*.

No cenário da Indústria 4.0 as competências mais requeridas são: criatividade, inovação, comunicação, solução de problemas e conhecimentos técnicos (AIRES *et al.*, 2017).

5 RESULTADOS DA PESQUISA

A pesquisa realizada apresenta as principais competências identificadas como necessárias para o profissional da Indústria 4.0. As competências requeridas foram classificadas como: i) competências funcionais; ii) competências comportamentais; e iii) competências sociais (RIOS; CÉSAR, 2019).

As competências funcionais são entendidas como competências técnicas necessárias para o desenvolvimento técnico e profissional das atividades com o uso das tecnologias habilitadoras da Indústria 4.0. Demandam conhecimento avançado em tecnologia da informação. Conhecimento que poderá ser adquirido por meio de um curso de nível técnico ou superior. No entanto, é possível introduzir conceitos tecnológicos na educação básica e outras competências relacionadas com o conhecimento específico de estatística e matemática.

Segundo o Ministério da Educação (2018), esses são conhecimentos específicos do currículo de matemática para o Ensino Fundamental e Médio, fazendo com que essas competências sejam desenvolvidas em conjunto com as tecnologias relacionadas com o tema no Ensino Médio.

As competências comportamentais e sociais estão relacionadas com as competências pessoais e organizacionais, as quais são relevantes para a formação de indivíduos íntegros, protagonistas tanto no ambiente escolar como nas atividades profissionais. (RIOS; CÉSAR, 2019).

O *The Future of Jobs Report: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution* - *World Economic Forum*, realizado em 2016, aponta a perda de 7,1 milhões de empregos, enquanto 2 milhões serão criados, resultando em um impacto negativo de 5,1 milhões de postos de trabalho até 2020, decorrentes da presença das tecnologias habilitadoras da Indústria 4.0 no ecossistema industrial.

Tais mudanças nos postos de trabalho demandam competências comportamentais e sociais (pessoais e organizacionais) e competências funcionais (técnicas), apresentadas no Quadro 2.

Quadro 2 – Competências

Competências comportamentais e sociais - pessoais e organizacionais	Competências funcionais - técnicas
Afinidade com as TIC	Análise de dados e informações
Aprendizado	Aplicação de TIC
Responsabilidades	Aprendizagem de máquina
Capacidade de abstração	Automação
Capacidade de gestão	*Big Data*
Compreensão do processo	Capacidade de formular metas
Comprometimento	Capacidade de interagir com interfaces modernas
Comunicação	Compreensão do processo
Comunicação escrita	Computação em nuvem
Criatividade	Comunicação *Machine-to-Machine* (M2M)
Design	Conhecimentos de TIC
Fabricação	Desenvolvimento de sistemas
Flexibilidade	Estatística
Foco no cliente	Gestão de projetos
Inclusão	Codificação
Inovação	Pesquisa
Interdisciplinaridade	Internet das coisas
Interpessoalidade	Manufatura aditiva
Liderança	Manutenção de equipamentos
Mídias sociais	Manutenção preditiva
Negociação	Matemática
Operação global	Modelagem e programação
Pensamento analítico	Processamento de dados e informações
Pensamento crítico	Processos de fabricação
Pensamento estratégico	Realidade aumentada
Planejamento e organização do trabalho	Robótica - Inteligência artificial
Resolução de problemas	Segurança cibernética
Respeito ético	Segurança de redes
Tomada de decisão	Simulação
Trabalho em ambientes interdisciplinares	Sistema de gerenciamento de banco de dados
Vendas	Sistemas embarcados
	Sistemas integrados - sensores
	Tecnologias de rede
	Tecnologias *mobile*

Fonte: *Center of the future of work* (2016) - Prifti *et al.* (2017) – Adaptado pelo autor

Na análise das competências comportamentais e sociais – pessoais e organizacionais foi possível identificar as seguintes questões apresentando um maior impacto para a Indústria 4.0: pensamento analítico e crítico, a interdisciplinaridade, aprendizado, afinidade com TIC,

resolução de problemas, criatividade, inovação, comunicação, liderança, negociação, flexibilidade, respeito ético e tomada de decisão (PRIFTI *et al*., 2017).

Já as competências funcionais – técnicas que apresentam um maior impacto para a Indústria 4.0 – são as seguintes: análise de dados, interpretação de dados, conhecimentos em tecnologia da informação, robótica, inteligência artificial, aprendizagem de máquinas, automação, computação em nuvem, sistemas integrados, sensores, automação, sistemas embarcados, estatística, matemática, processos da manufatura, codificação, análise e processamento de informações, *Big Data* e segurança cibernética (PRIFTI *et al*., 2017).

As exigências das novas competências para atender as demandas da Indústria 4.0, têm efeitos no processo de aprendizagem, o qual deve acompanhar o novo mercado, destacando a aplicação de novas tecnologias da Educação 4.0 e a revisão dos componentes curriculares.

O Quadro 3 apresenta a correlação entre as competências com maior impacto para a Indústria 4.0 e as competências da BNCC (2018), descritas no item 2.3 deste artigo.

Quadro 3 – Competências da Indústria 4.0 vs Competências da BNCC (2018)

Competências da Indústria 4.0	Competências da BNCC
Afinidade com as TIC Aprendizagem de máquinas Automação Analisar, interpretar dados e informações *Big Data* Conhecimentos em tecnologia da informação Computação em Nuvem Estatística Matemática Codificação Processos da manufatura Pensamento analítico e crítico Resolução de problemas Segurança cibernética Sistemas embarcados Sistemas integrados Sensores	- Conhecimento para valorizar os conhecimentos sobre o mundo físico, social, cultural e digital
	- Pensamento científico, crítico e criativo para exercitar a curiosidade intelectual e utilizar as ciências com criticidade e criatividade
	- Comunicação para utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital
	- Cultura digital para compreender, utilizar e criar tecnologias digitais de forma crítica, significativa e ética
	- Argumentação para argumentar com base em fatos, dados e informações confiáveis
Aprendizado Criatividade Flexibilidade Respeito ético Tomada de decisão	- Conhecimento para valorizar os conhecimentos sobre o mundo físico, social, cultural e digital
	- Pensamento científico, crítico e criativo para exercitar a curiosidade intelectual e utilizar as ciências com criticidade e criatividade
	- Cultura digital para compreender, utilizar e criar tecnologias digitais de forma crítica, significativa e ética
	- Empatia e cooperação para exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação
	- Responsabilidade e cidadania para agir pessoal e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação
Comunicação Liderança	- Conhecimento para valorizar os conhecimentos sobre o mundo físico, social, cultural e digital

Competências da Indústria 4.0	Competências da BNCC
Negociação Trabalhar em ambientes interdisciplinares	- Comunicação para utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital
	- Empatia e cooperação para exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação
	- Responsabilidade e cidadania para agir pessoal e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação

Fonte: O autor

O novo modelo industrial, segundo Aires *et al.* (2017), exige que o profissional inserido na Indústria 4.0, coloque seus conhecimentos em prática utilizando a criatividade e inovação para resolução de problemas.

Chen e Zhang (2015), Muñoz (2016) e Garbie (2017) apontam a necessidade de uma revisão das matrizes curriculares para assegurar uma formação profissional adequada baseada nas tecnologias habilitadoras da Indústria 4.0.

6 CONCLUSÃO

Cabe pontuar que a Indústria 4.0 está mudando a forma de aprendizado. Em um cenário de avanços tecnológicos os recursos educacionais estão possibilitando uma democratização e acesso à informação e conhecimento no ciberespaço.

Na educação do século XXI a universidade não terá mais o monopólio do conhecimento, em função das exigências do mercado. Sendo assim, surge um modelo pedagógico inovador, por meio de um currículo multidisciplinar e do repasse de conhecimento das universidades e instituições de pesquisa de forma integrada (SANTOS; ALMEIDA FILHO, 2008).

Diante dos desafios econômicos, ambientais e sociais, a educação é cada vez mais importante para o futuro das nações. As políticas e práticas educacionais demandam uma atualização para o desenvolvimento de conhecimentos requeridos por meio dos avanços tecnológicos do mundo atual.

Novas políticas educacionais que visam o desenvolvimento das competências da Indústria 4.0 são essenciais para enfrentar os desafios econômicos, ambientais e socais na visão de líderes empresariais, organizações educacionais e pesquisadores (*National Research Council,* 2012).

O profissional do futuro deverá estar capacitado para lidar com as tecnologias habilitadoras da Indústria 4.0, sendo assim, novas competências terão impacto na educação desse profissional. As contribuições desta pesquisa ocorrem no sentido de apresentar os impactos educacionais das competências exigidas pelos novos modelos de negócios, os quais estão presentes na Indústria 4.0.

Em síntese, as organizações desenvolvem as competências essenciais para a realização de suas estratégias de negócio por meio dos processos de aprendizagem. O desenvolvimento de competências agrega valor econômico para organização e valor social para indivíduo.

REFERÊNCIAS

AIRES, Regina Wundrack do Amaral Reis; KEMPNER-MOREIRA, Fernanda; FREIRE, Patricia de Sá. **Indústria 4.0: Competências requeridas aos profissionais da quarta revolução industrial.** In VII International Congress of Knowledge and Innovation, 2017.

BANCO MUNDIAL. **Competências e Empregos: uma agenda para a juventude.** Síntese de constatações, conclusões e recomendações de políticas. 2018.

BARDIN, Laurence. **Análise de conteúdo.** 3ª. reimpressão da 1ª. edição. Título original: L´analyse de contenu. São Paulo: Ed. 70, 2016.

BARTRAM, Dave. **The SHL Universal Competency Framework.** SHL Group Limited. Thames Ditton Inglaterra: SHL Group plc, p. 11, 2012.

BASE NACIONAL COMUM CURRICULAR. **BNCC.** 2018. Ministério da Educação.

BOSTON CONSULTING GROUP. **Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries.** 2015.

BOYATZIS, Richard E. **Competencies in the 21st century.** Journal of Management Development. v.27, n.1, 2008.

BUENO, Fabiana Mafeis; SANTOS, Jessica Vieira; MARQUES, Ana Paula Oliveira; ALBANEX, João Henrique; MORAES, Priscilla Aparecida Vieira; BAPTISTELLA, Márcia Maria Teresa; RIGON, Ederson Leandro Barbosa. **Fábricas inteligentes e os novos desafios na formação dos engenheiros: os impactos da indústria 4.0.** Revista Engenharia em Ação UniToledo, v. 2, n. 2, p. 34-45, set./dez. 2017.

CARLUCCI, Daniela; SCHIUMA, Giovanni. **The power of the arts in business.** Journal of Business Research. 2018.

CASTELLS, Manuel. **A Sociedade em rede: A era da informação: economia, sociedade e cultura.** Edição Revista e Atualizada, 17. ed. São Paulo: Paz e Terra, 2016.

CFoW. **CENTER OF THE FUTURE OF WORK.** 2016. Disponível: <https://www.cognizant.com/future-of-work>. Acesso: 15 de mai. 2019.

CHEN, G.; ZHANG, J. **Study on training system and continuous improving mechanism for mechanical engineering.** The Open Mechanical Engineering Journal, 9, p. 7-14, 2015.

CHIAVENATO, Idalberto. **Gestão de pessoas: o novo papel dos recursos humanos nas organizações.** 4 ed. São Paulo: Manole, 494 p, 2014.

DIAS, G.A; VIEIRA, A.N. **Big Data: questões éticas e legais emergentes.** Revista Ciência da Informação, Brasília, DF, v. 42 n. 2, p.174-184, 2013.

DURAND, Thomas. **Forms of incompetence.** In: Proceedings Fourth International Conference on Competence-Based Management. Oslo: Norwegian School of Management. 1998.

DUTRA, Joel Souza. **Competências: conceitos e instrumentos para a gestão de pessoas na empresa moderna.** 1 ed., 9 reimpressão. São Paulo: Atlas, 2011.

ESTRATÉGIA NACIONAL DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO. **ENCTI 2016-2022.** Ministério da Ciência, Tecnologia, Inovações e Comunicações. Disponível: <https://www.mctic.gov.br/mctic/export/sites/institucional/ciencia/SEPED/Arquivos/PlanosDeAcao/PACTI_Sumario_executivo_Web.pdf>. Acesso: 25 nov. 2019.

ETZKOWITZ, Henry; LEYDESDORFF, Loet. **Universities and the global knowledge economy: a triple helix of university-industry-government relations.** Amsterdam: University of Amsterdam, 1995.

ETZKOWITZ, Henry; ZHOU, Chunyan. **Hélice Tríplice: inovação e empreendedorismo universidade-indústria-governo.** Estudos Avançados*,* 31(90), 23-48, 2017.

FLEURY, Maria Tereza L.; FLEURY, Afonso. **Construindo o conceito de competência.** In: Revista de Administração Contemporânea- RAC, Curitiba, v.5 (Edição Especial), p. 183–196, 2001.

FRANÇA, Ana Cristina Limongi. **Práticas de recursos humanos – PRH: conceitos, ferramentas e procedimentos.** 1 ed. 14. Reimpressão. São Paulo: Atlas, 266 p., 2014.

GARBIE, Ibrahim H. **Incorporating Sustainability/Sustainable Development Concepts in Teaching Industrial Systems Design Courses.** Procedia Manufacturing, 8, 417-423 p., 2017.

GIL, Antonio Carlos. **Didática do ensino superior.** São Paulo: Atlas, 2011.

KAGERMANN, Henning.; WAHLSTER, Wolfgang.; HELBIG, Johannes. **Securing the future of German manufacturing industry - recommendations for implementing the strategic initiative INDUSTRIE 4.0.** Final report of the Industrie 4.0 Working Group. Frankfurt: Acatech - National Academy of Science and Enginering. 97 p., apr. 2013.

KOHN, Alfie. **Progressive Education: Why it's Hard to Beat, But Also Hard to Find.** Bank Street College of Education. Retrieved, 2015.

ISAACSON, Walter. **Einstein, sua vida, seu universo.** Tradução Celso Nogueira *et al*. São Paulo. Companhia das Letras, 2007.

MCCLELLAND, David. **Testing for Competence Rather Than for "Intelligence".** America Psychologyst 28, Massachusetts, p. 1-28. 1973. Disponível: <https://www.therapiebreve.be/documents/mcclelland-1973.pdf>. Acesso: 07 nov. 2019.

MINISTÉRIO DA EDUCAÇÃO. **Base Nacional Comum Curricular - Educação é a base**. 2018. Disponível: <http://basenacionalcomum.mec.gov.br/>. Acesso: 14 dez. 2019.

MOOR, J. H. **Towards a Theory of Privacy in the Information Age, Computers and Society.** September 1997.

MUÑOZ, M. M. **Unconventional cognitive enhancement options addressing structural unemployment in the technological context of the fourth industrial revolution.** Gazeta de Antropologia, 32, n. 2. 2016.

NATIONAL RESEARCH COUNCIL. **Education for Life and Work: Developing Transferable Knowledge and Skills in the 21st Century.** Washington, DC: The National Academies, 2012.

PLANO DE CT&I PARA MANUFATURA AVANÇADA NO BRASIL, 2017, **ProFuturo**, Ministério da Ciência, Tecnologia, Inovações e Comunicações.
Disponível:
<https://www.mctic.gov.br/mctic/export/sites/institucional/tecnologia/tecnologias_convergentes/arquivos/Cartilha-Plano-de-CTI_WEB.pdf>. Acesso: 25 nov. 2019.

PLANO NACIONAL DE EDUCAÇÃO, 2014-2024, **PNE**, Ministério da Educação. Disponível em: < http://pne.mec.gov.br/>. Acesso em: 20 nov. 2019.

PRIFTI, Loina; KNIGGE, Marlene.; KIENEGGER, Harald.; KRCMAR, Helmut. A **Competency Model for "Industrie 4.0" Employees.** In 13th International Conference on Wirtschaftsinformatik (pp. 46–60), 2017.

RESNICK, L.B; LEVINE, J. M; TASLEY, S. D. **Perspectives on social shared congnition**. Washington: APA, 1991.

RIOS, Juliana; CÉSAR, Francisco, I, Giocondo. **EDUCAÇÃO 4.0 – Educação em tempos da 4º Revolução Industrial, necessidade de um novo olhar para a educação: um estudo de caso.** II SENGI - Simpósio de Engenharia, Gestão e Inovação, Águas de Lindóia, São Paulo, 2019.

ROBBINS, Stephen P.; DECENZO, David A.; WOLTER, Robert M. **A nova administração.** Tradução: Luciano Antonio Gomide. 1 ed. São Paulo: Saraiva, 2014.

SANTOS, Boaventura de Souza; ALMEIDA FILHO, Naomar de. **A universidade no século XXI: para uma universidade nova.** Coimbra: Almedina, 2008.

SOUZA, Márcio Vieira. **Mídias Digitais, Globalização, Redes e Cidadania no Brasil.** In: Souza, Márcio Vieira e Giglio, Kamil (Org.). Mídias Digitais, Redes Sociais e Educação em Rede Experiências na Pesquisa e Extensão Universitária. São Paulo: Blucher, 15-45, 2015.

SCHWAB, Klaus. **A QUARTA REVOLUÇÃO INDUSTRIAL**. 1a Edição ed. São Paulo: Edipro, 2016.

THE FUTURE OF JOBS REPORT, 2016. **World Economic Forum.** Disponível: < http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf>. Acesso: 25 mai. 2019.

VEIGA, I. P. Alencastro. **Ensino e avaliação: uma relação intrínseca à organização do trabalho pedagógico.** In: (org.) Didática: o ensino e suas relações. 17a ed. Campinas, SP: Papirus. p.149-169., 2010.

ZARIFIAN, Philippe. **Objectif compétence.** Paris: Liaisons, 1999.

ZEN, M. W. **Organização do Trabalho Pedagógico na Sala de Aula: Planejamento, Metodologia e Avaliação.** Indaial: Uniasselvi. 186 p.: il., 2011.

CONSIDERAÇÕES FINAIS

Este estudo propôs o desenvolvimento de um Modelo de Maturidade da AI para as instituições pesquisadas, considerando os modelos apresentados no referencial teórico, das normas ISO/IEC, dos mecanismos de AI e o do alinhamento com a LGPD, desta forma atendendo o objetivo geral e os objetivos específicos da pesquisa.

Foram identificados os seguintes modelos de maturidade durante a revisão de literatura: *Cybersecurity Capability Maturity Model*, *National Institute of Standars and Technology Cybersecurity Framework* e *The Community Cyber Security Maturity Model*.

No levantamento bibliográfico, a disponibilidade de artigos é reduzida na combinação dos termos *Information Architecture* AND *Maturity Models*, *Information Architecture* AND *Cyber Security*, *Information Architecture* AND *Privacy of Information* e *Information Architecture* AND *Protection of Data*, apesar da importância da AI para a organização, apresentação, segurança e estruturação das informações nas instituições.

Assim sendo, foi realizada a análise de conteúdo com a fase de pré-análise, que foi a revisão da literatura, a fase de exploração do material, na qual foram organizados os domínios dos modelos selecionados e a fase de tratamento dos resultados para a interpretação dos temas e domínios comuns entre os modelos. A definição dos temas possibilitou o agrupamento de 8 (oito) domínios para o modelo proposto.

O modelo é composto por práticas, para cada um dos domínios, agrupadas por objetivos que apóiam a estrutura do modelo. Os objetivos e as práticas são ordenados por nível de maturidade. Na estrutura do modelo foi realizado um alinhamento com os artigos da LGPD, apresentado no Quadro 6.

A utilização do modelo permite que as instituições tenham informações sobre o seu nível atual de maturidade da AI, identifiquem o nível de maturidade desejado e elaborem planos de melhoria para alcançar o nível de desempenho desejável, considerando os seus objetivos estratégicos para mitigar os riscos relacionados com as vulnerabilidades, ameaças e incidentes de SegCiber.

O modelo foi aplicado por meio de um questionário *on-line* em instituições de ensino, de pesquisa, de fomento, públicas da APF, públicas da APE e empresas privadas. O questonário foi encaminhado para os gestores de TIC das 35 (trinta e cinco) instituições participantes.

Com os resultados da pesquisa identificou-se que a maioria das instituições está no nível 0 para os domínios do modelo proposto. Tendo como base a discussão dos resultados apresentada neste trabalho, fica demonstrada a necessidade de implementar nessas instituições ações para mitigar os impactos sociais decorrentes dos riscos relacionados com a privacidade, com a SI e com a perda de valor das informações, bem como o alinhamento com a LGPD, por meio do modelo de maturidade proposto.

A análise realizada neste trabalho permite abordar a problemática acerca dos riscos à privacidade, à segurança e organização das informações no ambiente do *Big Data*. Para enfrentar o tema, este estudo apresentou questões que permitem identificar os riscos e a preocupação com a privacidade, com a organização, com a segurança e a perda de valor das informações.

Fica evidente no contexto do trabalho o paradoxo dos benefícios que a coleta dos dados apresenta aos usuários, tendo em vista que os avanços tecnológicos estão promovendo maior facilidade na busca por serviços *on-line* e o aumento da exposição dos usuários no espaço cibernético com risco à privacidade.

No entanto, não é uma tarefa simples para as instituições que utilizam todo o potencial do volume de dados produzidos diariamente pelos usuários no ambiente do *Big Data* manter um nível de SI adequado. As instituições de qualquer setor estão sujeitas às ameaças cibernéticas que são disseminadas pelos *hackers*.

Para que todo o potencial do *Big Data* possa ser explorado pelas instituições, é fundamental assegurar a privacidade, a organização, a segurança e o valor das informações. Conhecer o estado atual da maturidade da AI possibilita implementar melhorias nos processos para preservar a privacidade dos usuários.

O avanço tecnológico não garante uma SI eficaz, sem uma conscientização, treinamento e capacitação das pessoas em relação à segurança. O acesso não autorizado aos dados, informações e conhecimento nas instituições, as tornam vulneráveis, uma vez que elas têm acesso a informações indevidas.

As políticas de privacidade dos serviços *on-line* oferecidos pelas instituições devem estar em conformidade com a LGDP e GDPR. As referidas leis podem aplicar penalidades para as empresas públicas e privadas que não se prepararem corretamente para coleta, gestão e uso dos dados dos usuários.

Estar *compliance* com a LGDP e GDPR será uma oportunidade para melhorar e aumentar o nível de privacidade, organização, SI e o gerenciamento de dados, bem como um diferencial para os novos modelos de negócios baseados em dados.

Em 2018, emerge o conceito de que somos o produto do espaço cibernético. Grande quantidade de informação é publicada no ciberespaço e os sistemas que recebem esses dados ficam cada vez mais inteligentes, ou seja, são capazes de fazer cruzamentos que nem imaginamos.

O *Big Data* é uma realidade. Os efeitos da tecnologia da informação estão no dia a dia das pessoas e das instituições, dominando as suas vidas de formas que elas não percebem.

Diante dos desafios e dos avanços tecnológicos do mundo atual, as políticas e práticas educacionais demandam uma atualização para o desenvolvimento de conhecimentos requeridos.

Sendo assim, novas políticas educacionais que visam o desenvolvimento das competências para lidar com o avanço das tecnologias terão impactos no contexto educacional do Estado.

Em síntese, as instituições públicas e privadas buscam desenvolver as competências essenciais para a realização de suas estratégias de negócio por meio dos processos de aprendizagem. O desenvolvimento de competências agrega valor econômico para organização e valor social para indivíduo.

Com o atual avanço das tecnologias impulsionando novos modelos de negócios, sugere-se como trabalho futuro que as empresas que utilizam em seus processos produtivos sensores, equipamentos conectados em rede, associados a sistemas ciberfísicos, dados, realidade aumentada, robôs autônomos, manufatura aditiva e serviços inteligentes de Internet, venham conhecer o seu estado atual da AI e desenvolver novas competências, por meio de um modelo de maturidade para mitigar os riscos à privacidade, à organização e à segurança das informações, visando ganhos de competitividade e SegCiber.

REFERÊNCIAS

ABNT – NBR ISO/IEC 27002:2013: **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2013.

ABNT - NBR ISO/IEC 27032:2015: **Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética.** Rio de Janeiro: ABNT, 2015.

ADLER, Richard M. A. **Dynamic Capability Maturity Model for Improving Cyber Security.** Technologies for Homeland Security (HST), IEEE International Conference on. Decision Path, Inc. Winchester, MA USA. 2013.

AL-SHAWI, A. **Data mining techniques for information security applications.** John Wiley & Sons, Inc., Volume 3, May/June 2011.

ARAGÃO, Alexandre. **Notícias falsas da Lava Jato foram mais compartilhadas que verdadeiras.** 2016.

ARAÚJO, Carlos Alberto Ávila. **A Ciência da Informação como ciência social.** Revista Ciência da Informação, Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), v. 32, n. 3 (2003), Brasília, 2004.

ASCENSÃO, José de Oliveira. **Direito da Internet e Sociedade da Informação.** Rio de Janeiro: Forense, 2002.

ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE INFRAESTRUTURA DE HOSPEDAGEM NA INTERNET. **Impactos da Lei Geral de Segurança de Dados Pessoais sobre Negócios do Setor de Hospedagem.** 2018.

AZEVEDO, M. M.; NEVES, J. M. S.; NOVO, R. F. **O crescimento do big data e as possíveis implicações éticas do seu uso na análise das redes sociais,** IX Workshop De Pós-Graduação E Pesquisa Do Centro Paula Souza, Estratégias Globais e Sistemas Produtivos Brasileiros, 2014.

BAILEY, S. **Information architecture: a brief introduction**. 2003.

BARDIN, Laurence. **Análise de conteúdo.** 3ª. reimpressão da 1ª. edição. Título original: L´analyse de contenu. São Paulo: Edições 70, 2016.

BARRETO, Aldo de Albuquerque. **Os agregados de informação: memórias, esquecimento e estoques de informação.** DataGramaZero: revista de Ciência da Informação, Rio de Janeiro, v.1, n.3, p.1-13, ago. 2000.

BARROS, O. S. R., GOMES U. M, FREITAS W. L. **Desafios estratégicos para segurança e defesa cibernética.** Biblioteca da Presidência da República. Secretaria de Assuntos Estratégicos da Presidência da República. Brasília, 2011.

BEAL, Adriana. **Segurança da Informação.** São Paulo: Atlas, 2005

BECKER, J.; KNACKSTEDT, R.; POPPELBUS, J. Developing Maturity Models for IT Management. **Business & Information Systems Engineering,** 1(3): 213-222. 2009.

BELANGER, F.; HILLER, J.S.; SMITH, W.J. **Trustworthiness in electronic commerce: the role of privacy, security, and site attributes.** Journal of Strategic Information Systems. v. 11 n. 3/4, p. 245 – 70, 2002.

BELANGER, F.; CROSSLER, R.E. **Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.** Mis Quarterly, v. 35, n. 4, p. 1017 – 1041, 2011.

BORKO, H. Information science: what is it? **American Documentation**, v. 19, n. 1, p. 3-5, 1968.

BOYD, D.; CRAWFORD, K. **Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon.** Information, communication & society, v. 15, n. 5, p. 662-679, jun. 2012.

BRASIL. **Decreto nº 7.485, de 14 de novembro de 2012.** Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento na Administração Pública Federal. 2000.

_____. **Glossário das Forças Armadas - 4ª Edição.** 2007.

_____. **Instrução Normativa do Gabinete de Segurança Institucional nº 1**, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. 2008.

_____. **Desafios estratégicos para segurança e defesa cibernética.** Secretaria de Assuntos Estratégicos da Presidência da República. Organizadores: Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. Brasília, 2011.

_____. **Norma complementar nº 10, de 10 de fevereiro de 2012.** Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta. 2012.

_____. **Presidência da República.** Gabinete de Segurança Institucional. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018: versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília, 2015.

_____. **Lei Geral de Proteção de Dados.** De 14 de agosto de 2018.

_____. **Decreto nº 9.637, de 26 de dezembro de 2018.** Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. 2018.

_____. **Ministério da Defesa.** 2010. Disponível em:<www.defesa.gov.br/>. Acesso em: 30 de abril de 2019.

BRYNJOLFSSON, E; MCAFEE, A. **Big Data - A Revolução da Gestão.** Harvard Business Review, 2012.

CAMENISCH, J.; FISCHER-HÜBNER, S.; RANNENBERG, K. **Privacy and identity management for life.** Springer. 2011.

CASTELLS, M. **A Sociedade em Rede: do Conhecimento à Política.** Organizado por Castells, M. e Cardoso, G. 2005.

_____. **A sociedade em rede**: a era de informação: a economia, sociedade e cultura. Edição revista e atualizada. 17ª. edição. Editora Paz e Terra. São Paulo, 2016.

CARVALHO, Paulo Sergio Melo. **A defesa cibernética e as infraestruturas críticas nacionais.** Brasília, 2010.

CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION. **Internet Security, Online Privacy & Trust.** 2019.

CHAPIN, D. A.; AKRIDGE, S. **How can security be measured.** Information Systems Control Journal, v. 2, p. 43-47, 2005.

CHELLAPPA, R. K.; SIN, R. G**. Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma.** Information Technology and Management, v. 6, pp. 181-202, 2005.

CHEN, K.; LIU, L. **Privacy preserving data classification with rotation perturbation.** In Proceedings of the Fifth IEEE International Conference on Data Mining. IEEE Computer Society, 2011.

CHEN X.S.; YANG L.; LUO Y.G. **Large data security protection technology, Engineering Science and technology,** 49(05), 1-12, 2017.

CLARKE, R. A.; KNAKE, R. **Cyber war: the next threat to national security and what to do about it.** Ecco, 2011.

COFFEY, A.; HOLBROOK, B.; ATKINSON, P. **Qualitative Data Analysis: Technologies and Representations.** Sociological Research Online, Guildford, 1(1), 1996.

CRESWELL, J.W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto.** 3ª ed., Porto Alegre, Artmed, 296 p., 2010.

DAVENPORT, Thomas H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação.** São Paulo: Futura, 1998.

_____. **Big Data at work, uncovering the opportunities,** 2014.

_____. **Dados demais! Como desenvolver habilidades analíticas para resolver problemas complexos, reduzir riscos e decidir melhor.** 1ª Ed. Rio de Janeiro: Elsevier, 2014.

DAVIS, K. **Ethics of Big Data.** Sebastopol: O`Reilly Media, 2012.

DOS SANTOS, R., F. **Arquitetura da Informação que permite a integração entre Informações Organizacionais, Processos de Negócio e Sistemas de Informação.** UnB, Brasília, 2013.

DRINKWATER, D. **Does a data breach really affect your firm's reputation.** 2016.

DUTRA, ANDRE MELLO CARVALHÃES. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro.** Simpósio de Aplicações Operacionais em Áreas de Defesa. São José dos Campos, 2008.

EARP, J. B.; ANTON, A. I.; SMITH, L. A.; STUFFLEBEAM, W. H. Examining Internet privacy policies within the context of user privacy values**. IEEE Transactions on Engineering Management.** v. 52, n. 2, p. 227 – 236, 2005.

EREVELLES, S.; FUKAWA, N.; SWAYNE, L. **Big data consumer analytics and the transformation of marketing**. Journal of Business Research, 69(2), 897–904, 2016.

FEATHERMAN, M.S.; MIYAZAKI, A.D.; SPROTT, D.E. **Reducing *online* privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility.** The Journal of Services Marketing, v. 24, n. 3, p. 219-229, 2010.

FONSECA, J. J. S. **Metodologia da pesquisa científica.** Fortaleza: UEC, 2002.

FURNELL, S., & THOMSON, K.-L. **From Culture to disobedience: recognizing the varying user acceptance of IT security.** Computer Fraud & Security, (2), 5-10, 2009.

GANDELMAN, Henrique. **De Gutemberg à Internet: direitos autorais das origens à era digital.** 5. ed. Rio de Janeiro: Record, 2007.

GARTNER. **Information Technology.** 2019.

GOLDMAN, A., *et al.* **Apache hadoop: conceitos teóricos e práticos, evolução e novas possibilidades.** In: XXXI Jornadas de Atualizações em Informática, 2012.

GRISOTO, A., P.; SANT'ANA, R.,C.,G., SEGUNDO, J.,E.,S. **A questão da privacidade no contexto da Ciência da Informação: uma análise das Teses e Dissertações do Programa de Pós-graduação em Ciência da Informação da UNESP Campus de Marília.** Revista Ibero-Americana de Ciência da Informação. Brasília, 2015.

HADNAGY, C. **Social engineering: The Art of Human Hacking.** Indianápolis: Willey Publishing Inc., 2011.

HARGREAVES, A. **O Ensino na Sociedade do Conhecimento: a educação na era da insegurança.** Colecção Currículo, Políticas e Práticas. Porto: Porto Editora. 2003.

HONG, W.Y.; THONG, J.Y.L**. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies.** MIS Quarterly, v. 37, n. 1, p. 275, 2013.

IBM, Ponemon Institute. **The 2019 Study on the Cyber Resilient Organization.** 2019.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. ISACA. **COBIT 5.0, Modelo Corporativo para Governança e Gestão de TI da Organização.** 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: **ISO/IEC 29100:2011: Information technology—Security technique—Privacy framework.** 2011.

_____: **ISO/IEC 29101:2013: Information technology—Security technique—Privacy architecture framework.** 2013.

_____: **ISO/IEC 27018:2014: Information technology—Security technique—Code of practice for protection of personally identifiable information in public clouds acting as personally identifiable information processors.** 2014.

_____: **ISO/IEC 29190:2015: Information technology—Security technique—Privacy capability assessment model.** 2015.

_____: **ISO/IEC DIS 29134: Information technology—Security technique—Privacy impact assessment—Guidelines.** 2016.

_____: **ISO/IEC 29151:2017: Information technology – Security technique – Code of practice for personally identifiable information protection.** 2017.

_____: **ISO/IEC 27701:2019 - Security techniques for privacy information management.** 2019.

JANSSEN, M.; VAN DER VOORT, H.; WAHYUDI, A. **Factors influencing big data decision-making quality.** Journal of Business Research, 70(1), 338–345, 2017.

JOHNSTON, A. C.; WARKENTIN, M. **Fear appeals and information security behaviors: An empirical study.** MIS Quarterly, v. 34, n. 3, p. 549 – 566, 2010.

KERZNER, Harold. **Using the Project Management Maturity Model: Strategic Planning for Project Management.** Kindle Edition. 2006.

KILLMEYER, J. **Information Security Architecture: An Integrated Approach to Security in Organization.** Florida: Auerbach Publications, 2006.

LAUDON, Kenneth C., LAUDON, Jane P. **Sistemas de Informação**. Rio de Janeiro: Editora LTC – Livros Técnicos e Científicos, 9ª. ed., 2010.

LÉVY, Pierre. **A Inteligência Coletiva: por uma antropologia do ciberespaço.** Rio de Janeiro: Loyola, 1998.

_____. **Cibercultura.** 3. ed. São Paulo: Ed. 34, 2010.

LIMA-MARQUES, M.; MACEDO, F.L.O. Arquitetura da informação**:** base para a gestão do conhecimento. *In:* TARAPANOFF, K. (Org.). **Inteligência, informação e conhecimento em corporações.** IBICT, UNESCO, Brasília, 2006.

MAI, J-E. **Big data privacy: The datafication of personal information.** The Information Society, 2016.

MALHOTRA, NK; KIM, SS; AGARWAL, J. **Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.** Information Systems Research. 2004.

MANDARINO JÚNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro.** Recife, Cubzac, 2010.

MANDIĆ, M. **Privacy and Security in E-Commerce. Art Design and Internet Technologies.** Privatnost I Sigurnost, v. XXI, br. 2, str. 247–260, 2009.

MARTINS, R. M. **Preocupação com a privacidade, confiança e disposição dos consumidores a fornecer informações on-line no contexto do Big Data.** Universidade Federal de Uberlândia, 2016.

MATTELART, Armand. **História da sociedade da informação**. São Paulo: Loyola, 2002.

MCGEE, J.; PRUSAK, L. **Gerenciamento Estratégico da Informação**. 24 ed. Rio de Janeiro: Campus, 1994.

MENEZES, J. C. **Gestão de Segurança da Informação.** Leme Mizuno, 2006.

MILNE, G. R.; CULNAN, M. J. **Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices.** Journal of Interactive Marketing, v. 18, n. 3, p. 15-29, 2004.

MIRANDA, ANTONIO. **Sociedade da informação: globalização, identidade cultural e conteúdos.** Ci. Inf., Brasília, v. 29, n. 2, 2000.

MONTEIRO, J. M.; BRANCO, E. C. JR; MACHADO, J. C. **Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem.** Tópicos em Gerenciamento de Dados e Informações, 2014.

MOOR, J. H. **Towards a Theory of Privacy in the Information Age,** Computers and Society, Sep., 1997.

MOUTON, Francois, LEENEN, Louise, MALAN Mercia, VENTER H. **Towards an ontological model defining the social engineering domain.** 11th IFIP International Conference on Human Choice and Computers (HCC), Jul 2014, Turku, Finland. p.266 - 279.

NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY CYBERSECURITY FRAMEWORK - NIST. **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.0. Gaithersburg, MD: National Institute of Standards and Technology. 2014.

_____: NISTIR-8062. **Privacy Risk Management for Federal Information Systems.** 2017.

OLIVEIRA, W.A. **Modelos de Maturidade – Visão Geral.** Revista Mundo PM. Vol. 06, Ano 1, dez/jan. 2006.

PFITZMANN, A; KÖHNTOPP, M. **Anonymity, unobservability, and pseudonymity – a proposal for terminology.** In Designing privacy enhancing technologies, Springer, 2005.

PINHEIRO, L.V.R. **Processo evolutivo e tendências contemporâneas da Ciência da Informação.** Informação & Sociedade: Estudos, João Pessoa, v.15, n.1, p.13-48, jan/jun. 2005.

PRICEWATERHOUSECOOPERS, CYBERSECURITY AND PRIVACY. **Revitalizing privacy and trust in a data-driven world.** 2018.

PROVOST, F.; FAWCETT, T. **Data science and its relationship to Big Data and data-driven decision making.** Big Data, v. 1, n. 1, p. 51-59, 2013.

REIS, G.A.D. **Centrando a Arquitetura de Informação no usuário.** Escola de Comunicação e Artes, Universidade de São Paulo. São Paulo, 2007.

ROSENFELD, L.; MORVILLE, P. **Information Architecture for the World Wide Web**. 3. ed. Cambridge: O' Reilly, 2006.

ROYCE, WALKER. **CMM vs CMMI: from conventional to modern software management**. Rational Edge. 2002.

SCHOENBACHLER, D. D.; GORDON, G. L. **Trust and customer willingness to provide information in database-driven relationship marketing.** Journal of Interactive Marketing, v. 16, n. 3, p. 2-16, 2002.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva** - 2 ed. São Paulo: Elsevier, 2014.

SERASA EXPERIAN. **Pesquisa Lei de Proteção de Dados Pessoais e Pesquisa de Fraude e Identidade.** 2019.

SHINATAKU, M; DUQUE, C. G.; SUAIDEN, E. J. **Análise sobre o uso das tendências tecnológicas nos repositórios brasileiros.** Pesquisa Brasileira em Ciência da Informação e Biblioteconomia. João Pessoa, v. 9, n. 2, p. 001-012, 2014.

SILVA, E.L.; MENEZES, E.M. **Metodologia da Pesquisa e Elaboração de Dissertação.** 4ª ed., Florianópolis, Universidade Federal de Santa Catarina, 138 p., 2005.

SIMÕES, Isabella de Araújo Gracia. **A sociedade em Rede e a Cibercultura: dialogando com o pensamento de Manuel Castells e de Pierre Lévy na era das novas tecnologias de comunicação.** Revista eletrônica Temática ano V, n. 05, maio 2009.

SMITH, H. J.; MILBERG, S. J.; BURKE, S. J. **Information Privacy: Measuring Individuals' Concerns About Organizational Practices.** MIS Quarterly, v. 20, n. 2, p. 167-196, 1996.

TABOSA, H., R.; PINTO, V., B. **Análise dos modelos de comportamento de busca e uso de informação nas dissertações e teses dos PPGCI: Uma proposta de ampliação ao modelo de Ellis.** Investigación Bibliotecológica, Vol. 29, Núm. 65. México, 2015.

TAKAHASHI, Tadao (Organizador). **Sociedade da informação no Brasil: Livro Verde.** Brasília: Ministério da Ciência e Tecnologia, 2000.

TAYLOR, D. G.; DAVIS, D. F.; JILLAPALLI, R. **Privacy concern and online personalization: the moderating effects of information control and compensation.** Electronic Commerce Resarch, v. 9, n. 3, p. 203-223, 2009.

THE PRESIDENT. The President of the United States: **Executive Order 13636 Improving Critical Infrastructure Cybersecurity.** Federal Register/Presidential Documents, 78(33): Washington, DC: U.S. National Archives and Records Administration, February 19, 2013.

TOMIZAWA, Guilherme. **A invasão de Privacidade Através da Internet**. Curitiba: J.M. livraria jurídica, 2008.

U.S. DEPARTMENT OF DEFENSE. The Software Engineering Institute. **Capability Maturity Model® Integration (CMMI), Version 1.1.** Carnegie Mellon University, 2002.

VILICIC, Filipe. **Rede de mentiras.** Veja, ano 49, v. 2506, n. 48, p. 92-94, 30 nov. 2016.

WEBER, C. V.; PAULK, C. MARK; CURTIS, B.; CHRISSIS, M. B. **Capability Maturity Model for Software, Version 1.l.** Software Engineering Institute, Technical Report, CMU/SEI-93-TR-024, Carnegie Mellon University, 1993.

WERSIG, G.; NEVELING U. **The phenomeno of interest to information Science. Information Sciense**, v.9, p. 127-140, 1975.

WHITE, Gregory B. **The Community Cyber Security Maturity Model (CCSMM).** Hawaii International Conference on System Sciences. The Center for Infrastructure Assurance and Security. The University of Texas at San Antonio. 2007.

WURMAN, R. S. **Ansiedade de Informação:** como transformar informação em compreensão. São Paulo: Cultura Editores Associados. São Paulo, 1991.

_____. **Ansiedade de Informação 2**. Editora de Cultura. São Paulo, 2005.

XU, H. *et al.* Measuring mobile users' concerns for information privacy. **Thirty Third International Conference on Information Systems (ICIS).** Orlando: [s.n.]. 2012.

ZWITTER, A. **Big Data ethics.** Big Data & Society, 2014.