

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA  
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA  
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM  
SISTEMAS PRODUTIVOS

DIOGO PEDRIALI

CONVERGÊNCIA DE TI E TO:  
IMPACTOS NA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS COM  
MANUFATURA AVANÇADA

São Paulo  
Março/2021

DIOGO PEDRIALI

CONVERGÊNCIA DE TI E TO:  
IMPACTOS NA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS COM  
MANUFATURA AVANÇADA

Dissertação apresentada como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Napoleão Verardi Galegale.

São Paulo

Março/2021

FICHA ELABORADA PELA BIBLIOTECA NELSON ALVES VIANA  
FATEC-SP / CPS CRB-8390

P495c      Pedriali, Diogo  
Convergência de TI e TO: impactos na segurança da informação em empresas com manufatura avançada / Diogo Pedriali. – São Paulo: CPS, 2021.  
119 f. : il.

Orientador: Prof. Dr. Napoleão Verardi Galegale

Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). – Centro Estadual de Educação Tecnológica Paula Souza, 2021.

1. Convergência de TI e TO. 2. Segurança da informação. 3. Manufatura avançada. 4. Segurança cibernética industrial. 5. Sistemas produtivos. I. Galegale, Napoleão Verardi. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

DIOGO PEDRIALI

CONVERGÊNCIA DE TI E TO:  
IMPACTOS NA SEGURANÇA DA INFORMAÇÃO EM EMPRESAS COM  
MANUFATURA AVANÇADA

---

Prof. Dr. Napoleão Verardi Galeale

---

Prof. Dr. Carlos Hideo Arima

---

Prof. Dr. Washington Lopes da Silva

São Paulo, 15 de março de 2021

Dedico esta dissertação à minha esposa, aos  
meus pais, aos meus familiares, aos meus  
Mestres e a meus alunos.

## **AGRADECIMENTOS**

Agradeço aos meus familiares por estarem ao meu lado sempre, pelo incentivo, apoio, confiança e compreensão.

Ao Prof. Dr. Carlos Hideo Arima, por todas as orientações, os ensinamentos constantes, as oportunidades, a disponibilidade, a paciência e o crescimento que me proporcionou.

Ao meu orientador Prof. Dr. Napoleão Verardi Galegale pela grande colaboração em meu projeto, pelos ensinamentos constantes, a disponibilidade e a paciência em compartilhar seu conhecimento.

A todos os colaboradores da Unidade de Pós-Graduação, Extensão e Pesquisa ligados ao Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza que me deram suporte, com atenção e gentileza.

Agradeço aos demais professores, colegas e profissionais que contribuíram de alguma forma para a conclusão desta dissertação.

“Aprendizado sem reflexão é trabalho perdido;  
reflexão sem aprendizado é perigoso.”  
(Confúcio, séc. VI a.C.)

## RESUMO

PEDRIALI, D. **Convergência de TI e TO: impactos na segurança da informação em empresas com manufatura avançada.** 119 f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2021.

O presente trabalho tem por objetivo identificar, descrever e avaliar os impactos da convergência das atividades de TI e de TO na segurança da informação em empresas que possuem tecnologias características de manufatura avançada implantadas em seu processo produtivo. Foram utilizados três métodos de pesquisa científica: revisão sistemática utilizando o protocolo PRISMA-P para identificação do estado da arte sobre o tema; levantamento do tipo *survey*; e análise de conteúdo das respostas obtidas por meio da realização de entrevistas semiestruturadas com profissionais de segurança da informação que atuam nas áreas de TI e de TO. Foi utilizada a base de dados Periódicos CAPES na revisão sistemática. Os profissionais para o *survey* e para entrevista foram identificados por meio da rede *LinkedIn*, no grupo de profissionais *ScadaSecBR* e *TI Safe Community*. Foram identificados 20 estudos relevantes na revisão sistemática da literatura; houve a participação de 33 profissionais das áreas de TI e TO no levantamento tipo *survey*; e 11 profissionais da área de segurança da informação participaram da etapa de entrevistas. Para a análise dos resultados foram utilizadas técnicas de estatística descritiva e análise de conteúdo. Os resultados indicam que há aceitação da convergência parcial das atividades de TI e de TO pelos profissionais de segurança cibernética industrial, com impactos positivos de prioridade em segurança humana, em infraestrutura e em meio ambiente e impactos negativos, com o aumento da superfície de ataque, proveniente do avanço da IIoT e da interoperabilidade dos dispositivos inteligentes de TI e de TO.

**Palavras-chave:** Convergência de TI e TO. Segurança da Informação. Manufatura Avançada. Segurança Cibernética Industrial. Sistemas Produtivos.



## ABSTRACT

PEDRIALI, D. **Convergência de TI e TO**: impactos na segurança da informação em empresas com manufatura avançada. 119 f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2021.

This work focuses to identify, describe and evaluate the impacts of the IT and OT activities convergence on information security in companies that have advanced manufacturing characteristics implanted in their production process. Three scientific methods were used: systematic review using the PRISMA-P protocol to identify the state of the art about the topic; survey-type questionnaire; and content analysis of the answers obtained through semi-structured interviews with information security professionals working in the IT and OT areas. The Periódicos CAPES database was used for systematic review. The professionals for the survey research and for the interview were identified through the LinkedIn network, in the group of professionals ScadaSecBR and TI Safe Community. Twenty relevant studies were identified in the systematic review; thirty tree professionals from the IT and OT areas participated in the survey; and eleven professionals from the information security area participated in the interview stage. Descriptive statistics and content analysis techniques were used to analyze the results. The results indicate that there is acceptance of the partial convergence of IT and OT activities by industrial cybersecurity professionals, with positive impacts of priority on human security, infrastructure and the environment and negative impacts, with the increase of the attack surface, from the advancement of IIoT and the interoperability of intelligent IT and OT devices.

**Keywords:** IT and OT Convergence. Information Security. Advanced Manufacturing. Industrial Cybersecurity. Productive Systems.

## LISTA DE QUADROS

|            |  |     |
|------------|--|-----|
| Quadro 1:  | Características conceituais dos recursos de TI e de TO.....  | 30  |
| Quadro 2:  | Descrição das tecnologias pilares da Indústria 4.0. ....   | 35  |
| Quadro 3:  | Termos utilizados nos programas de incentivo a transformação digital industrial pelos países. .... | 38  |
| Quadro 4:  | Termos utilizados para pesquisa de artigos sobre o tema da pesquisa. ....                          | 51  |
| Quadro 5:  | <i>Strings</i> de busca. ....  | 52  |
| Quadro 6:  | Filtro de refinamento aplicado em cada <i>string</i> . ....  | 52  |
| Quadro 7:  | Relação de artigos selecionados para análise de qualidade. ....                                    | 55  |
| Quadro 8:  | Questões orientadoras para avaliação da qualidade dos artigos. ....                                | 56  |
| Quadro 9:  | Classificação de qualidade mediante pontuação do artigo. ....                                      | 57  |
| Quadro 10: | Pontuação e nível de qualidade dos artigos selecionados. ....                                      | 57  |
| Quadro 11: | Classificação dos artigos pelo agrupamento de termos. ....   | 59  |
| Quadro 12: | Categorização dos códigos utilizados na análise de conteúdo.....                                   | 71  |
| Quadro 13: | Impactos identificados da convergência de TI e TO na segurança da informação. ....                 | 95  |
| Quadro 14: | Relação entre objetivos, fundamentação, pontos de investigação e resultados esperados.....         | 109 |
| Quadro 15: | Instrumento aplicado aos profissionais das áreas de TI e de TO.....                                | 110 |
| Quadro 16: | Categorização e perguntas para a entrevista semiestrutura.....                                     | 118 |

## LISTA DE TABELAS

|            |  |     |
|------------|--|-----|
| Tabela 1:  | Caracterização da cibersegurança para convergência de TI e de TO. ....   | 32  |
| Tabela 2:  | Formação dos respondentes. ....  | 112 |
| Tabela 3:  | Nacionalidade das empresas onde os respondentes atuam. ....  | 112 |
| Tabela 4:  | Tamanho das empresas onde os respondentes atuam. ....  | 112 |
| Tabela 5:  | Setor econômico das empresas onde os respondentes atuam. ....  | 113 |
| Tabela 6:  | Função atual dos respondentes.....   | 113 |
| Tabela 7:  | Tempo na função atual dos respondentes. ....   | 113 |
| Tabela 8:  | Tecnologias de automação industrial que os respondentes interagem.....   | 114 |
| Tabela 9:  | Área de atuação predominante dos respondentes. ....  | 115 |
| Tabela 10: | Percepção da necessidade da convergência de TI e TO pelos respondentes. .  | 115 |
| Tabela 11: | Opinião dos respondentes sobre oportunidades para a empresa com a convergência de TI e TO.....                                 | 115 |
| Tabela 12: | Opinião dos respondentes sobre limitações para a empresa com a convergência de TI e TO.....                                    | 116 |
| Tabela 13: | Opinião dos respondentes sobre os impactos à segurança da informação na empresa com a convergência de TI e TO.....             | 116 |
| Tabela 14: | Opinião dos respondentes sobre tecnologias que oportunizam a convergência de TI e TO em empresas com manufatura avançada. .... | 116 |
| Tabela 15: | Declaração dos respondentes sobre participação voluntária na etapa de entrevistas. ....  | 117 |

## LISTA DE FIGURAS

|            |   |    |
|------------|---|----|
| Figura 1:  | Quantidade de incidentes de segurança cibernética industrial reportados por ano.....                                    | 19 |
| Figura 2:  | Quantidade de incidentes de segurança cibernética industrial por países.....  | 19 |
| Figura 3:  | Quantidade de incidentes registrados por setores industriais no mundo. ....   | 20 |
| Figura 4:  | Anos de ocorrência dos ataques cibernéticos industriais mais citados pelos autores pesquisados.....                     | 21 |
| Figura 5:  | Quantidade de incidentes registrados por setores industriais no Brasil. ....  | 22 |
| Figura 6:  | As quatro revoluções industriais.....   | 33 |
| Figura 7:  | Tecnologias pilares da Indústria 4.0. ....  | 34 |
| Figura 8:  | Integração do modelo RAMI4.0 e dos pilares tecnológicos da Indústria 4.0. ...   | 36 |
| Figura 9:  | Representação da interoperabilidade de tecnologias inteligentes.....  | 41 |
| Figura 10: | Painel de caracterização da convergência de TI e TO. ....   | 47 |
| Figura 11: | Fluxograma PRISMA-P da seleção de artigos para revisão sistemática. ....  | 54 |
| Figura 12: | Ano de publicação dos artigos selecionados.....   | 60 |
| Figura 13: | Agrupamento dos artigos selecionados por temas tratados nos estudos.....  | 61 |
| Figura 14: | Qualidade dos artigos selecionados .....  | 61 |
| Figura 15: | Nacionalidade dos participantes. ....   | 76 |
| Figura 16: | Formação dos participantes.....   | 77 |
| Figura 17: | Nacionalidade das empresas. ....  | 78 |
| Figura 18: | Tamanho das empresas. ....  | 78 |
| Figura 19: | Setor econômico das empresas. ....  | 79 |
| Figura 20: | Função atual dos respondentes.....  | 79 |
| Figura 21: | Tempo no cargo relatado pelos respondentes. ....  | 80 |
| Figura 22: | Interação pelos respondentes com sensores e demais dispositivos de instrumentação industrial. ....                      | 80 |
| Figura 23: | Interação pelos respondentes com sistemas de instrumentação de segurança, CLPs e dispositivos controladores locais..... | 81 |
| Figura 24: | Interação dos respondentes com IHM local e sistemas supervisórios locais....  | 81 |
| Figura 25: | Interação pelos respondentes com centro de controle de processo e sistema supervisório central.....                     | 82 |

|            |  |    |
|------------|--|----|
| Figura 26: | Interação pelos respondentes com MES, sistemas automatizados auxiliares à gestão de produção e logística. ....     | 82 |
| Figura 27: | Interação pelos respondentes com ERP, sistemas automatizados auxiliares para gestão estratégica de operações. .... | 83 |
| Figura 28: | Principais impactos à segurança da informação citados pelos respondentes devido a convergência de TI e TO. ....    | 83 |
| Figura 29: | Área de atuação majoritária dos respondentes. ....   | 84 |
| Figura 30: | Relato dos respondentes se sentem a necessidade da convergência das atividades de TI e de TO. ....                 | 84 |
| Figura 31: | Principais oportunidades citadas pelos respondentes mediante a convergência de TI e TO. ....                       | 85 |
| Figura 32: | Principais limitações citadas pelos respondentes sobre a convergência de TI e TO. ....                             | 86 |
| Figura 33: | Tecnologias que oportunizam a convergência das áreas de TI e de TO citadas pelos respondentes. ....                | 86 |
| Figura 34: | Quantidade de respondentes que aceitam participar da etapa de entrevista da pesquisa. ....                         | 87 |

## LISTA DE SIGLAS

|       |   |
|-------|---|
| ABDI  | Agência Brasileira de Desenvolvimento Industrial        |
| ABNT  | Associação Brasileira de Normas Técnicas                |
| APT   | <i>Advanced Persistent Threat</i>                       |
| CEO   | <i>Chief Executive Officer</i>                          |
| CIA   | <i>Central Intelligence Agency</i>                      |
| CIRWA | <i>Critical Infrastructures Ransomware Attacks</i>      |
| CISA  | <i>Cybersecurity and Infrastructure Security Agency</i> |
| CISO  | <i>Chief Information Security Officer</i>               |
| CLP   | Controlador Lógico Programável                          |
| CNI   | Confederação Nacional da Indústria                      |
| CPS   | <i>Cyber-physical system</i>                            |
| CSO   | <i>Chief Security Officer</i>                           |
| CRM   | <i>Customer Relationship Management</i>                 |
| CTO   | <i>Chief Technical Officer</i>                          |
| DIN   | <i>Deutsches Institut für Normung</i>                   |
| DMZ   | <i>Demilitarized Zone</i>                               |
| ERP   | <i>Enterprise Resource Planning</i>                     |
| ETH   | Estrutura Taxonômica Hierárquica                        |
| FMEE  | <i>Federal Ministry for Economic Affairs and Energy</i> |
| HAZOP | <i>Hazard and Operability Study</i>                     |
| IACS  | <i>Industrial Automation and Control Systems</i>        |
| IBP   | Instituto Brasileiro de Petróleo e Gás                  |
| ICS   | <i>Industrial Control System</i>                        |
| IEC   | <i>International Electrotechnical Commission</i>        |
| IEEE  | <i>Institute of Electrical and Electronic Engineers</i> |
| ISA   | <i>International Society of Automation</i>              |
| ISO   | <i>International Organization for Standardization</i>   |
| IHM   | Interação Humano-Máquina                                |
| IoT   | <i>Internet of Things</i>                               |
| IIoT  | <i>Industrial Internet of Things</i>                    |

|          |   |
|----------|---|
| M2M      | <i>Machine to Machine</i>   |
| MES      | <i>Manufacturing Execution Systems</i>  |
| MTU      | <i>Master Terminal Unit</i>   |
| NGFW     | <i>Next Generation Firewall</i>   |
| OPC UA   | <i>Open Platform Communications Unified Architecture</i>                          |
| PLM      | <i>Product Lifecycle Management</i>   |
| PRISMA-P | <i>Preferred Reporting Items for Systematic Review and Meta-Analysis Protocol</i> |
| RAMI 4.0 | <i>Reference Architecture Model Industrie 4.0</i>                                 |
| RISI     | Repositório de Incidentes de Segurança Industrial                                 |
| RTU      | <i>Remote Terminal Unit</i>   |
| SGSI     | Sistema de Gestão da Segurança da Informação                                      |
| SI       | Segurança da Informação   |
| SIS      | Sistema Instrumentado de Segurança  |
| SOC      | <i>Security Operations Center</i>   |
| TI       | Tecnologia da Informação  |
| TO       | Tecnologia Operacional  |
| TSN      | <i>Time-Sensitive Networking</i>  |
| UML      | <i>Unified Modeling Language</i>  |
| WEF      | <i>World Economic Forum</i>   |

## SUMÁRIO

|  |    |
|--|----|
| <b>1. INTRODUÇÃO</b>   | 18 |
| 1.1. Motivação   | 22 |
| 1.2. Justificativa   | 23 |
| 1.3. Objetivos   | 25 |
| 1.4. Proposições   | 25 |
| 1.5. Estrutura da dissertação  | 26 |
| <b>2. FUNDAMENTAÇÃO TEÓRICA</b>  | 27 |
| 2.1. Conceitos, definições e padrões                                     | 27 |
| 2.1.1. Tecnologia da informação  | 27 |
| 2.1.2. Tecnologia operacional  | 28 |
| 2.1.3. Convergência de TI e de TO  | 29 |
| 2.1.4. Manufatura avançada   | 32 |
| 2.2. Cibersegurança e padrões de segurança da informação para indústrias | 38 |
| 2.2.1. Série de normas ISO 27000   | 41 |
| 2.2.2. Série de normas ISA 62443   | 42 |
| 2.2.3. Série de normas IEC 62541   | 43 |
| 2.2.4. Norma IEEE 1722:2016  | 44 |
| 2.3. Integração dos modelos e características identificadas              | 45 |
| <b>3. METODOLOGIA</b>  | 48 |
| 3.1. Estratégia de pesquisa  | 49 |
| 3.2. Relação entre objetivos, métodos e resultados                       | 49 |
| 3.3. Revisão sistemática da literatura                                   | 49 |
| 3.3.1. Etapas da revisão sistemática                                     | 50 |
| 3.3.2. Visão geral dos estudos localizados                               | 53 |
| 3.3.3. Avaliação da qualidade dos documentos localizados                 | 56 |
| 3.3.4. Extração dos dados  | 60 |
| 3.3.5. Síntese dos estudos selecionados                                  | 62 |
| 3.4. Levantamento tipo survey  | 64 |
| 3.4.1. Sujeitos da pesquisa  | 65 |
| 3.4.2. Instrumento do survey   | 66 |
| 3.5. Entrevista semiestruturada  | 67 |



|  |     |
|--|-----|
| 3.5.1. <i>Instrumento da entrevista semiestruturada</i> .....  | 67  |
| 3.5.2. <i>Coleta de dados</i> .....  | 68  |
| 3.5.3. <i>Tratamento dos dados</i> .....   | 70  |
| <b>4. ANÁLISE DOS RESULTADOS</b> .....   | 73  |
| <b>4.1. Resultados obtidos com a revisão sistemática da literatura</b> .....                             | 73  |
| 4.1.1. <i>Oportunidades evidenciadas na revisão sistemática</i> .....                                    | 74  |
| 4.1.2. <i>Limitações evidenciadas na revisão sistemática</i> .....                                       | 75  |
| <b>4.2. Resultados obtidos com o survey</b> .....  | 76  |
| 4.2.1. <i>Características sociodemográficas dos sujeitos da pesquisa</i> .....                           | 76  |
| 4.2.2. <i>Caracterização das tecnologias de manufatura avançada</i> .....                                | 80  |
| 4.2.3. <i>Caracterização da gestão da segurança da informação</i> .....                                  | 83  |
| 4.2.4. <i>Caracterização da convergência de TI e TO pelos respondentes</i> .....                         | 84  |
| <b>4.3. Resultados obtidos com a entrevista semiestruturada</b> .....                                    | 87  |
| 4.3.1. <i>Achados sobre manufatura avançada na entrevista semiestruturada</i> .....                      | 87  |
| 4.3.2. <i>Achados sobre segurança da informação na entrevista semiestruturada</i> .....                  | 90  |
| 4.3.3. <i>Achados sobre convergência de TI e TO na entrevista semiestruturada</i> .....                  | 91  |
| <b>4.4. Discussão dos resultados obtidos</b> .....   | 94  |
| <b>5. CONSIDERAÇÕES FINAIS</b> .....   | 97  |
| 5.1. <i>Síntese do trabalho</i> .....  | 97  |
| 5.2. <i>Contribuições para Sistemas Produtivos</i> .....   | 99  |
| 5.3. <i>Contribuições para a Academia</i> .....  | 99  |
| 5.4. <i>Trabalhos futuros</i> .....  | 100 |
| <b>REFERÊNCIAS</b> .....   | 102 |
| <b>APÊNDICE A: Instrumento do survey</b> .....   | 109 |
| <b>A.1. Matriz de amarração para o desenvolvimento do instrumento de levantamento tipo survey.</b> ..... | 109 |
| <b>A.2. Instrumento do survey.</b> .....   | 110 |
| <b>APÊNDICE B: Dados coletados no levantamento tipo survey.</b> .....                                    | 112 |
| <b>B.1. Dados de perfil sociodemográfico.</b> .....  | 112 |
| <b>B.2. Dados associados a manufatura avançada.</b> .....  | 114 |
| <b>B.3. Dados associados a convergência de TI e TO e segurança da informação.</b> .....                  | 115 |
| <b>B.4. Dados associados a participação na entrevista.</b> .....   | 117 |
| <b>APÊNDICE C: Entrevista semiestruturada.</b> .....   | 118 |
| <b>C.1. Instrumento da entrevista semiestruturada.</b> .....   | 118 |

## 1. INTRODUÇÃO

O primeiro incidente industrial de segurança da informação registrado ocorreu em 1982, onde um *Trojan* (cavalo de Tróia) desenvolvido pela CIA foi inserido em *chips* de computadores que seriam utilizados no sistema de controle automatizado para a operação do então novo gasoduto transiberiano. Os computadores com os *chips* infectados passaram nas análises de qualidade realizadas pelos soviéticos; quando entraram em operação, o sistema de controle automaticamente alterou as velocidades de rotação das bombas e as configurações das válvulas de controle de fluxo da planta para ocasionar pressões internas no gasoduto muito além das aceitáveis para as juntas e soldas, o que resultou numa enorme explosão (SAFIRE, 2004) .

Nos últimos anos, o número de incidentes ciberfísicos em sistemas de controle industrial aumentou (AHMADIAN; SHAJARI; SHAFIEE, 2020).

Segundo o banco de dados denominado *Incident Hub*<sup>1</sup>, organizado pela empresa TI Safe (2020), 903 incidentes de segurança cibernética industrial foram registrados do ano de 1982 até setembro de 2020. O banco de dados organizado pela empresa TI Safe também conta com os registros presentes nas bases de dados do RISI (2015) e do Projeto CIRWA desenvolvido pelo laboratório de segurança cibernética em aplicação, pesquisa e educação CARE Lab (2020). Vale salientar que a escolha pela base de dados *Incident Hub*, se deu principalmente porque no universo desta pesquisa, mostrou-se como a base de dados que mantém, até o momento da execução desta pesquisa, a maior frequência de atualizações de informações e registros de incidentes divulgados publicamente. A consulta à base de dados *Incident Hub* se deu no mês de outubro de 2020.

Em estudo realizado por Menze (2020), foi evidenciado que o desafio mais importante para a segurança cibernética industrial atualmente continua sendo o de proteger os funcionários contra ferimentos ou morte, e em sequência são citados os desafios de proteção contra danos à qualidade do produto ou serviço, proteção contra a perda de informações proprietárias ou confidenciais e proteção contra o aumento de custo de resposta a incidentes e mitigação.

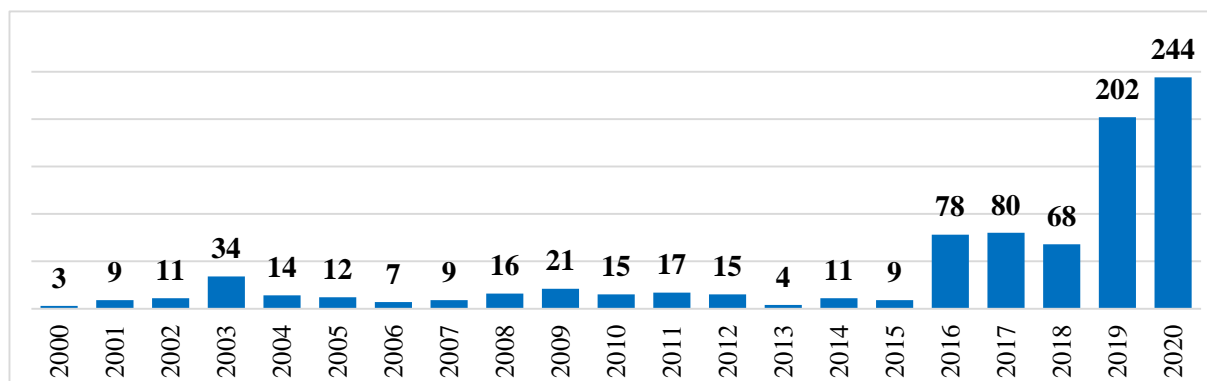
A Figura 1 apresenta a quantidade de incidentes de segurança cibernética industrial divulgados publicamente e inseridos no banco de dados da empresa TI Safe do ano 2000 ao

---

<sup>1</sup> <https://hub.tisafe.com/>

mês de setembro de 2020. É possível observar aumento na quantidade de incidentes ao longo dos anos e nota-se aumento abrupto a partir do ano de 2016, com 78 incidentes registrados, um aumento de aproximadamente nove vezes em comparação ao ano de 2015, que teve nove registros de incidentes de segurança da informação industrial.

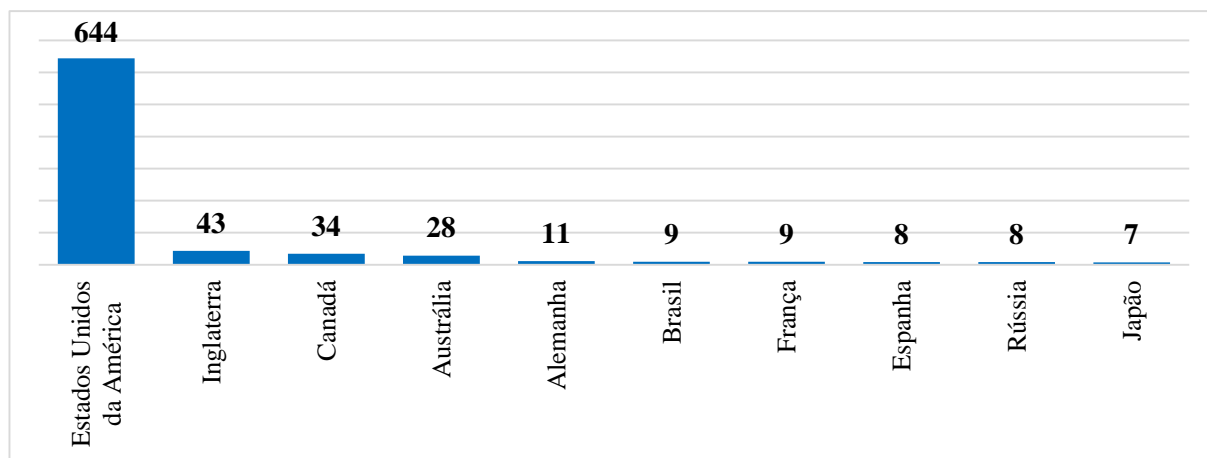
Figura 1: Quantidade de incidentes de segurança cibernética industrial reportados por ano.



Fonte: o autor.

Na Figura 2 é possível observar a distribuição das dez maiores quantidades de incidentes de segurança cibernética industrial nos registrados no banco de dados da empresa TI Safe país e é possível observar que os Estados Unidos da América é o país com maior quantidade de incidentes registrados, com 644 incidentes. O Brasil compartilha atualmente a sexta posição com a França, com o registro de 9 incidentes industriais a segurança da informação.

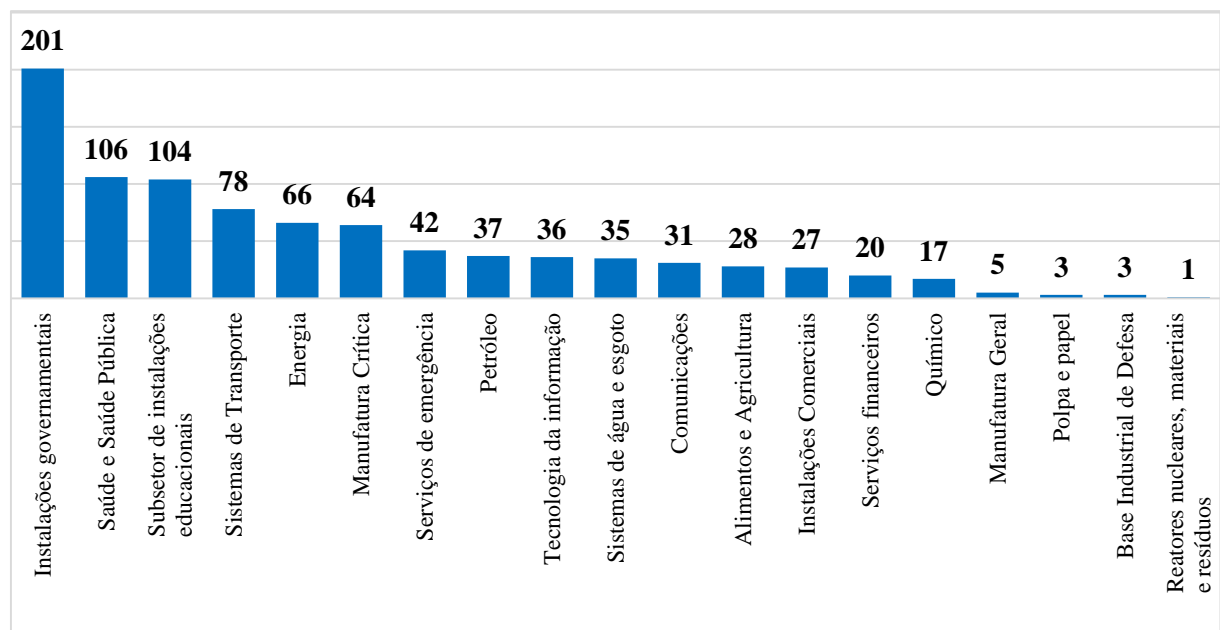
Figura 2: Quantidade de incidentes de segurança cibernética industrial por países.



Fonte: o autor.

A Figura 3 apresenta a quantidade de incidentes de segurança cibernética industrial categorizados por setores econômicos, categorização esta realizada pela empresa TI Safe; é possível observar que as indústrias que possuem a maior quantidade de incidentes registrados estão categorizadas como instalações governamentais, com 201 incidentes registrados no banco de dados. Outro dado relevante para esta pesquisa é que a somatória de incidentes categorizados como manufatura crítica e manufatura geral resulta em 69 incidentes.

Figura 3: Quantidade de incidentes registrados por setores industriais no mundo.



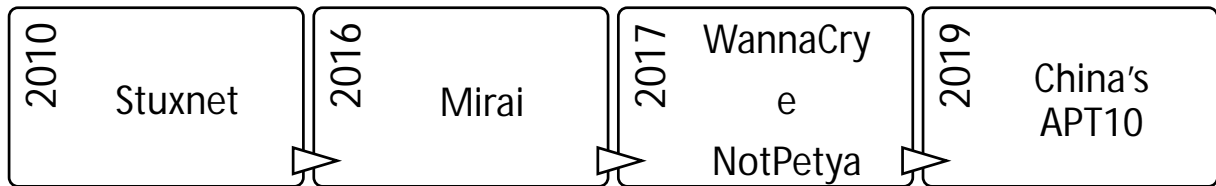
Fonte: o autor.

No relatório do projeto Kaspersky ICS CERT, de autoria de Goncharov (2020), é citado que as ameaças cibernéticas ao ambiente industrial estão se tornando mais direcionadas e como resultado, mais variadas e complexas. Além da existências de ocorrências envolvendo *ransomwares*, nota-se também a existência de mais famílias de *backdoors*, *spywares*, *exploits* Win32 e *malwares* construídos na plataforma .Net.

Muitos ataques cibernéticos foram realizados contra indústrias, com os mais variados objetivos, ao longo dos últimos anos, porém alguns são citados como mais frequência pelos autores pesquisados neste trabalho.

A Figura 4 apresenta a ocorrência dos ataques cibernéticos que afetaram a indústria e que foram publicamente divulgados.

Figura 4: Anos de ocorrência dos ataques cibernéticos industriais mais citados pelos autores pesquisados.



Fonte: o autor.

O Stuxnet é um *malware* complexo e multifacetado, do tipo *worm*, que desligou centrífugas de enriquecimento de urânio no Irã, atrasando o programa nuclear do país por vários anos, tanto que foi o primeiro a levantar o tema sobre o uso de armas cibernéticas contra sistemas industriais (SNOW, 2018).

O Mirai é um *malware* (*software* malicioso) que tem o objetivo de criar uma *botnet* (rede de computadores infectados). Em 21 de outubro de 2016 esse *malware* fez com que milhões de gravadores de vídeo, roteadores, câmeras IP e outros equipamentos inteligentes inundassem a Dyn, provedora de serviços de DNS, com solicitações. A Dyn simplesmente não foi capaz de suportar um ataque DDoS tão grande. O DNS, assim como os serviços que dependiam do sistema, ficaram indisponíveis (SNOW, 2018).

O *ransomware* criptógrafo WannaCry derrubou serviços de mais de 200 mil computadores, em 150 países, incluindo sistemas de controle de infraestruturas críticas. Algumas indústrias foram obrigadas a parar de produzir. Dentre os ataques recentes, o WannaCry foi o que obteve maior alcance (SNOW, 2018).

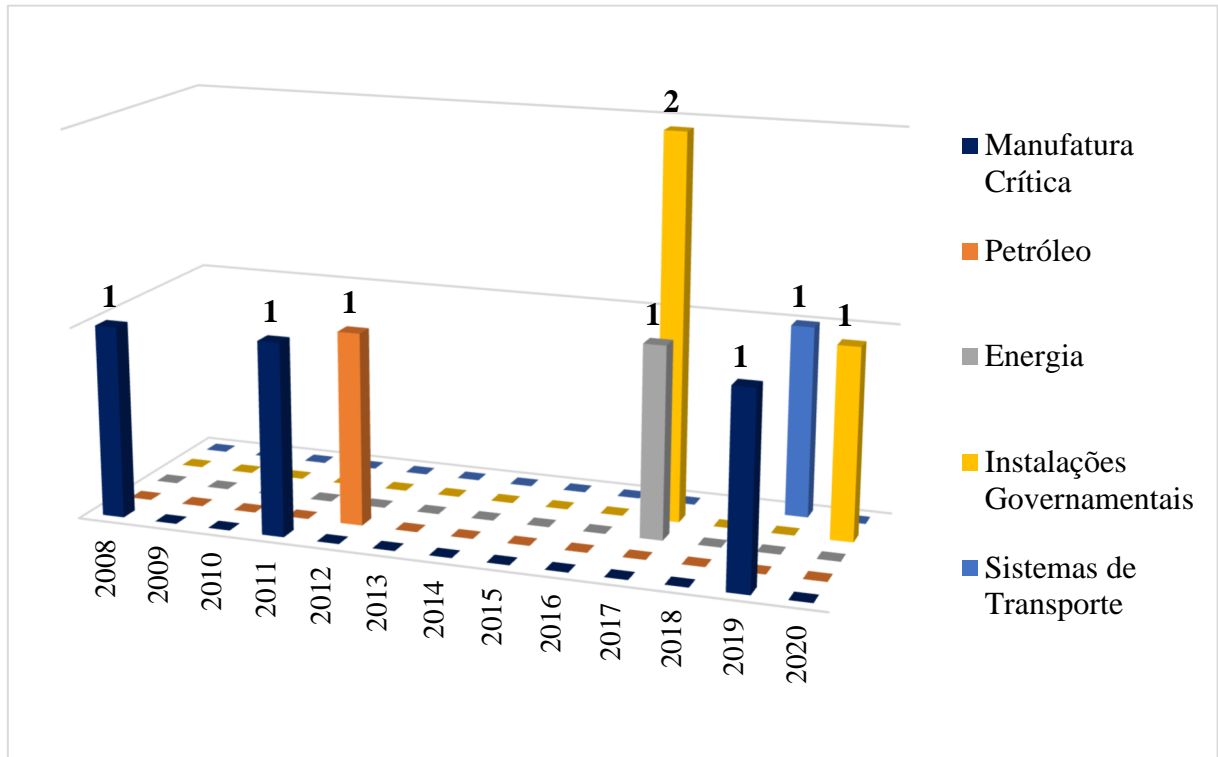
NotPetya é o nome de um *wiper*, um tipo de *malware* cujo objetivo principal é apagar dados presentes no disco rígido do computador infectado, que em 2017, atingiu usuários do *software* financeiro MeDoc. O NotPetya é considerado o ataque cibernético global mais caro da história (SNOW, 2018).

O China's APT10, como é chamado pelo Serviço Federal de Investigação dos Estados Unidos da América (FBI) um grupo de *hackers* de ameaça persistente avançada, que buscam afetar a água, as luzes, os dados dos clientes, os funcionários, e a propriedade intelectual de empresas (ROMEO, 2020).

Quando se analisa os registros de incidentes de segurança da informação industrial no Brasil, nota-se, conforme apresentado na Figura 5, que a maior partes dos ataques que

ocorreram no período de 2008 a setembro de 2020 focaram os setores de manufatura crítica com três ocorrências e instalações governamentais, também com três ocorrências.

Figura 5: Quantidade de incidentes registrados por setores industriais no Brasil.



Fonte: o autor.

Com base nas figuras e nos dados anteriormente apresentados é possível observar o aumento da quantidade de incidentes à segurança da informação em ambientes industriais no decorrer dos últimos anos, o que mostra que a atenção de sujeitos mal intencionados não somente se limitam aos ambientes comuns associados as responsabilidades da área de TI, mas ataques à segurança da informação de sistemas ciberfísicos comuns as plantas de infraestrutura crítica e manufatura avançada, que constituem em grande parte as atividades da área de TO, também vêm sendo realizados.

### 1.1. Motivação

Frente ao crescente aumento da quantidade de incidentes de segurança da informação nos setores industriais é importante: o estudo do estado da arte do tema; a identificação de como está sendo tratada a segurança da informação pelas empresas que fazem uso de tecnologias

comuns a manufatura avançada; a identificação da intenção de convergência das atividades de TI e TO em prol da segurança da informação e como está sendo realizado este processo; e a identificação dos impactos associados a convergência das atividades de TI e TO para a segurança da informação.

O avanço da tecnologia provocado pela manufatura avançada e pela RAMI 4.0 motiva a pesquisa científica para o entendimento da segurança da informação em indústrias, considerando os dados que trafegam desde o chão de fábrica até o mais alto nível administrativo empresarial.

Embora não haja muito na literatura acadêmica para descrever a convergência de TI e de TO e seus efeitos, evidências anedóticas reunidas de profissionais indicam que isso está ocorrendo. À medida que a TI é cada vez mais usada para exploração e análise de dados, e à medida que o TO fornece os sinais e dados a serem usados e analisados, observa-se que as duas áreas estão começando a convergir e obscurecer as linhas de distinção entre elas (EHIE; CHILTON, 2020).

A integração de sistemas de TI e TO certamente beneficia a comunicação e a criação de processos de negócios colaborativos, porém, ela também introduz novos vetores de ataque aos ecossistemas industriais (DIETZ; PERNUL, 2020).

## **1.2. Justificativa**

Mediante pesquisa para a composição do referencial teórico desta dissertação, percebe-se que as empresas brasileiras não estão priorizando de modo satisfatório medidas preventivas associadas a gestão da segurança da informação em indústrias com processos e tecnologias de manufatura avançada, quando se comparado a atenção que é dedicada para implantação dos demais pilares tecnológicos da Indústria 4.0, portanto, surge o interesse de explorar a oportunidade de pesquisa para a identificação dos impactos à segurança da informação em empresas com manufatura avançada, mediante a tendência identificada na literatura científica, de convergência das atividades de TI e de TO.

Com a tendência de convergência das atividades de TI e de TO, surge também uma nova configuração de possibilidades de ocorrência de incidentes de segurança da informação nos

processos de suporte e nos processos de fabricação industrial, desta forma é importante analisar antecipadamente os impactos que poderão ocorrer ao se optar pela convergência destas áreas.

Além de incidentes de segurança da informação, acidentes associados à segurança da infraestrutura da empresa e à saúde de seus colaboradores também são apontados na literatura científica consultado como uma nova prioridade pertinente não somente a área de TO, mas também para a área de TI.

Segundo Kamal *et al.* (2016), a convergência de TI e TO é a chave para melhorar a segurança física, aumentar a produtividade e a eficiência

Ao identificar, agrupar e analisar criticamente como está sendo tratada a convergência das atividade de TI e TO na literatura científica, os gestores empresariais poderão contar: com dados que subsidiarão a tomada de decisão assertiva de aderirem ou não a integração dos departamentos de TI e TO; poderão reconhecer as limitações de autoridade e responsabilidade dos colaboradores das áreas de TI e TO; poderão planejar programas de treinamento mais adequados aos colaboradores das áreas de TI e TO; poderão identificar, sob a perspectiva de cada uma das áreas (TI e TO), quais são os elementos de consideração relevante para verificação de concordância ou conflito de interesses nas gestões dos processos de TI e de TO.

Para a comunidade acadêmica esta pesquisa poderá: subsidiar o direcionamento de futuras pesquisas para diminuir as lacunas que por ventura possam surgir com a convergência das áreas de TI e TO; oportunizar o desenvolvimento de ferramentas e métodos para facilitar o processo de convergência das gestões de processos de TI e TO; oportunizar o desenvolvimento de métodos de coleta de dados para avaliar a eficiência das equipes integradas de TI e TO, uma vez que com a convergência não se tem certeza do padrão de funcionamento da rotina de trabalho como até então desassociado.

Esta pesquisa possui como elementos diferenciadores que validam-na: a determinação dos contornos operacionais das áreas de TI e de TO sob os relatos dos profissionais que atuam nestas áreas; o levantamento das opiniões e percepções dos profissionais que atuam nas áreas de TI e de TO em empresas com tecnologias de manufatura avançada sobre oportunidades, limitações, dificuldades e impactos à segurança da informação decorrentes da convergência de seus departamentos; indicações sob a percepção de profissionais de TI e de TO de como está sendo tratado o tema segurança da informação em empresas brasileiras que fazem uso de tecnologias de manufatura avançada, bem como quais são as tecnologias que os profissionais brasileiros julgam serem facilitadoras à convergência de TI e TO.



### **1.3. Objetivos**

Esta pesquisa tem como pergunta orientadora o que segue: quais são os impactos da convergência das atividades de TI e de TO na segurança da informação em empresas com tecnologias de manufatura avançada? A partir da questão de pesquisa foram definidos os objetivos que são apresentados na sequência.

O objetivo geral deste estudo consiste em identificar, descrever e avaliar os impactos da convergência das atividades de TI e de TO na segurança da informação em empresas com tecnologias de manufatura avançada. Para atingir o objetivo principal, os seguintes objetivos específicos foram estabelecidos:

- Identificar os impactos gerais da convergência das atividades de TI e de TO com o advento das tecnologias de manufatura avançada;
- Identificar os impactos na segurança da informação de empresas com manufatura avançada ao optar-se pela convergência das atividades de TI e de TO;
- Relacionar os impactos identificados na ocorrência da convergência de TI e TO com os pilares da segurança da informação.

### **1.4. Proposições**

Resultante da pesquisa bibliográfica realizada para esta pesquisa e com base nos objetivos definidos, foram instituídas as seguintes proposições de pesquisa de modo a auxiliar a discussão dos resultados obtidos neste trabalho:

- Um dos elementos motivadores da convergência das áreas de TI e TO é o avanço tecnológico associado a implantação da manufatura avançada com base na RAMI 4.0;
- Os impactos positivos (oportunidades) e negativos (limitantes) à segurança da informação, mediante a convergência das atividades operacionais de TI e TO, consideram a segurança da informação, do chão de fábrica até o nível de gestão estratégica industrial;
- A convergência de TI e TO é reconhecida e tratada em publicações acadêmicas.

### **1.5. Estrutura da dissertação**

Este capítulo apresentou a motivação, a justificativa, a questão de pesquisa, os objetivos, as proposições e a estrutura do trabalho de forma resumida. Os próximos capítulos deste trabalho estão organizados da seguinte forma:

O Capítulo 2 apresenta a fundamentação teórica que é composta pelos conceitos e definições utilizadas neste trabalho e as principais normas aplicadas à segurança da informação em manufatura avançada;

O Capítulo 3 apresenta a metodologia utilizada na pesquisa, o protocolo utilizado para a revisão sistemática e síntese dos estudos selecionados e a abordagem do *survey*;

O Capítulo 4 apresenta a análise dos dados obtidos;

E finalmente no Capítulo 5 são apresentadas as considerações finais e as oportunidades de continuidade do trabalho e novas pesquisas.

## 2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo inicialmente apresenta os conceitos e definições que são utilizados neste trabalho. Além disso são discutidos os conceitos sobre a segurança da informação presente na manufatura avançada e como o Brasil e demais países referenciam as tecnologias associadas a Indústria 4.0.

### 2.1. Conceitos, definições e padrões

Para o adequado entendimento das abordagens presentes no trabalho, fez-se necessária a definição dos termos tecnologia da informação, tecnologia operacional, convergência, manufatura avançada e cibersegurança.

#### 2.1.1. Tecnologia da informação

A tecnologia da informação é considerada como o conjunto de tecnologia, que inclui a infraestrutura de *hardware* e os aplicativos de *software* usados para transformar dados. Um sistema de TI pode, portanto, ser definido como um mecanismo que aceita fluxos de dados como uma entrada para entregar um novo fluxo de dados, mas não interfere no mundo físico. Exemplos de sistemas de TI relevantes incluem sistemas ERP ou aplicativos CRM (BRETON, 2012).

A TI é o domínio de grandes sistemas de nível estratégico (BUTRIMAS, 2020), composto por uma plataforma de tecnologia que possui hardware, software, redes e outros componentes que fundamentam as funções de suporte corporativo (GARVIN, 2015; KAMAL *et al.*, 2016; MERRIAM-WEBSTER, 2020; PAES *et al.*, 2020).

As soluções de TI de nível corporativo estão principalmente preocupadas com a contabilização do desempenho passado, enquanto a TO se concentra no caminho à frente (GARVIN, 2015).

A definição de tecnologia da informação utilizada neste trabalho é: a junção de tecnologias de *hardware* e *software* que possibilitam o processamento de informação e que estão associadas as áreas de gestão estratégica das empresas.

### 2.1.2. Tecnologia operacional

A tecnologia operacional é o conjunto de dispositivos e processos que atuam em tempo real em sistemas operacionais físicos, como redes de distribuição de energia elétrica, instalações ou montadoras de veículos. Exemplos de sistemas de TO o MES, o SCADA, instrumentos de medição, válvulas, sensores e motores (BRETON, 2012).

A TO está associada as atividades que ocorrem fora da administração ou da parte de TI do escritório da empresa, sendo a parte de uma operação industrial em que hardware e software de TI (por exemplo, SCADA) são usados para monitorar e controlar um processo físico que ocorre em outro local da planta produtiva (GARVIN, 2015; KAMAL *et al.*, 2016; PAES *et al.*, 2020; BUTRIMAS, 2020; GARTNER, 2020).

A TO é encontrada em uma sala de controle onde a TI também está presente, mas não está sendo usada principalmente para e-mail e faturamento, em vez disso, está monitorando e controlando os dispositivos eletrônicos localizados mais próximos de onde um processo físico está ocorrendo (BUTRIMAS, 2020).

Neste estudo a definição de TO utilizada é: a junção de tecnologias de hardware e software que possibilitam o processamento de informações provenientes de dispositivos instalados em máquinas presentes nos processos fabris, por meio de sistemas de monitoramento e controle de processo físico industrial, e estes estão alocados junto as áreas de gestão tática e operacional da empresa.

### 2.1.3. Convergência de TI e de TO

Embora tradicionalmente as áreas de TI e de TO funcionassem como entidades separadas, as tendências mais recentes mostram que as duas convergem. Esta integração entre TI e TO é uma etapa vital para a criação de uma rede inteligente de sucesso (JELACIC *et al.*, 2020).

Embora não haja uma definição oficial, Ehrenreich (2020) propõe como definição à convergência de TI e TO como sendo a conexão cibernética entre as zonas de TI, TO e IIoT, envolvendo colaboração entre pessoas, aderência a políticas e utilização de tecnologias para alcançar processos de negócios aprimorados, detecção aprimorada de falhas, maior produtividade, interrupções e danos minimizados e redução do custo de manutenção.

Uma integração horizontal e vertical de tecnologias é essencial para automatizar a troca de dados dentro das fábricas e para se comunicar com fornecedores e clientes. Tradicionalmente, esse tipo de integração tem sido fornecido por meio de plataformas MES, PLM, ERP e IoT, mas a Indústria 4.0 exige níveis de integração mais elevados, uma vez que as plataformas mencionadas não podem ser incluídas com outros parceiros industriais ou clientes (exigindo, portanto, integrações adicionais, que geralmente são muito caras) (FERNANDEZ-CARAMEZ; FRAGA-LAMAS, 2019).

Conforme os ambientes industriais são transformados digitalmente, eles se tornam mais conectados e por consequência se tornam mais vulneráveis. Ainda no mesmo trabalho, é citado que os Sistemas de Controle Industrial (ICS) são um dos elementos do ambiente de TO, e conforme os ICS evoluem, os ambientes de TO aproveitam mais soluções de tecnologia da informação que se conectam à rede para se tornarem ainda mais eficientes e produtivos (ROMETTY, 2019).

Muitos esforços são necessários para maximizar os efeitos da transformação digital por meio da integração e convergência da tecnologia da informação e da tecnologia operacional (KANAZAWA; SAKITA, 2019).

A convergência de TI e TO deve receber atenção apropriada pela alta direção a fim de estabelecer uma base empresarial adequada e com estratégias de negócios que envolvem a assimilação de novos tipos de dados de sensores em volumes sem precedentes (GARVIN, 2015).

Uma aplicação direta resultante da convergência de TI e TO, citada por Bonnetto *et al.* (2016) é para que as máquinas beneficiem os recursos de processamento de dados dos sistemas

de TI para otimizar a produção.

Kamal *et al.* (2016) citam que a convergência das atividades de TI e de TO efetivam a revolução digital industrial, e deve-se também buscar a convergência sistemática de pessoas, processos e tecnologia. Tian e Hu (2019), corroboram citando que a convergência de TI e TO é a chave para melhorar a segurança, aumentar a produtividade e a eficiência operacional.

Jelacic *et al.* (2020), comentam que embora os sistemas de TI e TO tradicionalmente funcionem como entidades separadas, as tendências mais recentes mostram que as duas áreas convergem; esta integração de TI e TO é considerada uma etapa vital para uma rede inteligente de geração de energia elétrica de sucesso, por exemplo.

A definição feita por Ehie e Chilton (2020), é que a convergência de TI e TO é a integração de sistemas de tecnologia da informação usados para computação centrada em dados com sistemas de tecnologia operacional projetados para fins de monitoramento e controle de processos industriais.

Para Paes *et al.* (2020), a convergência de TI e TO é a integração de sistemas de TI aplicados à computação centrada em dados, com sistemas de TO usados para monitorar eventos, processos e dispositivos que fazem ajustes em operações empresariais e industriais.

Os termos integração e fusão, oriundos de artigos traduzidos do idioma inglês para o idioma português neste trabalho, são associados ao termo convergência. Neste estudo a definição de convergência é: a união das atividades e responsabilidades, operacionais e gerenciais das áreas de TI e TO.

No trabalho de Kamal *et al.* (2016) é apresentada definição conceitual que detalha as especificidades das áreas de TI e TO por meio da análise de atributos, tais como apresentado no Quadro 1. Neste quadro é possível identificar características pertinentes aos departamentos de TI e de TO enquanto considerados não integrados. Acredita-se que as atividades de TI e de TO ao serem convergidas podem apresentar a reconfiguração destas características.

Quadro 1: Características conceituais dos recursos de TI e de TO.

| Atributo           | TI  | TO  |
|--------------------|---|---|
| Função e propósito | Gerenciar, otimizar e proteger a infraestrutura de TI, aplicativos financeiros, de relatórios e processos de negócios | Gerenciar, controlar e otimizar ativos (duros e subterrâneos), processos de produção, operação e manutenção |
| Arquitetura        | Relacional, transacional, lote, <i>data warehouses</i> , texto - comunicações internas e externas                     | Dados e cálculos de engenharia complexos, mecanismos de regras orientados por eventos em tempo real         |

(continuação)

|                                      |   |   |
|--------------------------------------|---|---|
| Interface                            | Clientes locais / grossos, navegadores da web, teclado, leitores de código de barras e RFID e dispositivos móveis                       | Sensores, gráficos, planta gráfica e outros modelos de engenharia, IHM de missão crítica e dispositivos móveis              |
| Propriedade                          | Departamento de CIO / TI, finanças, serviços de rede, operações corporativas, parceiros de terceirização                                | CIO e / ou TI técnico, operações, funções técnicas (por exemplo: E&P, P&D, operações de produção), LOB, propriedade própria |
| Conectividade e Segurança            | Redes corporativas com segurança e governança padrão da indústria   | Redes de controle proprietárias e protocolos mistos de IP padrão  |
| Tempo de vida útil dos equipamentos  | Sistema operacional da indústria de TI e expectativa de vida e suporte de SW de $\pm 5$ anos  | Ligado ao equipamento de processo / vida útil de 10 a 20 anos   |
| Tempo de atividade e disponibilidade | Missão crítica e não crítica. Interrupções planejadas para upgrades, atualizações, reinicializações, conforme necessário                | Zero tempo de inatividade inesperado, interrupções planejadas vinculadas ao encerramento e manutenção da instalação         |
| Segurança                            | Núcleo para proteger a integridade e confidencialidade dos dados corporativos / clientes  | A disponibilidade e / ou vida útil do equipamento pode substituir ou conceder   |
| Aplicações                           | Salas de servidores, Sistema em nuvem, finanças, ERP, SCM, CRM, <i>data warehouses</i> , painéis de relatórios, e-mail, logística, etc. | Redes / sistemas de controle, segurança, APC, vigilância e otimização, monitoramento de condições, etc.                     |

Fonte: Adaptado de Kamal *et al.* (2016).

Para Ehie e Chilton (2020), a convergência de TI e de TO refere-se à extensão em que as informações e as tecnologias de operação estão se unindo para compartilhar componentes, funções e equipe. Tradicionalmente, os sistemas, processos e pessoas dentro de TI e TO são gerenciados, controlados e administrados de forma independente uns dos outros. A convergência de TI e de TO promove uma visão única das informações corporativas e gerenciamento de processos para ajudar a garantir que cada pessoa, sensor, chave ou outro dispositivo tenha as informações certas, no formato certo e no momento certo.

Outro fator importante discutido por Kamal *et al.* (2016) são os recursos necessários para tomada de decisão, planejamento, implantação, continuidade e melhoria do projeto de convergência de TI e de TO e esses recursos, reconhecidos como elementos capacitadores da convergência, são categorizados em recursos humanos, processos e tecnologia. O grau de disponibilidade de cada um destes recursos implica diretamente em como a convergência das atividades de TI e TO pode ocorrer na empresa, bem como o retorno do valor esperado deste processo.

O autor Ehrenreich (2020), sobre a convergência das atividades de TI e TO, defende que nem todas as atividades devam ser convergidas e que as características de cada setor devem ser criteriosamente consideradas para não expor excessivamente a empresa a incidentes cibernéticos de segurança da informação. Desta forma foi sugerido a Tabela 1 que aborda as aplicações industriais, os níveis de importância com relação a segurança da informação industrial, a viabilidade da convergência de TI e TO e o método de segregação de zonas sugerido em prol da segurança cibernética de TI e TO.

Tabela 1: Caracterização da cibersegurança para convergência de TI e de TO.

| Aplicações<br>↓                               | Importância                  |   |  |   |                                      |   |   |
|---|------------------------------|---|--|---|--------------------------------------|---|---|
|   | Conveniência e Produtividade | Garantia à Segurança Humana da Operação | Garantia da Confiabilidade da Operação | Proteção da Confidencialidade da Informação | Segurança das Operações Cibernéticas | Convergência da Cibersegurança de TI e TO | Segregação entre as Zonas de Segurança de TI e TO |
| Coleta de dados para fins financeiros         | 3                            | 1                                       | 3                                      | 3   | 3                                    | Permitido                                 | <i>Firewalls</i>                                  |
| Gestão de Grandes Construções e Energia       | 3                            | 2                                       | 4                                      | 2   | 2                                    | Permitido                                 | <i>Firewalls</i> ou DMZ                           |
| Distribuição de Água e Energia                | 2                            | 2                                       | 4                                      | 2   | 3                                    | Fortemente Protegido                      | NGFW, DMZ ou Diodo de Dados                       |
| Gestão de aplicativos em Cidades Inteligentes | 4                            | 1                                       | 3                                      | 1   | 2                                    | Permitido                                 | <i>Firewalls</i>                                  |
| Processos de Fabricação                       | 2                            | 4                                       | 3                                      | 2   | 4                                    | Permitido                                 | NGFW, DMZ ou Diodo de Dados                       |
| Gestão de Grandes Usinas de Energia           | 3                            | 4                                       | 4                                      | 2   | 5                                    | Proibido                                  | Diodo de Dados ou <i>Air-Gap</i>                  |
| Processos Nucleares e Químicos                | 2                            | 5                                       | 4                                      | 2   | 5                                    | Proibido                                  | Diodo de Dados ou <i>Air-Gap</i>                  |
| 1-Baixa importância                           | 2-Média Importância          | 3-Alta Importância                      | 4-Crítica                              | 5-Extremamente Crítica                      |                                      |   |   |

Fonte: adaptado de Ehrenreich (2020).

#### 2.1.4. Manufatura avançada

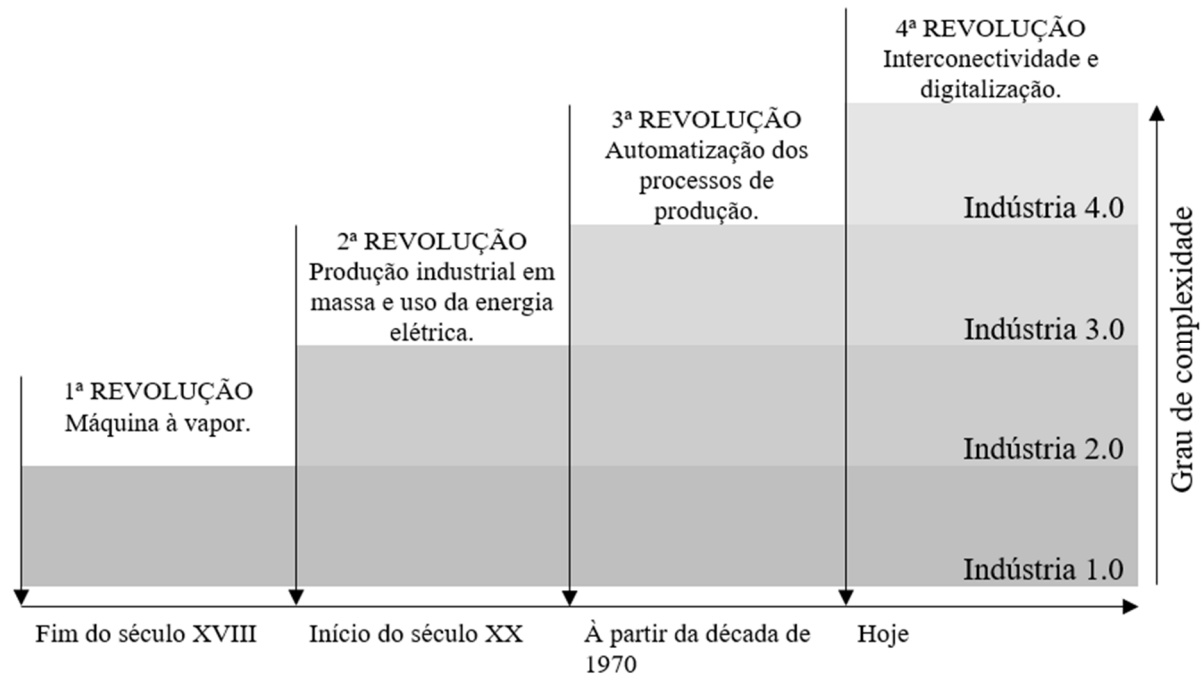
Desde a década de 1970, a tecnologia da informação foi incorporada aos negócios, por meio do uso de computadores para auxiliar a automação industrial, o que marcou a terceira revolução industrial. A digitalização da produção está ganhando um novo nível de qualidade com a rede mundial de computadores e anuncia a quarta revolução industrial. Na quarta



revolução industrial não é o computador que é a tecnologia central, mas sim a *internet*. (FMEE, 2019).

A Figura 6 apresenta a ocorrência temporal das revoluções industriais.

Figura 6: As quatro revoluções industriais.



Fonte: adaptado de Gomes e Coelho (2016).

Em 2006, foi lançado o projeto *High Tech Strategy*, desenvolvido pelo governo alemão para aumentar a produtividade da indústria alemã através da inovação e elevar a competitividade frente a manufatura asiática. Neste projeto foram reunidos os principais atores de inovação e tecnologia da Alemanha (governo, indústrias e academia) para alavancar e difundir novas tecnologias em âmbito nacional. Em 2010 o projeto resultou no plano de ação *High Tech Strategy 2020 - Action Plan*, que estabelecia a Alemanha como principal país fornecedor de soluções de ciência e tecnologia em diversas áreas de conhecimento. Entre os projetos incluídos no plano de ação estava a Indústria 4.0 (GOMES; COELHO, 2016).

Foi em 2011, na Feira de Hannover, na Alemanha, que o termo Indústria 4.0, do alemão *Industrie 4.0*, foi apresentado ao mundo (CULOT *et al.*, 2020; FRANK; DALENOGARE; AYALA, 2019; GOMES; COELHO, 2016; NOLTING *et al.*, 2019).

A aplicação em larga escala da digitalização à produção industrial deu origem ao conceito manufatura avançada. Devido aos impactos significativos da digitalização na produção, no desenvolvimento de produtos e na forma de se fazer negócio, considera-se a o presente momento como pertencente a quarta revolução industrial, dando origem ao termo

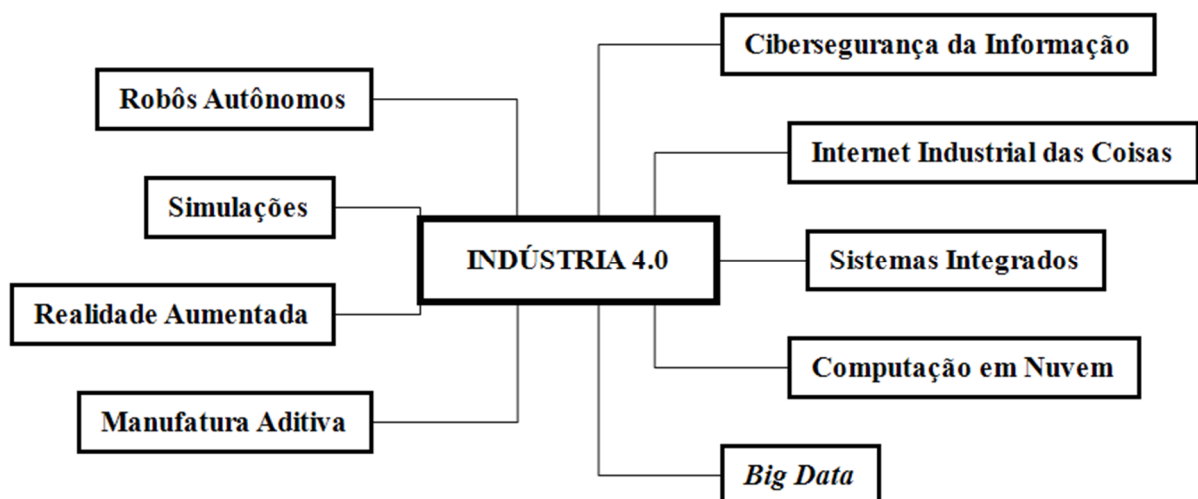
indústria 4.0 como alternativa termo manufatura avançada (GONÇALVES, 2016).

A abordagem principal da Indústria 4.0 é baseada nos sistemas cibernéticos físicos, ou sistemas ciberfísicos, permitindo que os sistemas de controle sejam interconectados e se comuniquem (ANDERL, 2015).

Na quarta revolução industrial, a análise digital permite um novo nível de produtividade operacional por se basear em sistemas ciberfísicos que proporcionam níveis de dados sem precedentes, maior poder computacional, conectividade onipresente em toda a cadeia de abastecimento, tecnologia universal de atuadores e sensoriamento, análise de dados impulsionando a eficiência e a eficácia, amadurecimento de novas tecnologias ciberfísicas (MCKINSEY GLOBAL INSTITUTE, 2017).

Segundo Frank, Dalenogare e Ayala (2019), as tecnologias comumente associadas a manufatura avançada são: sensores, atuadores, CLP; sistemas SCADA, MES, ERP, comunicação M2M; sistemas de comissionamento virtual, simulação de processos, Inteligência Artificial para manutenção preditiva e para planejamento de produção; robôs, sistemas de identificação automática de não conformidades na produção; identificação e rastreabilidade de matérias-primas e de produtos finais; manufatura aditiva, linhas flexíveis e autônomas; sistemas de monitoramento e melhoria de eficiência energética. A Figura 7 apresenta as tecnologias pilares da Indústria 4.0.

Figura 7: Tecnologias pilares da Indústria 4.0.



Fonte: adaptado de Frank, Dalenogare e Ayala (2019).

No Quadro 2 são apresentadas as descrições das tecnologias entendidas como pilares da Indústria 4.0.

Quadro 2: Descrição das tecnologias pilares da Indústria 4.0.

| <b>Tecnologia pilar</b>         | <b>Descrição</b>   |
|---------------------------------|--|
| Robôs Autônomos                 | São robôs capazes de interagir com outras máquinas e com os seres humanos, atuando de maneira mais flexível e colaborativa.  |
| Manufatura Aditiva              | Permite a produção através de impressoras 3D.  |
| Simulação Virtual               | Permite que os processos e produtos sejam testados e ensaiados durante a fase de concepção, reduzindo custos com falhas e o tempo de projeto.  |
| Sistemas Integrados             | São sistemas ERP, MES, SAP que integram toda a cadeia de valor produtiva, por meio da análise e tomada de decisão de dados.  |
| <i>Internet</i> das Coisas      | Permite conectividade entre os diversos dispositivos flexibilizando o acesso e controle em todo o processo produtivo.  |
| <i>Big Data &amp; Analytics</i> | São sistemas inteligentes que identificam falhas nos processos, melhorando a qualidade da produção em tempo real, economizando energia e melhorando a eficiência na utilização de todos os recursos produtivos.  |
| Computação em Nuvem             | Possibilidade de acesso ao banco de dados e suporte de qualquer local do planeta, permitindo a integração de sistemas e plantas em locais distintos, mesmo que distantes fisicamente, da mesma forma o controle e o suporte podem ser efetuados de maneira global. |
| Segurança Cibernética           | Referencia sistemas de comunicação cada vez mais seguros e evoluídos garantindo a "prestação de contas" do processo de produção.   |
| Realidade Aumentada             | Suporte que permite que o usuário atue dentro dos sistemas cibernéticos físicos (CPS) com uma visão e tutoria assertiva indicando passo a passo todas as instruções e comandos necessários para um reparo, ou uma nova parametrização do processo.                 |

Fonte: adaptado de Vitalli (2018).

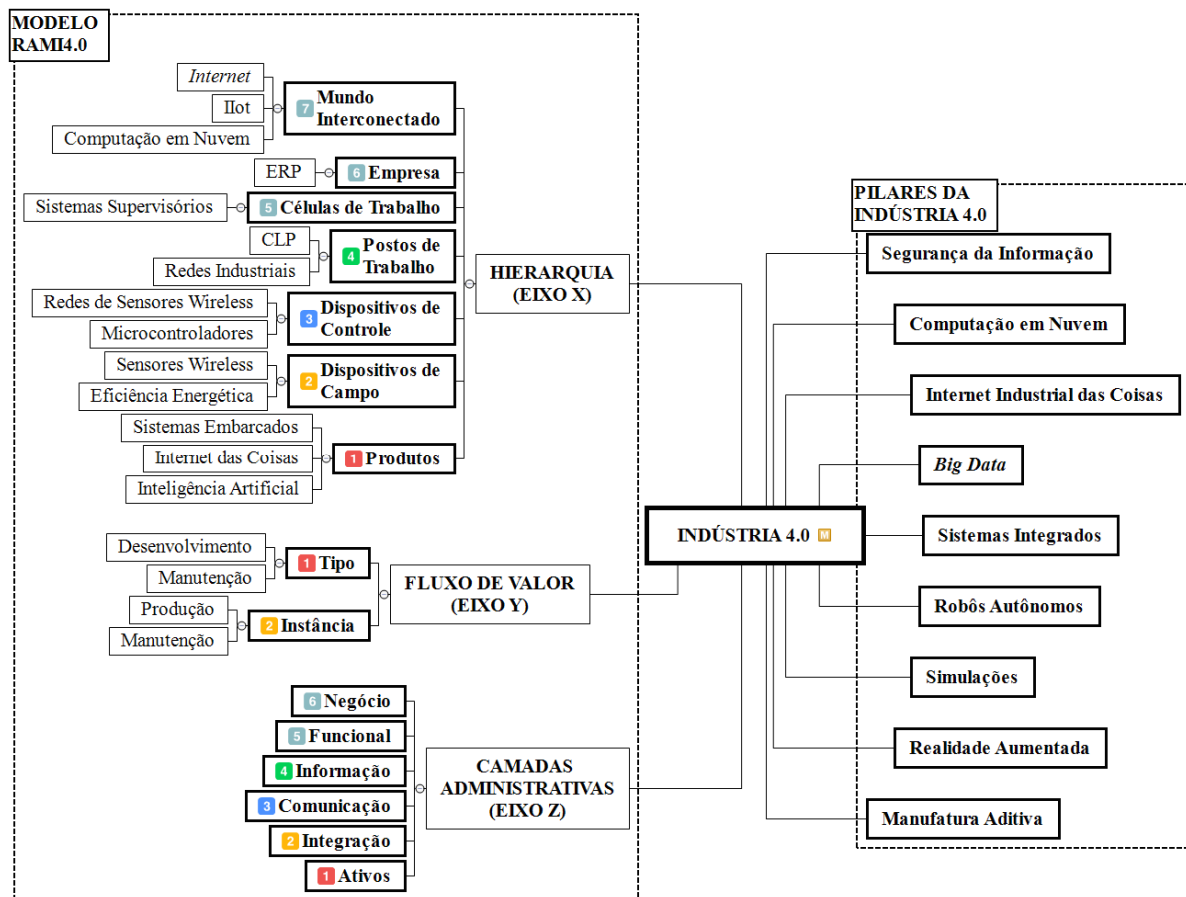
Em abril de 2016 foi publicado o Modelo de Arquitetura de Referência para *Industrie 4.0* - RAMI 4.0, cujo objetivo deste modelo é representar o objeto técnico, e todos os aspectos relevantes para ele, desde o seu desenvolvimento, produção e utilização até o seu descarte. A *Industrie 4.0* fornece uma descrição digital do objeto, tornando possível representá-lo virtualmente (ADOLPHS *et al.*, 2016).

O RAMI 4.0 é representado como um modelo tridimensional de interconexão das informações em sistemas ciberfísicos. O eixo X (hierarquia) é baseado no modelo de arquitetura de referência para uma fábrica, com linhas de produção, com integração de TI corporativa e sistemas de controle. O eixo Y (fluxo de valor) é usado para descrever um ativo em um determinado ponto no tempo durante sua vida útil, desde sua produção e uso até sua eliminação.

O eixo Z (vertical) descreve a arquitetura em termos de propriedades e estruturas de sistema com suas funções e dados específicos da função na forma de camadas. As seis camadas do eixo vertical são usadas para descrever as propriedades estruturais de um ativo ou a combinação de ativos<sup>2</sup>. A segurança é um aspecto elementar do RAMI 4.0 e deve sempre ser incluída na descrição de cada seção dos três eixos (ADOLPHS *et al.*, 2016).

A Figura 8 representa a conexão entre os eixos do modelo tridimensional para indicação dos interconexão dos ativos referenciados pela RAMI 4.0 e as tecnologias que suportam a Indústria 4.0.

Figura 8: Integração do modelo RAMI4.0 e dos pilares tecnológicos da Indústria 4.0.



Fonte: o autor.

A *Internet Industrial das Coisas* é um tipo de infraestrutura que está intimamente conectada com pessoas, indústrias e redes, e oportuniza o baixo custo e a alta eficiência da

<sup>2</sup> objeto que tem valor para uma organização (ADOLPHS *et al.*, 2016).

produção inteligente. Para implantar adequadamente a IIoT deve-se promover a convergência das atividades de TI e de TO (TIAN; HU, 2019).

Segundo Tian e Hu (2019), a *Internet Industrial* é o núcleo da Indústria 4.0, na qual a revolução industrial trouxe avanços em máquinas, equipamentos e oficinas, e a revolução da rede trouxe avanços nos sistemas de computação e comunicação, como por exemplo, a comunicação OPC UA TSN, que também indica que terá um papel importante no processo de convergência de TI e TO.

Quase todas as organizações industriais no planeta - desde empresas de serviços públicos, empresas de petróleo e gás, redes elétricas, tratamento de águas residuais e empresas de manufatura, estão empenhadas em colocar suas redes em funcionamento com a Indústria 4.0 por meio da IIoT (ROMEO, 2020).

Os desenvolvimentos recentes em IIoT e o aumento da conexão de máquinas à *internet* industrial estão acelerando ainda mais a digitalização dos processos de manufatura avançada o que impulsiona o fenômeno de convergência de TI e de TO (KAMAL *et al.*, 2016).

Segundo Nolting *et al.* (2019), há uma falta de adaptação e uso comum do termo Indústria 4.0 em âmbito mundial, embora o termo atualmente se apresente como altamente internacional.

Iniciativas internacionais são identificadas no relatório de políticas e programas nacionais de transformação digital publicado pela European Commission (2017) e neste é possível identificar os nomes dos programas associados a transformação digital dos processos industriais de cada país coligado.

Segundo Culot *et al.* (2020), conceitos semelhantes, usados como sinônimos, tais como “manufatura inteligente”, “transformação digital” e “quarta revolução industrial”, aumentaram a sensação de confusão em torno do escopo e das características do fenômeno inicialmente nomeado por *Industrie 4.0* e Nolting *et al.* (2019) sugerem que mais trabalhos devem ser realizados para reduzir os problemas tautológicos acerca da diversidade de termos utilizados pela ciência para tratar do paradigma Indústria 4.0.

No Brasil os termos mais utilizados ao se referenciar a transformação digital das indústrias são “manufatura avançada”, “indústria 4.0” e “fábrica do futuro” (ABDI, 2020).

No Quadro 3 são apresentados os termos associados aos projetos de transformação digital do Brasil e dos países coligados a União Européia.

Quadro 3: Termos utilizados nos programas de incentivo a transformação digital industrial pelos países.

| <b>País</b>     | <b>Termo associado a manufatura avançada</b>          |
|-----------------|---|
| Brasil          | Manufatura Avançada, Indústria 4.0, Fábrica do Futuro |
| Áustria         | <i>Industrie 4.0 Oesterreich</i>                      |
| Bélgica         | <i>Made different - Factories of the future</i>       |
| República Checa | <i>Průmysl 4.0</i>                                    |
| Alemanha        | <i>Industrie 4.0</i>                                  |
| Dinamarca       | <i>Manufacturing Academy of Denmark (MADE)</i>        |
| Espanha         | <i>Industria Conectada 4.0</i>                        |
| França          | <i>Alliance pour l'Industrie du Futur</i>             |
| Hungria         | <i>IPAR4.0 National Technology Initiative</i>         |
| Itália          | <i>Industria 4.0</i>                                  |
| Lituânia        | <i>Pramonė 4.0</i>                                    |
| Luxemburgo      | <i>Digital For Industry Luxembourg</i>                |
| Holanda         | <i>Smart Industry</i>                                 |
| Polônia         | <i>Initiative and Platform Industry 4.0</i>           |
| Portugal        | <i>Indústria 4.0</i>                                  |
| Suécia          | <i>Smart Industry</i>                                 |

Fonte: o autor.

Neste trabalho o termo utilizado para referenciar a plataforma Indústria 4.0 e suas tecnologias de suporte é manufatura avançada.

## 2.2. Cibersegurança e padrões de segurança da informação para indústrias

A cibersegurança é solicitada quando se observa o aumento da complexidade dos processos de comunicação devido a integração de redes de informações, como proposto pela plataforma RAMI 4.0 tratada na norma DIN SPEC 91345, redigida por Adolphs *et al.* (2016), e também com a convergência das demandas e responsabilidades das gestões de TI e TO.

Ao utilizar o termo cibersegurança percebe-se a correlação com o termo ciberfísico. No estudo de Givchchi *et al.* (2017) há a associação da TO como a responsável pela parte “física” do termo e da TI como responsável pela parte cibernética do termo, de onde provem a conjunção de palavras “sistemas ciberfísicos”.

O objetivo de um programa de segurança é integrar todos os aspectos da segurança cibernética, incorporando os sistemas de computação empresarial com sistemas de controle e automação industrial. Muitas organizações têm programas de segurança cibernética

razoavelmente detalhados e completos para seus sistemas de computador de negócios (TI), mas as práticas de gerenciamento de segurança cibernética não são totalmente desenvolvidas para IACS (TO) (ISA, 2007).

O autor Ehrenreich (2020) complementa que a expansão dos Sistemas de Controle Industrial de TO com ecossistemas de *Internet Industrial das Coisas* melhora o desempenho dos negócios e a produtividade, mas também aumenta a superfície de ataque cibernético e o risco de ataque contra a organização.

Segundo Romeo (2020), as capacidades dos *hackers* estão sendo constantemente demonstradas e os incidentes cibernéticos estão aumentando em frequência e complexidade. Somente construir uma rede com perímetro reforçado não é mais adequado. Proteger o ICS contra ameaças<sup>3</sup> modernas requer estratégias bem planejadas e bem implementadas que fornecerão às equipes de defesa de rede uma chance de detectar, contra-atacar e expulsar um adversário de forma rápida e eficaz.

Os Estados Unidos reconhecem 16 setores de infraestrutura crítica cujos ativos, sistemas e redes, sejam físicos ou virtuais, são considerados tão vitais que sua incapacitação ou destruição teria um efeito debilitante na segurança da informação, segurança econômica nacional e saúde pública nacional (WALES, 2020).

De acordo com a CISA, os setores classificados como infraestrutura crítica nacional são: setor químico, comércio, comunicações, manufatura crítica, barragens, indústria de defesa, serviços de emergência, energia, serviços financeiros, alimentos e agricultura, instalações governamentais, saúde pública, tecnologia da informação, material nuclear, sistemas de transporte e setor de água e esgoto (WALES, 2020).

Os sistemas de infraestrutura crítica contam com sistemas de controle industrial e, portanto, possuem demandas de atividades ora associadas às atividades de TI, ora associadas às atividades de TO.

Devido ao fato dos sistemas de controle industrial gerenciarem processos operacionais físicos, a crescente convergência de TI e TO cria oportunidades para exploração da segurança da informação que podem resultar em consequências catastróficas, incluindo perda de vidas, danos econômicos e interrupção dos sistemas de infraestrutura crítica nacional as quais a sociedade depende (WALES, 2019).

Embora as defesas de TI sejam essenciais, elas não podem proteger o sistema físico no nível de processo básico, o que demonstra o reconhecimento da necessidade de defesas

---

<sup>3</sup> ações potencialmente prejudiciais (intencional ou não) ou capacidade (interna ou externa) de impactar adversamente por meio de uma vulnerabilidade é chamada de ameaça (ISA, 2007).

específicas de segurança da informação aos sistemas de TO, que serve como uma linha adicional de defesa quando as defesas de TI são contornadas (SUNDARAM; ABDEL-KHALIK; ASHY, 2020).

No ambiente de controle industrial, em atividades de TO, a ordem e o peso das entidades associadas a segurança da informação mudam, se comparado a convenção de TI. Na indústria o foco das equipes de TO na gestão dos controles de segurança da informação é primeiramente a segurança a vida humana, a infraestrutura e o meio ambiente (*safety*), depois em sequência decrescente de prioridade, segue a disponibilidade, a integridades e a confidencialidade das informações (PREMINGER, 2020; ISA, 2007).

Associado ao termo *safety* também se torna necessário definir o que se trata como Sistema Instrumentado de Segurança (SIS). Nesta dissertação será utilizada a definição presente na norma ISA 62443-1-1 (2007) na qual informa que trata-se de sistema usado para implementar uma ou mais funções com instrumentos de segurança e um sistema com instrumentos de segurança é composto por qualquer combinação de sensores, CLPs e atuadores.

No estudo desenvolvido por Paes *et al.* (2020), os recursos de TO que mais demandam disponibilidade ao processo, da maior para a menor disponibilidade são: os dispositivos de rede industrial (como roteadores e *gateways* 27,8%); controladores lógicos programáveis (CLP) (14,9%); sistemas de controle, supervisão e aquisição de dados (SCADA) (10,3%); inversores de frequência (8,8%) e interfaces homem-máquina (IHM) (7,0%).

A arquitetura complexa da manufatura avançada apresenta interconexões de dispositivos e redes, que exigem padronização de protocolos para oferecer suporte à comunicação entre plataformas e controles de segurança à fim de preservar a confidencialidade, integridade e, principalmente, a disponibilidade (WATSON *et al.*, 2017).

Segundo Timpson e Moradian (2018), a interoperabilidade aumentou o risco<sup>4</sup> potencial para a segurança e proteção da infraestrutura crítica.

A interoperabilidade<sup>5</sup> de tecnologias surge da interconexão de dispositivos de diferentes fabricantes e/ou de diferentes protocolos de comunicação, da interconexão de redes com tráfego competitivo crítico ou não, e o aumento do acesso a redes anteriormente isoladas (WATSON *et al.*, 2017).

Como representada pela Figura 9, a interoperabilidade e a segurança, são objetivos justificadores e diferenciais para a manufatura avançada.

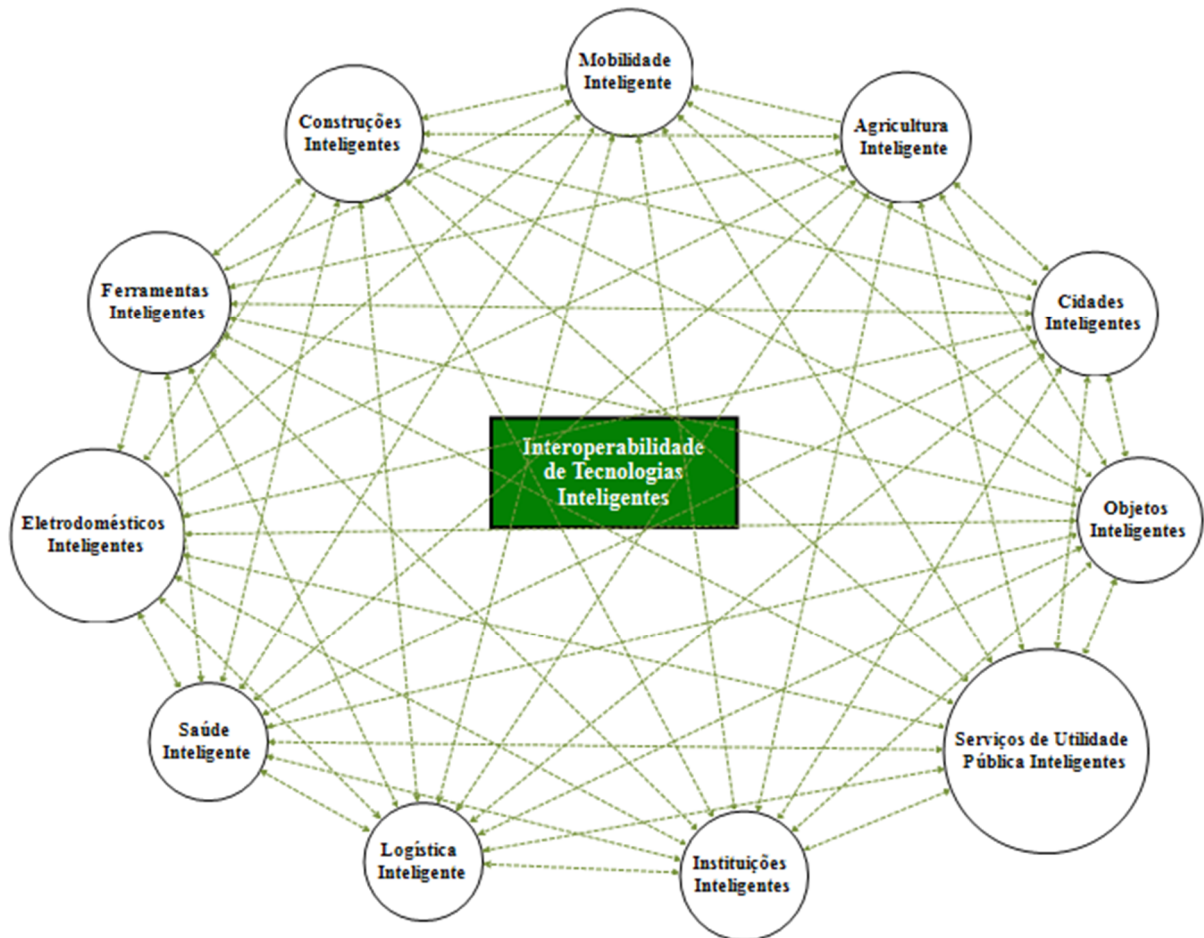
---

<sup>4</sup> efeito da incerteza sobre os objetivos (ABNT, 2018).

<sup>5</sup> a capacidade de comunicação de sistemas distintos (EHIE; CHILTON, 2020).



Figura 9: Representação da interoperabilidade de tecnologias inteligentes.



Fonte: Adaptado de Fernández-Caramés e Fraga-Lamas (2019).

Watson *et al.* (2017) citam que as séries de normas ISO 27000, ISA 62443, IEC 62541 e a norma IEEE 1722:2016 abordam em seus requisitos elementos associados aos desafios da interoperabilidade e segurança dos dispositivos industriais comumente utilizados em IACS.

### 2.2.1. Série de normas ISO 27000

A série de normas ISO 27000 propõe requisitos para manter a segurança de ativos de informação nas organizações. A norma ISO 27001 é o padrão mais conhecido na família de normas ISO 27000, pois fornece requisitos para um sistema de gerenciamento de segurança da informação (SGSI). A norma ISO 27002 fornece recomendações de melhores práticas de gerenciamento de segurança da informação para uso por aqueles responsáveis por iniciar, implementar ou manter o SGSI (WATSON *et al.*, 2017).

A ISO 27019, com base na ISO 27002, fornece orientação aplicada aos sistemas de controle de processo usados pela indústria de energia para controlar e monitorar a produção ou geração, transmissão, armazenamento e distribuição de energia elétrica, gás, óleo e calor e para o controle dos processos de suporte associados (ISO, 2017). O objetivo da ISO 27019 é estender a série de normas ISO 27000 para o domínio de sistemas de controle de processos e tecnologia de automação (WATSON *et al.*, 2017).

### 2.2.2. Série de normas ISA 62443

A série de normas ISA 62443 trata da segurança da informação em sistemas industriais. A série de normas possui quatro partes principais e estas por sua vez são subdivididas em várias partes (WATSON *et al.*, 2017). A parte 1 referencia elemento gerais, tais como conceitos, modelos, glossário, métricas de segurança e elementos que associados ao ciclo de vida seguro de IACS; a parte 2 aborda requisitos de políticas e procedimentos para a segurança de IACS; a parte 3 aborda requisitos de sistemas de segurança, tecnologias de segurança, requisitos para o projeto de sistemas seguros de IACS e as especificações para a determinação de níveis de segurança; e a parte 4 aborda os requisitos de segurança para componentes, tais como especificações para o desenvolvimento de produtos e requisitos técnicos de segurança para componentes de IACS (ISA, 2015).

O objetivo da aplicação da série de normas ISA 62443 é melhorar a segurança dos colaboradores, da infraestrutura e do meio ambiente, a disponibilidade, a integridade e a confidencialidade de componentes ou sistemas usados para automação e controle industrial, e fornecer critérios para aquisição e implementação de sistemas seguros de automação e controle industrial (ISA, 2015).

Partes da ISA 62443 têm escopo semelhante com a série ISO 27000 sobre aspectos de segurança da informação. Por exemplo, a ISA 62443 também descreve aspectos como gerenciamento de programa de segurança e análise de risco de segurança. A ISA 62443 também fornece um modelo de um sistema de controle de automação industrial e apresenta ainda diferentes zonas que cobrem diferentes áreas do sistema com os mesmos requisitos de segurança (WATSON *et al.*, 2017).

A norma ISA 62443-1-1 aborda a terminologia, os conceitos e os modelos de segurança da informação para sistemas de controles industriais.

Este trabalho utiliza as definições dos termos segurança (*safety*), segurança (*security*) e incidente de segurança (*security*) presentes em ISA 62443-1-1 (2007) e em WEF (2018):

- Segurança (*safety*): condição do sistema operando sem causar risco inaceitável de lesões físicas ou danos à saúde das pessoas, seja direta ou indiretamente, como resultado de danos à propriedade ou ao meio ambiente (WEF, 2018).

- Segurança (*security*): propriedade de ser protegido contra acesso não intencional ou não autorizado, alteração ou destruição garantindo disponibilidade, integridade e confidencialidade (WEF, 2018).

- Incidente de segurança: evento adverso em um sistema ou rede ou a ameaça de ocorrência de tal evento. O termo “quase acidente” às vezes é usado para descrever um evento que poderia ter sido um incidente em circunstâncias ligeiramente diferentes (ISA, 2007).

Devido as traduções dos termos provenientes do idioma inglês, *safety* e *security*, em tradução direta para o idioma português resultar no termo segurança, faz-se necessário definir que neste trabalho o termo segurança física assumirá a definição do termo *safety* e o termo segurança da informação assumirá a definição do termo *security*.

### 2.2.3. Série de normas IEC 62541

Em 1996, o padrão OPC era restrito ao sistema operacional Windows. Como tal, a sigla OPC nasceu de OLE (vinculação e incorporação de objetos) para controle de processos e foi amplamente adotada em vários setores, incluindo manufatura, automação predial, petróleo, gás, energia renovável e serviços públicos. Com a introdução de arquiteturas orientadas a serviços em sistemas de manufatura, surgiram novos desafios em segurança e modelagem de dados, então a OPC Foundation desenvolveu as especificações OPC UA para buscar atender as necessidades de interoperabilidade para a manufatura avançada (BRYANT, 2020).

Atualmente o acrônimo de OPC UA, em tradução livre para o idioma português significa arquitetura unificada de comunicações de plataforma aberta.

A série de normas IEC 62541 apresenta em suas várias divisões requisitos de suporte a OPC UA para promover a interoperabilidade de diferentes dispositivos (WATSON *et al.*, 2017). A parte 1 da IEC 62541 apresenta os conceitos e a visão geral da OPC UA (IEC, 2016a). A parte 2 da IEC 62541, descreve o modelo de segurança da OPC UA. Ele descreve as ameaças à segurança da infraestrutura, do *hardware* e do *software* nos quais o OPC UA deve ser executado, a dependência de outros padrões de segurança (IEC, 2016b).

Como o OPC UA especifica um protocolo de comunicação, o foco está na proteção dos dados trocados entre os aplicativos, o que não significa que um desenvolvedor de aplicativos pode ignorar os outros aspectos da segurança, como por exemplo, a proteção de dados persistentes contra adulteração. É importante que os desenvolvedores examinem todos os aspectos de segurança e decidam como eles podem ser tratados no aplicativo (IEC, 2016b).

#### 2.2.4. Norma IEEE 1722:2016

A norma IEEE 1722-2016 apresenta um protocolo de transporte para aplicações sensíveis ao tempo (TSN) em redes locais em ponte. A TSN abordada na IEEE 1722-2016 é um conjunto de sub padrões da rede Ethernet IEEE 802 que introduz recursos em tempo real para a rede Ethernet padrão (IEEE, 2016).

No protocolo proposto pela IEEE 1722-2016, é dada consideração ao contexto industrial (automação industrial e redes de controle), onde a TSN é usada para se referir ao controle industrial e outros fluxos de dados de aplicação que não são de áudio ou vídeo por natureza (IEEE, 2016).

A TSN oferece vantagens competitivas para redes industriais, particularmente em infraestruturas de IIoT, onde a comunicação de tempo crítico e a proteção contra congestionamento de tráfego são requisitos essenciais (IEEE, 2016; WATSON *et al.*, 2017).

Os recursos da TSN também podem ser aproveitados com padrões de interoperabilidade, como a OPC UA. Nesse sentido, enquanto a OPC UA facilita a comunicação entre os dispositivos, a TSN garante uma conexão bem-sucedida entre esses dispositivos e permite uma comunicação de dados em tempo real (WATSON *et al.*, 2017).

### 2.3. Integração dos modelos e características identificadas

A norma ISA 95 é o padrão internacional para a integração de sistemas corporativos (TI) e de controle (TO). Compreende modelos e terminologia que podem ser usados para determinar as informações a serem trocadas entre sistemas administrativos e sistemas de produção, manutenção e qualidade. As informações são estruturadas em UML que também servem de base para o desenvolvimento de interfaces entre sistemas de TI e TO (BRETON, 2012).

Provem do comitê organizador da norma ISA 95 a base para a elaboração da norma IEC 62264-3, a qual apresenta modelos de atividades de gestão de operações de manufatura e nesta norma é possível evidenciar verticalmente os níveis hierárquicos da automação industrial em processos de manufatura e que podem ser conectados a certos tipos de informações, sistemas e tempos de transmissão das informações (IEC, 2016c). Desde a utilização pública da ISA 95 o modelo de hierarquia das tecnologias de manufatura começou a ser citado como a pirâmide da automação (BRETON, 2012).

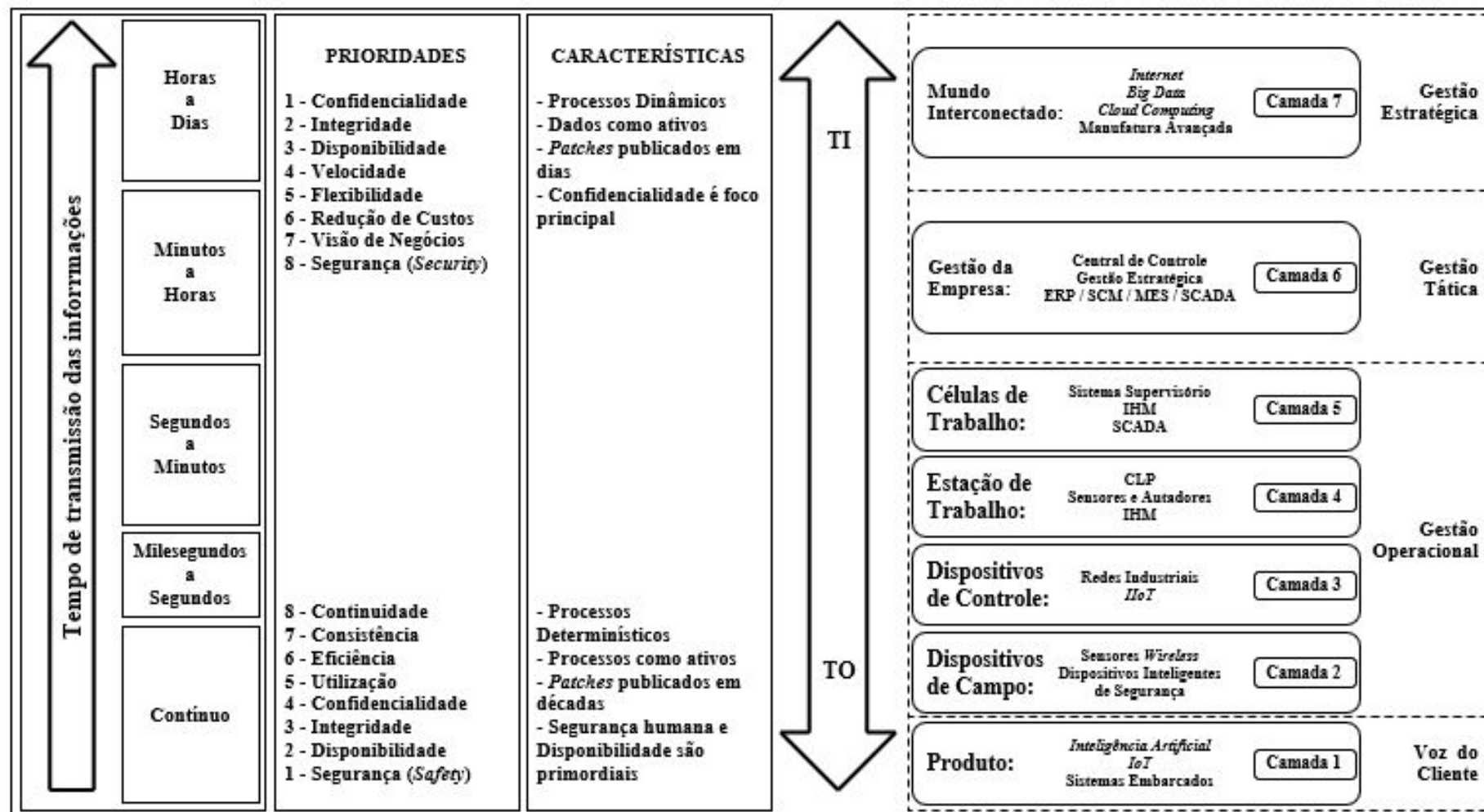
O nível superior realiza o planejamento de negócios e logística e conta com auxílio de sistema ERP. O nível abaixo controla as operações de manufatura, quais processos devem ser executados e em que ordem, conta com o auxílio de MES. Abaixo está o nível de monitoramento e supervisão onde o equipamento é monitorado por meio de IHM ou SCADA. No nível operacional o equipamento é controlado por meio de detecção e manipulação com auxílio de CLP (IEC, 2016c).

Ahmadian, Shajari e Shafiee (2020), fazem a associação de sistemas e tecnologias com redes de hierarquias comuns a TI, como por exemplo: a rede corporativa inclui os sistemas ERP e MES; a rede de supervisão inclui os sistemas IHM, SCADA, registrador de histórico e estação de trabalho de engenharia; a rede de controle local inclui RTU, CLP e MTU; o campo ou rede de instrumentação inclui sensores e atuadores.

No intuito de resumir os conceitos, definições, terminologias e modelos apresentados neste capítulo, foi elaborada a Figura 10, que representa em formato de painel bidimensional a convergência de TI e TO em empresas com manufatura avançada, segue representado da esquerda à direita, a indicação das responsabilidades das áreas de TI e de TO e o tempo de transmissão das informações (ANI; HE; TIWARI, 2017; BRETON, 2012; FABRO; GORSKI; SPIERS, 2016; GIVEHCHI *et al.*, 2017), as prioridades e as características específicas de TI e

de TO (PREMINGER, 2020; ISA, 2007), e os modelos integrados das camadas hierárquicas de tecnologias de automação presentes na manufatura avançada (ADOLPHS *et al.*, 2016; ISA, 2007). Ao centro do painel consta a seta vertical bidirecional indicando as áreas de TI e de TO, como sugerido por Garvin (2015), intencionalmente não há marcação da separação, para refletir uma área dinâmica de interação entre as duas áreas.

Figura 10: Painel de caracterização da convergência de TI e TO.



Fonte: o autor.

### 3. METODOLOGIA

Para o desenvolvimento deste trabalho, foi escolhida a realização de pesquisa científica básica, com características exploratórias e descritivas.

As abordagens da pesquisa quantitativa e qualitativa para realização da triangulação dos dados coletados. A combinação das abordagens e dos métodos possibilita um entendimento melhor dos problemas de pesquisa que cada uma das abordagens permitiria isoladamente e seu propósito é combinar o que há de melhor de cada abordagem (CAUCHICK-MIGUEL *et al.*, 2018).

Com relação aos métodos de pesquisa são utilizados levantamento tipo *survey* e levantamento teórico-conceitual (CAUCHICK-MIGUEL *et al.*, 2018; GUPTA; VERMA; VICTORINO, 2006).

Segundo Cauchick-Miguel *et al.* (2018), um levantamento do tipo *survey*, tem como objetivo geral contribuir para o conhecimento em uma área particular de interesse, por meio da coleta de dados/informações sobre indivíduos ou sobre seus ambientes.

O *survey* utilizado na pesquisa, como conceituado por Forza (2002), é do tipo exploratório, pois buscou-se adquirir maior visão sobre a questão da convergência das atividades de TI e de TO.

Como realização do levantamento dos constructos e do estado da arte sobre o tema foi realizada revisão sistemática da literatura à partir do protocolo PRISMA-P. Segundo Moher *et al.* (2015), um protocolo tem como objetivo fornecer a justificativa para a revisão e uma abordagem metodológica e analítica pré-planejada, antes do início de uma revisão.

Uma revisão sistemática tenta agrupar todas as evidências relevantes que se encaixam nos critérios de elegibilidade pré-especificados para responder a uma pesquisa específica e utiliza métodos explícitos e sistemáticos para minimizar o viés na identificação, seleção, síntese e resumo dos estudos (MOHER *et al.*, 2015).



### 3.1. Estratégia de pesquisa

Como estratégia de pesquisa foram utilizados instrumentos que possibilitam a realização de análises de dados quantitativos e de dados qualitativos. Os dados foram obtidos por meio da realização de revisão sistemática da literatura utilizando o protocolo PRISMA-P, da aplicação do instrumento do *survey*, cujas perguntas são apresentadas no Quadro 15 presente no Apêndice A e da realização de análise de conteúdo de entrevistas semiestruturadas, cujo instrumento é apresentado no Quadro 16 do Apêndice C.

### 3.2. Relação entre objetivos, métodos e resultados

Foi utilizado o instrumento denominado matriz de amarração, apresentado no Quadro 14 do APÊNDICE AAPÊNDICE A: Instrumento do *survey*, para relacionar os objetivos da pesquisa, com a fundamentação teórica, os pontos de investigação e os resultados esperados.

Uma matriz de amarração tem por objetivo avaliar a aderência e compatibilidade entre instrumento de pesquisa, objetivos da pesquisa, hipóteses ou proposições de pesquisa e técnicas de análise planejadas para tratamento dos dados (RIBEIRO; PLONSKI, 2016; TELLES, 2001).

A matriz de amarração foi estabelecida a partir dos dados coletados por meio do método revisão sistemática, para subsidiar a elaboração do instrumento de pesquisa *survey*. As lacunas identificadas mediante análise dos dados obtidos nas respostas coletadas do instrumento *survey* foram consideradas como pontos de investigação na elaboração das perguntas realizadas na entrevista semiestruturada.

### 3.3. Revisão sistemática da literatura

Como elemento auxiliar à análise quantitativa da bibliometria e à análise qualitativa da revisão sistemática, escolheu-se a utilização do protocolo de pesquisa PRISMA-P, que vem sendo amplamente utilizado em pesquisas associadas às ciências humanas. Este protocolo conta com quatro etapas previstas: identificação, triagem, elegibilidade e documentos incluídos para análise crítica.

O protocolo PRISMA-P foi desenvolvido como um guia para ajudar os autores a planejarem revisões sistemáticas e meta-análises que retornem um conjunto mínimo de itens importantes a serem incluídos no protocolo de pesquisa (MOHER *et al.*, 2015).

As autoras Marconi e Lakatos (2003), sugerem para a realização de pesquisa bibliográficas as seguintes etapas: definição do tema; elaboração do plano de trabalho; identificação, localização, compilação, fichamento, análise e interpretação e redação de síntese dos estudos selecionados.

Para Moher *et al.* (2015), as principais características de uma revisão sistemática são: conjunto de objetivos claramente definidos com uma metodologia explícita e reproduzível; busca sistemática que tente identificar todos os estudos que atendam aos critérios de elegibilidade; avaliação da validade dos resultados dos estudos incluídos (por exemplo, avaliação do risco de viés e confiança em estimativas cumulativas); e apresentação sistemática dos achados presentes nos estudos incluídos.

As etapas desta revisão sistemática também foram espelhadas nos trabalhos de Oliveira (2018) e de Pedriali e Arima (2019), e o levantamento de documentos para a revisão sistemática foi realizado nos meses de agosto e setembro de 2020.

### 3.3.1. Etapas da revisão sistemática

Inicialmente foram definidos os objetivos da pesquisa, conforme apresentado no Capítulo 1, os quais foram utilizados como fator de inclusão e exclusão dos estudos científicos encontrados.

Depois foram definidos os termos de pesquisa, em inglês, bem como a combinação dos termos, aqui chamada de strings de busca.

Como sugerido por Cauchick-Miguel *et al.* (2018), foi escolhido o uso de termos no idioma inglês devido os metadados comuns aos documentos pesquisados serem em inglês, em especial, os títulos, subtítulos, resumos e palavras-chaves.

O termos escolhidos para a realização da pesquisa utilizando a máquina de busca do *site* Periódicos CAPES<sup>6</sup> são apresentados no Quadro 4, e é possível observar os três grupos de associação dos termos, sendo o grupo 1 formado pelos termos sobre tecnologia operacional, o grupo 2 formado pelos os termos associados a segurança da informação e o grupo 3 é formado pela a associação de termos referentes a manufatura avançada.

Quadro 4: Termos utilizados para pesquisa de artigos sobre o tema da pesquisa.

| Idioma | Grupo 1  | Grupo 2   | Grupo 3   |
|--------|--|---|---|
| Inglês | <i>Operational Technology</i><br><i>OT</i><br><i>IT/OT</i><br><i>IT/OT convergence</i><br><i>IT/OT interoperability</i><br><i>IT/OT Integration</i><br><i>IT/OT fusion</i> | <i>OT Information Security</i><br><i>Industrial Information Security</i><br><i>Advanced Manufacturing Security</i><br><i>Industry 4.0 Security</i><br><i>Industrie 4.0 Security</i><br><i>Industrial Control System Security</i><br><i>ICS Security</i><br><i>IACS Security</i><br><i>SCADA Security</i><br><i>Industrial Cybersecurity</i> | <i>Advanced Manufacturing</i><br><i>Smart Factory</i><br><i>Smart Manufacturing</i><br><i>Industry 4.0</i><br><i>Industrie 4.0</i><br><i>Industrial Control System</i><br><i>ICS</i><br><i>IACS</i><br><i>SCADA</i><br><i>Cybersecurity</i> |

Fonte: o autor.

Foi utilizada a plataforma de pesquisa disponível no *site* Periódicos CAPES com acesso livre, sem vínculo com instituição de ensino.

A base de dados do portal Periódicos CAPES, no momento da realização da revisão sistemática, contava com um acervo de 100 bases de dados associadas as áreas de Engenharias, tais como ACM Digital Library<sup>7</sup>, Web of Science<sup>8</sup>, Scopus<sup>9</sup>, Google Acadêmico<sup>10</sup>, Emerald<sup>11</sup>, SciELO<sup>12</sup>, entre outras.

Para inclusão dos termos na máquina de pesquisa foram criadas *strings* que agruparam os termos por meio da utilização de operadores booleanos, como é apresentado no Quadro 5.

<sup>6</sup> <http://www.periodicos.capes.gov.br/>

<sup>7</sup> <https://dl.acm.org/>

<sup>8</sup> <http://www.webofknowledge.com/>

<sup>9</sup> <https://www.scopus.com/>

<sup>10</sup> <https://scholar.google.com.br/>

<sup>11</sup> <https://www.emerald.com/insight/>

<sup>12</sup> <https://scielo.org/>

Quadro 5: *Strings* de busca.

|                 |   |
|-----------------|---|
| <i>String 1</i> | "Operational Technology" OR "OT" OR "IT/OT" OR "IT/OT convergence" OR "IT/OT interoperability" OR "IT/OT Integration" OR "IT/OT fusion"   |
| <i>String 2</i> | "OT Information Security" OR "Industrial Information Security" OR "Advanced Manufacturing Security" OR "Industry 4.0 Security" OR "Industrie 4.0 Security" OR "Industrial Control System Security" OR "ICS Security" OR "IACS Security" OR "SCADA Security" OR "Industrial Cybersecurity" |
| <i>String 3</i> | "Advanced Manufacturing" OR "Smart Factory" OR "Smart Manufacturing" OR "Industry 4.0" OR "Industrie 4.0" OR "Industrial Control System" OR "ICS" OR "IACS" OR "SCADA" OR "Cybersecurity"   |

Fonte: o autor.

Após a aplicação de cada *string* de buscar na máquina de pesquisa selecionada, foram aplicados filtros disponíveis na plataforma à fim de refinar a pesquisa, tais como apresentado no Quadro 6.

Quadro 6: Filtro de refinamento aplicado em cada *string*.

| <i>String</i> | Refinado por   | Documentos Identificados |
|---------------|--|--------------------------|
| 1             | nível superior: Periódicos revisados por pares<br>tipo de recurso: Artigo<br>data de publicação: 2015 até 2020<br>tópico: <i>Engineering</i>                                     | 20                       |
| 2             | nível superior: Periódicos revisados por pares<br>tipo de recurso: Artigos<br>data de publicação: 2015 até 2020<br>tópico: <i>Engineering</i>                                    | 12                       |
| 3             | nível superior: Periódicos revisados por pares<br>tipo de recurso: Artigos<br>data de publicação: 2015 até 2020<br>tópico: <i>Engineering; Smart Manufacturing; Industry 4.0</i> | 25                       |

Fonte: Resultado da pesquisa.

A análise de busca dos termos presentes nas strings foi direcionada para o metadado título de artigos. Também foi priorizada a localização de artigos em PDF, artigos revisados por pares, com período de data de publicação de 2015 até 2020, classificados pela área de engenharia. Quando a quantidade de artigos localizados ultrapassava o valor de 30 achados, mais um refinamento foi aplicado, como na *string 3*, que se adicionou o refinamento de áreas *smart manufacturing* e *Industry 4.0*.

Estudos duplicados foram excluídos da amostra, bem como artigos que não atendiam o escopo do trabalho. Para a verificar se o artigo atendia ou não ao escopo do trabalho, no primeiro

momento foram lidos os títulos e seus resumos e em um segundo momento, os artigos foram lidos na íntegra, a fim de identificar a qualidade dos estudos, para então ser realizada a extração de dados dos estudos.

### 3.3.2. *Visão geral dos estudos localizados*

A partir das buscas realizadas nas bases de dados disponíveis na plataforma de pesquisa Periódicos CAPES, com as *strings* descritas, foram retornados 57 artigos, provenientes da busca automática refinada da máquina de pesquisa, a esses artigos foram aplicados critérios de inclusão e exclusão (artigos duplicados, ano de publicação, adequação aos objetivos da dissertação, respostas às questões de pesquisa). Não foram identificados artigos duplicados.

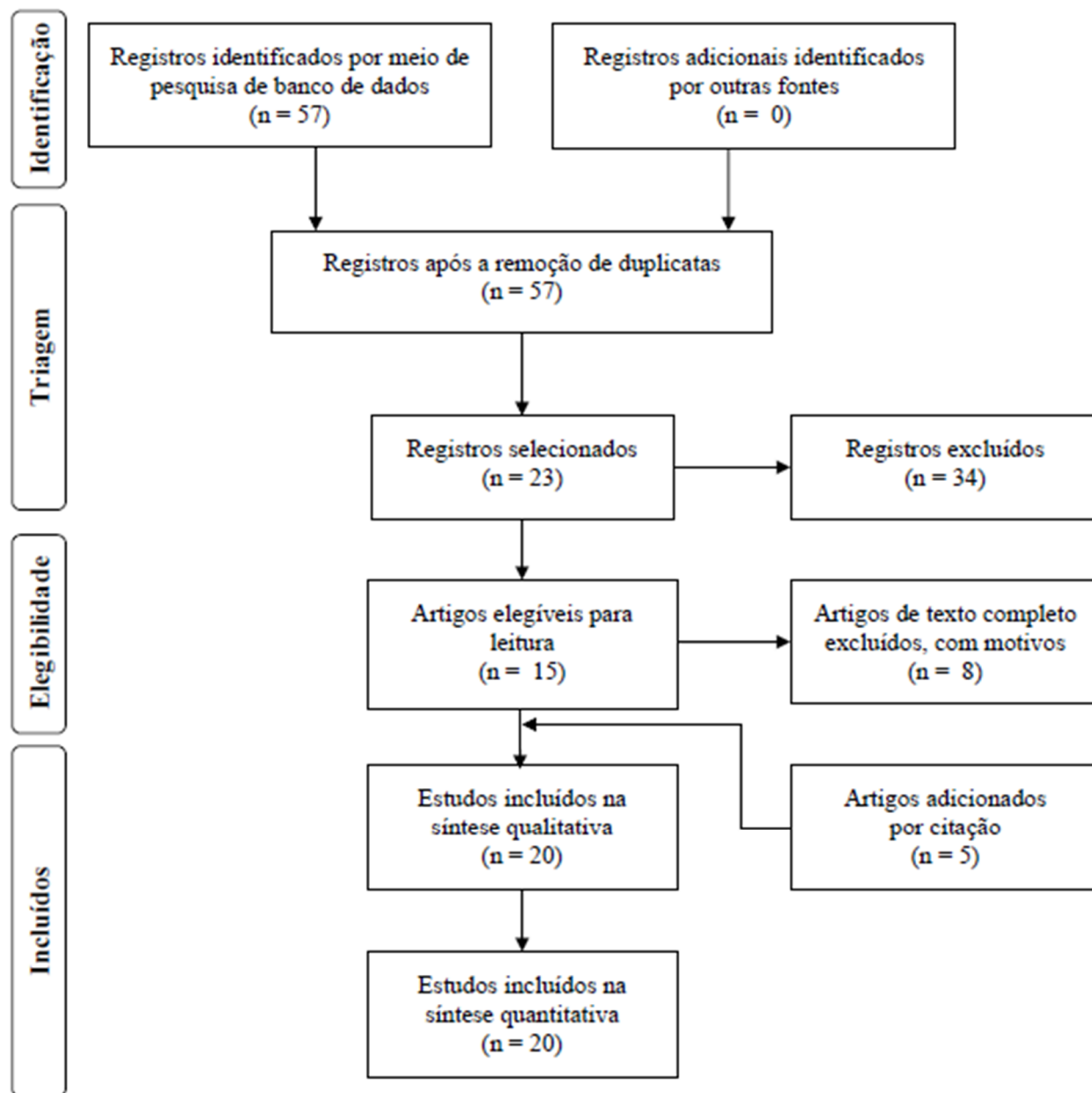
Foram excluídos 34 artigos por estarem fora do tema da dissertação, seguindo para análise do título e do resumo 23 artigos.

Após análise dos títulos e resumos dos artigos, 8 artigos foram excluídos por estarem fora do escopo do trabalho, sendo selecionados 15 artigos para leitura integral e análise de qualidade/extração de dados.

No processo de leitura integral dos artigos, cinco artigos foram adicionados para leitura integral, por serem referenciados nos trabalhos pré-selecionados, passando para 20 artigos para serem analisados quanto à qualidade e uso na presente dissertação.

A Figura 11 apresenta a síntese do processo de seleção dos artigos.

Figura 11: Fluxograma PRISMA-P da seleção de artigos para revisão sistemática.



Fonte: Resultado da pesquisa.

Os artigos selecionados para análise da qualidade e extração de dados para buscar respostas aos objetivos da pesquisa da dissertação, são apresentados no Quadro 7.

Quadro 7: Relação de artigos selecionados para análise de qualidade.

| ID | Título   | Autores   | Periódico  |
|----|--|---|--|
| 1  | <i>A categorization of customer concerns for an OT front-end of innovation process in IT/OT convergence context</i>            | Bonnetto, Emilie; Yannou, Bernard; Bertoluci, Gwenola; Boly, Vincent; Alvarez, Jorge  | Proceedings of International Design Conference                 |
| 2  | <i>A data analytical approach for assessing the efficacy of operational technology active defenses against insider threats</i> | Sundaram, Arvind; Abdel-Khalik, Hany S.; Ashy, Oussama  | Progress in Nuclear Energy                                     |
| 3  | <i>A guide to securing industrial control networks: integrating IT and OT systems</i>  | Paes, Richard; Mazur, David C.; Venne, Bruce K.; Ostrzenski, Jack   | IEEE Industry Applications Magazine                            |
| 4  | <i>A methodology to enhance industrial control system security</i>   | Timpson, Dominic; Moradian, Esmiralda   | Procedia Computer Science                                      |
| 5  | <i>A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories</i>            | Fernandez-Carames, Tiago M.; Fraga-Lamas, Paula   | IEEE Access  |
| 6  | <i>Behind the definition of industry 4.0: analysis and open questions</i>  | Culot, Giovanna; Nassimbeni, Guido; Orzes, Guido; Sartor, Marco   | International Journal of Production Economics                  |
| 7  | <i>Generating transparency in the worldwide use of the terminology industry 4.0</i>  | Nolting, Lars; Priesmann, Jan; Kockel, Christina; Rödler, Georg; Brauweiler, Tobias; Hauer, Ines; Robinius, Martin; Praktijn, Aaron | Applied Sciences   |
| 8  | <i>Industrial control system security taxonomic framework with application to a comprehensive incidents survey</i>             | Ahmadian, Mohammad Mehdi; Shajari, Mehdi; Shafiee, Mohammad Ali   | International Journal of Critical Infrastructure Protection    |
| 9  | <i>Industry 4.0 technologies: implementation patterns in manufacturing companies</i>   | Frank, Alejandro Germán; Dalenogare, Lucas Santos; Ayala, Néstor Fabián   | International Journal of Production Economics                  |
| 10 | <i>IT and OT convergence - opportunities and challenges</i>  | Kamal, S. Z.; Al Mubarak, S. M.; Scodova, B. D.; Naik, P.; Flichy, P.; Coffin, G.   | SPE Intelligent Energy International Conference and Exhibition |
| 11 | <i>IT and OT convergence, or collision? managing the merger for Greenfield LNG</i>   | Garvin, Thomas  | Abu Dhabi International Petroleum Exhibition and Conference    |
| 12 | <i>Operating digital manufacturing in industry 4.0: the role of advanced manufacturing technologies</i>                        | Da Silva, Elias Ribeiro; Shinohara, Ana Carolina; Nielsen, Christian Petersson; de Lima, Edson Pinheiro; Angelis, Jannis            | Procedia CIRP  |
| 13 | <i>Requirements of the smart factory system: a survey and perspective</i>  | Mohammed, M. Mabkhot; Abdulrahman, M. Al-Ahmari; Bashir, Salah; Hisham, Alkhalefah  | Machines (MDPI)  |
| 14 | <i>Security risk assessment-based cloud migration methodology for smart grid OT services</i>                                   | Jelacic, Bojan; Lendak, Imre; Stoja, Sebastijan; Stanojevic, Marina; Rosic, Daniela   | Acta Polytechnica Hungarica                                    |

(continuação)

|    |  |   |  |
|----|--|---|--|
| 15 | <i>Technology transfer in the supply chain oriented to industry 4.0: a literature review</i>   | Da Silva, Vander Luiz;<br>Kovaleski, João Luiz;<br>Pagani, Regina Negri | Technology Analysis & Strategic Management |
| 16 | <i>The future of IT operational technology supply chains</i>   | Paulsen, Celia  | Computer                                   |
| 17 | <i>The role of OPC UA TSN in IT and OT convergence</i>   | Tian, Shuo; Hu, Yihong  | 2019 Chinese Automation Congress           |
| 18 | <i>Understanding the influence of IT/OT convergence on the adoption of internet of things (IoT) in manufacturing organizations: an empirical investigation</i>                           | Ehie, Ike C.; Chilton, Michael A.                                       | Computers in Industry                      |
| 19 | <i>Unleashing the digital twin's potential for ICS security</i>  | Dietz, Marietheres; Pernul, Gunther                                     | IEEE Security & Privacy                    |
| 20 | <i>You've been hacked: words we hope to never hear: coming to grips with the looming risk of cyber-attacks on operational technology: the clear and present danger, often overlooked</i> | Romeo, J.   | Plastics Engineering                       |

Fonte: Resultado da pesquisa.

### 3.3.3. Avaliação da qualidade dos documentos localizados

Após aplicar os critérios de inclusão e exclusão, foi realizada a avaliação da qualidade dos estudos selecionados, para isso, foi utilizado um questionário adaptado de Dybå e Dingsøyr (2008). As questões utilizadas para avaliação da qualidade de cada estudo são apresentadas no Quadro 8.

Quadro 8: Questões orientadoras para avaliação da qualidade dos artigos.

|  |
|--|
| 1. É um artigo de pesquisa?  |
| 2. Existe uma descrição clara dos objetivos da pesquisa?                         |
| 3. Existe uma descrição adequada do contexto em que o estudo foi realizado?      |
| 4. O desenho de pesquisa foi adequado para atender os objetivos da pesquisa?     |
| 5. A estratégia de seleção da amostragem foi adequada aos objetivos da pesquisa? |
| 6. Os dados foram coletados de maneira adequada a responder as questões?         |
| 7. A análise dos dados foi suficientemente rigorosa?                             |
| 8. A relação entre os pesquisadores foi adequadamente considerada?               |
| 9. Há uma descrição clara dos resultados?  |
| 10. O estudo possui valor para a academia ou para a indústria?                   |

Fonte: Adaptado de Dybå e Dingsøyr (2008).



Com intuito de quantificar a avaliação e obter uma pontuação que possa ser associada ao nível de qualidade foi utilizada como base escala de três pontos de Likert (1932), onde: pontuação igual a 0 representa que não há nada no artigo que atenda ao critério avaliado; 0,5 representa que o artigo não deixa claro se atende ou não ao critério; e 1 quando o artigo atende ao critério avaliado.

No Quadro 9 são apresentadas as faixas de nível de qualidade dos artigos, mediante o valor de pontos N, decorrente da somatória de pontos dados no processo de avaliação.

Quadro 9: Classificação de qualidade mediante pontuação do artigo.

| Baixa               | Média               | Alta                | Muito Alta         |
|---------------------|---------------------|---------------------|--------------------|
| $0 \leq N \leq 3,5$ | $4 \leq N \leq 5,5$ | $6 \leq N \leq 8,5$ | $9 \leq N \leq 10$ |

Fonte: Adaptado de Likert (1932).

Os artigos que foram classificados nas faixas de qualidade média, alta e muito alta, seguiram para a extração de dados e os artigos classificados na faixa de qualidade baixa foram excluídos nesta etapa.

No Quadro 10 são apresentadas as pontuações e as classificações em nível de qualidade de cada artigo selecionado.

Quadro 10: Pontuação e nível de qualidade dos artigos selecionados.

| ID | Título   | Pontuação | Qualidade  |
|----|--|-----------|------------|
| 1  | <i>A categorization of customer concerns for an OT front-end of innovation process in IT/OT convergence context</i>            | 9         | Muito Alta |
| 2  | <i>A data analytical approach for assessing the efficacy of operational technology active defenses against insider threats</i> | 9         | Muito Alta |
| 3  | <i>A guide to securing industrial control networks: integrating IT and OT systems</i>  | 8,5       | Alta       |
| 4  | <i>A methodology to enhance industrial control system security</i>   | 9         | Muito Alta |
| 5  | <i>A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories</i>            | 9         | Muito Alta |
| 6  | <i>Behind the definition of industry 4.0: analysis and open questions</i>  | 8         | Alta       |
| 7  | <i>Generating transparency in the worldwide use of the terminology industry 4.0</i>  | 5,5       | Média      |
| 8  | <i>Industrial control system security taxonomic framework with application to a comprehensive incidents survey</i>             | 7         | Alta       |

(continuação)

|    |  |     |            |
|----|--|-----|------------|
| 9  | <i>Industry 4.0 technologies: implementation patterns in manufacturing companies</i>   | 7,5 | Alta       |
| 10 | <i>IT and OT convergence - opportunities and challenges</i>  | 9   | Muito Alta |
| 11 | <i>IT and OT convergence, or collision? managing the merger for Greenfield LNG</i>   | 8,5 | Alta       |
| 12 | <i>Operating digital manufacturing in industry 4.0: the role of advanced manufacturing technologies</i>  | 7,5 | Alta       |
| 13 | <i>Requirements of the smart factory system: a survey and perspective</i>  | 7   | Alta       |
| 14 | <i>Security risk assessment-based cloud migration methodology for smart grid OT services</i>   | 9   | Muito Alta |
| 15 | <i>Technology transfer in the supply chain oriented to industry 4.0: a literature review</i>   | 7   | Alta       |
| 16 | <i>The future of IT operational technology supply chains</i>   | 6,5 | Alta       |
| 17 | <i>The role of OPC UA TSN in IT and OT convergence</i>   | 8,5 | Alta       |
| 18 | <i>Understanding the influence of IT/OT convergence on the adoption of internet of things (IoT) in manufacturing organizations: an empirical investigation</i>                           | 9,5 | Muito Alta |
| 19 | <i>Unleashing the digital twin's potential for ICS security</i>  | 5   | Média      |
| 20 | <i>You've been hacked: words we hope to never hear: coming to grips with the looming risk of cyber-attacks on operational technology: the clear and present danger, often overlooked</i> | 5   | Média      |

Fonte: Resultado da pesquisa.

Além da classificação quanto a qualidade de cada um dos artigos, no momento da realização da leitura integral dos estudos, cada artigo foi classificado de acordo com o agrupamento de termos utilizados para a definição das *strings* de pesquisa, desta forma os estudos foram identificados quanto a abordagem aos temas convergência de TI e de TO, segurança da informação e manufatura avançada.

Quando o estudo aborda a temática do agrupando é identificado com a palavra “Sim” e quando aborda de modo não claro, ou não aborda a temática do agrupamento é identificado com a palavra “Não”. O resultado desta identificação é apresentado no Quadro 11.

Quadro 11: Classificação dos artigos pelo agrupamento de termos.

| ID | Título   | Convergência de TI/TO | Segurança da Informação | Manufatura Avançada |
|----|--|-----------------------|-------------------------|---------------------|
| 1  | <i>A categorization of customer concerns for an OT front-end of innovation process in IT/OT convergence context</i>  | Sim                   | Não                     | Sim                 |
| 2  | <i>A data analytical approach for assessing the efficacy of operational technology active defenses against insider threats</i>   | Sim                   | Sim                     | Sim                 |
| 3  | <i>A guide to securing industrial control networks: integrating IT and OT systems</i>  | Sim                   | Sim                     | Sim                 |
| 4  | <i>A methodology to enhance industrial control system security</i>   | Sim                   | Sim                     | Sim                 |
| 5  | <i>A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories</i>  | Não                   | Sim                     | Sim                 |
| 6  | <i>Behind the definition of industry 4.0: analysis and open questions</i>  | Não                   | Não                     | Sim                 |
| 7  | <i>Generating transparency in the worldwide use of the terminology industry 4.0</i>  | Não                   | Não                     | Sim                 |
| 8  | <i>Industrial control system security taxonomic framework with application to a comprehensive incidents survey</i>   | Não                   | Sim                     | Sim                 |
| 9  | <i>Industry 4.0 technologies: implementation patterns in manufacturing companies</i>   | Não                   | Não                     | Sim                 |
| 10 | <i>IT and OT convergence - opportunities and challenges</i>  | Sim                   | Sim                     | Sim                 |
| 11 | <i>IT and OT convergence, or collision? managing the merger for Greenfield LNG</i>   | Sim                   | Sim                     | Sim                 |
| 12 | <i>Operating digital manufacturing in industry 4.0: the role of advanced manufacturing technologies</i>  | Não                   | Sim                     | Sim                 |
| 13 | <i>Requirements of the smart factory system: a survey and perspective</i>  | Não                   | Não                     | Sim                 |
| 14 | <i>Security risk assessment-based cloud migration methodology for smart grid OT services</i>   | Sim                   | Sim                     | Sim                 |
| 15 | <i>Technology transfer in the supply chain oriented to industry 4.0: a literature review</i>   | Não                   | Sim                     | Sim                 |
| 16 | <i>The future of IT operational technology supply chains</i>   | Não                   | Sim                     | Sim                 |
| 17 | <i>The role of OPC UA TSN in IT and OT convergence</i>   | Sim                   | Sim                     | Sim                 |
| 18 | <i>Understanding the influence of IT/OT convergence on the adoption of internet of things (IoT) in manufacturing organizations: an empirical investigation</i>                           | Sim                   | Não                     | Sim                 |
| 19 | <i>Unleashing the digital twin's potential for ICS security</i>  | Não                   | Sim                     | Sim                 |
| 20 | <i>You've been hacked: words we hope to never hear: coming to grips with the looming risk of cyber-attacks on operational technology: the clear and present danger, often overlooked</i> | Não                   | Sim                     | Sim                 |

Fonte: Resultado da pesquisa.

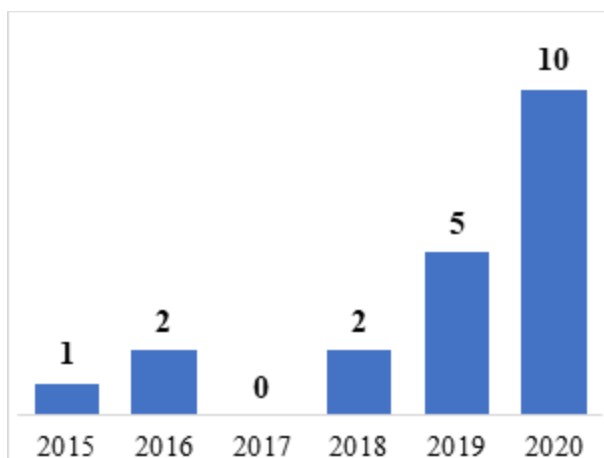
### 3.3.4. Extração dos dados

Para a extração dos dados, foram obtidos os arquivos em PDF e seus metadados foram coletados, gerenciados e gerenciados com auxílio do programa computacional EndNote X7<sup>13</sup>, ferramenta esta que possibilita entre outras ações, a criação de fichamento digital dos documentos, a eliminação automática de documentos duplicados e a extração de dados bibliométricos para coleta de dados.

Além da obtenção dos campos obrigatórios para identificação de artigos científicos para composição da referência científica, normatizada pela ABNT, foram adicionados aos campos de extração de dados para fichamento a descrição geral do estudo, o método de pesquisa utilizado, o tratamento dos dados, trabalhos futuros, e as respostas às questões de pesquisa: i) quais os impactos da convergência de TI e de TO em empresas com manufatura avançada? ii) quais os impactos na segurança da informação mediante a convergência de TI e de TO? iii) quais as relações entre os impactos<sup>14</sup> identificados com os pilares da segurança da informação em manufatura avançada?

Ao analisar a Figura 12 é possível evidenciar que mediante a seleção realizada, a quantidade de artigos publicados por ano se mostrou crescente, no período de 2015 a 2020, sendo o ano de 2020 o ano com maior quantidade de publicados dos artigos selecionados. Importante salientar que este a quantidade identificada no ano de 2020 não reflete a período anual total.

Figura 12: Ano de publicação dos artigos selecionados.



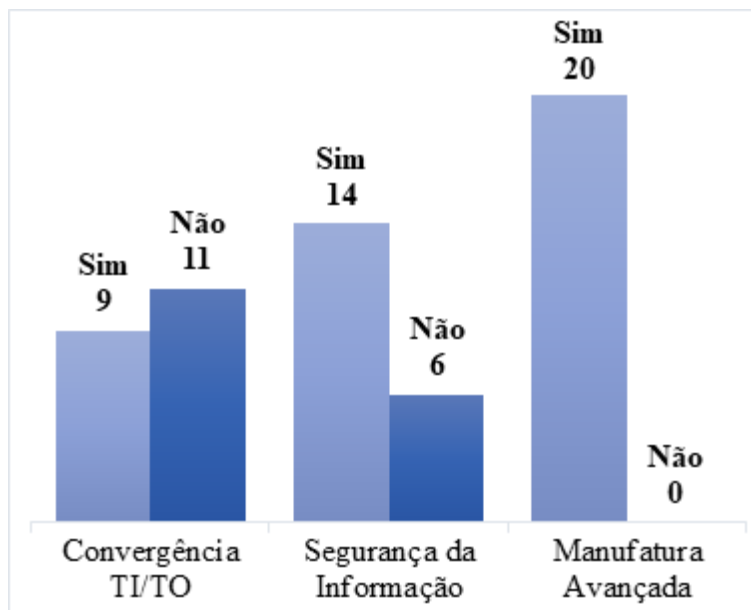
Fonte: Resultado da pesquisa.

<sup>13</sup> <https://endnote.com/>

<sup>14</sup> é o dano potencial que é infligido pelo incidente de segurança sobre o sistema (AHMADIAN; SHAJARI; SHAFIEE, 2020).

A Figura 13 apresenta o agrupamento dos artigos selecionados por abordagem das temáticas utilizadas para identificação das *strings* de pesquisa e é possível evidenciar que nove artigos abordam a convergência de TI e TO em seus estudos, 14 artigos abordam a segurança da informação e 20 artigos abordam a temática manufatura avançada. Cabe salientar que nesta classificação o mesmo artigo pode abordar mais do que somente uma temática e desta forma foi contabilizado em mais de um agrupamento.

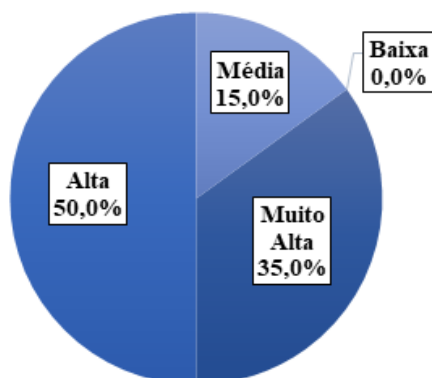
Figura 13: Agrupamento dos artigos selecionados por temas tratados nos estudos.



Fonte: Resultado da pesquisa.

A Figura 14 apresenta a síntese do agrupamento dos artigos selecionados pelo nível de qualidade. Nota-se que 35,0% dos artigos selecionados foram classificados com qualidade muito alta; 50,0% com qualidade alta e 15,0% com qualidade média.

Figura 14: Qualidade dos artigos selecionados



Fonte: Resultado da pesquisa.

### 3.3.5. Síntese dos estudos selecionados

No trabalho de Bonnetto *et al.* (2016), é criado um banco de dados de preocupações de clientes que utilizam aplicações de TO. São realizadas entrevistas com engenheiros especialistas de TO e é proposto método de inovação para empresas provedoras de automação industrial.

Sundaram, Abdel-Khalik e Ashy (2020) avaliam a capacidade das defesas ativas de TO, de permanecerem invisíveis para os invasores e discutem os desafios associados que devem ser enfrentados para garantir resiliência contra atores de ameaças persistentes avançadas (APT).

Paes *et al.* (2020) abordam impactos, benefícios e desafios sobre a convergência de TI e de TO em indústrias, tratam da técnica de defesa em profundidade e complementam que a primeira e mais importante etapa prática para realização da convergências das atividades de TI e de TO é envolver todas as partes interessadas e faz uso de rede robusta com espaço para expansão.

Timpson e Moradian (2018) discutem a necessidade de criação de metodologia que permite a integração da segurança da informação e da segurança humana nos ambientes ICS, e apresentam sugestão de metodologia para atender esta necessidade. Os resultados indicam que as abordagens de segurança existentes não consideram adequadamente a interdependência e a interrelação entre segurança e proteção (*security and safety*).

É apresentando no estudo de Fernández-Caramés e Fraga-Lamas (2019) a utilização dos conceitos e técnicas de blockchain para melhorar o nível de segurança da informação em fábricas modernas que utilizam tecnologias associadas a plataforma Indústria 4.0. O estudo fornece um guia para os desenvolvedores de aplicativos industriais de segurança cibernética.

Culot *et al.* (2020) desenvolvem estudo que aborda, por meio da análise de quase 100 definições da Indústria 4.0 e conceitos relacionados, o mapeamento da terminologia utilizada para referenciar a plataforma Indústria 4.0 e as tecnologias associadas. Estudo semelhante foi realizado por Nolting *et al.* (2019), buscou identificar geograficamente os termos mais utilizados para tratar da temática da Indústria 4.0.

Ahmadian, Shajari e Shafiee (2020) fazem breve revisão de várias ameaças e taxonomias de incidentes de segurança no âmbito ciberfísico, e propõem Estrutura Taxonômica Hierárquica (ETH) com as características necessárias para classificar ataques e incidentes de segurança em ICS.

Frank, Dalenogare e Ayala (2019), propõem uma estrutura de identificação de camadas de tecnologias para a Indústria 4.0 e apresentam os níveis de adoção dessas tecnologias e suas implicações para as empresas de manufatura. Dividem as tecnologias da Indústria 4.0 em *front-end* (dimensões: manufatura inteligente, produtos inteligentes, cadeia de suprimentos inteligente e trabalho inteligente) e em base (elementos: *internet* das coisas, serviços em nuvem, *big data* e *analytics*).

Kamal *et al.* (2016) tratam da classificação de nível de maturidade para analisar a convergência de TI e de TO no setor de Óleo e Gás. A classificação de maturidade acerca da convergência de TI e de TO proposta possui cinco níveis: identificação, realização, alinhamento, integração e otimização.

É discutido por Garvin (2015), em seu artigo, o espectro mais amplo de convergência de TI e de TO e compartilha percepções e lições aprendidas com a entrega de programas de integração de sistemas complexos para grandes projetos de capital de gás natural liquefeito. Propõe-se estratégia de convergência de TI e TO, para o setor de Óleo e Gás, que pode ajudar a traçar um curso mais suave para a convergência dos domínios.

Da Silva *et al.* (2020), buscam em seu estudo, diferenciar as ferramentas e as tecnologias associadas a Indústria 4.0. Os resultados revelam uma nova estrutura que define o domínio de aplicação da manufatura digital na Indústria 4.0, bem como a manufatura digital opera dentro da plataforma Indústria 4.0.

Mabkhot *et al.* (2018) destacam as perspectivas que moldam o paradigma “fábrica inteligente” e investigam os elementos e recursos dos sistemas utilizados pelas fábricas inteligentes.

Jelacic *et al.* (2020) apresentam metodologia de avaliação de risco e sugerem diagrama de arquitetura de segurança da informação para sistemas de controle industrial alinhados com o modelo presente na norma IEC 62443. Realizaram teste da metodologia proposta em dois estudos de caso: um grande operador de sistema de distribuição de energia elétrica com um ambiente de TO complexo; e um pequeno operador de sistema de distribuição de energia elétrica, com recursos de TO, orçamento e equipe de TI limitados.

Os resultados presentes no estudo de Da Silva, Kovaleski e Pagani (2019), inferem que no cenário industrial 4.0, a cadeia de suprimentos passará por mudanças, tais como visibilidade em tempo real de toda a cadeia de suprimentos e colaboração contínua entre cada uma das etapas da cadeia de suprimentos. Já Paulsen (2020), foca no estudo do futuro das soluções

tecnológicas para a segurança cibernética da cadeia de suprimentos. Também aborda o futuro dos ambientes político e de negócios.

Os autores Tian e Hu (2019) descrevem o modelo de Arquitetura Unificada OPC (OPC UA) e Rede Sensível ao Tempo (TSN) para tentar incentivar e resolver problemas relacionados a interoperabilidade, para auxiliar o processo de convergência de TI e de TO.

Ehie e Chilton (2020), em seu estudo, apresentam os resultados de *survey* realizado em 239 indústrias de manufatura nos Estados Unidos da América para identificar a influência da convergência de TI e de TO sobre a adoção de IoT nas indústria. Os resultados sugerem que a infraestrutura de TI, a governança de TI, a interoperabilidade e a colaboração da equipe, impactam positivamente na convergência de TI e de TO, que por sua vez influencia positivamente a adoção de IoT em organizações de manufatura.

Dietz e Pernul (2020) discutem a aplicação e os limitantes do uso de gêmeos digitais para análise da segurança da informação em situação de convergência de TI e de TO, enquanto Romeo (2020) discute aspectos da segurança cibernética decorrente da IIoT e da Indústria 4.0.

### **3.4. Levantamento tipo *survey***

O instrumento de coleta de dados para o levantamento tipo *survey*, utilizado neste trabalho foi questionário com questões abertas; fechadas dicotômicas, e de múltipla escolha, cuja classificação foi baseada no trabalho de Cauchick-Miguel *et al.* (2018).

O questionário foi previamente testado, para evitar perguntas com interpretações dúbias (CAUCHICK-MIGUEL *et al.*, 2018; MARCONI; LAKATOS, 2003), antes de ser enviado aos sujeitos da amostragem via *internet*.

Como suplemento a pesquisa *survey*, foi realizada entrevista com questionário semiestruturado com questões abertas e fechadas dicotômicas para comprovação de dados fornecidos anteriormente com o propósito da obtenção de dados para o fechamento das lacunas que foram identificadas com a análise dos dados coletados na primeira etapa de levantamento do tipo *survey*. Esta etapa da pesquisa é detalhada na seção 3.5. Entrevista semiestruturada.



### 3.4.1. *Sujeitos da pesquisa*

Para a realização da pesquisa do tipo *survey* e posteriormente a condução das entrevistas semiestruturadas, foram escolhidos profissionais das áreas de TI e de TO que atuam em empresas que têm em seus processos elementos industriais de controle associados as tecnologias de manufatura avançada.

Foram estabelecidos nove cargos envolvidos com as atividades de TI e de TO em empresas com tecnologias de suporte a manufatura avançada: CISO, CSO, Gerente de Tecnologia Operacional, Gerente de Tecnologia da Informação, Gerente de Segurança da Informação, Líder de Tecnologia da Informação, Líder de Tecnologia Operacional, Integrador de Tecnologia Operacional, Consultor de Tecnologia Operacional.

Alguns dos sujeitos participantes atuam em mais de uma função, em funções diferentes das especificadas no instrumento, então foi adicionada a opção ao participante descrever no campo outros, a descrição de seu cargo, caso não houvesse a identificação com nenhuma das opções dadas.

Foram localizados 130 profissionais na rede social *LinkedIn*, 719 profissionais registrados no grupo do *Telegram* ScadaSecBR e 232 profissionais registrados no grupo de *WhatsApp* gerido pela empresa TI Safe. Estas quantidades de contatos foram aferidas em agosto de 2020.

Após a eliminação da duplicidade de registros dos contatos profissionais nas três fontes de contatos selecionada, obteve-se a quantia de 660 contatos passíveis de serem utilizados para a submissão do questionário *survey*. Não foram utilizados os contatos que possuíam em seus nomes de usuário a identificação por abreviatura ou apelidos que impossibilitassem a adequada identificação do profissional.

### 3.4.2. *Instrumento do survey*

O instrumento do *survey* foi elaborado por meio da ferramenta Google Forms<sup>15</sup> e é composto por um questionário de 14 perguntas, aplicado aos profissionais de TI e TO que atuam em empresas com manufatura avançada. As perguntas foram elaboradas com base na revisão bibliográfica realizada. Sendo assim, para o desenvolvimento do instrumento desta pesquisa a seguinte estratégia foi adotada:

- Levantamento do perfil sociodemográfico dos participantes: por meio da identificação da nacionalidade; formação acadêmica; nacionalidade, tamanho e setor econômico da empresa; cargo que ocupa e tempo de experiência;
- Identificação da interação dos participantes com tecnologias de manufatura avançada: as tecnologias foram separadas nos níveis hierárquicos de automação como propostos na ISA 62443-1-1 (2007) e na DIN SPEC 91345, redigida por Adolphs *et al.* (2016);
- Identificação da aceitação da convergência de TI e TO pelos participantes: realização de perguntas fechadas dicotômicas se o participante pertence a área de TI ou de TO e se julga necessária a convergência de TI e de TO. Foi realizado o registro das opiniões dos participantes sobre as oportunidades, limitações e as tecnologias que oportunizam a convergência de TI e de TO;
- Identificação dos impactos à segurança da informação: registro das opiniões dos participantes sobre os principais impactos à segurança da informação mediante a convergência de TI e de TO;
- Ao final do questionário foi adicionada a possibilidade de coleta de declaração de interesse por parte dos respondentes em participarem da entrevista semiestruturada que seria aplicada diretamente pelo pesquisador. Os especialistas respondentes que declararam interesse em participar compõem os sujeitos da entrevista semiestruturada realizada nesta pesquisa.

Mais detalhes sobre o instrumento desenvolvido para o levantamento tipo *survey* poderão ser consultados no instrumento do *survey* disponível no Quadro 15.

---

<sup>15</sup> <https://docs.google.com/forms/>

### 3.5. Entrevista semiestruturada

Nesta seção, é detalhado o processo de desenvolvimento do questionário utilizado na execução da entrevista semiestruturada aplicada nesta pesquisa. Os especialistas, aqui citados como sujeitos participantes foram escolhidos a partir da lista de sujeitos que declararam disponibilidade para a entrevista, em pergunta específica no questionário *survey*. Ainda nesta seção é apresentado o instrumento utilizado, a coleta e o tratamento dos dados.

#### 3.5.1. Instrumento da entrevista semiestruturada

O instrumento da entrevista semiestruturada foi criado a partir das lacunas identificadas na análise dos dados compilados do *survey* realizado. Além da busca de preenchimento das lacunas identificadas também foram realizadas perguntas para confirmação de informações e aprofundamento no tema por meio da realização de perguntas abertas.

As questões foram categorizadas como explicações de introdução a entrevista, identificação da experiência profissional do entrevistado, identificação de lacunas associadas a temática segurança da informação, identificação de lacunas associadas a temática manufatura avançada, identificação da percepção do respondente sobre a convergência das atividades de TI e de TO, e por último a categoria que reúne as explicações do fechamento da entrevista pelo pesquisador com o profissional participante.

Na categoria introdução constaram as explicações sobre os objetivos da entrevista, as informações sobre a pesquisa e a unidade de Pós-graduação, Extensão e Pesquisa do Centro Paula Souza e a solicitação verbal formal de autorização por parte dos profissionais participantes quanto a gravação audiovisual da entrevista.

Em identificação da experiência profissional do entrevistado foram direcionadas perguntas sobre: o sistema de gestão da segurança da informação; a ciência do entrevistado sobre o uso das informações; a sua experiência e o papel do entrevistado no chão de fábrica.

A categoria segurança da informação contou com perguntas abertas para identificação da consciência do entrevistado sobre seu papel na segurança da informação, sob responsabilidade de qual departamento se encontra a gestão da segurança da informação, como

são analisados os requisitos de segurança da informação e como se dá a estratégia de investimentos em gestão da segurança da informação.

Na categoria manufatura avançada constaram perguntas abertas para identificar o conhecimento do entrevistado sobre a integração de atividades oportunizadas pela utilização de tecnologias da manufatura avançada, se há automação dedicada a segurança humana (*safety*), quais as tecnologias presentes no chão de fábrica e destas quais demandam suporte de TI e quais demandam suporte de TO, e por fim questionou-se ao especialista a vida útil dos equipamentos e sistemas de controle utilizados nas empresas nas quais os entrevistados atuam ou atuaram.

Para levantamento de dados sobre a temática convergência de TI e de TO, foram aplicadas perguntas abertas aos entrevistados, tais como: se já ouviram falar da convergência das áreas, da gestão e das atividades de TI e de TO; se são a favor ou contra a convergência; e se o entrevistado julga ser possível a integração das atividades de TI e de TO em empresas com processos de manufatura avançada implantados.

Na categoria fechamento constou pergunta direcionada ao especialista sobre quem seria interessante participar da etapa da pesquisa de entrevista semiestruturada e são realizadas explanações para incentivar a comunicação de pensamentos relevantes por parte dos entrevistados ao pesquisador, mesmo após o final da entrevista. Também houve revisão da programação da entrevista e agradecimento do pesquisador aos participantes.

O instrumento utilizado para agrupar as questões da entrevista semiestrutura encontra-se no Quadro 16 do APÊNDICE C.

### 3.5.2. Coleta de dados

Antes da disponibilização do instrumento, foram enviadas mensagens de convite para participação na pesquisa aos profissionais encontrados por meio da utilização da máquina de pesquisa do *site LinkedIn*<sup>16</sup>, onde foi possível ter retorno positivo quanto a disponibilidade de participação de 69 profissionais. Nos grupos de profissionais presentes no *WhatsApp*<sup>17</sup> e *Telegram*<sup>18</sup>, foi realizada apresentação no ambiente geral dos aplicativos, sobre a pesquisa, e então foi realizado o convite aberto a todos os profissionais cadastrados nos grupos.

---

<sup>16</sup> <https://www.linkedin.com/>

<sup>17</sup> <https://www.whatsapp.com/>

<sup>18</sup> <https://telegram.org/>

Após o convite realizado na primeira semana de agosto de 2020, nas três bases de contatos, foi evidenciado retorno positivo de 94 profissionais quanto a disponibilidade de participação na pesquisa. Além dos profissionais que informaram que participariam da pesquisa o instrumento de pesquisa *survey* também foi submetido aos demais profissionais que não deram retorno ao convite. O instrumento *survey* foi enviado para 660 profissionais em agosto de 2020.

Foram realizadas três comunicações de lembrete de participação na pesquisa aos profissionais que ainda não haviam dado retorno de resposta ao questionário, em intervalos de uma semana entre um lembrete e outro, na tentativa de aumentar a quantidade de respondentes, assim como sugerido por Forza (2002) e por Cauchick-Miguel *et al.* (2018).

Ao final do protocolo de execução da coleta de dados do levantamento tipo *survey*, foram obtidas as respostas provenientes de 33 profissionais.

Seguindo as informações de Larson e Farber (2015) identifica-se os seguintes parâmetros estatísticos: o tamanho da amostra composto por 33 profissionais respondentes; o tamanho da população é de 660 profissionais; o nível de confiança determinado foi de 90% e a margem de erro amostral é de aproximadamente 14%.

Caracteriza-se a amostra como sendo do tipo não probabilística por conveniência (MARTINS; LUIZ; FERREIRA, 2011), pois foram utilizados os contatos elencados dos três grupos de profissionais citados e não houve distinção alguma na escolha dos respondentes que compunham a população identificada.

Por se tratar de uma *survey* exploratória não há uma quantidade mínima de taxa de retorno de respostas (FORZA, 2002). Mesmo considerando que a quantidade de participantes respondentes seja pequena em comparação a população focal identificada, ainda assim os resultados são relevantes e aplicáveis como base de dados para pesquisa-piloto (CAUCHICK-MIGUEL *et al.*, 2018), o que valida a qualidade da pesquisa.

Após a obtenção das respostas no instrumento *survey*, 16 profissionais foram convidados para participar da entrevista semiestruturada. Foram enviados por e-mail os convites de participação e solicitação de disponibilidade para agendamento de reunião via Microsoft Teams<sup>19</sup> somente aos 16 profissionais que relataram no *survey* que tinham interesse e disponibilidade para participar da entrevista semiestruturada.

---

<sup>19</sup> <https://www.microsoft.com/microsoft-teams/>

Obteve-se o retorno via e-mail de 11 profissionais e estes compuseram o total de participantes da etapa de entrevista semiestruturada que foi realizada nos meses de janeiro e fevereiro de 2021.

As respostas dos participantes às perguntas realizadas pelo pesquisador foram transcritas com auxílio do programa computacional Microsoft Stream<sup>20</sup> que dispunha de recursos que possibilitaram a criação automática de transcrição/legendagem dos arquivos audiovisuais obtidos a partir de cada reunião realizada. Posteriormente foi realizada revisão dos textos transcritos utilizando o programa Microsoft Word<sup>21</sup> para garantir que tudo que foi respondido foi convertido fidedignamente para texto.

Todos os participantes solicitaram confidencialidade quanto a citação de seus nomes, nomes de outras pessoas e nomes de instituições que porventura fossem apresentados nas respostas. Também solicitaram compartilhamento dos resultados da pesquisa após a compilação pelo pesquisador e validação do manuscrito pelos responsáveis do Programa de Mestrado Profissional, ao qual a pesquisa está vinculada.

A partir das respostas obtidas com o levantamento tipo *survey* e com a entrevista semiestruturada, foi possível identificar e descrever como está sendo tratada a segurança da informação em empresas que investem em tecnologia de processos, bem como obter as opiniões dos profissionais de TI e de TO sobre a convergência das atividades de suas áreas.

### 3.5.3. Tratamento dos dados

Para o tratamento dos dados coletados nas questões abertas da entrevista semiestruturada, planeja-se utilizar a técnica de análise de conteúdo.

O procedimento padrão para a análise de conteúdo consiste na definição de categorias, por meio do agrupamento de elementos com características comuns, à fim de potencializar a análise e comparação entre grupos de termos.

As etapas básicas para a análise de conteúdo são: pré análise, exploração do material, tratamento dos resultados, inferência e interpretação. A pré análise refere-se a seleção do

---

<sup>20</sup> <https://web.microsoftstream.com/>

<sup>21</sup> <https://www.microsoft.com/pt-br/microsoft-365/word>

material e a definição dos procedimentos à serem seguidos. A exploração do material diz respeito a implementação destes procedimentos. O tratamento e a interpretação, referem-se a geração de inferências e análise dos resultados da investigação, sendo previsto nesta última fase ocorrer a confirmação de suposições ou não (BARDIN, 2011; SILVA *et al.*, 2017; VERGARA, 2005).

A análise de conteúdo realizada nesta pesquisa utilizou os textos transcritos e revisados, obtidos por meio das entrevistas semiestruturadas realizadas com auxílio do instrumento desenvolvido, presente no Quadro 16 do Apêndice A.2. Na pré análise identificou-se que todas as 11 transcrições estavam adequadas para serem utilizadas.

Na etapa de exploração do material foi utilizado o programa computacional ATLAS.ti<sup>22</sup> para realização da codificação, em sua versão 9.

A etapa de codificação é composta pela determinação das unidades de registros e das unidades de contexto (BARDIN, 2011).

As unidades de registros foram definidas de acordo com as temáticas identificadas nas respostas dos profissionais, de modo a obter dados consistentes que auxiliem na resposta as questões da pesquisa. A unidade de contexto é a análise dos parágrafos das respostas dos entrevistados que continham uma ou mais unidades de registro.

Após definir as unidades de registros e as unidades de contexto foi realizada a categorização dos códigos criados. No Quadro 12 é possível identificar a categorização utilizada na análise de conteúdo das entrevistas.

Quadro 12: Categorização dos códigos utilizados na análise de conteúdo.

| <b>Categoria</b>    | <b>Unidades de Registro</b> | <b>Unidades de Contexto</b>   |
|---------------------|-----------------------------|---|
| Manufatura Avançada | Manufatura Avançada         | Manufatura Avançada / Integração de tecnologias / Tecnologias inovadoras / Inovação disruptiva / Indústria 4.0  |
|                     | Tecnologias                 | Nomes de tecnologias / Conceitos tecnológicos diferenciados / Projetos inovadores                               |
|                     | Vida Útil                   | Vida útil / Equipamentos obsoletos / Obsolescência / Atualização tecnológica / Paradas programadas / Manutenção |

<sup>22</sup> <http://www.atlasti.com/>

(continuação)

|                         |                            |   |
|-------------------------|----------------------------|---|
| Segurança da Informação | <i>Security</i>            | <i>Security</i> / Segurança da Informação / Incidentes de segurança da informação   |
|                         | <i>Safety</i>              | <i>Safety</i> / Segurança humana / Segurança do meio ambiente / Segurança da infraestrutura / SIS   |
|                         | Separação de TI e TO       | Separação de Departamentos / Departamento de TI / Departamento de TO / Modelagem de ameaças / Integração de departamentos                 |
| Convergência            | Opinião sobre Convergência | Opinião sobre convergência / Diferenças entre profissionais, cultura, departamentos, cargos, salários / À favor / Contra / Com restrições |
|                         | Oportunidades              | Convergado / Oportunidades / Aumento / Melhoria / Redução / Diminuição / Participação   |
|                         | Desafios                   | Convergado / Desafios / Cultura / Priorização / Determinação / Necessidade  |
|                         | Limitações                 | Convergado / Limitações / Alternativa / Falta   |

Fonte: o autor.

A categorização dos códigos baseou-se nas respostas obtidas das entrevistas e verificando sua conformidade com os objetivos da pesquisa.

A análise de conteúdo foi embasada em procedimentos interpretativos e qualitativos com base nos dados obtidos.

Já para a análise dos dados obtidos com as perguntas fechadas dicotômicas, e de múltipla escolha, presentes predominantemente no levantamento tipo *survey*, aplicou-se a estatística descritiva e a elaboração de gráficos, para a realização da análise dos resultados.



## **4. ANÁLISE DOS RESULTADOS**

Este capítulo apresenta os resultados obtidos com a aplicação dos instrumentos descritos nos capítulos 3.3, 3.4 e 3.5. Ele consiste em dados que foram coletados por meio de revisão sistemática da literatura, aplicação de questionários e realização de entrevistas focadas na temática convergência das atividades de TI e de TO em empresas que fazem uso de tecnologias associadas a manufatura avançada.

Na revisão sistemática da literatura, além da identificação do estado da arte do tema, foram analisadas as oportunidades e os limitantes indicados pelos autores selecionados.

No levantamento tipo *survey*, para cada um dos participantes foram analisados os seguintes aspectos: (1) características sociodemográficas dos profissionais que atuam ou atuaram em empresas com manufatura avançada; (2) característica das tecnologias presentes nos processos de manufatura avançada das empresas em que atuam ou atuaram; (3) características dos sistemas de gestão da segurança da informação das empresas em que atuam ou atuaram; e (4) percepção sobre os impactos da convergência das atividades de TI e de TO.

Na análise dos resultados obtidos com o desenvolvimento de análise de conteúdo das entrevistas semiestruturadas, foram apresentados os seguintes aspectos categorizados: (1) achados sobre a temática manufatura avançada; (2) achados sobre a segurança da informação; e (3) achados sobre a convergência das atividades de TI e de TO.

### **4.1. Resultados obtidos com a revisão sistemática da literatura**

Nesta seção são apresentados os achados sobre as oportunidades e desafios citados pelos autores selecionados mediante a realização da revisão sistemática da literatura.

Na seção 4.1.1 são apresentadas as oportunidades (impactos positivos) e na seção 4.1.2 são apresentadas as limitações (impactos negativos) relacionadas à segurança da informação (security) e a segurança ocupacional (safety) na ocasião da convergência de TI e TO, de acordo com as evidências coletadas na literatura científica selecionada

#### 4.1.1. Oportunidades evidenciadas na revisão sistemática

Para Bonnetto *et al.* (2016) a utilização de máquinas para beneficiar os recursos de processamento de dados dos sistemas de TI para melhorar a eficiência dos processos produtivos e a introdução de novos conceitos de produtos ou serviços são oportunidades que contribuem para a convergência de TI e TO.

São oportunidades para Sundaram, Abdel-Khalik e Ashy (2020): a implantação de segurança da informação com abordagem passiva de defesa baseada no uso da inteligência artificial e nos modelos de sistema para monitorar as variáveis do processo em busca de correlações que podem ser usadas para detectar falsificações das variáveis do processo; a análise dos históricos de atacantes para procurar vulnerabilidades<sup>23</sup> que podem ser usadas para infligir danos físicos ao sistema; a segurança da informação de TO representa um paradigma de defesa novo e complementar para defesas consideradas comuns a TI; os avanços no campo da análise de *big data* para derivação de recursos de habilitação que podem ser explorados para fins de segurança. Frank, Dalenogare e Ayala (2019) e Da Silva, Kovaleski e Pagani (2019) também citaram o uso das tecnologias *big data* e *analytics* em empresas de manufatura, e citam que a adoção sistêmica das tecnologias associada a manufatura inteligente (*smart manufacturing*) são oportunidades que podem ser observadas com a convergência de TI e TO.

No trabalho de Paes *et al.* (2020) são citadas como oportunidades os avanços da conectividade relacionados às redes de chão de fábrica que tornam as empresas globalmente conectadas, a IIoT, os novos projetos de dispositivos eletrônicos inteligentes, de comunicações Ethernet e de tecnologia de armazenamento em nuvem, a redução de custos, a redução de riscos, a melhoria de desempenho, a melhoria do nível de manutenção preditiva e preventiva, e a implantação de técnica de defesa em profundidade para proteger o sistema de informação. Ahmadian, Shajari e Shafiee (2020), também citaram a interconectividade, em especial, de sistemas SCADA com redes corporativas e com a *internet*, como sendo uma oportunidade da convergência de TI e de TO.

As oportunidades associadas a convergência de TI e TO citadas no trabalho de Fernández-Caramés e Fraga-Lamas (2019) foram a utilização de técnicas associadas a *blockchain* associada a cibersegurança para propiciar a integridade dos dados e o uso de

---

<sup>23</sup> são fraquezas no projeto ou especificação, implementação ou operação e gerenciamento (configuração) de um sistema que pode ser explorada para violar a política de segurança do sistema (AHMADIAN; SHAJARI; SHAFIEE, 2020).

tecnologias que permitem comunicações autônomas entre vários dispositivos industriais e a *internet*.

A integração de processos; a disponibilidade de informações em tempo real; a representação virtual do mundo real; a autonomia de processos de fabricação; a previsibilidade, a modularidade e a configurabilidade, são oportunidades citadas no trabalho de Culot *et al.* (2020).

Kamal *et al.* (2016) citaram como oportunidades o aumento da segurança da informação, da eficiência e da produtividade, por meio da convergência de TI e TO. Paulsen (2020) complementa citando que a capacidade de comunicar dados de forma rápida, segura e automática entre sistemas e organizações também é uma oportunidade.

A possibilidade de execução de HAZOP por uma equipe multidisciplinar e convergida é uma oportunidade citada por Garvin (2015).

Mabkhot *et al.* (2018) citam que a convergência de TI e TO pode ser utilizada como oportunidade estratégica para implantação de redes inteligentes de comunicação.

Tian e Hu (2019) veem como oportunidade a convergência de TI e TO para reduzir a conexão ineficaz entre os departamentos, a simplificação do processo de fabricação, a expansão do lucro comercial e o fornecimento de serviço com mais qualidade.

A determinação de prioridade à segurança da tecnologia operacional, que se traduz em segurança humana, é uma oportunidade citada por Romeo (2020).

#### 4.1.2. Limitações evidenciadas na revisão sistemática

No trabalho de Sundaram, Abdel-Khalik e Ashy (2020) é citada como limitação à convergência de TI e TO que a digitalização, um dos possíveis resultados do processo de convergência, pode resultar no aumento de vulnerabilidades devido o aumento da superfície de ataque.

Paes *et al.* (2020) destacam dois limitantes da convergência de TI e TO, o primeiro é que a disponibilização de dados críticos de TO para todas as áreas do negócio pode ser uma ameaça a segurança da informação e o segundo é que podem haver conflitos de interesse com

a convergência e estes devem ser resolvidos pela liderança (nível executivo). Garvin (2015) e Kamal *et al.* (2016) também citaram limitantes associados a gestão de pessoas se convergidos os departamentos de TI e de TO.

O aumento da interconectividade dos dispositivos inteligentes de TI e de TO também pode aumentar a superfície de ataque à segurança da informação é indicado por Timpson e Moradian (2018) como um possível limitante. Jelacic *et al.* (2020) também citaram o mesmo tema como limitante associado a possibilidade de aumento de ameaças à segurança da informação.

Para Tian e Hu (2019) são limitantes da convergência de TI e TO, os riscos de conectividade associados a operações remotas, a falta de engenheiros qualificados, a possibilidade de existência de responsabilidades ambíguas da equipe e a falta de protocolos padronizados.

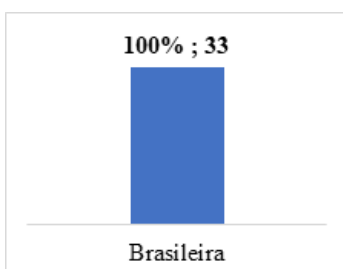
#### 4.2. Resultados obtidos com o *survey*

Nesta seção são apresentados os resultados obtidos com o levantamento *survey*, de acordo com os objetivos definidos na seção 1.3. Todos os dados obtidos na pesquisa *survey* estão tabulados e se encontram disponíveis no APÊNDICE B.

##### 4.2.1. Características sociodemográficas dos sujeitos da pesquisa

Todos os participantes da pesquisa, conforme apresentado na Figura 15, possuem nacionalidade brasileira.

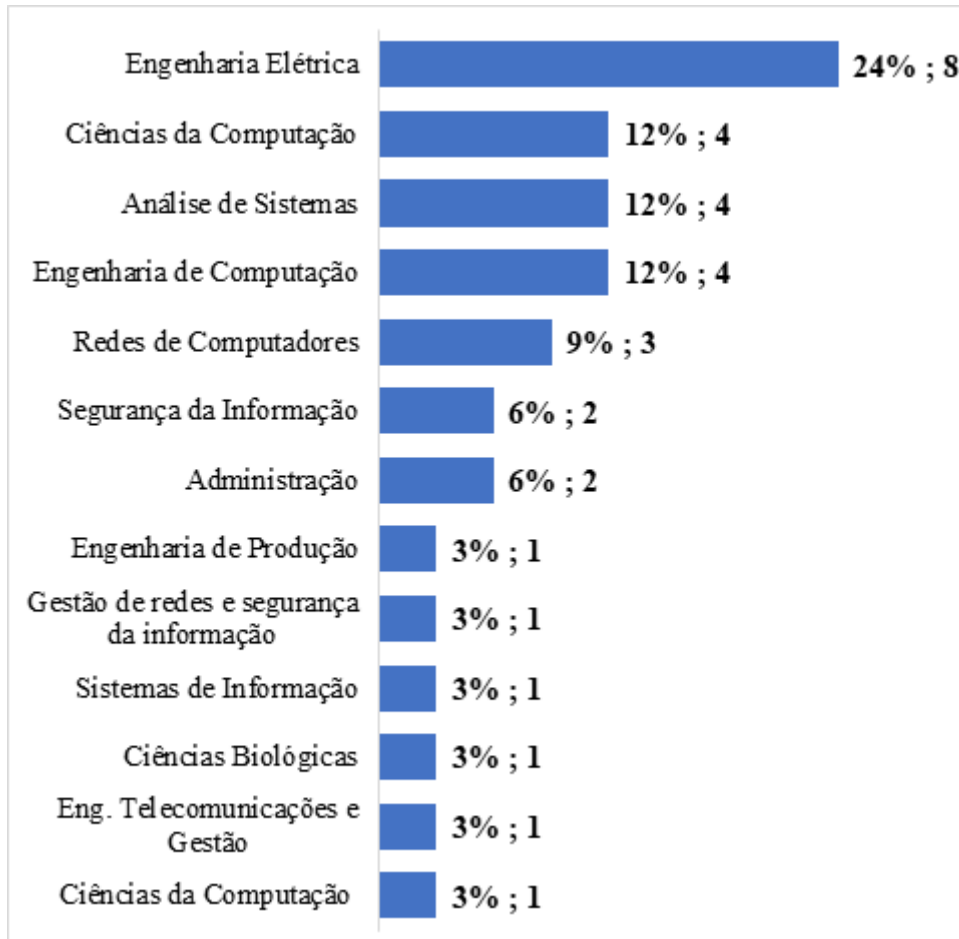
Figura 15: Nacionalidade dos participantes.



Fonte: Resultado da pesquisa.

Conforme a apresentado na Figura 16, a formação predominante foi Engenharia Elétrica, com 8 (24%) participantes. Nota-se que 32 participantes possuem formação na área de exatas e um respondente possui formação em Ciências Biológicas.

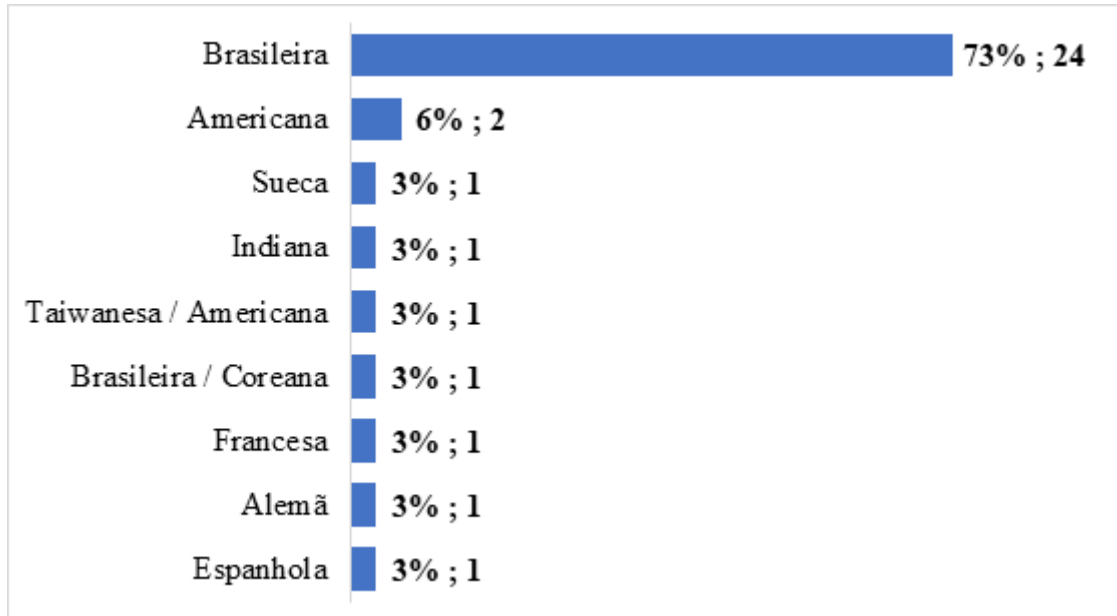
Figura 16: Formação dos participantes.



Fonte: Resultado da pesquisa.

Na Figura 17 é possível identificar que a nacionalidade predominante, das empresas em que os participantes atuam, é Brasileira, com 24 (73%) respondentes informando esta opção.

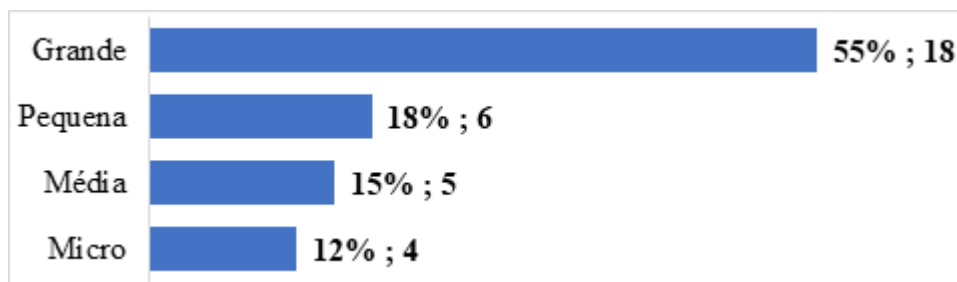
Figura 17: Nacionalidade das empresas.



Fonte: Resultado da pesquisa.

A identificação do tamanho das empresas em que os respondentes atuam é apresentada na Figura 18, e é possível evidenciar que 18 (55%) respondentes atuam em empresa de grande porte.

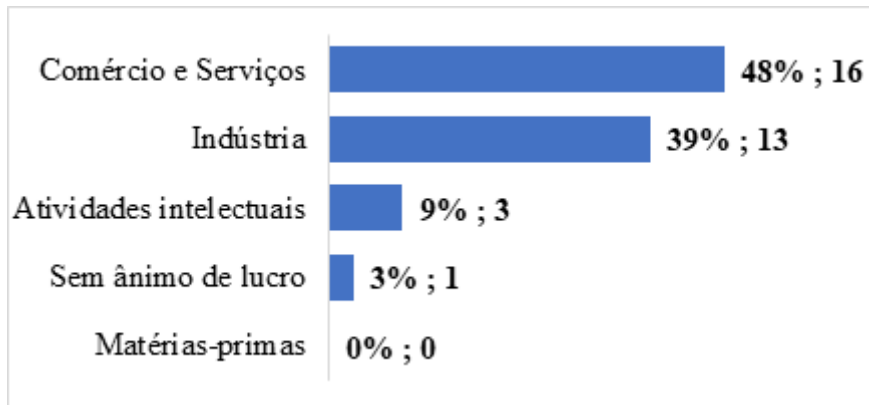
Figura 18: Tamanho das empresas.



Fonte: Resultado da pesquisa.

Sobre o setor econômico das empresas em que os respondentes atuam, identifica-se na Figura 19, que 16 (48%) respondentes informaram que suas empresas atuam no setor de comércio e serviços.

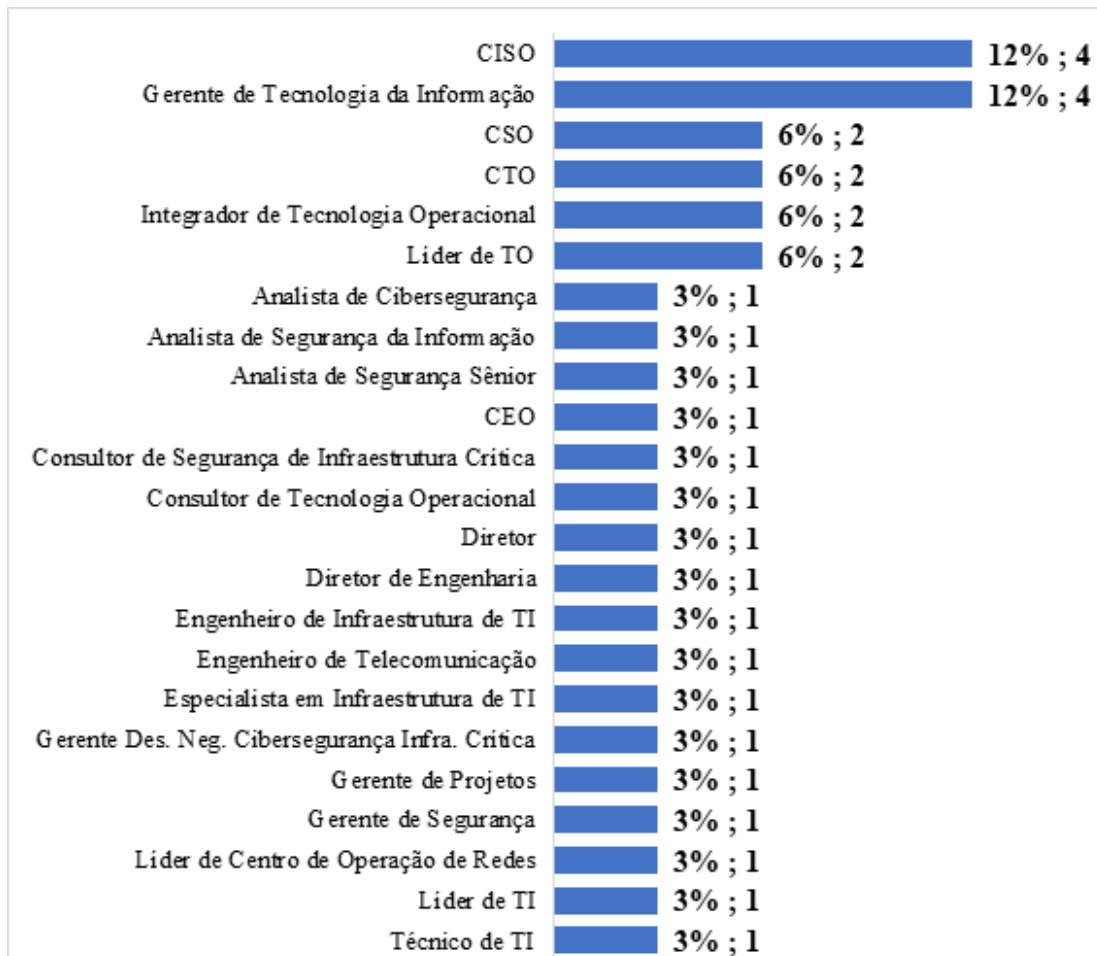
Figura 19: Setor econômico das empresas.



Fonte: Resultado da pesquisa.

A Figura 20 apresenta a função atual dos respondentes, onde é possível observar que 4 (12%) respondentes informaram que ocupam a função de CISO nas empresas onde atuam, e outros 4 (12%) respondentes informaram que exercem a função de Gerente de Tecnologia da Informação.

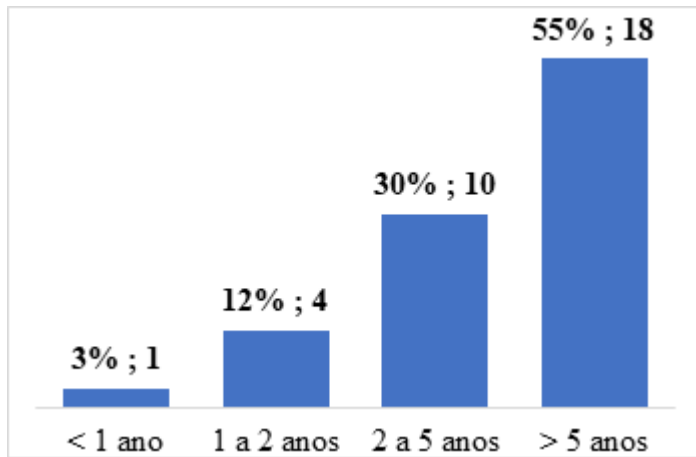
Figura 20: Função atual dos respondentes.



Fonte: Resultado da pesquisa.

Ao serem questionados sobre o tempo no cargo relatado, 18 (55%) respondentes informaram que ocupam o cargo a mais de 5 anos, conforme apresentado na Figura 21.

Figura 21: Tempo no cargo relatado pelos respondentes.

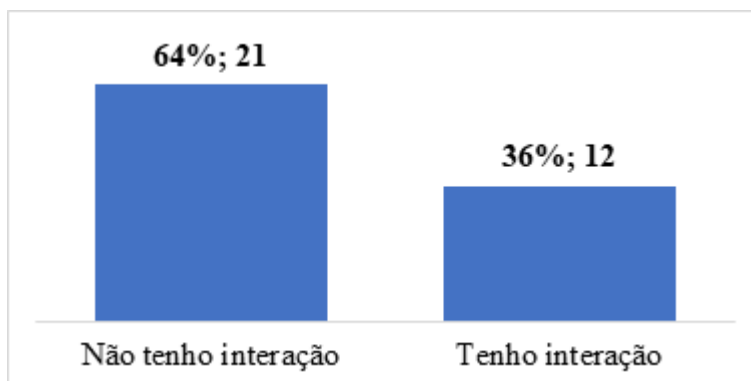


Fonte: Resultado da pesquisa.

#### 4.2.2. Caracterização das tecnologias de manufatura avançada

A Figura 22 evidencia que 21 (64%) respondentes não possuem interação com sensores e demais dispositivos de instrumentação industrial.

Figura 22: Interação pelos respondentes com sensores e demais dispositivos de instrumentação industrial.

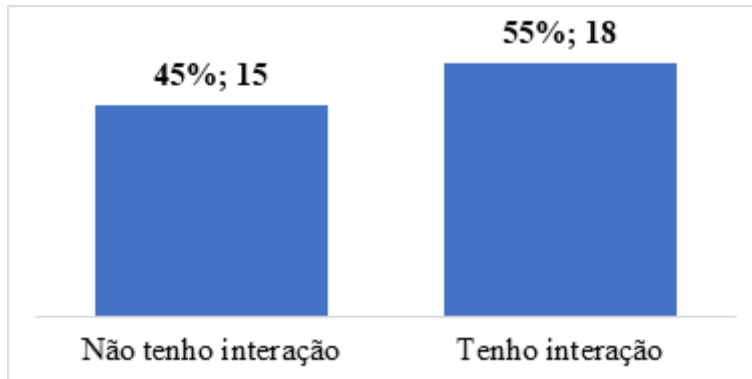


Fonte: Resultado da pesquisa.



Foram indicados por 18 (55%) respondentes, que possuem interação com sistemas de instrumentação de segurança, CLP e dispositivos controladores locais, conforme apresentado na Figura 23.

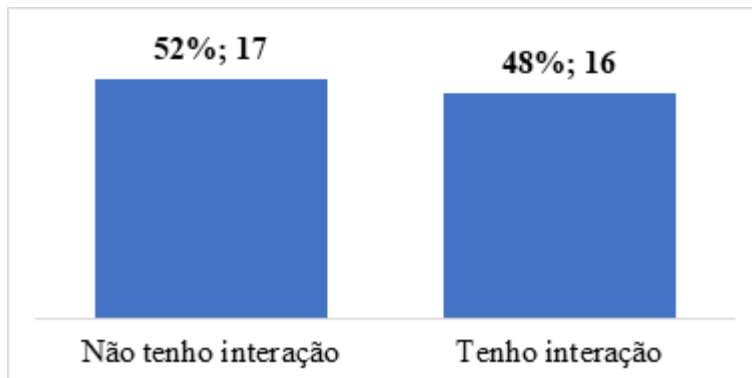
Figura 23: Interação pelos respondentes com sistemas de instrumentação de segurança, CLPs e dispositivos controladores locais.



Fonte: Resultado da pesquisa.

Com a Figura 24 é possível identificar que 17 (52%) respondentes informaram que não interagem com tecnologias IHM Local e sistemas supervisórios locais.

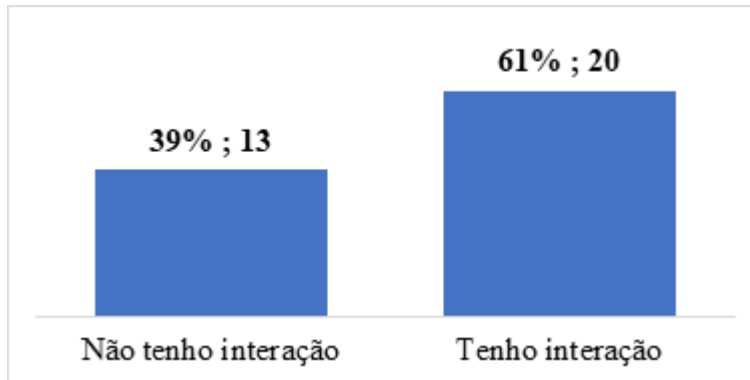
Figura 24: Interação dos respondentes com IHM local e sistemas supervisórios locais.



Fonte: Resultado da pesquisa.

A Figura 25 mostra que 20 (61%) respondentes interagem com o centro de controle de processo e sistema supervisório central, nas empresas em que atuam.

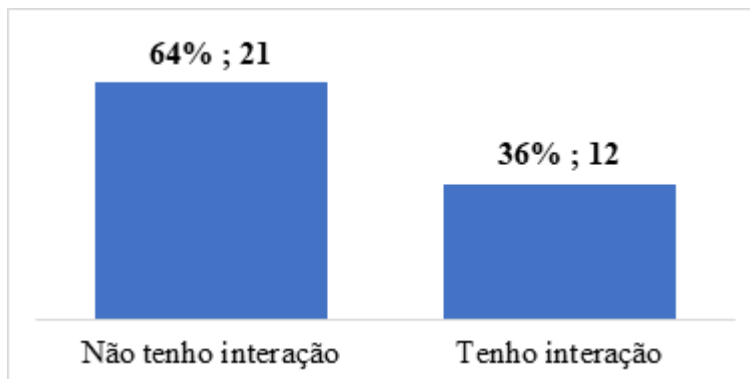
Figura 25: Interação pelos respondentes com centro de controle de processo e sistema supervisorio central.



Fonte: Resultado da pesquisa.

A Figura 26 representa o resultado da interação dos respondentes com sistemas MES e sistemas automatizados auxiliares à gestão de produção e logística, sendo possível verificar que 21 (64%) respondentes informaram que não interagem com estas tecnologias.

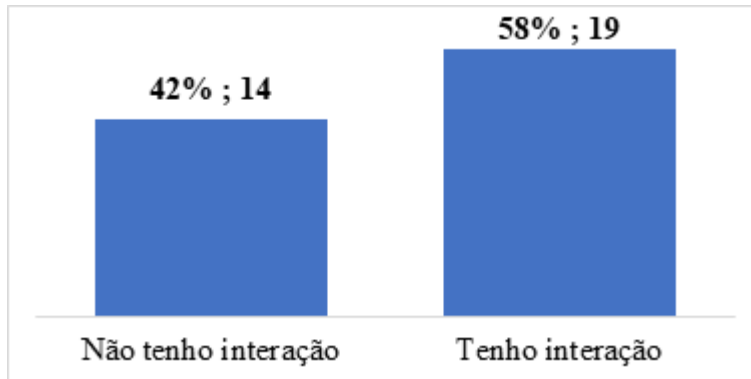
Figura 26: Interação pelos respondentes com MES, sistemas automatizados auxiliares à gestão de produção e logística.



Fonte: Resultado da pesquisa.

A Figura 27 representa o resultado da interação com sistemas ERP e sistema automatizados auxiliares para gestão estratégica de operações, onde que 19 (58%) respondentes informaram que interagem com estas tecnologias.

Figura 27: Interação pelos respondentes com ERP, sistemas automatizados auxiliares para gestão estratégica de operações.



Fonte: Resultado da pesquisa.

#### 4.2.3. Caracterização da gestão da segurança da informação

A Figura 28 apresenta a percepção dos especialistas participantes na pesquisa, sobre os impactos sobre a segurança da informação que estão correlacionados com a convergência das atividades de TI e TO, sendo possível evidenciar que 27 (27%) respondentes indicaram a necessidade de equipe multifuncional (TI e TO) dedicada para a gestão da segurança da informação.

Figura 28: Principais impactos à segurança da informação citados pelos respondentes devido a convergência de TI e TO.

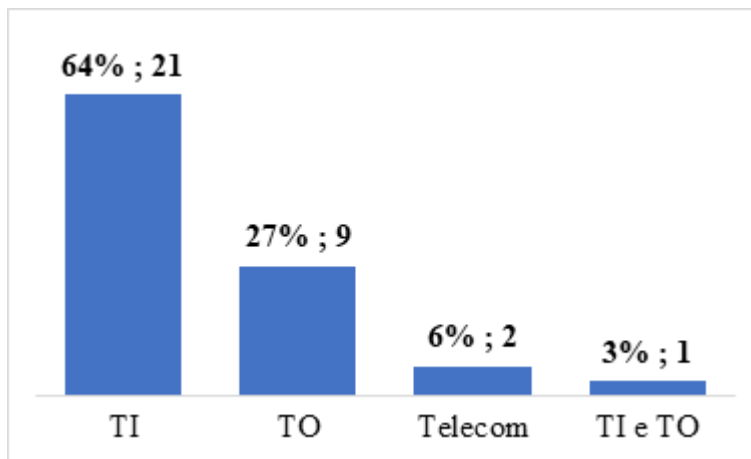


Fonte: Resultado da pesquisa.

#### 4.2.4. Caracterização da convergência de TI e TO pelos respondentes

Na Figura 29 evidencia-se que 21 (64%) respondentes se identificam como pertencentes ao departamento de TI. Também vale ressaltar que um dos respondentes se identificou como pertencente em ambos os departamentos (TI e TO).

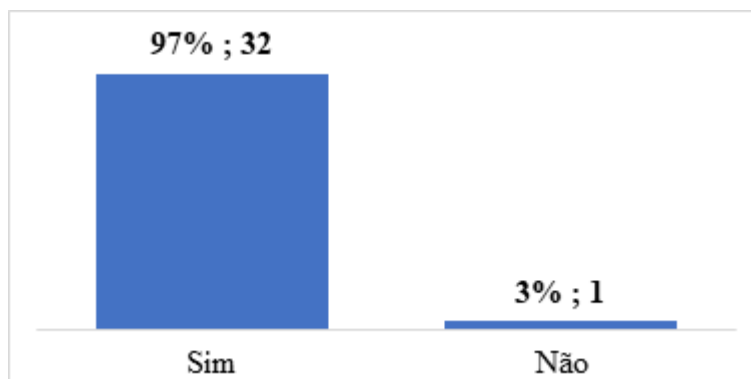
Figura 29: Área de atuação majoritária dos respondentes.



Fonte: Resultado da pesquisa.

A Figura 30 mostra a percepção dos especialistas sobre a necessidade da convergência das atividades de TI e de TO, e é possível verificar que 32 (97%) dos respondentes afirmam que sentem a necessidade da convergência.

Figura 30: Relato dos respondentes se sentem a necessidade da convergência das atividades de TI e de TO.



Fonte: Resultado da pesquisa.

Quanto às oportunidades relacionadas a convergência de TI e TO, como exibido na Figura 31, a segurança total da informação (que compreende as informações que transitam desde o chão de fábrica até as redes externas de comunicação) foi a oportunidade mais citada pelos participantes, com a quantidade de 28 (20%) citações.

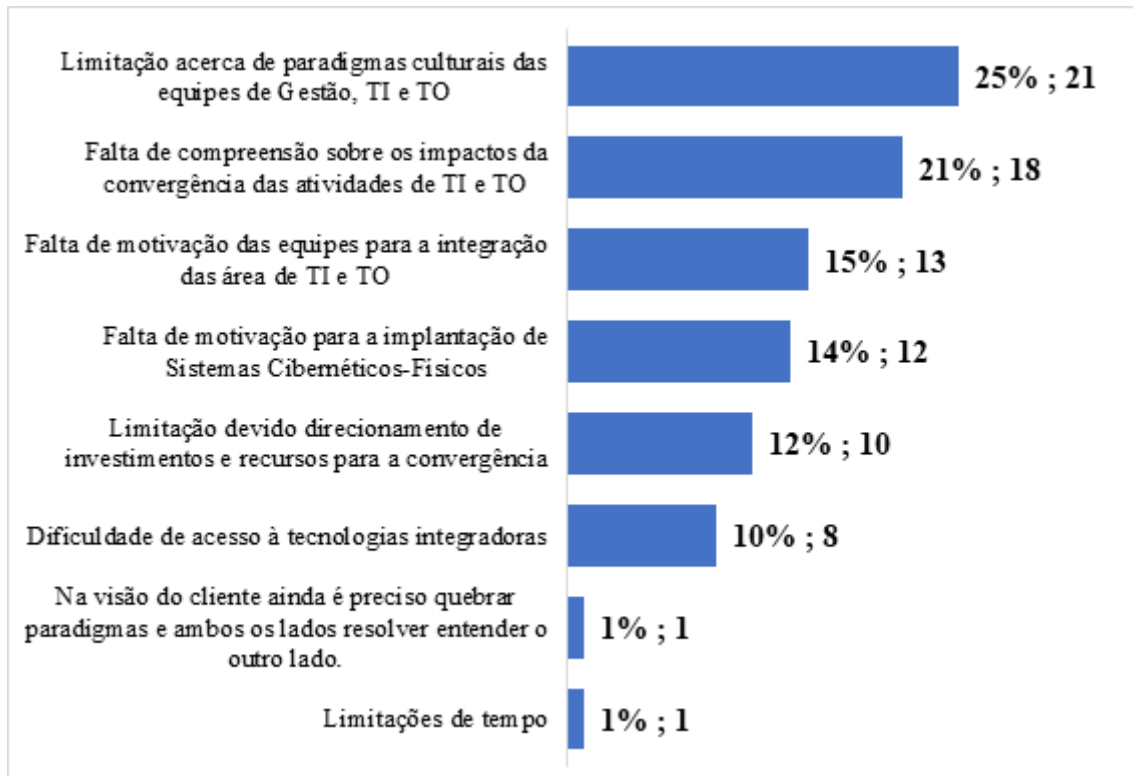
Figura 31: Principais oportunidades citadas pelos respondentes mediante a convergência de TI e TO.



Fonte: Resultado da pesquisa.

A principal limitação sobre a convergência das atividades de TI e de TO indicada pelos respondentes foi a limitação acerca de paradigmas culturais das equipes de gestão, da equipe de TI e da equipe de TO, onde a Figura 32 apresenta que 21 (25%) dos respondentes indicaram esta limitação.

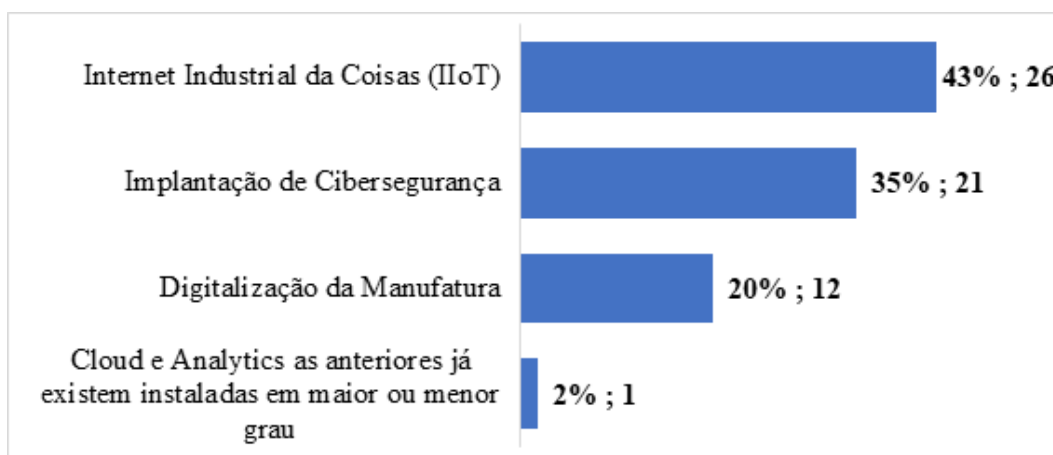
Figura 32: Principais limitações citadas pelos respondentes sobre a convergência de TI e TO.



Fonte: Resultado da pesquisa.

Quanto a tecnologia que mais oportuniza a convergência das áreas de TI e de TO, como indicado na Figura 33, foi a *Internet Industrial das Coisas*, com a citação realizada por 26 (43%) profissionais

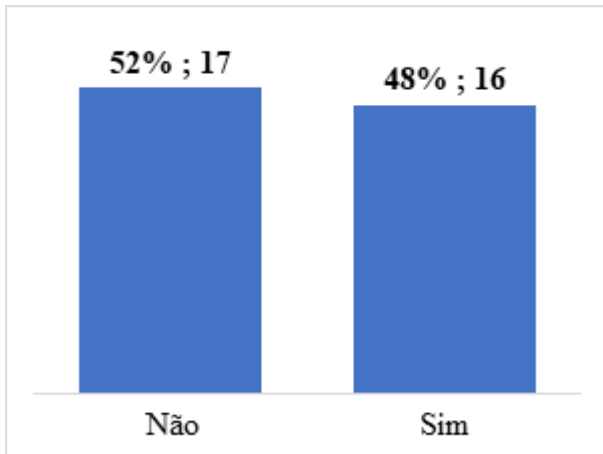
Figura 33: Tecnologias que oportunizam a convergência das áreas de TI e de TO citadas pelos respondentes.



Fonte: Resultado da pesquisa.

Sobre a declaração de disponibilidade de participação da entrevista semiestruturada diretamente com o pesquisador, 16 (48%) respondentes afirmaram que possuem disponibilidade de participação, como evidenciado na Figura 34.

Figura 34: Quantidade de respondentes que aceitam participar da etapa de entrevista da pesquisa.



Fonte: Resultado da pesquisa.

#### **4.3. Resultados obtidos com a entrevista semiestruturada**

Para garantir a confidencialidade solicitada pelos profissionais participantes, nesta pesquisa, estes são referenciados como Entrevistado, ocultando o gênero e utilizando números referentes a sequência das reuniões realizadas da entrevista semiestruturada.

##### *4.3.1. Achados sobre manufatura avançada na entrevista semiestruturada*

Sobre manufatura avançada foi identificado nas respostas dos 11 profissionais participantes, a citação por 8 entrevistados, os entrevistados 1, 2, 3, 4, 6, 7, 8 e 11, que já ouviram falar da integração de tecnologias associadas a manufatura avançada. O Entrevistado 2 comentou que não ouviu sobre este assunto dentro da antiga empresa em que trabalhava e que lá não havia tratativa para integração de tecnologias associadas a manufatura avançada. O Entrevistado 7 julga que nem a TI tem realizado este processo de integração a contento.

Os Entrevistados 3 e 11 citam que existia um movimento de integração de tecnologias associadas a manufatura avançada e Indústria 4.0 nas antigas empresas. O Entrevistado 8 cita que a empresa atual está buscando se adequar tecnologicamente para a manufatura avançada.

Nota-se a não uniformidade do entendimento sobre os conceitos, a tipificação, a caracterização e a exemplificação de tecnologias associadas a manufatura avançada, com base nos achados na entrevista semiestruturada. Como é apresentado nos parágrafos abaixo:

O Entrevistado 1 citou que não sabia informar se existia tecnologia inovadora implantada na atual empresa, porém na antiga empresa em que trabalhou havia robôs e células robotizadas implantadas.

O Entrevistado 2 deu exemplos de processos que se caracterizam como tecnologia, tais como processo de reaproveitamento dos resíduos gerados na antiga empresa em prol da sustentabilidade ambiental, uso de programa computacional para auxiliar a manutenção preditiva de máquinas do chão de fábrica, existência de tecnologia para redução do tempo de resfriamento do material fabricado e sistema implantado que contava com câmeras para inspeção visual em ambientes insalubres.

O Entrevistado 3 citou computação em nuvem, classificação de dados em prol de automatização de processos de robótica, inteligência artificial, geração automática de dashboards e o programa computacional Power BI.

Os exemplos dados pelo Entrevistado 4 foram a implantação de criptografia de dados, a integração de ERP, a existência de centro de controle redundante em nuvem, a computação em nuvem, a leitura e exibição de dados em tempo real, *virtual patching*.

Foi citado pelo Entrevistado 5, como tecnologias a fábrica digital, a digitalização de processos de fabricação, gêmeos digitais, subestações elétricas digitais, robôs industriais, tecnologia 5G. Vale salientar que o Entrevistado 5 cita que a indústria automotiva, mais especificamente suas linhas de montagem são exemplos de caracterização e implantação tecnológica industrial.

O Entrevistado 6 citou IoT e *machine learning*. Sobre *machine learning* o Entrevistado 7 ainda associa outras tecnologias citando o uso integrados de programas computacionais tais como Tensorflow, Grafana, Elasticsearch.

O Entrevistado 7 citou que no Brasil não há exemplos de tecnologia de ponta implantado a contento, em especialmente dentro da área de cibersegurança. Já o Entrevistado 8 comenta



que o Brasil não está tão atrasado com relação ao avanço tecnológico no setor químico, quando é comparado com o mesmo setor a Alemanha.

O Entrevistado 8 citou como exemplo de tecnologia implantado e em uso na atual empresa capacete com realidade aumentada e *tablets* com Wi-Fi para consulta de documentação. Julgou que IoT e IIoT trata-se de tecnologias que já não devem ser mais entendidas como disruptivas.

Para o Entrevistado 9 a computação em nuvem, inteligência artificial, e os programas computacionais inteligentes que proporcionam atendimento humanizado aos clientes, são exemplos de tecnologia.

A tecnologia citada pelo Entrevistado 10 foi *data mining*.

O Entrevistado 11 citou que nem o departamento de TI possui implantação de tecnologia de ponta ou consideradas disruptivas atualmente, mas citou como exemplo de tecnologias inovadoras a implantação de *threat intelligence* e *incident response* em prol da cibersegurança industrial.

Baseado nas observações de Romeo (2020), também foi questionada a percepção dos entrevistados quanto a vida útil dos equipamentos de suporte ao sistema informatizado do chão de fábrica.

O Entrevistado 1 citou que nota certo avanço quanto a atualização de *firmwares*, mesmo assim julga que alguns equipamentos computacionais presentes no chão de fábrica estão obsoletos de acordo com o que já evidenciou durante sua experiência profissional.

O Entrevistado 3 evidenciou equipamentos computacionais obsoletos presentes em empresas do setor elétrico, enquanto o Entrevistado 4 evidenciou equipamentos computacionais obsoletos presentes no chão de fábrica de uma mineradora.

O Entrevistado 5 comentou que a vida útil dos equipamentos computacionais segue as paradas programadas das plantas.

Os Entrevistados 6, 7, 8 e 11 apenas comentaram que já evidenciaram equipamentos computacionais obsoletos presentes no chão de fábrica das empresas que atuaram.

O Entrevistado 10 comentou que percebe que a TO não acompanha a evolução e a atualização tecnológica que a TI está acostumada a acompanhar.

#### 4.3.2. Achados sobre segurança da informação na entrevista semiestruturada

Quanto a responsabilidade de suporte à incidentes de segurança da informação nos ambientes característicos de TO, os Entrevistados 1 e 3 citaram que dentre de suas experiências o suporte à incidentes de segurança da informação de TO era de responsabilidade do departamento de TO. Os Entrevistados 2, 4 e 8 citaram que de acordo com suas experiências o suporte à incidentes de segurança da informação de TO era de responsabilidade do departamento de TI.

Os Entrevistado 6 e 10 comentaram que o suporte à incidentes de segurança da informação tem que ser de responsabilidade concomitantemente de TI e de TO.

Os Entrevistados 2, 6 e 7 citaram que não existia pessoa ou departamento dedicado para análise da segurança da informação de TO ou para a modelagem de ameaças de incidentes de segurança da informação de TO.

O Entrevistado 11 informou que na antiga empresa quem liderava a tratativa de incidentes de segurança da informação era o departamento de TI porque este tinha esse procedimento mais bem estruturado do que a TO. O Entrevistado 11 também comentou que existia analista de segurança da informação designado para TO.

Durante a execução das entrevistas foi possível identificar que não há o entendimento do conceito de *safety* de modo uniforme no ambiente de segurança da informação de TO, como tratado na ISA 62443-1-1 (2007) e por Timpson e Moradian (2018) e Preminger (2020).

O Entrevistado 4 acredita que somente exista SIS em empresas com maturidade elevada quanto a segurança da informação industrial. O Entrevistado 5 observa que há distância a ser vencida entre o reconhecimento da gravidade de incidentes de segurança da informação que afetam o *safety* e a implantação efetiva de SIS no chão de fábrica.

Também foi evidenciada a falta de clara compreensão por parte das empresas citadas pelos entrevistados, sobre os impactos ao *safety* na ocorrência de incidentes de segurança da informação em TO.

Para o Entrevistado 8 o *safety* e o *security* trata-se da mesma coisa, mudando apenas a relação: *security* é a causa possível de um evento de *safety*.

Nota-se no geral, que o atendimento do elemento *safety* se dá pela existência ou não de SIS, onde que os Entrevistados 1, 3, 8 e 11 informaram que existe SIS na atual empresa ou nas

empresas que têm contato, e os Entrevistados 4 e 8 informaram que não presenciaram até o momento SIS implantado em empresas que tiveram contato.

O Entrevistado 7 informou que nota que não existe SIS, nas empresas que tem contato, porque essa implantação fica sob responsabilidade do departamento de TI e TI não entende ainda a diferença dos conceitos de *safety* e *security*.

Quanto a separação e reconhecimento distinto dos departamentos de TI e de TO pelos participantes da entrevista semiestruturada, notou-se que no Brasil ainda não há entendimento consolidado sobre a segurança da informação para a área de TO de modo uniforme. Foram citadas 15 empresas que possuem a designação de atividades de TO, ou seja, possuem formalizado o departamento de TO ou a designação de ao menos um colaborador para tratar da segurança da informação da área de TO de modo separado do departamento de TI. Dos 11 entrevistados apenas 2 (Entrevistados 1 e 11) citaram que nas atuais empresas há separação dos departamentos de TI e TO. O Entrevistado 4 comentou que nas empresas que atualmente possui contato, nota-se a separação dos departamentos de TI e de TO.

#### *4.3.3. Achados sobre convergência de TI e TO na entrevista semiestruturada*

Sobre a convergência das atividades de TI e TO, foram questionadas as opiniões dos participantes quanto este serem à favor ou não a convergência, e na ocorrência da convergência dos departamentos quais seriam as oportunidades, desafios e limitações percebidas.

Os Entrevistados 1, 2 e 3 são a favor da convergência das atividades de TI e de TO.

O Entrevistado 11 não é a favor da convergência das atividades de TI e de TO, porém acredita que estes departamentos devem ser mais proativos em benefícios da segurança e dos demais interesses do negócio. Também comentou que na antiga empresa havia a integração das atividades de TI e de TO devido estes departamentos responderem à mesma gerência.

Os Entrevistados 4, 6 e 7 são a favor da convergência das atividades de TI e de TO, porém acreditam que esta não deve ser total. Para o Entrevistado 4 a segurança da informação não deve ser convergida, portanto deve ser tratada de modo separado. O Entrevistado 5 é a favor da convergência à partir da existência de conhecimento equalizado entre os colaboradores envolvidos. Os Entrevistado 8 e 10 são a favor da convergência das atividades de TI e de TO,

porém acreditam que deve haver estruturação organizacional para administração de departamentos convergidos e que não haja preferências características em benefício de um departamento ou de outro.

Muitas oportunidades foram indicadas pelos entrevistados, na ocasião da convergência das atividades de TI e de TO.

Segundo o Entrevistado 1 há oportunidade de melhoria do desempenho das duas áreas (TI e TO), em especial da área de TO, e melhoria da comunicação entre departamentos e colaboradores envolvidos.

Para o Entrevistado 2 poderá haver redução de custos, melhoria da utilização de recursos, diminuição de duplicação de aplicativos de mesma função, porém de fabricantes diferentes, possibilidade de realização rotineira de modelagem de ameaças à segurança da informação por meio da participação de uma equipe multidisciplinar e integrada.

Na visão do Entrevistado 3 o trabalho convergido dos profissionais de TI e de TO auxiliará na diminuição da complexidade dos processos e por consequência a maturação do negócio.

O Entrevistado 4 citou como oportunidades a economia de recursos, a diminuição da quantidade de departamentos, a simplificação de processos, o aumento do envolvimento dos colaboradores bem como o aumento da sensibilidade às “dores” do departamento convergido.

O Entrevistado 5 indica que a convergência oportunizará a criação de equipe multifuncional e assim haverá ganho cultural para a empresa e para os colaboradores envolvidos.

O Entrevistado 6 citou que haverá melhoria no processo de escolha de dispositivos tecnológicos para serem implantados na empresa à fim de evitar a escolha de dispositivos de mesma finalidade de fabricantes diferentes.

Uma oportunidade citada pelo Entrevistado 8 é de que o departamento de segurança da informação de TO desfrutaria dos investimentos destinados para a área de TI.

A criação de mais um nível de especialização profissional foi a oportunidade identificada pelo Entrevistado 9. E para o Entrevistado 10 há oportunidade de aumento da vantagem técnica de profissionais que possuem perfil multidisciplinar.

A mudança cultural de trabalho dos departamentos, bem como a mudança de prioridades de atividades são desafios preponderantes e que foram identificados pelos Entrevistados 1 e 7.

O Entrevistado 2 comentou que participou do início do processo de convergência de TI e de TO na antiga empresa e que na ocasião o que se mostrou um grande desafio foi a necessidade de convencer os colaboradores envolvidos a não terem medo de perderem o emprego mediante a convergência dos departamentos.

Para o Entrevistado 5 a superação do ego dos colaboradores envolvidos nos dois departamentos (TI e TO) é um elemento desafiador a convergência de TI e de TO.

O Entrevistado 7 viu como desafio a atualização de equipamentos computacionais obsoletos presentes no chão de fábrica e comentou que para ele é um fato os profissionais de TI e de TO terem atividades, prioridades e necessidades diferentes, o que proporciona um limitante e ao mesmo tempo um desafio à ser superado para efetividade da convergência das atividades destes departamentos.

Quando questionado sobre as possíveis limitações à convergência de TI e de TO, o Entrevistado 3 comentou sua percepção quanto a limitação. Para ele a limitação é definida a partir do que atualmente se conhece e portanto, assim que se começa a desenvolver atividades desconhecidas e novas, as limitações tendem a diminuir.

Para os Entrevistados 4 e 5, o orgulho e o preconceito por parte dos colaboradores envolvidos podem se mostrar como limitantes a convergência. Bonnetto *et al.* (2016) também comenta como limitação associada, que a introdução de um novo produto ou serviço pode induzir conflitos de interesses entre os colaboradores da empresa, devido a introdução de novas rotinas de trabalho e novas tecnologias.

O Entrevistado 9 citou como limitante a falta de mão de obra qualificada para trabalhar em um processo com atividades convergidas de TI e de TO.

A falta de recurso financeiro destinado para a convergência das atividades de TI e de TO é um limitante na opinião do Entrevistado 10.

#### 4.4. Discussão dos resultados obtidos

Frente aos dados coletados nesta pesquisa, nota-se que os resultados deste trabalho mapeiam as percepções de profissionais brasileiros com mais de 5 anos de experiência em cargos associados as atividades de segurança da informação. A maioria dos profissionais respondentes atuam em empresas brasileiras de grande porte e interagem com tecnologias características do ambiente de automação industrial e com tecnologias características das camadas de gestão estratégica das empresas.

Revisitando a pergunta orientadora desta pesquisa, “quais são os impactos da convergência das atividades de TI e de TO na segurança da informação em empresas com tecnologias de manufatura avançada?” é possível fundamentar como resposta, a identificação de impactos positivos (oportunidades), neutros (desafios) e negativos (limitantes). As oportunidades identificadas na revisão sistemática, no levantamento tipo *survey* e nas entrevistas foram apresentadas e discutidas respectivamente nas seções 4.1.1, 4.2.4 e 4.3.3. Os desafios foram apresentados e discutidos nas seções 4.2.4 e 4.3.3 e os limitantes foram apresentados e discutidos nas seções 4.1.2, 4.2.4 e 4.3.3.

Os profissionais indicaram que com a convergência das atividades de TI e de TO surgirão impactos à segurança da informação até então desconhecidos e assim sendo preveem a necessidade de criação de equipes multifuncionais para a gestão da segurança da informação em empresas com processos de manufatura avançada. Este fato é entendido como um desafio ao processo de convergência.

A maioria dos respondentes se identificaram como pertencentes ao departamento de TI e a maioria relatou que sente a necessidade da convergência das atividades de TI e de TO.

A oportunidade preponderantemente indicada, acerca da convergência das atividades de TI e de TO, foi a possibilidade de analisar a segurança da informação de modo holístico, tratando as informações que transitam nos dispositivos presentes no chão de fábrica até as redes externas de comunicação e armazenamento de dados.

A limitação mais significativa que foi identificada nesta pesquisa está associada aos paradigmas culturais das equipes de gestão, das equipes de TI e das equipes de TO. Os autores selecionados e os profissionais especialistas expuseram que o processo de convergência poderá sentir o impacto negativo associado as características e limitações culturais dos colaboradores envolvidos e que estes podem ser contrários a execução das atividades de convergência.

A tecnologia associada a manufatura avançada que demonstra a maior oportunidade, portanto, um elemento motivador para a implantação do processo de convergência das atividades de TI e TO, é a IIoT. Assim como a IoT, a IIoT também é uma tecnologia associada a RAMI 4.0.

O Quadro 13 apresenta, em resumo, os impactos positivos e negativos na segurança da informação decorrentes da convergência entre TI e TO identificados no levantamento *survey* e na análise de conteúdo das entrevistas realizadas.

Quadro 13: Impactos na segurança da informação decorrentes da convergência entre TI e TO.

| Impactos Positivos   |
|--|
| <p>Com a convergência de TI e TO, a priorização da disponibilidade (TO) e da confidencialidade (TI) é sobreposta pela segurança humana, da infraestrutura e do meio ambiente, pois os colaboradores reconhecem que na ocorrência de um incidente de segurança da informação em uma indústria pode causar impactos diretos à segurança humana.</p> <p>Este impacto foi identificado no <i>survey</i> e na análise de conteúdo e condiz com ISA (2007), Timpson e Moradian (2018), Romeo (2020), Ehrenreich (2020) e Preminger (2020).</p> |
| <p>A convergência de TI e TO oportuniza abordagem holística da segurança da informação nas indústrias, uma vez que une a experiência de profissionais que atuam com tecnologias implantadas, do chão de fábrica até ambientes externos à indústria.</p> <p>Este impacto foi identificado no <i>survey</i> e é suportado por Garvin (2015) e Kamal <i>et al.</i> (2016).</p>  |
| <p>Com a convergência dos departamentos de TI e TO, as tomadas de decisões estratégicas em prol da segurança da informação são mais assertivas, pois as demandas indicadas partem das necessidades evidenciadas em todas as camadas de automação.</p> <p>Este impacto positivo foi identificado no <i>survey</i> e na entrevista, porém não consta no material agrupado no referencial teórico.</p>  |
| <p>Os colaboradores que atuam no departamento convergido podem apresentar melhoria de desempenho em suas atividades e comunicações, pois a convergência estimula a proatividade e institui-se também equipe multidisciplinar para modelagem de ameaças a segurança da informação.</p> <p>Este impacto foi identificado na entrevista e não consta nos documentos do referencial teórico.</p>   |
| <p>A convergência das atividades de TI e de TO proporciona a redução de custos, pois a equipe enxuta de colaboradores tem cultura igualitária o que facilita as aquisições de tecnologias ligadas a segurança da informação.</p> <p>Identificado na análise de conteúdo, este impacto é suportado por Ehrenreich (2020) e Paes <i>et al.</i> (2020).</p>   |

(continuação)

| <b>Impactos Negativos</b>  |
|--|
| <p>O avanço da IIoT e da interoperabilidade dos dispositivos inteligentes estimulam a convergência de TI e de TO, em contrapartida, há um aumento da superfície de ataque. Este aumento da superfície de ataque é um impacto negativo identificado à segurança da informação em indústrias.</p> <p>Este impacto foi identificado no levantamento <i>survey</i> e tem coerência com as citações de Timpson e Moradian (2018), Ahmadian, Shajari e Shafiee (2020), Ehrenreich (2020) e Jelacic <i>et al.</i> (2020).</p> |
| <p>A limitação acerca de paradigmas culturais das equipes de Gestão, TI e TO, pode dificultar a convergência da atividade de TI e de TO e impactar negativamente o desenvolvimento das atividades associadas a segurança da informação em todos os níveis de automação.</p> <p>Este impacto foi identificado no levantamento <i>survey</i> e na análise de conteúdo e é citado por Kamal <i>et al.</i> (2016).</p>   |
| <p>A falta de compreensão sobre os impactos da convergência das atividades de TI e TO, pode afetar negativamente a gestão da segurança da informação na indústria, pois limita o planejamento de ações adequadas.</p> <p>Este impacto foi identificado na análise de conteúdo, porém não é citado pelos autores que constituem o referencial teórico desta pesquisa.</p>   |
| <p>A falta de motivação dos colaboradores pode impactar de modo negativo o processo de convergência das área de TI e TO, o que demanda habilidade de gestão de recursos humanos pelos gestores responsáveis pela convergência.</p> <p>Este impacto foi evidenciado no levantamento <i>survey</i> e citado na entrevista semiestruturada, porém não é citado nos documentos do referencial teórico.</p>   |
| <p>O orgulho e o preconceito, por parte dos colaboradores de TI e de TO, impacta negativamente o processo de convergência e o desenvolvimento de atividades associadas a segurança da informação.</p> <p>Este impacto foi identificado na análise de conteúdo das respostas obtidas por meio da entrevista, mas não há citação nos documentos do referencial teórico .</p>   |
| <p>A falta de mão de obra qualificada para trabalhar em um processo com atividades convergidas foi um impacto negativo identificado durante a análise das entrevistas com os especialistas. Atualmente são utilizados profissionais de TI para tratar de incidentes de segurança cibernética industrial.</p> <p>Foi citado este impacto na entrevista, porém não é suportado pelos documento que constituem o referencial teórico.</p>   |

Fonte: Resultado da pesquisa.



## 5. CONSIDERAÇÕES FINAIS

Este capítulo apresenta a síntese desta dissertação, as contribuições e a identificação de trabalhos futuros.

### 5.1. Síntese do trabalho

Esta dissertação teve como objetivo identificar e descrever e avaliar os impactos da convergência das atividades de TI e de TO na segurança da informação em empresas com tecnologias de manufatura avançada.

Para tanto, os seguintes objetivos específicos foram definidos: (1) identificar os impactos gerais da convergência das atividades de TI e de TO com o advento das tecnologias de manufatura avançada; (2) identificar os impactos na segurança da informação de empresas com manufatura avançada ao optar-se pela convergência das atividades de TI e de TO; e (3) relacionar os impactos identificados na ocorrência da convergência de TI e TO com os pilares da segurança da informação.

Os objetivos específicos foram alcançados por meio de realização de revisão sistemática da literatura, de um levantamento do tipo *survey* respondido por 33 profissionais especialistas da área de segurança da informação e da análise de conteúdo das respostas obtidas com entrevistas semiestruturadas que contou com a participação de 11 profissionais especialistas da área de segurança da informação. A coleta de dados foi realizada levando em consideração as citações dos autores de artigos científicos públicos e dos relatos das rotinas atuais e das experiências anteriores dos profissionais de segurança da informação que participaram do *survey* e das entrevistas. Os resultados obtidos com a metodologia proposta, permitiram avaliar o estado da convergência de TI e de TO em empresas que possuem processos de manufatura avançada implantados. Eles indicam que há uma parcela de profissionais que são a favor da convergência das atividades de TI e TO, mas defendem que esta convergência não deve ser total. Dentre os profissionais participantes houve o comentário que a segurança da informação de TO deve manter-se sob responsabilidade de profissional com conhecimentos de

cibersegurança industrial.

Como impacto positivo, aqui entendido como oportunidade, foi identificado nos resultados que com a convergência das atividades de TI e TO a prioridade já comum à área de TO, que se traduz em segurança humana, segurança da infraestrutura e do meio ambiente, passa a ser também da área de TI, onde até o momento é considerada a confidencialidade o elemento prioritário nas ações de segurança da informação.

Relacionado aos impactos negativos, nesta pesquisa entendido como limitantes, os resultados mostram que a aumento da interoperabilidade dos dispositivos inteligentes de TI e de TO, proveniente do avanço da IIoT, pode aumentar a superfície de ataque e a possibilidade de aumento de ameaças à segurança da informação.

Os resultados mostram que o paradigma cultural das equipes de TI e de TO podem apresentar-se como elemento dificultador do processo de convergência das atividades de TI e TO e que cabe atenção por parte dos responsáveis pela decisão de convergir os departamentos, deliberar a gestão estratégica das pessoas e de conflitos, de modo imparcial, para garantir o favorecimento de um departamento em detrimento do outro.

Os dados obtidos também indicam que atividades de segurança da informação da área de TO, como por exemplo a análise de incidentes, são direcionadas para colaboradores do departamento de TI. Observa-se que as empresas ainda não reconhecem ou não possuem o departamento de TO formalmente definido, e até mesmo não apresentam maturidade quando a ciência dos impactos de incidentes de segurança cibernética em TO.

Uma limitação do trabalho é a pequena quantidade de participantes no levantamento tipo *survey* e na entrevista semiestruturada. Isso reflete a falta de oportunidade ou de preocupação com a convergência das atividades de TI e de TO. Muitos profissionais apontaram que não há entendimento claro pelas empresas no Brasil sobre as atividades de TO, e que desta forma muitos profissionais de TI acabam interagindo com dispositivos industriais, porém, utilizando métodos característicos da área de TI corporativa, resultando na ocorrência de novos problemas à segurança cibernética industrial.

## **5.2. Contribuições para Sistemas Produtivos**

Os resultados deste trabalho podem servir de base para gestores de sistemas produtivos e demais partes interessadas que visam implantar o processo de convergência das atividades dos departamentos de TI e de TO em empresas que utilizam tecnologias associadas à manufatura avançada. Também pode servir para embasamento de planejamento de gestão de atividades de segurança cibernética industrial.

Os gestores podem utilizar os dados apresentados como um elemento para a tomada de decisão assertiva de aderirem ou não a convergência dos departamentos de TI e TO, podem reconhecer as limitações de autoridade e responsabilidade de seus colaboradores das áreas de TI e TO, podem planejar programas de treinamento mais adequados aos colaboradores das áreas de TI e TO, podem identificar, sob a perspectiva de cada uma das áreas (TI e TO), quais são os elementos importantes para verificar a concordância ou conflito de interesses nas gestões destes processos.

Ao ter a identificação dos impactos a segurança da informação, presentes nesta pesquisa, o mercado poderá utilizar estas informações para desenvolver soluções técnicas para diminuição das ameaças de segurança da informação e os gestores podem optar por estratégias administrativas que proporcionem a garantia da segurança da informação e planos de tratativas de incidentes, de modo que a segurança humana, a segurança da infraestrutura e a segurança do meio ambiente, sejam também garantidas.

## **5.3. Contribuições para a Academia**

Esta dissertação apresenta resultados obtidos por meio da aplicação de três métodos de pesquisa: revisão sistemática; levantamento tipo *survey*; e análise de conteúdo das respostas obtidas a partir de entrevistas semiestruturadas, descreveu e comparou, de modo quantitativo e qualitativo, o estado da convergência das atividades de TI e de TO em empresas com processos de manufatura avançada e seus impactos à segurança da informação.

Para a comunidade acadêmica, os resultados apresentados nesta dissertação subsidiam o direcionamento de pesquisas para diminuir as lacunas que porventura possam surgir com a

convergência das áreas de TI e TO, oportunizam o desenvolvimento de ferramentas e métodos para facilitar o processo de convergência das gestões de processos de TI e TO, e oportunizam o desenvolvimento de métodos de coleta de dados para avaliação da eficiência das equipes integradas de TI e TO.

#### 5.4. Trabalhos futuros

São ainda poucos os estudos que tratam da convergência das atividades de TI e TO em empresas com processos de manufatura avançada, indicando os impactos associados a atuação dos profissionais de TI e de TO. Além disso, poucos tratam dos benefícios obtidos com a convergência de TI e de TO. Assim, os seguintes trabalhos futuros são propostos para dar continuidade a esta pesquisa:

- Aplicação das ferramentas de *survey* e entrevista semiestrutura a mais profissionais especialistas em segurança cibernética industrial (TO);
- Realização de estudo dedicado aos conceitos e terminologia da área de TO, pois nota-se, a utilização não uniforme de termos e definições, como por exemplo, a referência da área de TO com os termos “tecnologia de automação (TA)”, “tecnologia de operações” e “tecnologia industrial”; a falta de entendimento do termo manufatura avançada, que durante a entrevista foi considerado por alguns profissionais como “infraestrutura crítica”; e a segurança da informação de TO que foi referenciado com o uso dos termos “cibersegurança”, “segurança cibernética”, “cibersegurança da informação”;
- Proposta de *roadmap* para convergência das atividades de TI e TO, considerando a segurança cibernética das informações, por todas as camadas do negócio e incluindo o ambiente externo de comunicação (fornecedores, clientes, entre outras partes interessadas);
- Avaliação do estado da convergência de TI e de TO e da segurança cibernética industrial “*in loco*”, isto é, nas organizações;
- Uso de outras técnicas estatísticas para identificar novos elementos associados a convergência de TI e de TO e confirmar as afirmações já obtidas neste estudo;
- Identificar na rotina dos profissionais de TI e de TO, quais camadas da automação industrial possuem a interação, a autoridade e a responsabilidade destes, buscando evidenciar a

atuação dos profissionais de TI em direção a camada operacional, e dos profissionais de TO em direção à camada de gestão estratégica das empresas. A criação de processos de implantação de convergência de TI e TO poderá ser beneficiada com esta identificação.

## REFERÊNCIAS

ADOLPHS, Peter *et al.* **DIN SPEC 91345: Reference Architecture Model Industrie 4.0 (RAMI4.0)**. Berlim: Deutsches Institut für Normung, 2016.

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL. **Indústria 4.0**. 2020. Disponível em: <<http://www.industria40.gov.br/>>. Acesso em: 2 nov. 2020.

AHMADIAN, Mohammad Mehdi; SHAJARI, Mehdi; SHAFIEE, Mohammad Ali. Industrial control system security taxonomic framework with application to a comprehensive incidents survey. **International Journal of Critical Infrastructure Protection**, v. 29, p. 1–22, 2020. Disponível em: <<https://doi.org/10.1016/j.ijcip.2020.100356>>. Acesso em: 2 nov. 2020.

ANDERL, Reiner. Industrie 4.0: fundamentals, scenarios for application and strategies for implementation. **Diálogo Brasil-Alemanha de Ciência, Pesquisa e Inovação**, São Paulo, v. 4, 2015. Disponível em: <[https://dwih.com.br/sites/default/files/imce\\_default/reiner\\_anderl.pdf](https://dwih.com.br/sites/default/files/imce_default/reiner_anderl.pdf)>. Acesso em: 2 jun. 2019.

ANI, Uchenna P. Daniel; HE, Hongmei; TIWARI, Ashutosh. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. **Journal of Cyber Security Technology**, v. 1, n. 1, p. 32–74, 2017. Disponível em: <<https://dx.doi.org/10.1080/23742917.2016.1252211>>. Acesso em: 2 nov. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000: Gestão de riscos - diretrizes**. Rio de Janeiro. 2018.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BONNETTO, Emilie *et al.* A categorization of customer concerns for an OT front-end of innovation process in IT/OT convergence context. In: PROCEEDINGS OF INTERNATIONAL DESIGN CONFERENCE 2016, Dubrovnik. **Anais...** Dubrovnik. 2016.

BRETON, Thierry. **The convergence of IT and Operational Technology**. Bezons. 2012.

BRYANT, Michael. **What is OPC?** 2020. Disponível em: <<https://opcfoundation.org/about/what-is-opc/>>. Acesso em: 3 nov. 2020.

BUTRIMAS, Vytutas. **Is there a problem with our understanding of the terms IT, OT and ICS when seeking to protect critical infrastructure?** 2020. Disponível em: <<http://scadamag.infracritical.com/index.php/2020/08/17/is-there-a-problem-with-our-understanding-of-the-terms-it-ot-and-ics-when-seeking-to-protect-critical-infrastructure/>>. Acesso em: 9 set. 2020.

CARE LAB. **CIRWA: Critical Infrastructure Ransomware Attacks**. 2020. Disponível em: <<https://sites.temple.edu/care/ci-rw-attacks/>>. Acesso em: 1 nov. 2020.

CAUCHICK-MIGUEL, Paulo Augusto *et al.* **Metodologia de pesquisa em engenharia de produção e gestão de operações**. 3. ed. Rio de Janeiro: Elsevier, 2018.

CULOT, Giovanna *et al.* Behind the definition of Industry 4.0: Analysis and open questions. **International Journal of Production Economics**, v. 226, n. January, p. 107617, 2020. Disponível em: <<https://doi.org/10.1016/j.ijpe.2020.107617>>. Acesso em: 2 nov. 2020.

DA SILVA, Elias Ribeiro *et al.* Operating digital manufacturing in industry 4.0: the role of advanced manufacturing technologies. **Procedia CIRP**, v. 93, p. 174–179, 2020. Disponível em: <<https://doi.org/10.1016/j.procir.2020.04.063>>. Acesso em: 2 nov. 2020.

DA SILVA, Vander Luiz; KOVALESKI, João Luiz; PAGANI, Regina Negri. Technology transfer in the supply chain oriented to industry 4.0: a literature review. **Technology Analysis and Strategic Management**, v. 31, n. 5, p. 546–562, 2019. Disponível em: <<https://doi.org/10.1080/09537325.2018.1524135>>. Acesso em: 2 nov. 2020.

DIETZ, Marietheres; PERNUL, Gunther. Unleashing the Digital Twin's Potential for ICS Security. **IEEE Security & Privacy**, v. 18, n. 4, p. 20–27, 2020. Disponível em: <<https://ieeexplore.ieee.org/document/8966454/>>. Acesso em: 2 nov. 2020.

DYBÅ, Tore; DINGSØYR, Torgeir. Empirical studies of agile software development: A systematic review. **Information and Software Technology**, v. 50, n. 9–10, p. 833–859, 2008. Disponível em: <<https://linkinghub.elsevier.com/retrieve/pii/S0950584908000256>>. Acesso em: 2 nov. 2020.

EHIE, Ike C.; CHILTON, Michael A. Understanding the influence of IT/OT convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: an empirical investigation. **Computers in Industry**, v. 115, p. 103166, 2020. Disponível em: <<https://doi.org/10.1016/j.compind.2019.103166>>. Acesso em: 02 nov. 2020.

EHRENREICH, Daniel. **ICS-OT Security is not a one-size-fits-all system**. 2020. Disponível em: <<https://cyberstartupobservatory.com/ics-ot-security-is-not-a-one-size-fits-all-system/>>. Acesso em: 2 fev. 2021.

EUROPEAN COMMISSION. **National initiatives for digitising industry across the EU**. Bruxelas. 2017.

FABRO, Mark; GORSKI, Ed; SPIERS, Nancy. **Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies**. Washington. 2016.

FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND ENERGY. **What is Industrie 4.0?** 2019. Disponível em: <<http://www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html>>. Acesso em: 20 jul. 2019.

FERNANDEZ-CARAMES, Tiago M.; FRAGA-LAMAS, Paula. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. **IEEE Access**, v. 7, p. 45201–45218, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8678753/>>. Acesso em: 2 nov. 2020.

FORZA, Cipriano. Survey research in operations management: a process-based perspective. **International Journal of Operations & Production Management**, v. 22, n. 2, p. 152–194, 2002. Disponível em: <<https://www.emerald.com/insight/content/doi/10.1108/01443570210414310/full/html>>. Acesso em: 2 nov. 2020.

FRAGA-LAMAS, Paula *et al.* A Review on Internet of Things for Defense and Public Safety. **Sensors (Basel, Switzerland)**, v. 16, n. 10, p. 1–44, 2016.

FRANK, Alejandro Germán; DALENOGARE, Lucas Santos; AYALA, Néstor Fabián. Industry 4.0 technologies: Implementation patterns in manufacturing companies. **International Journal of Production Economics**, v. 210, n. September 2018, p. 15–26, 2019. Disponível em: <<https://doi.org/10.1016/j.ijpe.2019.01.004>>. Acesso em: 2 nov. 2020.

GARTNER. **Tecnologia operacional**. 2020. Disponível em: <<https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>>. Acesso em: 19 ago. 2020.

GARVIN, Thomas. IT and OT Convergence, or Collision? Managing the Merger for Greenfield LNG. In: ABU DHABI INTERNATIONAL PETROLEUM EXHIBITION AND CONFERENCE 2015, **Anais...** : Society of Petroleum Engineers, 2015. Disponível em: <<http://www.onepetro.org/doi/10.2118/177443-MS>>. Acesso em: 2 nov. 2020.

GIVEHCHI, Omid *et al.* Interoperability for industrial cyber-physical systems: an approach for legacy systems. **IEEE Transactions on Industrial Informatics**, v. 13, n. 6, p. 3370–3378, 2017. Disponível em: <<http://ieeexplore.ieee.org/document/8012471/>>. Acesso em: 2 nov. 2020.

GOMES, Bruno; COELHO, Carlos de Mello Rodrigues. **Panorama da Inovação: Indústria 4.0**. Rio de Janeiro. 2016.

GONÇALVES, João Emilio Padovani. Indústria 4.0: novo desafio para a indústria brasileira. **Indicadores CNI**, Brasília, v. 17, n. 2, p. 13, 2016.

GONCHAROV, Evgeny. **Kaspersky ICS CERT: Threat landscape for industrial automation systems H1 2020**. Moscou. Disponível em: <<https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/>>. Acesso em: 16 fev. 2021.

GUPTA, Sushil; VERMA, Rohit; VICTORINO, Liana. Empirical research published in production and operations management (1992-2005): trends and future research directions. **Production and Operations Management**, v. 15, n. 3, p. 432–448, 2006.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 1722: IEEE Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks**. Nova Jersey. 2016. Disponível em: <<https://standards.ieee.org/standard/1722-2016.html>>. Acesso em: 3 nov. 2020.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC TR 62541-1: OPC unified architecture - Part 1: overview and concepts**. Genebra. 2016a. Disponível em: <[https://webstore.iec.ch/preview/info\\_iec62541-1%7Bed2.0%7Den.pdf](https://webstore.iec.ch/preview/info_iec62541-1%7Bed2.0%7Den.pdf)>. Acesso em: 3 nov. 2020.



INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC TR 62541-2: OPC unified architecture - Part 2: security model**. Genebra. 2016b. Disponível em: <[https://webstore.iec.ch/preview/info\\_iec62541-2%7Bed2.0%7Den.pdf](https://webstore.iec.ch/preview/info_iec62541-2%7Bed2.0%7Den.pdf)>. Acesso em: 3 nov. 2020.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 62264-3: Enterprise control system integration - Part 3: Activity models of manufacturing operations management**. Genebra. 2016c. Disponível em: <<https://www.iso.org/obp/ui/#iso:std:iec:62264:-3:ed-2:v1:en>>. Acesso em: 3 nov. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27019: Information technology - Security techniques: information security controls for the energy utility industry**. Genebra. 2017. Disponível em: <<https://www.iso.org/obp/ui/#iso:std:iso-iec:27019:ed-1:v2:en>>. Acesso em: 3 nov. 2020.

INTERNATIONAL SOCIETY OF AUTOMATION. **ISA 62443-1-1: terminology, concepts, and models**. Carolina do Norte. 2007.

INTERNATIONAL SOCIETY OF AUTOMATION. **The 62443 series of standards: industrial automation and control systems security**. Carolina do Norte. 2015. Disponível em: <<http://isa99.isa.org>>. Acesso em: 3 nov. 2020.

JELACIC, Bojan *et al.* Security risk assessment-based cloud migration methodology for smart grid OT services. **Acta Polytechnica Hungarica**, Novi Sad, Serbia, v. 17, n. 5, p. 113–134, 2020.

KAMAL, S. Z. *et al.* IT and OT Convergence - Opportunities and Challenges. In: SPE INTELLIGENT ENERGY INTERNATIONAL CONFERENCE AND EXHIBITION 2016, **Anais...** : Society of Petroleum Engineers, 2016. Disponível em: <<http://www.onepetro.org/doi/10.2118/181087-MS>>. Acesso em: 3 nov. 2020

KANAZAWA, Akira; SAKITA, Tomohiro. Yokogawa's Approach to IT/OT Convergence for Successful Digital Transformation. **Yokogawa Technical Report**, Tóquio, v. 62, n. 2, p. 57–60, 2019. Disponível em: <<https://web-material3.yokogawa.com/1/29090/files/rd-te-r06202-001.pdf>>. Acesso em: 27 jul. 2020.

LARSON, Ron; FARBER, Betsy. **Estatística aplicada**. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

LIKERT, Rensis. **A technique for the measurement of attitudes**. Nova Iorque. Disponível em: <[https://legacy.voteview.com/pdf/Likert\\_1932.pdf](https://legacy.voteview.com/pdf/Likert_1932.pdf)>. Acesso em: 2 jun. 2019.

MABKHOT, Mohammed *et al.* Requirements of the smart factory system: a survey and perspective. **Machines**, v. 6, n. 2, p. 23, 2018. Disponível em: <<http://www.mdpi.com/2075-1702/6/2/23>>. Acesso em: 3 nov. 2020

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARTINS, Claudia Garrido; LUIZ, Miguel; FERREIRA, Ribeiro. O survey como tipo de pesquisa aplicado na descrição do conhecimento do processo de gerenciamento de riscos em projetos no segmento da construção. In: VII CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO 2011, Rio de Janeiro. **Anais...** Rio de Janeiro, 2011.

MCKINSEY GLOBAL INSTITUTE. **Ops 4.0: Fueling the next 20 percent productivity rise with digital analytics**. 2017. Disponível em: <<https://www.mckinsey.com/business-functions/operations/our-insights/ops-4-0-fueling-the-next-20-percent-productivity-rise-with-digital-analytics#>>. Acesso em: 2 nov. 2020.

MENZE, Thomas. **The state of industrial cybersecurity in the era of digitalization**. Dusseldorf. 2020. Disponível em: <[https://ics.kaspersky.com/media/Kaspersky\\_ARC\\_ICS-2020-Trend-Report.pdf](https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf)>. Acesso em: 16 fev. 2021.

MERRIAM-WEBSTER. **Tecnologia da informação**. 2020. Disponível em: <[https://www.merriam-webster.com/dictionary/information technology#h1](https://www.merriam-webster.com/dictionary/information%20technology#h1)>. Acesso em: 19 ago. 2020.

MOHER, David *et al.* Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. **Systematic Reviews**, v. 4, n. 1, p. 1, 2015. Disponível em: <<https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/2046-4053-4-1>>. Acesso em: 2 nov. 2020.

NOLTING, Lars *et al.* Generating Transparency in the Worldwide Use of the Terminology Industry 4.0. **Applied Sciences**, v. 9, n. 21, p. 4659, 2019. Disponível em: <<https://www.mdpi.com/2076-3417/9/21/4659>>. Acesso em: 2 nov. 2020.

OLIVEIRA, Giovana Fadini de. **Indeterminação temporal e dados temporais em narrativas e textos clínicos: uma revisão sistemática da literatura**. 2018. Centro Estadual de Educação Tecnológica Paula Souza, 2018. Disponível em: <<https://www.cps.sp.gov.br/pos-graduacao/wp-content/uploads/sites/4/2018/12/Dissertação-Giovana-Fadini-Sistemas-ProdutivosI.pdf>>. Acesso em: 2 nov. 2020.

PAES, Richard *et al.* A guide to securing industrial control networks: integrating IT and OT systems. **IEEE Industry Applications Magazine**, v. 26, n. 2, p. 47–53, 2020. Disponível em: <<https://ieeexplore.ieee.org/document/8938806/>>. Acesso em: 2 nov. 2020.

PAULSEN, Celia. The Future of IT Operational Technology Supply Chains. **IEEE Computer Society**, v. 53, n. 1, p. 30–36, 2020. Disponível em: <<https://ieeexplore.ieee.org/document/8960936/>>. Acesso em: 2 nov. 2020.

PEDRIALI, Diogo; ARIMA, Carlos Hideo. **Segurança da informação para a Indústria 4.0: levantamento de lacunas de pesquisa**. São Paulo: Pós-Graduação e Pesquisa do Centro Paula Souza, 2019.

PREMINGER, Amir. **The critical convergence of IT and OT security in a global crisis weathering a perfect storm and preparing for a post-pandemic future**. Nova Iorque. 2020.

RIBEIRO, Artur Tavares Vilas Boas; PLONSKI, Guilherme Ary. A matriz de amarração de Mazzon em um contexto de validação de empresas nascentes de base tecnológica. **III EMPRAD**, p. 15, 2016. Disponível em: <<https://www.researchgate.net/publication/312301337>>. Acesso em: 4 nov. 2020.

RISI. **The Repository of Industrial Security Incidents**. 2015. Disponível em: <[https://www.risidata.com/Database/event\\_date/asc](https://www.risidata.com/Database/event_date/asc)>. Acesso em: 1 nov. 2020.

ROMEO, Jim. You've Been Hacked: Words We Hope to Never Hear. **Plastics Engineering**, v. 76, n. 1, p. 26–33, 2020. Disponível em: <<https://onlinelibrary.wiley.com/doi/abs/10.1002/peng.20237>>. Acesso em: 2 nov. 2020.

ROMETTY, Ginni. **The OT Security imperative: what is your strategy?** IBM Security. Nova Iorque. 2019

SAFIRE, William. **The Farewell Dossier**. 2004. Disponível em: <<https://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html>>. Acesso em: 1 nov. 2020.

SILVA, Andressa Hennig *et al.* Análise de conteúdo: fazemos o que dizemos? um levantamento de estudos que dizem adotar a técnica. **Conhecimento Interativo**, v. 11, n. 1, p. 168–184, 2017.

SNOW, John. **Os ciberataques mais famosos dos últimos tempos**. 2018. Disponível em: <<https://www.kaspersky.com.br/blog/five-most-notorious-cyberattacks/11042/>>. Acesso em: 16 fev. 2021.

SUNDARAM, Arvind; ABDEL-KHALIK, Hany S.; ASHY, Oussama. A data analytical approach for assessing the efficacy of Operational Technology active defenses against insider threats. **Progress in Nuclear Energy**, v. 124, p. 103339, 2020. Disponível em: <<https://linkinghub.elsevier.com/retrieve/pii/S0149197020300950>>. Acesso em: 2 nov. 2020.

TELLES, Renato. A efetividade da matriz de amarração de Mazzon nas pesquisas em Administração. **Revista de Administração**, v. 36, n. 4, p. 64–72, 2001. Disponível em: <<http://200.232.30.99/download.asp?file=v36n4p64ap72.pdf>>. Acesso em: 2 nov. 2020.

TI SAFE. **Incident Hub: banco de dados de incidentes de segurança cibernética industrial**. 2020. Disponível em: <<https://hub.tisafe.com/>>. Acesso em: 1 nov. 2020.

TIAN, Shuo; HU, Yihong. The role of OPC UA TSN in IT and OT convergence. In: 2019 CHINESE AUTOMATION CONGRESS (CAC) 2019, **Anais...** : IEEE, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8996645/>>. Acesso em: 2 nov. 2020.

TIMPSON, Dominic; MORADIAN, Esmiralda. A Methodology to Enhance Industrial Control System Security. **Procedia Computer Science**, v. 126, p. 2117–2126, 2018. Disponível em: <<https://linkinghub.elsevier.com/retrieve/pii/S187705091831216X>>. Acesso em: 2 nov. 2020.

VERGARA, Sylvia Constant. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005. Disponível em: <<https://madmunifacs.files.wordpress.com/2016/08/vergara-mc3a9todos-de-pesquisa-em-administrac3a7ao-sylvia-vergara.pdf>>. Acesso em: 4 nov. 2020.

VITALLI, Rogério. **Os 10 pilares da Indústria 4.0**. 2018. Disponível em: <<https://www.industria40.ind.br/artigo/16751-os-10-pilares-de-industria-40>>. Acesso em: 2 nov. 2020.

WALES, Brandon D. **Securing industrial control systems: a unified initiative FY 2019-2023**. Washington. 2019. Disponível em: <<https://www.cisa.gov/national-critical-functions-overview>>. Acesso em: 21 jul. 2020.

WALES, Brandon D. **Critical Infrastructure Sectors**. Washington. 2020. Disponível em: <<https://www.cisa.gov/critical-infrastructure-sectors>>. Acesso em: 2 nov. 2020.

WATSON, Venesa *et al.* Interoperability and security challenges of industry 4.0. **INFORMATIK 2017**, p. 973–985, 2017.

WORLD ECONOMIC FORUM. **Industrial Internet of Things Safety and Security Protocol**. Genebra. 2018.

## APÊNDICE A: Instrumento do *survey*

### A.1. Matriz de amarração para o desenvolvimento do instrumento de levantamento tipo *survey*.

Quadro 14: Relação entre objetivos, fundamentação, pontos de investigação e resultados esperados.

| Objetivo geral do estudo   | Objetivos específicos do estudo   | Fundamentação teórica   | Pontos de investigação  | Resultados esperados  |
|--|---|---|---|---|
| O objetivo geral deste estudo consiste em identificar, descrever e avaliar os impactos da convergência das atividades de TI e TO na segurança da informação de empresas com manufatura avançada, pela perspectiva dos profissionais especialistas das áreas de TI e de TO. | <p>OE 1 - Identificar as interações dos especialistas entre os departamentos de TI e TO na execução das atividades de rotina.</p> <p>OE 2 - Identificar as opiniões dos profissionais quanto as oportunidades, desafios e limitantes da convergência de TI e TO face ao advento da manufatura avançada.</p> <p>OE 3 - Identificar as opiniões dos profissionais de TO sobre os impactos na segurança da informação na ocasião da convergência de TI e TO para a manufatura avançada.</p> <p>OE 4 - Identificar como atualmente está sendo tratada a segurança da informação pelos profissionais de TI e TO em empresas com manufatura avançada.</p> <p>OE 5 - Identificar as opiniões dos profissionais de TO sobre quais tecnologias seriam facilitadoras a convergência de TI e TO.</p> | <p>Interoperabilidade e integração de processos ocasionada pela plataforma Indústria 4.0.</p> <p>Cibersegurança como pilar da manufatura avançada.</p> <p>Aumento da importância dos dados (ativo digital) com o desenvolvimento das tecnologias associadas a manufatura avançada.</p> <p>Aumento dos ataques às informações industriais com a interoperabilidade dos dispositivos e <i>softwares</i> presentes também nos processos de manufatura avançada.</p> <p>Tendência de integração e convergência das atividades de departamentos que possuem atividades correlatas, tais como TI e TO para “fazer mais, com menos”.</p> | <p>PI 1 – Quais as camadas hierárquicas de tecnologia da automação industrial que estão caracterizadas as interações dos profissionais de TI e de TO?</p> <p>PI 2 – Qual o grau de adesão dos profissionais a convergência de TI e TO em empresas com manufatura avançada no Brasil?</p> <p>PI 3 – Quais as oportunidades acerca da convergência de TI e TO em empresas com manufatura avançada no Brasil, na visão dos profissionais?</p> <p>PI 4 - Quais os limitantes acerca da convergência de TI e TO em empresas com manufatura avançada no Brasil, na visão dos profissionais?</p> | <p>Identificar o panorama da segurança da informação no Brasil.</p> <p>Identificar o panorama da manufatura avançada no Brasil.</p> <p>Identificar como está sendo tratada a segurança da informação em empresas que investem em tecnologia de processos.</p> <p>Identificar as opiniões dos profissionais de TI e TO sobre a convergência das áreas frente aos paradigmas da I4.0.</p> |

Fonte: o autor.

## A.2. Instrumento do *survey*.

Quadro 15: Instrumento aplicado aos profissionais das áreas de TI e de TO.

| <b>Categorização</b>                      | <b>Pergunta</b>  | <b>Alternativas de Resposta</b>  | <b>Objetivos Específicos</b> |
|---|--|--|------------------------------|
| <b>Perfil Sociodemográfico da Amostra</b> | PSD 1 - Qual sua nacionalidade?  | Brasileira / Outra   | OE 1                         |
|   | PSD 2 - Qual sua formação acadêmica?   | Análise de Sistemas / Engenharia de Computação / Engenharia de Automação / Engenharia Elétrica / Outra   | OE 1                         |
|   | PSD 3 - Qual a nacionalidade da empresa onde você trabalha?  | Brasileira / Americana / Alemã / Outra   | OE 1                         |
|   | PSD 4 - Qual o tamanho da empresa?   | Micro (até 19 empregados) / Pequena (de 20 a 99 empregados) / Média (de 100 a 499 empregados) / Grande (mais de 500 empregados)  | OE 1                         |
|   | PSD 5 - Qual o setor econômico que melhor classifica a empresa onde você trabalha?                               | Setor primário: matérias-primas. / Setor secundário: indústria. / Setor terciário: comércio e serviços. / Setor quaternário: atividades intelectuais. / Setor quinquário: sem ânimo de lucro.  | OE 1                         |
|   | PSD 6 - Qual sua atual função?   | CISO (Chief Information Security Officer) / CSO (Chief Security Officer) / Gerente de Tecnologia Operacional / Gerente de Tecnologia da Informação / Gerente de Segurança da Informação / Líder de Tecnologia da Informação / Líder de Tecnologia Operacional / Integrador de Tecnologia Operacional / Consultor de Tecnologia Operacional / Outro | OE 1                         |
|   | PSD 7 - Há quantos anos exerce esta função?  | Há menos de 1 ano / De 1 ano a 2 anos / De 2 anos a 5 anos / Há mais de 5 anos   | OE 1                         |
| <b>Constructo: Manufatura Avançada</b>    | MA 1 - Indique quais grupos de tecnologias de automação industrial você interage na execução de suas atividades: | Sensores e demais dispositivos de instrumentação industrial - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |
|   |  | Sistemas de instrumentação de segurança, CLPs e dispositivos controladores locais - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |
|   |  | IHM Local e Sistemas supervisórios locais - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |
|   |  | Centro de Controle de Processo e Sistema supervisório central - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |
|   |  | MES, Sistemas automatizados auxiliares à Gestão de Produção e Logística - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |
|   |  | ERP, Sistemas automatizados auxiliares para Gestão Estratégica de Operações - Tenho Interação / Não tenho interação  | OE 1 a OE5                   |

(continuação)

|  |   |  |                |
|--|---|--|----------------|
| <b>Constructo:<br/>Segurança da<br/>Informação</b> | CV 1 - Você é majoritariamente de Tecnologia Operacional (TO) ou de Tecnologia da Informação (TI)?                                  | TO / TI  | OE 1           |
|  | CV 2 - Você sente a necessidade da convergência das atividades de TI e de TO?   | Sim / Não  | OE 1 e<br>OE 2 |
|  | CV 3 - Na sua opinião, quais seriam as Oportunidades para a sua empresa, na ocasião da convergência de TI e TO?                     | Possibilidade de interoperabilidade de tecnologias / Concordância com formatos de troca de dados (sintaxe e semântica) / Segurança total da informação (desde o chão de fábrica até as redes externas de comunicação) / Melhor entendimento das demandas dos usuários do processo produtivo / Digitalização precisa da manufatura / Criação de novas informações (conhecimento) / Aumento da precisão na tomada de decisões / Outros                             | OE 2 e<br>OE 5 |
|  | CV 4 - Na sua opinião, quais seriam as Limitações para a sua empresa, na ocasião da convergência de TI e TO?                        | Limitação devido direcionamento de investimentos e recursos para a convergência / Limitação acerca de paradigmas culturais das equipes de Gestão, TI e TO / Falta de motivação das equipes para a integração das área de TI e TO / Falta de compreensão sobre os impactos da convergência das atividades de TI e TO / Falta de motivação para a implantação de Sistemas Cibernéticos-Físicos / Dificuldade de acesso à tecnologias integradoras / Outros         | OE 2 e<br>OE 5 |
|  | CV 5 - Na sua opinião, quais seriam os Impactos na Segurança da Informação, ocasionado pela convergência das atividades de TI e TO? | Aumento das ameaças à segurança da informação / Necessidade de equipe multifuncional dedicada para gestão da segurança da informação / Aumento da dedicação à segurança da informação de sistemas críticos (ligados a segurança operacional e ambiental) / Aumento da dificuldade em manter a estabilidade operacional / Aumento da dificuldade em manter a integridade das informações / Aumento das possibilidades de ataque cibernético à manufatura / Outros | OE2 a<br>OE 5  |
|  | CV 6 - Na sua opinião, quais tecnologias oportunizam a convergência das áreas de TI e de TO em empresas com manufatura avançada?    | Implantação de Cibersegurança / <i>Internet</i> Industrial da Coisas (IIoT) / Digitalização da Manufatura / Outros   | OE1 e<br>OE 5  |
| <b>Entrevista</b>                                  | EN 1 - Você aceita participar de entrevista sobre o tema "convergência de TI e TO"?   | Sim / Não  | OE 2 a<br>OE 5 |

## APÊNDICE B: Dados coletados no levantamento tipo *survey*.

### B.1. Dados de perfil sociodemográfico.

Tabela 2: Formação dos respondentes.

| Formação                                  | Quantidade | (%)  |
|---|------------|------|
| Engenharia Elétrica                       | 8          | 24%  |
| Análise de Sistemas                       | 4          | 12%  |
| Ciências da Computação                    | 4          | 12%  |
| Engenharia de Computação                  | 4          | 12%  |
| Redes de Computadores                     | 3          | 9%   |
| Administração                             | 2          | 6%   |
| Segurança da Informação                   | 2          | 6%   |
| Ciências Biológicas                       | 1          | 3%   |
| Ciências da Computação                    | 1          | 3%   |
| Eng. Telecomunicações e Gestão            | 1          | 3%   |
| Engenharia de Produção                    | 1          | 3%   |
| Gestão de redes e segurança da informação | 1          | 3%   |
| Sistemas de Informação                    | 1          | 3%   |
| Total Geral                               | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 3: Nacionalidade das empresas onde os respondentes atuam.

| Nacionalidade         | Quantidade | (%)  |
|-----------------------|------------|------|
| Brasileira            | 24         | 73%  |
| Americana             | 2          | 6%   |
| Alemã                 | 1          | 3%   |
| Brasileira / Coreana  | 1          | 3%   |
| Espanhola             | 1          | 3%   |
| Francesa              | 1          | 3%   |
| Indiana               | 1          | 3%   |
| Sueca                 | 1          | 3%   |
| Taiwanesa / Americana | 1          | 3%   |
| Total Geral           | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 4: Tamanho das empresas onde os respondentes atuam.

| Tamanho     | Quantidade | (%)  |
|-------------|------------|------|
| Grande      | 18         | 55%  |
| Pequena     | 6          | 18%  |
| Média       | 5          | 15%  |
| Micro       | 4          | 12%  |
| Total Geral | 33         | 100% |

Fonte: Resultado da pesquisa.



Tabela 5: Setor econômico das empresas onde os respondentes atuam.

| Setor econômico         | Quantidade | (%)  |
|-------------------------|------------|------|
| Comércio e Serviços     | 16         | 48%  |
| Indústria               | 13         | 39%  |
| Atividades intelectuais | 3          | 9%   |
| Sem ânimo de lucro      | 1          | 3%   |
| Matérias-primas         | 0          | 0%   |
| Total Geral             | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 6: Função atual dos respondentes.

| Função   | Quantidade | (%)  |
|--|------------|------|
| CISO   | 4          | 12%  |
| Gerente de Tecnologia da Informação  | 4          | 12%  |
| CSO  | 2          | 6%   |
| CTO  | 2          | 6%   |
| Integrador de Tecnologia Operacional   | 2          | 6%   |
| Líder de TO  | 2          | 6%   |
| Analista de Cibersegurança   | 1          | 3%   |
| Analista de Segurança da Informação  | 1          | 3%   |
| Analista de Segurança Sênior   | 1          | 3%   |
| CEO  | 1          | 3%   |
| Consultor de Segurança de Infraestrutura Crítica                                     | 1          | 3%   |
| Consultor de Tecnologia Operacional  | 1          | 3%   |
| Diretor  | 1          | 3%   |
| Diretor de Engenharia  | 1          | 3%   |
| Engenheiro de Infraestrutura de TI   | 1          | 3%   |
| Engenheiro de Telecomunicação  | 1          | 3%   |
| Especialista em Infraestrutura de TI   | 1          | 3%   |
| Gerente de Desenvolvimento de Negócios de Cibersegurança para Infraestrutura Crítica | 1          | 3%   |
| Gerente de Projetos  | 1          | 3%   |
| Gerente de Segurança   | 1          | 3%   |
| Líder de Centro de Operação de Redes   | 1          | 3%   |
| Líder de TI  | 1          | 3%   |
| Técnico de TI  | 1          | 3%   |
| Total Geral  | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 7: Tempo na função atual dos respondentes.

| Tempo       | Quantidade | (%)  |
|-------------|------------|------|
| > 5 anos    | 18         | 55%  |
| 2 a 5 anos  | 10         | 30%  |
| 1 a 2 anos  | 4          | 12%  |
| < 1 ano     | 1          | 3%   |
| Total Geral | 33         | 100% |

Fonte: Resultado da pesquisa.

## B.2. Dados associados a manufatura avançada.

Tabela 8: Tecnologias de automação industrial que os respondentes interagem.

| Tecnologias   | Quantidade de seleções pelos respondentes |                     |
|---|---|---------------------|
|   | Tenho interação                           | Não tenho interação |
| Sensores e demais dispositivos de instrumentação industrial                       | 12  | 21                  |
| Sistemas de instrumentação de segurança, CLPs e dispositivos controladores locais | 18  | 15                  |
| IHM Local e Sistemas supervisórios locais   | 16  | 17                  |
| Centro de Controle de Processo e Sistema supervisório central                     | 20  | 13                  |
| MES, Sistemas automatizados auxiliares à Gestão de Produção e Logística           | 12  | 21                  |
| ERP, Sistemas automatizados auxiliares para Gestão Estratégica de Operações       | 19  | 14                  |

Fonte: Resultado da pesquisa.

### B.3. Dados associados a convergência de TI e TO e segurança da informação.

Tabela 9: Área de atuação predominante dos respondentes.

| Área             | Quantidade | (%)  |
|------------------|------------|------|
| TI               | 21         | 64%  |
| TO               | 9          | 27%  |
| Telecomunicações | 2          | 6%   |
| TI e TO          | 1          | 3%   |
| Total Geral      | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 10: Percepção da necessidade da convergência de TI e TO pelos respondentes.

| Necessidade | Quantidade | (%)  |
|-------------|------------|------|
| Sim         | 32         | 97%  |
| Não         | 1          | 3%   |
| Total Geral | 33         | 100% |

Fonte: Resultado da pesquisa.

Tabela 11: Opinião dos respondentes sobre oportunidades para a empresa com a convergência de TI e TO.

| Oportunidades  | Quantidade | (%)   |
|--|------------|-------|
| Segurança total da informação (desde o chão de fábrica até as redes externas de comunicação)         | 28         | 20,4% |
| Possibilidade de interoperabilidade de tecnologias   | 21         | 15,3% |
| Aumento da precisão na tomada de decisões  | 20         | 14,6% |
| Criação de novas informações (conhecimento)  | 17         | 12,4% |
| Melhor entendimento das demandas dos usuários do processo produtivo                                  | 16         | 11,7% |
| Aumento da quantidade de dados coletados em tempo real do processo produtivo                         | 14         | 10,2% |
| Concordância com formatos de troca de dados (sintaxe e semântica)                                    | 12         | 8,8%  |
| Digitalização precisa da manufatura  | 7          | 5,1%  |
| Convergência Tecnológica e de Governança   | 1          | 0,7%  |
| Vejo grande oportunidade para a existência de tecnologias que utilizem de técnicas de Process Mining | 1          | 0,7%  |
| Total de Citações  | 137        | 100%  |

Fonte: Resultado da pesquisa.

Tabela 12: Opinião dos respondentes sobre limitações para a empresa com a convergência de TI e TO.

| Limitações  | Quantidade | (%)  |
|---|------------|------|
| Limitação acerca de paradigmas culturais das equipes de Gestão, TI e TO                                 | 21         | 25%  |
| Falta de compreensão sobre os impactos da convergência das atividades de TI e TO                        | 18         | 21%  |
| Falta de motivação das equipes para a integração das áreas de TI e TO                                   | 13         | 15%  |
| Falta de motivação para a implantação de Sistemas Cibernéticos-Físicos                                  | 12         | 14%  |
| Limitação devido direcionamento de investimentos e recursos para a convergência                         | 10         | 12%  |
| Dificuldade de acesso à tecnologias integradoras  | 8          | 10%  |
| Limitações de tempo   | 1          | 1%   |
| Na visão do cliente ainda é preciso quebrar paradigmas e ambos os lados resolver entender o outro lado. | 1          | 1%   |
| Total de Citações   | 84         | 100% |

Fonte: Resultado da pesquisa.

Tabela 13: Opinião dos respondentes sobre os impactos à segurança da informação na empresa com a convergência de TI e TO.

| Impactos à segurança da informação  | Quantidade | (%)  |
|---|------------|------|
| Necessidade de equipe multifuncional dedicada para gestão da segurança da informação                              | 27         | 27%  |
| Aumento das ameaças à segurança da informação   | 23         | 23%  |
| Aumento da dedicação à segurança da informação de sistemas críticos (ligados a segurança operacional e ambiental) | 22         | 22%  |
| Aumento das possibilidades de ataque cibernético à manufatura   | 18         | 18%  |
| Aumento da dificuldade em manter a estabilidade operacional   | 5          | 5%   |
| Aumento da dificuldade em manter a integridade das informações  | 5          | 5%   |
| Total de Citações   | 100        | 100% |

Fonte: Resultado da pesquisa.

Tabela 14: Opinião dos respondentes sobre tecnologias que oportunizam a convergência de TI e TO em empresas com manufatura avançada.

| Tecnologias  | Quantidade | (%)  |
|--|------------|------|
| Internet Industrial da Coisas (IIoT)   | 26         | 43%  |
| Implantação de Cibersegurança  | 21         | 35%  |
| Digitalização da Manufatura  | 12         | 20%  |
| Cloud e Analytics as anteriores já existem instaladas em maior ou menor grau | 1          | 2%   |
| Total de Citações  | 60         | 100% |

Fonte: Resultado da pesquisa.

**B.4. Dados associados a participação na entrevista.**

Tabela 15: Declaração dos respondentes sobre participação voluntária na etapa de entrevistas.

| Disponibilidade | Quantidade | (%)  |
|-----------------|------------|------|
| Não             | 17         | 52%  |
| Sim             | 16         | 48%  |
| Total Geral     | 33         | 100% |

Fonte: Resultado da pesquisa.

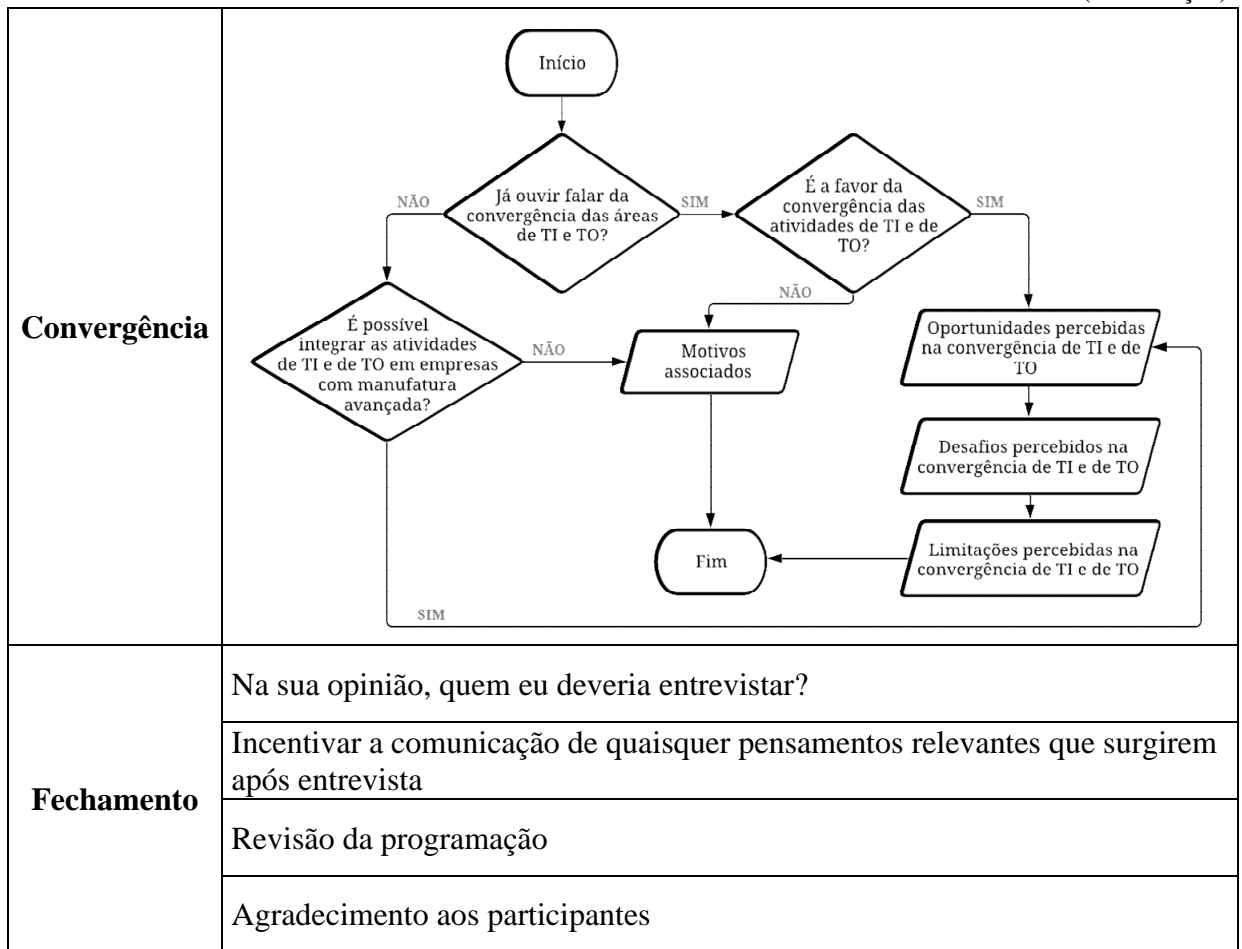
## APÊNDICE C: Entrevista semiestruturada.

### C.1. Instrumento da entrevista semiestruturada.

Quadro 16: Categorização e perguntas para a entrevista semiestruturada.

| <b>Categorização</b>                                | <b>Perguntas</b>   |
|---|--|
| <b>Introdução</b>                                   | Objetivos da entrevista  |
|   | Informações sobre: Dissertação, Centro Paula Souza, Programa de Mestrado e Áreas de pesquisa   |
|   | Permissão para gravar a conversa e descrição de como as gravações serão armazenadas e excluídas  |
|   | Menção que, como nenhuma entrevista foi feita antecipadamente, algumas perguntas podem parecer idiotas ou confusas e não há respostas certas ou erradas. |
| <b>Identificação da experiência do entrevistado</b> | Como é o sistema de gestão da segurança da informação do processo produtivo, na empresa onde você trabalha?  |
|   | Você sabe quem usa estas informações?  |
|   | Você sabe como estas informações são utilizadas?   |
|   | Qual a sua experiência na área em que atua?  |
|   | Quais suas atuais atividades e responsabilidades?  |
|   | Qual seu papel em relação ao sistema de informação do chão de fábrica da empresa?  |
| <b>Segurança da Informação</b>                      | Qual seu papel na segurança da informação na empresa onde trabalha?  |
|   | A gestão da segurança da informação atualmente está sob responsabilidade de qual área? TI ou TO?   |
|   | Na empresa onde você trabalha é analisada separadamente a segurança da informação da área de TO?   |
|   | Existe destinação estratégica de investimentos para gestão da segurança da informação da área de TO?   |
| <b>Manufatura Avançada</b>                          | Você já ouviu falar da integração de atividades ocasionadas pelas tecnologias da manufatura avançada ou Indústria 4.0?                                   |
|   | Na empresa onde você trabalha, existe automação em áreas críticas a segurança humana, infraestrutura, meio ambiente?                                     |
|   | Quais tecnologias estão presentes no chão de fábrica que apresentem alto nível de automação de manufatura?   |
|   | Quais tecnologias demandam suporte de TI e de TO?  |
|   | Como você classifica a vida útil atual dos elementos do sistema de controle na empresa onde você trabalha?   |

(continuação)



Fonte: o autor.