Análise dos Workshops
do Primeiro Congresso de Normalização
Internacional no contexto da Indústria 4.0

Desafios da Normalização para a Indústria 4.0 no Brasil

Desenvolvimento:

NEO
NÚCLEO DE ENGENHARIA ORGANIZACIONAL | UFRGS

UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

2022

Núcleo de Engenharia Organizacional - Universidade Federal do Rio Grande do Sul
Ministério da Economia - Governo Federal do Brasil
(Organizadores)

Análise dos Workshops do Primeiro Congresso de Normalização Internacional no contexto da Indústria 4.0

Desafios da Normalização para a Indústria 4.0 no Brasil

Porto Alegre
UFRGS
2022

Elaboração do relatório

A presente nota técnica foi elaborada no âmbito do 1º Congresso Nacional de Normalização de Indústria 4.0, realizado pela Associação Brasileira de Normas Técnicas (ABNT) e Câmara Brasileira da Indústria 4.0. O trabalho contou com apoio do Projeto Global Infraestrutura da Qualidade (PGIQ).

O Ministério Federal da Economia e Ação Climática (BMWK) encarregou a Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH de implementar o Projeto Global de Infraestrutura da Qualidade.

O conteúdo foi elaborado com base nas discussões de especialistas, durante três workshops técnicos, pela equipe do Núcleo de Engenharia Organizacional da UFRGS:

- Prof. Alejandro G. Frank, Dr.
- Prof. Néstor F. Ayala, Dr.
- Profa. Camila Costa Dutra, Dra.
- Laura Visintainer Lerman, MSc.
- Márcia Possa Forcelini
- Júlia Battaglin Pierdoná

Sumário

Siglas utilizadas

ABNT: Associação Brasileira de Normas Técnicas

AIOps: Inteligência Artificial para Operações de TI

ALO: Ant Colony Optimization

APIs: Application Programming Interface

CD: Committee Draft

CGEE: Centro de Gestão e Estudos Estratégicos

CLP: Controlador lógico programável

CySA+: CompTIA Cybersecurity Analyst

DHT: Distributed Hash Table

DIS: Draft Internacional Standard

DW: Datawarehouse

EBIA: Estratégia Brasileira de Inteligência Artificial

ERPs: Enterprise Resource Planning

ESI: Informações Armazenadas Eletronicamente

FDIS: Final DIS

GIZ Alemanha: Deutsche Gesellschaft für Internationale Zusammenarbeit (Agência Alemã de Cooperação Internacional)

IA: Inteligência Artificial

IaaS: Infraestrutura como serviço

IEC: International Electrotechnical Commission

IIoT: Industrial Internet of things

IoT: Internet das coisas

ISO: International Standard

ITU: International Telecommunication Union (União Internacional de Telecomunicações)

KDD: Knowledge Discovery in Database

LGPD: Lei Geral de Proteção de Dados

MAPE: Mean Absolute Percentual Error

MCTI: Ministério de Ciência, Tecnologia e Inovação

MES: Manufacturing Execution System

ML: Aprendizado de Máquina (Machine Learning)

MSE: Mean Squared Error

NIST: National Institute Standards and Technologies

PaaS: Platform as a Service
Normalização Internacional no contexto da Indústria 4.0 7

PAS: Public Available Specification

PO: Pesquisa Operacional

RNA: Redes Neurais Artificiais

SaaS: Software as a Service

SGSI: Sistema de Gestão de Segurança da Informação

SNRA: Sensor Network Reference Architecture

SSCO: Segurança de Sistemas

TA: Tecnologia da Automação

THOMP: Training by Highly Ontology-oriented Tutoring Host (Aprendizagem por Servidor de Tutoria com Alta Orientação a Ontologias)

TI: Tecnologia da Informação

TIC: Tecnologia da Informação e Comunicação

TR: Technical Report

TS: Technical Specification

VPN: Virtual Private Network

WD: Rascunho de Trabalho

1 Sumário Executivo

1.1 Foco do estudo

Esta Nota Técnica é a quarta nota técnica sobre Normalização no contexto da Indústria 4.0 desenvolvidas pelo Núcleo de Engenharia Organizacional em parceria com a GIZ Alemanha – Deutsche Gesellschaft für Internationale Zusammenarbeit (Agência Alemã de Cooperação Internacional) – a pedido da Câmara da Indústria 4.0 com intuito de analisar os problemas debatidos durante o workshop de Normalização e a lista de especialistas que podem auxiliar a Associação Brasileira de Normas Técnicas (ABNT) no desenvolvimento de normas brasileiras sobre a transformação digital e a Indústria 4.0.

O estudo é uma continuação das notas técnicas anteriores e tem como tema central a normalização em relação à transformação digital e à Indústria 4.0 e analisa os problemas enfrentados pelas indústrias e fornecedoras de tecnologia em relação às normas de Inteligência Artificial e Machine learning, Cibersegurança e Internet das Coisas no contexto da Indústria 4.0. Para tanto, são analisados os problemas dos seguintes grupos prioritários de normalização internacional da ISO: (i) Inteligência Artificial (ISO/IEC/JTC1/SC42), (ii) Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC JTC 1/SC 27) e (iii) Internet das Coisas e Gêmeos Digitais (ISO/IEC JTC 1/SC 41).

1.2 Abordagem metodológica

O relatório utiliza uma abordagem mista que combina a análise das normas/regulações com a análise de conteúdo de workshops e entrevistas com especialistas nos temas tratados, a fim de compreender a abrangência dos problemas enfrentados na indústria e o alcance das normas técnicas existentes e em desenvolvimento.

1.3 Resultados

O relatório apresenta diversos resultados:

- Em relação à **Inteligência Artificial, destacaram-se 13 problemas.** Além disso, **foram analisadas 32 normas** técnicas publicadas e em desenvolvimento sobre Inteligência Artificial que podem ajudar a solucionar os problemas das indústrias e fornecedoras de tecnologia correlacionando os problemas às normas técnicas. Identificou-se a necessidade de desenvolvimento e melhoria de normas técnicas, visto que muitas normas técnicas desse grupo estão em desenvolvimento e necessitam serem aprofundadas para cobrirem totalmente os problemas destacados pelos participantes do workshop de normalização. Também, algumas normas técnicas existentes sobre Big Data podem expandir seu escopo para abranger problemas enfrentados no campo de IA.
- No que concerne ao grupo prioritário **Internet das Coisas, Gêmeos Digitais**

e Interoperabilidade, foram evidenciados **7 problemas.** Ademais, **foram analisadas 40 normas técnicas** publicadas e em desenvolvimento sobre Internet das Coisas e Gêmeos digitais a fim de verificar se as normas solucionavam os problemas apontados pelas indústrias e fornecedoras de tecnologia no respectivo workshop. Como o workshop abordou também o tema interoperabilidade, além dos dispositivos IoT, foi realizada análises de normas técnicas sobre outras tecnologias, como sensores e Blockchain.

- No que se refere à **Cibersegurança,** foram destacados **8 problemas** e foram analisadas **40 normas técnicas** publicadas e em desenvolvimento em relação a este tópico. Ainda, quando necessário, foram analisadas outras normas do mesmo grupo que contém cerca de 290 normas técnicas publicadas e em desenvolvimento. Com base na análise, verificou-se que muitas das normas técnias sobre cibersegurança para a resolução dos problemas estão em desenvolvimento. Por isso, há uma oportunidade de debate sobre quais os problemas que as normas técnicas solucionarão e se serão necessárias mais normas ou uma readaptação das mesmas.
- Mesmo que tenha havido um workshop específico para Cibersegurança, o tópico também foi abordado nos outros dois workshops, demonstrando a necessidade de desenvolvimento de normas técnicas sobre o assunto nas diferentes aplicações de tecnologias da Indústria 4.0, como Inteligência Artificial, Machine Learning e Internet das Coisas. Além disso, destaca-se a necessidade de alinhamento entre as normas técnicas e a Lei Geral de Proteção de Dados (LGPD). Dessa forma, é importante relacionar as normas de Inteligência Artificial e Internet das Coisas com as de Cibersegurança para que os grupos prioritários de transformação digital e/ou comitês desenvolvam normas técnicas que estejam relacionadas a necessidades da indústria como um todo e possam refletir a necessidade futura dessas indústrias.

2 Introdução

Este estudo forma parte de um projeto maior do Grupo de Trabalho "Regulação, Normalização Técnica e Infraestrutura para Normalização" da Câmara Brasileira da Indústria 4.0, que tem o intuito de expor e explicar o estado atual do trabalho normativo bem como propostas em discussão dos principais fóruns internacionais de normalização com foco na Indústria 4.0 e transformação digital, facilitando a compreensão de empresas e entidades nacionais da relevância dos mesmos para o desenvolvimento da transformação digital da indústria brasileira.

O projeto desse grupo de trabalho iniciou com o desenvolvimento da nota técnica sobre Normalização na Indústria 4.0, elaborada pela CGEE em parceria com o Núcleo de Engenharia Organizacional, e que contemplou os seguintes grupos prioritários de normalização: a) Inteligência artificial e 5GS, b) Segurança e cibersegurança, e c) Redes industriais e interoperabilidade. Essa nota técnica serviu como subsídio para a elaboração do Primeiro Congresso de Normalização sobre o tema. Nele, foram desenvolvidos workshops para identificar os problemas mais frequentes enfrentados pelos profissionais da indústria.

A partir dessa série de workshops desenvolvidos, a presente nota técnica tem por objetivo expor e analisar as discussões técnicas dos workshops durante o congresso e analisar interfaces com projetos de normalização. Assim sendo, esta nota técnica apresenta uma visão detalhada da análise de especialistas sobre o assunto, permitindo identificar principais oportunidades e desafios no campo da normalização associada com a Indústria 4.0.

2.1 Conteúdo deste Relatório

O relatório desta quarta nota técnica contempla três grupos prioritários, os problemas relatados pelos profissionais e as normas técnicas relacionadas, sendo estes:

1. Inteligência Artificial (ISO/IEC/JTC1/SC42)

2. Segurança da informação, cibersegurança e proteção da privacidade (ISOIEC JTC 1/SC 27)

3. Internet das Coisas e Gêmeos Digitais (ISO/IEC JTC 1/SC 41)

2.2 Grupos para o desenvolvimento de Normas

Os grupos de trabalho são Comissões de Estudo sobre temas específicos que tem como objetivo desenvolver normalizações sobre temas relevantes no desenvolvimento nacional a nível mundial.

Dessa forma, os grupos de trabalho são essenciais para as empresas que precisam se basear nas normas técnicas para o desenvolvimento de produtos e serviços. De forma geral, a participação nessas

comissões é aberta a qualquer parte interessada representante dos países envolvidos. O Brasil, em alguns grupos, possui participação. É importante salientar que o país pode ser um membro Participante, que é mais atuante e tem a obrigação de emitir opiniões sobre os assuntos, ou membro Observador, que participa apenas como ouvinte e para ter acesso aos documentos em desenvolvimento.

Complementando esses aspectos dos grupos, é imprescindível entender a que instituições de normalização eles estão associados. Por exemplo, nesse relatório, são abordados grupos das instituições ISO, IEC e ITU. A ISO é a Organização Internacional de Normalização que desenvolve normas técnicas e relatórios técnicos quando há necessidade de mercado. Para isso, as normas técnicas são criadas por especialistas que podem ser profissionais da indústria, do governo, da universidade e outros atores. Além disso, os membros dos comitês devem ser capazes de identificar os especialistas a fim de alinhar as necessidades de normalização com o mercado. Para que as necessidades estejam alinhadas e direcionadas para um objetivo de crescimento, a Secretaria da ISO suporta o desenvolvimento das normas técnicas.

Complementarmente, a IEC (International Electrotechnical Commission) é a organização mundial que prepara e publica Normas Internacionais para as áreas elétrica, eletrônica e tecnologias relacionadas, complementando as normas da ISO e, por vezes, desenvolvendo normas técnicas em parceria. Dessa maneira, eles fazem publicações para a aplicação em fábricas e em diversos ambientes. É importante salientar que o desenvolvimento de normas técnicas é feito através do Comitê Nacional da IEC de cada país. Além da ISO e da IEC, a ITU engloba a padronização da área de Telecomunicações do ITU - União Internacional de Telecomunicações ("International Telecommunication Union"), focada também no desenvolvimento de normas técnicas.

Com base nessas informações, a ITU é focada na parte de telecomunicações enquanto a IEC aborda temas de eletroeletrônica. De forma geral, as três entidades se complementam entre si, desenvolvendo normalização para suportar as empresas nos diferentes campos do conhecimento.

Em relação às normas da ISO, é importante entender alguns aspectos relacionados ao desenvolvimento de normas e diferentes tipologias. Por exemplo, a escala de evolução do projeto até se tornar uma norma completa envolve diversas etapas:

1. Estágio preliminar: que gera a aprovação de uma nova votação para o projeto;

2. Estágio de proposta: que gera um documento chamado New work Item proposal (NP);

3. Estágio preparatório: que se desenvolve um rascunho de trabalho (WD – Work Draft);

4. Estágio do comitê: que gera um documento chamado Committee Draft (CD);

5. Estágio de investigação: que gera um rascunho de investigação, comumente conhecido como Draft Internacional

Standard (DIS);

6. Estágio de aprovação: aprovação do Final DIS (FDIS);

7. Estágio de publicação: publicação da International Standard (ISO);

8. Estágio de revisão: que pode gerar a confirmação da norma ou encaminhamento para revisão;

9. Estágio de suspensão: que pode gerar a suspensão ou não da norma. O detalhamento destas etapas se encontra no Apêndice A. Em relação a tipologias de documentos, a ISO pode desenvolver normas técnicas internacionais, porém também aborda outros documentos, tais como Technical Specification (TS), Public Available Specification (PAS) e TechnicalReport (TR).

3 Metodologia

A partir do desenvolvimento e da análise das Notas Técnicas A, B e C, foi desenvolvido o Primeiro Congresso de Normalização Brasileiro com atividades em quatro dias distintos. O primeiro dia foi realizada a abertura do congresso com as principais entidades e atores de normalização brasileiros. Nos outros três dias, foram desenvolvidos workshops sobre os grupos prioritários: (i) Inteligência Artificial (ISO/IEC/JTC1/SC42), destacando-se aspectos em relação a casos de uso das empresas e no gerenciamento de dados, (ii) Segurança da informação, cibersegurança e proteção da privacidade, com foco na cibersegurança (ISO/IEC JTC 1/SC 27) e (iii) Internet das Coisas e Gêmeos Digitais (ISO/IEC JTC 1/SC 41), destacando o tema de interoperabilidade.

Estes workshops foram divididos em duas partes: (i) a primeira parte constou da apresentação dos principais aspectos das notas técnicas dos temas a serem debatidos, e (ii) a segunda parte constou de uma dinâmica de grupo com a participação de autodeclarados especialistas em cada tema. A dinâmica de grupo constou de três etapas:

- **Etapa 1 - *Brainwriting:*** conduziu-se um *brainstorming* com o uso de post its para que os especialistas pudessem expressar os principais problemas para cada um dos temas. O objetivo da etapa foi responder à seguinte questão: Quais os principais problemas que você enfrenta ou identifica no uso Inteligência Artificial, Cibersegurança ou Interoperabilidade, que possam estar relacionados à falta de normas ou padrões?
- **Etapa 2 - Agrupamento e priorização dos problemas:** com a ajuda dos especialistas, conduziu-se uma discussão para identificar possíveis agrupamentos de problemas por afinidade ou similaridade. Após, os problemas eram realocados e unificados nos clusters para que se pudesse iniciar a priorização. Na etapa de priorização, os especialistas votaram com o objetivo de identificar os problemas mais relevantes. Cada especialista pode distribuir um máximo de 5 votos no total. Com base na votação dos especialistas da etapa 2, os problemas foram ranqueados
- **Etapa 3 - Aprofundamentos dos problemas:** Os problemas priorizados foram debatidos pelo grupo de especialistas com o objetivo compreender e aprofundar a importância desses problemas e como a normalização poderia auxiliar em sua solução.

Na parte expositiva de congresso, ao total, participaram 170 especialistas de diversas entidades, indústrias e órgãos. Nessa parte, foram expostos alguns temas importantes, como: apresentação das notas técnicas; relevância do grupo prioritário; escopo dos grupos prioritários; os principais problemas e as normas técnicas; passo a passo de como as normas técnicas

podem ser encontradas; e apresentação da ABNT sobre o processo de normalização.

No workshop de **Inteligência artificial**, participaram 70 pessoas na parte expositiva e **32 especialistas** divididos em dois grupos de 16 pessoas na dinâmica de grupo, gerando um total de 96 problemas na etapa 1 de brainwriting e 68 problemas consolidados na etapa 2 de agrupamento e priorização dos problemas.

O workshop de **Cibersegurança** contou com 55 especialistas na etapa expositiva. Já, na dinâmica de grupo, participaram **30 especialistas** nas duas salas, na etapa de brainwriting, foram identificados 95 problemas e, na etapa de agrupamento, esse número se reduziu para 32 problemas consolidados.

Por fim, foi realizado o workshop de **interoperabilidade,** que contou com a presença de 45 participantes na parte expositiva. Já, na parte participativa, a dinâmica foi desenvolvida com **22 especialistas,** divididos em dois grupos de 11 para promover uma maior interação. Nessa dinâmica, na etapa 1 de brainwriting, foram identificados 61 problemas. Posteriormente, na etapa 2 de agrupamento e priorização, foram consolidados 53 problemas.

Após o desenvolvimento do workshop, foi realizada a consolidação dos resultados das dinâmicas através uma análise de conteúdo tanto da parte escrita quanto da gravação das mesmas. Além disso, foram feitas entrevistas com alguns especialistas para o entendimento dos problemas.

Com base nessas avaliações, consolidaram-se 13 problemas para Inteligência Artificial com base na priorização realizada pelos especialistas durante o workshop e nas entrevistas conduzidas. E, após, realizou-se o cruzamento com 32 normas técnicas do grupo de Inteligência Artificial. Para o grupo de cibersegurança, foram consolidados 8 problemas enfrentados. E, novamente, cruzou-se com 40 normas técnicas dos grupos prioritários analisados. Por fim, no que tange ao workshop de interoperabilidade, consolidaram-se 7 problemas em relação à interoperabilidade e IoT. Posteriormente, foi realizado o cruzamento com 40 normas técnicas publicadas e em desenvolvimento.

Além do cruzamento entre os problemas e as normas técnicas[1], também se realizou o cruzamento dos problemas com alguns relatórios, artigos e normas técnicas brasileiras sobre o assunto (Estratégia Brasileira de Inteligência Artificial; Plano Nacional de Internet das Coisas; Lei Geral de Proteção de Dados Pessoais). No Apêndice B é apresentada a lista de referências utilizadas.

Assim, as próximas seções são organizadas da seguinte forma: primeiramente, apresentado o problema destacado pelos especialistas nos workshops; em segundo lugar, o problema é aprofundado com base nos debates dos especialistas e literatura existente; por fim, são apresentadas as normas técnicas existentes que poderiam apresentar algum tipo de solução para os referidos problemas.

4 Grupo de Inteligência Artificial (ISO/IEC/JTC1/SC42)

4.1 Escopo

A proposta do grupo de trabalho de Inteligência Artificial (IA) é elaborar normas técnicas baseadasnos padrões internacionais para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA.

A seguir serão detalhados os problemas destacados pelos especialistas durante o workshop de IA. Em cada subtítulo, entre parêntesis, são apresentados o número de votos que o problema recebeu dos especialistas e sua posição na priorização. Quando a posição apresenta um asterisco, significa que os problemas ficaram empatados. A ordem de apresentação dos problemas aqui não segue a ordem de priorização, mas uma sequência organizada por afinidade.

4.2 Falta de padronização para coleta de dados (12 – 3º)

Durante o workshop, os especialistas relataram uma falta de uma padronização na coleta de dados de forma clara e objetiva, visto que os dados são coletados de diferentes formas por diferentes fornecedores ou profissionais. Por exemplo, os equipamentos de diversos fornecedores utilizam diversos métodos de coleta e exportação de dados. De forma geral, os especialistas relataram os seguintes problemas ao serem questionados sobre o assunto: necessidade de definição e padronização de dados estruturados e não estruturados; necessidade de padronização de métodos de otimização em busca de dados; necessidade de uniformização de dados históricos (bases de dados legadas) antes do uso.

Complementarmente, os especialistas enfatizaram os problemas relacionados a ausência de um padrão para data lakes, o que faz com que as necessidades sejam tratadas de forma individualizadas e não coletivas. De acordo com a IBM, “os data lakes são soluções de gerenciamento de dados híbridos de nova geração que podem atender aos grandes desafios de dados e impulsionar novos níveis de análise em tempo real”[2]. Porém, sem um padrão, os dados neste data lakes não são plausíveis de análise, ou demandam grandes retrabalhos. É importante salientar que data lakes estão introduzindo novos desafios, como padrões para a extração de dados, limpeza de dados, integração de dados, controle de versão de dados e gerenciamento de metadados[3].

Consequentemente, as normas técnicas podem ajudar as empresas e as

fornecedoras de soluções de inteligência artificial a diminuírem os desafios do uso de data Lakes. Por exemplo, em um projeto na área da saúde relacionado ao COVID-19, foi necessária a junção de 25 bases de dados para que se pudessem realizar as análises necessárias, e a criação de uma arquitetura de Data Lake própria[4]. Logo, os pesquisadores necessitaram criar uma estrutura de Data Lake com base na literatura pelo desconhecimento de uma norma internacional e/ou um framework.

Além do data lake, os especialistas destacaram a importância de um padrão para coleta de dados. Em relação ao tema, a EBIA discorre que "nos casos em que a regulamentação da IA é inevitável, deve ser desenvolvida com ponderação e com tempo suficiente para permitir que várias partes interessadas identifiquem, articulem e implementem os principais princípios e melhores práticas". Nesse sentido, se algo mudar na regulamentação de IA em relação à coleta de dados e a criação de data lakes, é importante que seja discutido se as regulamentações brasileiras e internacionais estão alinhadas para que possa existir uma sinergia a fim de propiciar um ambiente para o uso de tecnologias. Além disso, a EBIA enfatiza a seguinte ação estratégica: "Criar e implementar melhores práticas ou códigos de conduta com relação à coleta, implantação e uso de dados, incentivando as organizações a melhorar sua rastreabilidade, resguardando os direitos legais." A partir disso, é importante ressaltar que a coleta de dados deve ser padronizada com base nas melhores práticas conforme discutido pelos especialistas e evidenciado na EBIA.

Ademais, conforme exemplificado no workshop, a EBIA exemplifica o uso de IA com base na coleta e análise de informações para evitar prescrição dos crimes pelo Ministério Público do Rio de Janeiro. Dessa forma, se houver uma padronização, todos os estados poderão utilizar o mesmo processo e a sistematizar a análise utilizada pelo Ministério Público do Rio de Janeiro. É crucial ressaltar como isso impacta nos fornecedores de soluções de IA que precisam oferecer soluções padronizadas. De forma geral, considerando esses aspectos, as fornecedoras de solução de IA hoje despendem muito tempo para padronização dos dados pelo uso de diferentes bases de dados e redundância das fontes. Além disso, elas também sofrem com a falta uma limpeza dos dados e ausência de um padrão de Data Lake, principalmente.

Existem já algumas normas técnicas importantes para esse problema, mas ainda há muito o que precisa ser discutido. Há uma série de normas técnicas (ISO/IEC AWI 5259) que estão em desenvolvimento, entre elas, estão Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples (ISO/IEC AWI 5259-1 – Estágio 20.20); Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures (ISO/IEC AWI 5259-2 – Estágio 20.00); Artificial intelligence — Data quality for analytics and machine learning

(ML) — Part 3: Data quality management requirements and guidelines (ISO/IEC AWI 5259-3 – Estágio 20.00); Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework (ISO/IEC AWI 5259-4 – Estágio 20.00).

Como essas normas técnicas ainda estão em desenvolvimento, seria necessário entender como a parte de coleta de dados e o desenvolvimento de Data Lakes poderiam ser incluídos com a ajuda dos especialistas. Além disso, poderia ser desenvolvida uma norma para qualidade de dados na coleta e outra sobre o desenvolvimento de Data Lakes para compor a série, se os especialistas acharem apropriado. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de padronização para coleta de dados

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWI 5259-1	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples	Estágio 20.20	Incluir normas que abrajam aspectos de coleta, organização e qualidade de dados em Data Lakes
ISO/IEC AWI 5259-2	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures	Estágio 20.00	
ISO/IEC AWI 5259-3	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines	Estágio 20.00	
ISO/IEC AWI 5259-4	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework	Estágio 20.00	

4.3 Falta de integração e comunicação para a troca de dados (19 – 2º)

Os especialistas trouxeram no workshop diversos problemas em relação à falta integração e comunicação para a troca de dados entre dispositivos, aplicações, e plataformas, uma vez que que as indústrias necessitam da consolidação da informação em um único lugar e da integração entre várias informações para conseguirem desenvolver uma IA mais adequada aos objetivos estratégicos da empresa.

Particularmente, os especialistas relataram a falta de padrão de comunicação entre diferentes fornecedores e falta de padrão de comunicação e troca de dados na cadeia de valor (entre clientes e fornecedores), já que a integração dos fornecedores com uso de tecnologias da Indústria 4.0 é essencial para que as indústrias consigam realizar análises com dados de diversas hierarquias para a tomada de decisão. Existindo uma padronização de dados na cadeia, a adoção de IA permitiria o desenvolvimento de um modelo de tomada de decisão mais eficiente para enfrentar o contexto dinâmico das cadeias de valor[5].

Outrossim, para que as cadeias de valor possam ser mais colaborativas que visem a integração de dados, é discutido sobre como as técnicas de IA podem apoiar a comunicação, coordenação e cooperação em indústrias[6]. Por exemplo, conforme a EBIA, o Brasil já possui plataformas cooperativas para alguns setores estratégicos, tais como agricultura, mineração e indústria petroquímica. Dessa forma, as fornecedoras de soluções de IA e as empresas entendem a necessidade de integração das diferentes aplicações e que a falta de uma comunicação clara das aplicações pode afetar as operações da empresa. Portanto, as indústrias percebem a necessidade de um padrão de comunicação para criar a sinergia entre os dados e os equipamentos, criando, assim, um padrão de compartilhamento de dados. Além da EBIA, é importante citar a LGPD, principalmente o artigo 6º, que trata sobre os princípios do tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilidade e prestação de contas. Dependendo de como é realizada a troca de dados e se envolvem dados pessoais, é necessária uma análise com base nos princípios da LGPD.

Em relação às normas técnicas que estão sendo desenvolvidas e publicadas sobre o assunto, destacam-se: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC DIS 23053 – Estágio 40.60), que está em desenvolvimento. A norma estabelece uma estrutura de Inteligência Artificial (IA) e Aprendizado de Máquina (ML) para descrever um sistema de AI genérico usando a tecnologia de ML. Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos que estão implementando ou usando

sistemas de IA. Para isso, existem, na norma, algumas questões relacionadas a dados: aquisição de dados, pré-processamento de dados, fluxos de dados no aprendizado de máquina supervisionado e uso de dados no aprendizado de máquina. Dessa forma, a norma atende parcialmente o problema pois apresenta um modelo de estrutura para sistemas de Inteligência Artificial utilizando Machine Learning.

Complementarmente, existe a norma Information technology — Big data reference architecture — Part 3: Reference architecture (ISO/IEC 20547-3:2020 – Estágio 60.0), que foi publicada e é focado em Big Data. A norma se destina a: fornecer uma linguagem comum para as várias partes interessadas; encorajar a adesão a padrões, especificações e padrões comuns; fornecer consistência de implementação de tecnologia para resolver conjuntos de problemas semelhantes; facilitar a compreensão dos meandros operacionais em big data; ilustrar e compreender os vários componentes, processos e sistemas de big data, no contexto de um modelo conceitual geral de big data; fornecer uma referência técnica para departamentos governamentais, agências e outros consumidores para entender, discutir, categorizar e comparar soluções de big data; e facilitar a análise de padrões candidatos para interoperabilidade, portabilidade, reutilização e extensibilidade. Nela, há uma parte de governança de dados, além de prover uma linguagem comum com stakeholders. É importante salientar que a norma atende para Big Data, porém, em algumas partes, pode ser extensível par ao uso de IA e, além disso, os especialistas podem ajudar a replicar as melhores práticas de Big Data para IA. Por isso, como as normas técnicas destacadas atendem parcialmente o problema, os especialistas são fundamentais para que essa transição e aproveitamento da norma seja viável.

Complementarmente, a norma Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations (ISO/IEC FDIS 38507 – Estágio 50.20), que está em desenvolvimento, também pode ajudar o problema, porque fornece orientação para membros do corpo diretivo de uma organização para habilitar e governar o uso de IA, a fim de garantir seu uso seguro dentro da organização. A norma exemplifica o uso de IA em organizações. Esses casos podem servir de modelo para integração das diferentes aplicações. Portanto, o somatório de normas técnicas atende parcialmente o problema, uma vez que as normas técnicas de IA não propiciam uma visão integrada das soluções em um nível mais operacional. Por exemplo, a norma de governança fornece uma visão de alto nível da solução, e o framework mostra um pouco como flui os dados, porém em uma visão mais interna da situação. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de integração e comunicação para a troca de dados			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	Estágio 40.60	Incluir normas que propiciem uma visão integrada de IA analisando os níveis estratégicos e operacionais
ISO/IEC 20547-3:2020	Information technology — Big data reference architecture — Part 3: Reference architecture	Estágio 60.0	
ISO/IEC FDIS 38507	Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations	Estágio 50.20	

4.4 Falta de entendimento entre as áreas de negócio e de tecnologia da informação (8 – 5°*)

No workshop, os especialistas discutiram sobre a falta de entendimento entre as áreas de negócio e de tecnologia da informação (TI) para o desenvolvimento de projetos de IA e como será montada a estratégia da análise dos dados e do desenvolvimento de algoritmos com base nos inputs da área de negócios e do conhecimento técnico e gerencial da área de TI. Ademais, apesar do grande potencial das tecnologias de IA para a resolução de problemas, ainda existem questões envolvidas no uso prático e falta de conhecimento no que diz respeito ao uso da IA de forma estratégica, a fim de criar valor de negócio[7]. Conforme o MIT Sloan, as iniciativas de IA e Estratégia de Negócios exploram o uso crescente de IA no cenário de negócios, propiciando, assim, melhores resultados operacionais. É importante entender isso, porque a exploração examina especificamente como a IA está afetando o desenvolvimento e a execução da estratégia nas organizações, tornando-se, assim, uma tecnologia estratégica para as empresas[8].

Para facilitar o entendimento sobre os objetivos do que deve ser feito e a comunicação assertiva entre a equipe de TI e as demais áreas da empresa, alguns

autores recomendam a adoção de AIOps (Inteligência Artificial para Operações de TI), que permite às equipes de TI um gerenciamento completo de performance, maior eficiência no controle de negócios automatizados, correção automática de processos e autocorreção de falhas de rede[9]. O uso de AIOps também permite automatizar a comunicação das responsabilidades e empacotar dados importantes para a equipe de operações de TI[10], já que muitas vezes há dúvidas sobre as informações necessárias para o bom funcionamento da área de TI.

Em um lado mais estratégico, há a norma de Tecnologia da informação — Governança da TI — Implicações de governança do uso de inteligência artificial por organizações (ISO/IEC FDIS 38507 – Estágio 50.20) que ainda está em desenvolvimento. Como a norma está em desenvolvimento, os especialistas podem também discutir sobre o tema e trazer os principais conceitos para normas brasileiras ou criar uma norma com base nas necessidades locais que também foi destacada na Seção 4.3. Além dessa norma, há outra norma que está em desenvolvimento, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML (ISO/IEC DIS 23053 – Estágio 40.60), que é aplicável a todos os tipos e tamanhos de empresas. A norma atende parcialmente o problema destacado, porque consegue que as empresas sigam o framework, o que pode facilitar a comunicação entre os stakeholders. Por causa disso, se os stakeholders conhecem e seguem o framework fica mais fácil de consolidar as informações e traçar os objetivos, alinhando as expectativas e promovendo o uso de soluções de IA de longo prazo.

Há também uma terceira norma que pode ajudar nesse problema: Information Technology — Artificial intelligence — Management system (ISO/IEC CD 42001 – Estágio 30.60), que está em desenvolvimento. A norma tem como foco principal o sistema de gestão para IA e pode atender ao problema pois fornece às empresas um recurso para transmitir as informações aos setores necessários por meio de um sistema de gestão. No entanto, como foca em gestão, é importante que as empresas tenham uma visão mais abrangente que pode ser da norma de governança (ISO/IEC FDIS 38507 – Estágio 50.20).

Com base nessa perspectiva, as empresas precisam utilizar sistemas de gestão, porém, se elas tiverem um framework padrão, elas conseguem ter uma visão de como a adoção de tecnologia pode ocorrer de forma positiva nas empresas. No entanto, sugere-se que os especialistas discutam sobre o tema, porque a criação de diretrizes para facilitar o entendimento para as empresas conseguirem os melhores resultados possíveis. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de entendimento entre as áreas de negócio e de tecnologia da informação			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	Estágio 40.60	Incluir normas que englobem a criação de diretrizese frameworks para ajudar as empresas em relação a tópicos de TI e IA
ISO/IEC 20547-3:2020	Information technology — Big data reference architecture — Part 3: Reference architecture	Estágio 60.0	
ISO/IEC FDIS 38507	Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations	Estágio 50.20	

4.5 Falta de um padrão claro sobre o processamento das informações (8– 5°*)

Conforme os especialistas que estavam presentes no workshop, as empresas sofrem com a falta de um padrão claro de como e onde devem ser feitos os processamentos das informações. Por exemplo, se as empresas farão processamento de IA localmente ou terceirizando as operações com alguma empresa externa, ou se o processamento será feito na nuvem ou não. Com base nesses aspectos, os especialistas acreditam na necessidade de estabelecer padrões de processamento de IA de forma segura. Ademais, a necessidade de desenvolvimento de melhores práticas e definição de arquitetura de processamento (Edge, OnPrem, Cloud) na coleta, armazenamento, treinamento dos algoritmos e processo de inferência. Os algoritmos de IA podem ser processados localmente, diretamente no dispositivo ou no servidor próximo ao dispositivo[11].

Além disso, embora a IA tenha começado muito antes da computação em nuvem, a computação em nuvem e suas tecnologias melhoraram muito a IA[12]. Dessa forma, existem várias soluções de computação em nuvem que se destacam no contexto da IA[13]:

- IaaS (Infraestrutura como serviço) ajudou o uso de IA a ter um ambiente de infraestrutura - CPU, memória, disco, red – com intuito de diminuir espera por uma equipe de infraestrutura para prepará-lo;

- PaaS (Platform as a Service) promoveu a utilização de serviços de ciência de dados, incluindo notebooks jupyter, serviços de catálogo de dados para desenvolver aplicativos de nova geração com facilidade, rapidez e segurança;
- SaaS (Software as a Service) ajudou os usuários a consumir serviços de IA em um aplicativo, por exemplo, CRM, aplicativos de pagamento mais eficientes.

Dessa forma, existem várias soluções que propiciam o uso de IA. Mais especificamente em relação a aspectos de processamento de informações, os grandes volumes de dados que precisam ser processados na indústria hoje certamente são um dos grandes desafios enfrentados na adoção da Indústria 4.0. Segundo a IBM[14], cerca de 80% deles não são estruturados, ou seja, não podem ser analisados por algoritmos tradicionais. Com isso, a adoção de algoritmos de deep learning, que utilizam redes neurais para o processamento, se tornou uma solução adequada em alguns casos. Essa tecnologia é de fácil compreensão: as redes neurais são algoritmos que atravessam informações pela sua rede de neurônios, chamada de camadas, e apresenta uma saída. Se a saída for incorreta, é esperado que o algoritmo aprenda com o erro e apresente a resposta correta da próxima vez. O aprendizado das redes ocorre com os dados que são fornecidos a ela. Ou seja, esse tipo algoritmo é capaz de processar um grande volume de dados com uso de IA. Sumarizando, as fornecedoras e as próprias empresas têm dificuldades para entender onde será feito o processamento da informação e qual é o lugar que é seguro deixar a informação.

Em relação a aspectos de segurança, há a norma de Impact of security and privacy in artificial intelligence (ISO/IEC DTR 27563 – Estágio 30.20) que está sendo desenvolvida. Como o documento ainda está em desenvolvimento, o escopo ainda está sendo definido, mas a ideia geral é abordar os impactos da segurança e da privacidade na IA. O problema de segurança pode ser solucionado com essa norma, porém ainda é necessário se entender em que local será feito o processamento da informação. Além disso, é essencial destacar que o grupo de cibersegurançada ISO está desenvolvendo uma norma sobre o tema, uma vez que muitas empresas optam por contratar uma empresa de cibersegurança.

Dessa forma, eles contratam o serviço de segurança com mensalidades para se manterem protegidos. Com base nisso, é interessante pensar em normas técnicas para as fornecedoras de soluções de cibersegurança. De forma geral, uma norma que está sendo desenvolvida é Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines (ISO/IEC AWI

5259-3 – Estágio 20.00), que já foi mencionada anteriormente. Como a norma ainda está sendo desenvolvida, o escopo ainda não está consolidado, porém acredita-se que pode trazer requisitos importantes para mitigar o problema destacado por garantir a qualidade dos dados e como pode propiciar a qualidade dos processamentos.

Logo, o problema poderá ser solucionado parcialmente pela norma, pois ela aborda requisitos e diretrizes para o gerenciamento de dados, assim os colaboradores sabem onde será realizado o processamento da informação e onde ela será guardada de forma segura. Por conseguinte, a presença de especialistas é fundamental para o desenvolvimento de normas técnicas para que haja um padrão de processamento e uma melhor integração com os fornecedores de soluções tecnológicas de IA e ML que promovam esse processamento. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de um padrão claro sobre o processamento das informações

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DTR 27563	Impact of security and privacy in artificial intelligence	Estágio 30.20	Incluir nas normas um padrão de processamento e diretrizes para uma melhor integração com os fornecedores de soluções tecnológicas de IA e ML
ISO/IEC AWI 5259-3	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines	Estágio 20.00	

4.6 Necessidade de definição de requisitos mínimos para projetos de IA (11 – 4º)

Durante o workshop, foram discutidos alguns aspectos em relação ao desenvolvimento de projetos de IA. Os especialistas destacaram que os projetos de IA necessitam que requisitos mínimos sejam definidos e atendidos para o início da definição do tipo de algoritmo que será utilizado na modelagem. As empresas que buscam adotar a IA devem estar cientes dos problemas ao definir o escopo e gerenciar projetos de IA[15]. Mesmo aqueles familiarizados com a implementação de projetos de software tradicionais ainda podem enfrentar dificuldades para implementar projetos de IA devido à sua natureza única[16]. Conforme a literatura[17], a escolha do algoritmo correto está ligada à definição do problema, podendo, assim, economizar tempo e dinheiro das indústrias. Com base no debate entre stakeholders, as empresas e os fornecedores de soluções de IA precisam definir em conjunto quais são os requisitos mínimos e fundamentais necessários com o intuito de definir as necessidades da empresa e de escolher o melhor algoritmo que atenda a essas necessidades.

Uma das normas técnicas já publicadas, Information technology — Artificial intelligence (AI) — Use cases (ISO/IEC TR 24030:2021 – Estágio 90.92) fornece uma coleção de casos de uso representativos de aplicativos de IA em uma variedade de domínios. É importante ressaltar que essa norma está em processo de revisão, logo os especialistas podem ajudar a desenvolver uma norma mais robusta com estudos de casos que contemplem os requisitos mínimos. Com o documento, as empresas podem ver quais algoritmos foram aplicados em determinadas situações e comparar com o que está sendo utilizado no seu contexto. Nesse sentido, é importante ressaltar que a EBIA também fornece casos de uso sobre o IA de forma resumida. Nela, são apresentados casos de uso em logística, transporte, serviços financeiros, serviços profissionais (por exemplo, advogados, engenheiros, arquitetos), assistência virtual, marketing, agricultura e assistência médica. Nos workshops, também foram ressaltadas as áreas de agricultura e saúde. Por isso, os especialistas podem discutir os casos de uso presentes na norma ISO/IEC TR 24030:2021 e na EBIA para conseguirem definir os requisitos mínimos do projeto.

Há outras normas técnicas em desenvolvimento que também podem ajudar a minimizar os efeitos. Entre elas, destaca-se a norma Information Technology — Artificial Intelligence — Guidelines for AI applications (ISO/IEC AWI 5339 – Estágio 20.00). Como a norma ainda está em desenvolvimento, com a ajuda de especialistas, ela poderia abranger diversos tipos de orientações, inclusive alguma parte de orientações para algoritmos, visto que falta esta orientação. Ainda, uma terceira norma já foi publicada, Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence (ISO/IEC TR 24028:2020 – Estágio 60.60), examina

tópicos relacionados à confiabilidade em sistemas de IA incluindo abordagens para estabelecer confiança em sistemas de IA por meio de transparência, explicabilidade e controlabilidade. A norma contempla o problema apresentado, uma vez que aborda não apenas a questão da confiança, mas também os requisitos de transparência e controlabilidade que refletem os requisitos mínimos e necessários para definir o algoritmo mais adequado para cada empresa. Além disso, a norma traz diversos desafios em relação a IA sobre especificações de sistema de IA, implementação de sistema de IA e uso de sistema de IA.

Portanto, mesmo que existam normas técnicas que abordam o assunto, é necessária a discussão com especialistas sobre o desenvolvimento de projetos de IA, visto que, em diversas situações, é de difícil implementação e é necessário desenvolver uma equipe multidisciplinar. A discussão sobre o problema deve ser realizada para que se tenha a melhor solução possível e que os especialistas discutam o problema em relação à IA. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Necessidade de definição de requisitos mínimos de projetos de IA

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC TR 24030:2021	Information technology — Artificial intelligence (AI) — Use cases	Estágio 90.92	Incluir normas sobre o desenvolvimento de projetos de IA
ISO/IEC AWI 5339	Information Technology — Artificial Intelligence — Guidelines for AI applications	Estágio 20.00	
ISO/IEC TR 24028:2020	Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence	Estágio 60.60	

4.7 Necessidade de requisitos mínimos para a qualidade de algoritmos de IA (7 – 6º)

Na realização do workshop, os especialistas relataram que os algoritmos de IA precisam ter um mínimo de qualidade para que eles possam entrar no mercado, porém existem diversas métricas e padrões que podem ser utilizados. Dessa forma, os algoritmos de IA precisam ser testados para a sua validação. Por exemplo, os especialistas comentaram da necessidade de suíte de testes para autenticar algoritmos de IA para testar de integração de aplicação e a necessidade de simuladores para a validação e aplicação de IA. Ou seja, a necessidade de criação de Sandboxes.

O AI Sandbox é o hardware, software, dados, ferramentas, interfaces e políticas de desenvolvimento necessários para iniciar uma prática empresarial de aprendizado profundo[18]. Há muitos esforços por parte da União Europeia de criar uma métrica padrão para a regulação de algoritmos, especialmente para Inteligências Artificiais que trabalham com dados e informações sigilosas. Um estudo da Universidade de Cambridge[19] analisou o uso de Sandbox e de apenas regras de responsabilização para validação dos algoritmos. Segundo os autores, o uso de um Sandbox permite que haja um equilíbrio entre a proteção e regulamentação de dados e o fomento de inovações tecnológicas nas áreas, já que os avanços acontecem de maneira muito rápida. Além disso, no EBIA, há uma ação estratégica em relação a criar um sandbox regulatório no Brasil relacionado sistemas de IA em segurança pública, o item destaca o seguinte: “implementar um sandbox regulatório da privacidade e proteção de dados para sistemas de IA voltados para a segurança pública.” Considerando esses aspectos, além de ser importante para as empresas, os sandboxes são essenciais para o governo também, logo é importante que tanto as empresas quanto o governo invistam nesse sentido para conseguirem desenvolver as soluções de IA alinhadas a suas necessidades.

Além da criação desses dois ambientes (suíte de testes e sandboxes) que facilitam o desenvolvimento de algoritmos de IA com a qualidade necessária, os especialistas relataram a necessidade de elaboração de um método padrão para avaliação de qualidade mínima da IA resultante por aplicação, visto que existem diversas técnicas e não há uma métrica padrão. Desse modo, não há como definir a melhor solução, o que pode acarretar o aumento de ofertas de soluções de baixa qualidade e dificulta a escolha do cliente.

De forma geral, em diversos projetos, as fornecedoras de soluções de IA precisam garantir a qualidade mínima no uso do seu algoritmo. Como existem diversas técnicas, métricas e padrões ainda não estão bem definidos, e os especialistas salientaram a falta simuladores para validar a aplicação de IA em diversos contextos, as fornecedoras possuem dificuldade na construção de soluções com o melhor custo-benefício para os clientes. Por exemplo, existem algumas fornecedoras

que encontram soluções de IA com um ótimo custo-benefício para pequenas e médias empresas com o uso de IoT e de fácil implementação para gestão da manutenção. No entanto, em caso de grandes empresas, às vezes, os projetos são complexos e podem levar um ano para ser implementado. Dessa forma, com o auxílio das normas, os projetos de IA podem ser implementados com maior facilidade.

No que tange à normalização, existem normas técnicas em processo de desenvolvimento. Por exemplo, como já fora explicado acima, o Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC DIS 23053 – Estágio 40.60) estabelece uma estrutura de Inteligência Artificial (IA) e Aprendizado de Máquina (ML) para descrever um sistema de AI genérico usando a tecnologia de ML. Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos que estão implementando ou usando sistemas de IA. A norma aborda parcialmente o problema analisado, porque explora, de uma forma geral, os diversos tipos de abordagens, pipelines, modelos de avaliações e uso das tecnologias.

Como os modelos de avalições são importantes, a norma auxilia nesse sentido. Outra norma que está em desenvolvimento e pode ajudar nesse problema é a Artificial intelligence — Quality evaluation guidelines for AI systems (ISO/IEC AWI TS 5471 – Estágio 20.00). A norma pode atender o problema no futuro, pois estabelece métricas para a avaliação dos sistemas que poderão ser utilizadas pelas empresas fornecedoras para avaliar se os projetos atendem aos requisitos mínimos de qualidade. Com essas duas normas técnicas, é possível ter uma visão geral dos requisitos mínimos. Entretanto, é importante os especialistas discutirem sobre os simuladores de IA para garantir a qualidade e o desenvolvimento de Sandboxes. Além disso, como as duas normas técnicas estão em desenvolvimento, não se pode ter certeza de como as indústrias e as fornecedoras de soluções de IA podem aplicar. Sendo assim, é uma boa oportunidade de discussão.

Além dessas duas normas, existe outra que está sendo desenvolvida, Information Technology — Artificial Intelligence — Guidelines for AI applications (ISO/IEC AWI 5339 - Estágio 20.00) que poderá ajudar na solução do problema destacado. Como a norma ainda está em desenvolvimento, o escopo ainda não está bem definido. Os especialistas podem ajudar a incluir requisitos mínimos na norma para o desenvolvimento de soluções de IA. Como o documento fornecerá orientações, ele pode trazer também alguma parte de orientações de algoritmos e da criação de ambientes de teste e sandbox. Sendo assim, é um problema que deve ser debatido junto a um grupo de especialistas para que sejam desenvolvidas novas apropriadas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado

pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Necessidade de requisitos mínimos para a qualidade de algoritmos de IA			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)	Estágio 40.60	Incluir requisitos mínimos de qualidade de algoritmos para o desenvolvi-mento de soluções de IA
ISO/IEC AWI TS 5471	Artificial intelligence — Quality evaluation guidelines for AI systems	Estágio 20.0	
ISO/IEC AWI 5339	Information Technology — Artificial Intelligence — Guidelines for AI applications	Estágio 20.00	

4.8 Falta de padronização de ferramentas, melhores práticas e frameworks para algoritmos (6 – 7º*)

No workshop, os especialistas discutiram problemas relacionados à falta de padronização de ferramentas, melhores práticas e frameworks que podem ser utilizados no desenvolvimento de algoritmos de IA. De forma geral, durante a dinâmica proposta, os especialistas relataram a necessidade de elaboração de melhores práticas e frameworks baseados na aplicação e a dificuldade na padronização de ferramentas utilizadas na IA e na padronização dos algoritmos de IA.

Conforme o Google[20], sistemas confiáveis e eficazes de IA centrados no usuário devem ser projetados de acordo com as práticas recomendadas gerais para sistemas de software, juntamente com práticas que abordem considerações exclusivas do aprendizado de máquina. O Google destaca algumas melhores práticas que podem ser abordadas, por exemplo: utilizar um design centrado no usuário; identificar diversas métricas para treinamento e monitoramento; examinar

o dado, quando possível; entender as limitações dos dados e do modelo; testar; continuar atualizando e monitorando o sistema.

Além disso, as empresas têm acumulado grandes quantidades de dados, e, portanto, aumentam a necessidade de tecnologias para analisar e aproveitar esses dados. É por isso que IA torna-se uma ótima solução[21]. De forma geral, um framework de IA permite a criação mais fácil e rápida de aplicativos de IA[22], porém existem diversos no mercado e, muitas vezes, as indústrias não os conhecem e as fornecedoras de soluções de IA também não. Como existem diversos frameworks, as indústrias e fornecedoras de soluções de IA devem pensar qual está mais alinhado a necessidades, e o desenvolvimento de normas técnicas com a ajuda de especialistas podem auxiliar na escolha do framework correto para determinada situação.

Complementarmente, de acordo com a EBIA publicada em 2021[23], o Ministério de Ciência, Tecnologia e Inovação (MCTI) em parceria com outras entidades também ligadas ao uso e desenvolvimento de IA já estão trabalhando no desenvolvimento de frameworks seguros e guias para o uso padronizado de ferramentas. O objetivo do MCTI é que os frameworks sejam construídos com base em modelos já consolidados internacionalmente. Além disso, há a intenção de publicar um guia de autoavaliação para as entidades que utilizam algum tipo de IA, o que deve auxiliar na adoção de melhores práticas.

Consequentemente, considerando esses aspectos, as fornecedoras de soluções de IA têm dificuldades em relação a diversos aspectos do desenvolvimento do algoritmo de IA. Entre eles, destacam-se a necessidade de utilizar frameworks e melhores práticas para melhorar o uso do algoritmo; definir os limites de utilização do algoritmo e padronização do uso dos algoritmos.

No que tange à normalização, a Artificial intelligence — Quality evaluation guidelines for AI systems (ISO/IEC AWI TS 5471 – Estágio 20.00) está sendo desenvolvida e pode solucionar parcialmente o problema, pois os especialistas podem estabelecer diretrizes para a avaliação dos sistemas de IA com base em requisitos mínimos dos algoritmos e quais são os melhores algoritmos a serem utilizados em determinado contexto. Estas diretrizes podem ser utilizadas pelas fornecedoras de solução em IA para verificar qual o algoritmo mais adequado.

Há também outras normas técnicas que estão em desenvolvimento, como a série Artificial intelligence — Data quality for analytics and machine learning (ML) (ISO/IEC AWI 5259-1 – Estágio 20.00). A série, como um todo, analisa a qualidade dos

Problema: Falta de padronização de ferramentas, melhores práticas e frameworks para algoritmos			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWI TS 5471	Artificial intelligence — Quality evaluation guidelines for AI systems	Estágio 20.00	Incluir normas com melhores práticas, diretrizes e frameworks para o desenvol-vimento de algoritmos de IA
ISO/IEC AWI 5259-1	Artificial intelligence — Data quality for analytics and machine learning (ML)	Estágio 20.00	

4.9 Falta de uma clareza de como os algoritmos podem ser utilizados por temas diferentes (3 – 8°)

Os especialistas relataram que as fornecedoras de IA e as empresas têm dificuldade em saber qual algoritmo utilizar e quando. Por exemplo, eles destacaram que tem problemas semelhantes em relação aos algoritmos serem utilizados na área de manutenção, na agricultura e na saúde (Inteligência Artificial para diagnóstico por imagem). Dessa forma, é possível aplicar o mesmo algoritmo em dados de diferentes áreas. Por exemplo, estudos exploram o uso de algoritmo para gestão de estoque e logística como o uso de veículos autônomos em centros de distribuição[24]. Ainda, em sistemas mais complexos, a IA pode ser utilizada para preços em tempo real e leilão reverso envolvendo parceiros da cadeia de suprimentos[25]. Além disso, Zhao et al.[26] desenvolveram um sistema de decisão de energia eólica baseado na otimização de inteligência artificial, que inclui dois módulos: avaliação da energia eólica e previsão da velocidade do vento.

Outros pesquisadores utilizaram IA para detecção de tráfego rodoviário, auxiliando no desenvolvimento de sistemas de vigilância de tráfego[27]. Além disso, na literatura atual é possível encontrar

artigos que relatam diversos usos para os algoritmos de IA, e como foi feita sua aplicação. Entre os principais, destaca-se[28]: problemas de otimização, problemas numéricos e de escalonamento de trabalho. Em relação às indústrias, a aplicação de algoritmos para Aprendizado de Máquina é bastante comum, sendo utilizados principalmente para predição e classificação de problemas. Outro uso comum é para aspectos particulares dos sistemas de aprendizagem, como criação de redes neurais e sensores para robôs. No âmbito da economia, a predição de mercados emergentes e o desenvolvimento de estratégias para lances são alguns exemplos de aplicação. Além disso, a EBIA apresenta o eixo vertical de aplicação nos setores produtivos. Por exemplo, destacam-se o uso da IA na medicina para automatizar exames, realizar análises patológicas e utilizar drones para entrega de medicamentos. Logo, percebe-se que a IA pode ser utilizada nas mais diferentes áreas.

A norma já publicada que atende ao tema é Information technology — Artificial intelligence (AI) — Use cases (ISO/IEC TR 24030:2021 – Estágio 90.92), que fornece uma coleção de casos de uso representativos de aplicativos de IA em uma variedade de domínios. Os estudos de caso são os mais diversos, sendo aplicados em agricultura, marketing digital, educação, energia, saúde, logística e manufatura, por exemplo. Portanto, tanto as empresas quanto as fornecedoras de soluções de IA podem ter uma visão geral de casos, porque a norma ilustra a aplicabilidade do trabalho de padronização de IA em uma variedade de domínios de aplicação; aborda o compartilhamento dos casos de uso coletados em apoio ao trabalho de padronização de IA com organizações externas e entidades internas para promover a colaboração; investiga casos de uso, se possível, encontra os novos requisitos técnicos (demanda padronizada) do mercado, acelerando a transformação das conquistas científicas e tecnológicas. Com base nessas questões, a norma pode alcançar novos interessados na aplicabilidade da IA, ampliando, assim, a sua atuação. A norma Artificial intelligence (AI) — Overview of computational approaches for AI systems (ISO/IEC TR 24372:2021 – Estágio 60.60), que foi publicada em 2021, fornece uma visão geral do estado da arte das abordagens computacionais para sistemas de IA, descrevendo: a) as principais características computacionais dos sistemas de IA; b) principais algoritmos e abordagens utilizadas em sistemas de IA, referenciando casos de uso contidos na ISO / IEC TR 24030, que foi citada anteriormente e também publicada em 2021. Com base nessa norma, é possível que as empresas e as fornecedoras de soluções de IA busquem novos algoritmos que podem ser utilizados em contextos diversos.

Além das duas normas técnicas já publicadas, há também outra norma que está em desenvolvimento, Information Technology — Artificial Intelligence — Guidelines for AI applications (ISO/IEC AWI 5339 – Estágio 20.00). Como o escopo ainda não está bem definido, acredita-se

Problema: Falta de uma clareza de como os algoritmos podem ser utilizados por temas diferentes			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC TR 24030:2021	Information technology — Artificial intelligence (AI) — Use cases	Estágio 90.92	Incluir normas sobre diretrizes e frameworks que abordem o uso de algoritmos de IA em temas específicos para disseminar o conhecimento
ISO/IEC TR 24372:2021	Artificial intelligence (AI) — Overview of computational approaches for AI systems	Estágio 60.60	
ISO/IEC AWI 5339	Information Technology — Artificial Intelligence — Guidelines for AI applications	Estágio 20.00	

4.10 Falta de um entendimento dos modelos de IA e da base estatística (2– 9°*)

Durante o workshop, os especialistas relataram dificuldades em relação ao entendimento dos modelos de IA e da base estatística para se realizar a comparação entre os modelos de IA e entreos modelos de IA e outros modelos, como os modelos de Pesquisa Operacional (PO). Por exemplo, as fornecedoras de soluções tecnológicas sentem dificuldade para comparar os modelos. Os especialistas debateram sobre alguns problemas interessantes, como determinação de metodologias de comparação de modelos inteligentes e modelos de meta-heurística. Conforme Sucupira[29], "as meta-heurísticas são estruturas algorítmicas gerais adaptáveis a diversos problemas de otimização". Por exemplo, o modelo colônia de formigas (Ant Colony Optimizatiom - ALO) baseia-se no comportamento das formigas que desejam encontrar uma fonte de alimento. [30] Esse algoritmo está sendo utilizado para encontrar melhores rotas de transporte público em grandes cidades. No entanto, estudo de IA também podem trazer inúmeros benefícios para esse tipo de modelagem como o uso de redes neurais artificiais (RNA) para computar todos os caminhos possíveis entre uma parada e outras paradas antes determinar o caminho ideal[31]. Portanto,

tanto o ALO e RNA podem ser utilizados para a determinação do caminho ideal, como existem diversas possibilidades de algoritmos e métodos de serem utilizados, os especialistas relatam problemas em relação a essa questão. Por isso, as fornecedoras de solução de IA buscam normas nesse sentido, porque sofrem com dificuldades em relação a comparar os modelos utilizados a fim de verificar qual é o mais adequado, o que inclui aspectos de potência estatística, tipo de dados e o tipo de modelo.

A escolha das métricas de desempenho para a comparação dos modelos também pode ser uma tarefa difícil para as empresas e fornecedoras de tecnologia já que atualmente não há um padrão para escolha. Muitos dos métodos de comparação apresentados na literatura atual utilizam a avaliação de erros para chegar à uma conclusão[32]. Os erros de previsão equivalem a diferença entre a resposta correta e resposta incorreta apresentada pela IA. Entre os mais citados, destacam-se: MSE (Mean Squared Error) e MAPE (Mean Absolute Percentual Error). Ambos os métodos utilizam ambientes computacionais, como o MatLab, Python, R para calcular os resultados.

No que concerne às normas técnicas de IA, no contexto das redes neurais, há uma norma publicada Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview (ISO/IEC TR 24029-1:2021 – Estágio 60.60) que fornece informações básicas sobre os métodos existentes para avaliar a robustez das redes neurais. Como o poder estatístico dos modelos é um problema relatado pelos especialistas em relação à escolha do modelo, a norma aborda métricas de robustez disponíveis usando métodos estatísticos e usa métodos estatísticos para medir a robustez de uma rede neural. Entretanto, a norma aborda o tema direcionado a redes neurais, seria necessário ter para outros tipos de modelos para permitir a comparação entre os modelos, porque a norma soluciona parcialmente o problema evidenciado.

Existem outras normas técnicas que estão em desenvolvimento, como a Artificial intelligence — Quality evaluation guidelines for AI systems (ISO/IEC AWI TS 5471 - Estágio 20.00). Como a norma está em desenvolvimento, entende-se que o escopo seria o estabelecimento de orientações a fim de avaliar a qualidade dos sistemas que utilizam IA em diversos contextos. A norma poderá solucionar de forma parcial o problema pois estabelecerá diretrizes para a avaliação dos sistemas de IA e poderá promover comparações entre os diferentes modelos estabelecidos. Essas diretrizes podem ser utilizadas pelas fornecedoras de solução de IA para verificar qual o algoritmo mais adequado. Com base na análise das normas técnicas publicadas e em desenvolvimento, é possível perceber que os especialistas podem discutir muito sobre a falta de entendimento dos modelos de IA e da base estatística, mas existem já normas técnicas para eles se basearem.

A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de um entendimento dos modelos de IA e da base estatística			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC TR 24029-1:2021	Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview	Estágio 60.60	Incluir nas normas diretrizes, frameworks e/ou checklists sobre modelos de IA e a base estatísticas para IA
ISO/IEC AWI TS 5471	Artificial intelligence — Quality evaluation guidelines for AI systems	Estágio 20.00	

4.11 Falta de entendimento de como utilizar os algoritmos de IA para criar pesquisas alinhadas com as necessidades da academia e das empresas (2 – 9º*)

Os especialistas destacaram que a academia tem dificuldade em direcionar as boas práticas para artigos de IA sobre diversos temas, visto que é uma nova metodologia sendo criada e utilizada em pesquisas acadêmicas de relevância internacional. Dessa forma, os especialistas buscam, através de normas técnicas, a elaboração de boas práticas para o desenvolvimento de bons resultados de artigos de pesquisa. Alguns autores exploram que há uma série de práticas recomendadas que todas as organizações devem se esforçar para implementar a fim de obter um retorno positivo do investimento em IA e ML[33]. Mesmo que essas boas práticas sejam com foco nas empresas, estas também podem ser exploradas na literatura para o desenvolvimento de novos artigos com base em IA.

Por exemplo[34], investimento no conhecimento de domínio necessário para analisar dados adequadamente em áreas altamente especializadas; utilização de apenas dados de qualidade para treinamento de modelos; utilização de uma metodologia padrão para o planejamento do ciclo de vida dos dados; utilização de um sistema de gerenciamento de modelo; etc. Por exemplo, outros artigos realizaram uma revisão sistemática da literatura baseada em ML de 4.973 artigos com intuito de analisar oportunidades futuras dos modelos de indústria 4.0[35]. Os pesquisadores precisam entender como e onde utilizar o mesmo método com intuito de gerar novas pesquisas sobre o tema.

Complementarmente, muitas tentativas têm sido feitas com o intuito de direcionar o uso e a pesquisa de IA não somente no Brasil, mas no mundo. Em 2019, dois projetos de lei foram encaminhados com a intenção de estabelecer princípios para o uso de IA no Brasil, no entanto a proposta não define o que será deverá ser considerado como IA, já que não existe uma definição universal deste conceito. No que tange às pesquisas sobre IA, autores dizem que é difícil estabelecer cenários regulatórios e boas práticas pois a visibilidade da infraestrutura da IA é muitas vezes limitada[36]. A EBIA apresenta como um dos eixos vertical "Pesquisa, Desenvolvimento, Inovação e Empreendedorismo". Destacam-se algumas ações prioritárias: "Ampliar as possibilidades de pesquisa, desenvolvimento, inovação e aplicação de IA, por meio da viabilização do aporte de recursos específicos para esse tema e da coordenação entre iniciativas já existentes." e "Estabelecer conexões e parcerias entre setor público, setor privado e instituições científicas e universidades em prol do avanço no desenvolvimento e utilização da IA no Brasil."

Portanto, é necessário um investimento em pesquisa no país e, por isso, é tão importante que os atores da triple hélice interajam para esse fim. Considerando esses aspectos, os responsáveis pela tecnologia podem fazer parte de organizações diferentes (governo, academia, empresas) ou residirem em diferentes países. No entanto, estes comportamentos também são vistos em outras tecnologias mais amplamente difundidas, que podem servir de base para a elaboração de um guia de boas práticas. Sumarizando, a partir dessa perspectiva, é possível observar que os especialistas esperam que seja possível entender, com base nas normas técnicas e nas regulações, quando utilizar uma revisão sistemática baseada em ML ou quando não usar e quais são as melhores práticas que acadêmicos e empresas podem utilizar para conseguir explorar os benefícios do uso da IA.

Outrossim, em relação a normas técnicas que podem solucionar o problema destacado, a norma em desenvolvimento Information Technology — Artificial Intelligence — Guidelines for AI applications (ISO/IEC AWI 5339 – Estágio 20.00) ainda não tem um escopo tão definido, porém pretende estabelecer diretrizes

para a aplicação de Inteligência Artificial (IA) em diversos casos. Dessa forma, a norma terá como assunto principal as diretrizes para a aplicação da tecnologia de IA que podem ser no mundo acadêmico ou empresarial, dependendo da necessidade. Isso se relaciona parcialmente com o problema na medida em que essas diretrizes podem servir de base para a academia e para as empresas estabelecerem as boas práticas e os pontos necessários para alinhadas as necessidades e o desenvolvimento de algoritmos de IA robustos suficientes para serem utilizados como método de artigos internacionais, por exemplo. Além disso, principalmente, em relação quais são os algoritmos que podem ser utilizados dependendo do contexto acadêmico e/ou empresarial.

Complementarmente, como integrar o uso de outros métodos acadêmicos com IA e ML, por exemplo, se é possível utilizar um estudo de caso mais uma análise de conteúdo com ML. Consequentemente, ainda há muito o que ser explorado pelos especialistas sobre esse problema nos grupos de discussão sobre IA em pesquisas acadêmicas e empresas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de entendimento de como utilizar os algoritmos de IA para criar pesquisas

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWI 5339	Information Technology — Artificial Intelligence — Guidelines for AI applications	Estágio 20.00	Incluir nas normas diretrizes de como algoritmos de IA podem alinhar as necessidades da academia e empresas em relação a soluções de IA

4.12 Falta de um padrão mínimo de segurança em IA (22 – 1º)

Durante os workshops, os especialistas discutiram sobre a falta de um padrão mínimo de segurança que precisa ser mantido para o desenvolvimento de soluções de IA e que a segurança se mantenha no padrão pré-estabelecido, o que também está relacionado ao workshop e ao grupo prioritário de cibersegurança. Por isso, algumas empresas contratam mensalmente serviços de cibersegurança para se manterem seguranças, porém há, em alguns casos, algumas dificuldades. Entre elas, os especialistas destacaram os seguintes: dificuldade em estabelecer definições e um mínimo de segurança na implementação de modelos de IA em empresas; necessidade de conformidade com requisitos globais de privacidade, entre eles, destaca-se a LGPD; dificuldade em relação à padronização da segurança de dados; necessidade de criação de políticas de cibersegurança.

Além desses aspectos destacados pelos especialistas, há outros problemas, conhecido também por AI Safety. Por exemplo, o risco de falhas no sistema causando danos significativos aumenta à medida que o ML se torna mais amplamente usado, especialmente em áreas onde a proteção e a segurança são críticas[37]. Para mitigar esse risco, a pesquisa em "AI Safety" busca identificar as causas potenciais de comportamento não intencional em sistemas de aprendizado de máquina e desenvolver ferramentas para reduzir a probabilidade de tal comportamento ocorrer[38].

Dessa maneira, considerando esses aspectos analisados, as fornecedoras de soluções de IA e as próprias empresas possuem dificuldades de implementar soluções mínimas de segurança que garantam a cibersegurança e a padronização da segurança dos dados e das plataformas, bem como os mecanismos de segurança dos dados com conformidade com terceiros. Atualmente, existem diversos artigos que abordam a relação entre segurança e Inteligência Artificial, já que muitas vezes essa tecnologia é utilizada para o tratamento de dados importantes ou sigilosos. Embora não exista nenhuma ação estratégia com este foco em desenvolvimento no Ministério de Tecnologia, Ciência e Inovação (por exemplo, a EBIA tem um eixo vertical de segurança pública, mas não de cibersegurança), existem diversos sistemas capazes de contribuir para segurança de dados. O artigo Cibersegurança e Inteligência Artificial[39] aborda 16 sistemas de cibersegurança para Inteligência Artificial que podem ser utilizados na tentativa de proteção dos dados. No entanto, não existe um sistema padrão e a escolha entre eles deve levar em consideração as necessidades da empresa e os pontos altos e baixos de cada sistema.

Com base nesses aspectos, as normas técnica referentes a esse tema estão em desenvolvimento[40]: Artificial intelligence — Functional safety and AI systems (ISO/IEC AWI TR 5469 - Estágio 10.99); Information technology — Artificial intelligence — Risk management (ISO/IEC DIS 23894 - Estágio 40.00); Impact of security

and privacy in artificial intelligence (ISO/IEC DTR 27563 - Estágio 30.20). A norma ISO/IEC AWI TR 5469 é muito recente, logo seu escopo não está bem definido, porém outros Roadmaps de IA[41] confirmam que essa norma é importante de ser monitorada porque pode ajudar em relação aos seguintes itens: segurança e privacidade; ética; e segurança em sistemas de IA. Essa norma poderá solucionar parcialmente o problema pois trata da segurança nos processos que envolvem IA e pode auxiliar na criação de um padrão para o desenvolvimento de um sistema de IA funcional. Já a Information technology — Artificial intelligence — Risk management também está com o escopo em desenvolvimento e pode atender parcialmente o problema, uma vez que tratará sobre o gerenciamento de riscos e poderá ser utilizada como base para um padrão de segurança. Com base nisso, as empresas poderão gerenciar o risco de segurança e cibersegurança de IA.

Complementarmente a essas duas normas, há também a Impact of security and privacy in artificial intelligence (ISO/IEC DTR 27563 - Estágio 30.20) cujo escopo ainda está em desenvolvimento, porém abordará os impactos da segurança e da privacidade na IA. De forma geral, considerando a análise das normas técnicas supracitadas em desenvolvimento, as normas podem ser utilizadas concomitantemente para a criação do padrão de segurança, porém a presença de especialistas na área pode ajudar o aprofundamento das normas citadas e o desenvolvimento de novas normas alinhadas às necessidades das empresas.

Além disso, é importante a interação dos especialistas com o Grupo de Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27) com intuito de que as normas de segurança sejam desenvolvidas de forma sinérgica. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de um padrão mínimo de segurança em IA			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWITR 5469	Artificial intelligence — Functional safety and AI systems	Estágio 10.99	Incluir nas normas padrões de segurança mínimos em soluções de IA
ISO/IEC DIS 23894	Information technology — Artificial intelligence — Risk management	Estágio 40.00	
ISO/IEC DTR 27563	Impact of security and privacy in artificial intelligence	Estágio 30.20	

4.13 Falta de entendimento dos aspectos éticos da utilização de algoritmos de IA e do uso dos dados (6 – 7º*)

Os especialistas participantes do workshop ressaltaram que há falta de entendimento dos aspectos éticos da utilização de algoritmos de IA e do uso dos dados em diversos ambientes. Por exemplo, os especialistas citaram os seguintes problemas: a necessidade de desenvolvimento de uma padronização das questões éticas por possíveis falhas da IA e a necessidade e a importância da elaboração de requisitos regulatórios para uso de dados e a regulação ética do seu uso.

Estudos mostram que os desenvolvimentos recentes em IA, ML e robótica levantaram pre ocupações sobre as consequências éticas da pesquisa em IA nos âmbitos acadêmicos e industriais[42]. Consequentemente, os atores da triple hélice têm expressado um número crescente de perguntas sobre as consequências da IA não só sobre as pessoas, mas também sobre as consequências em grande escala no futuro do trabalho e do emprego, suas consequências sociais[43].

Além desses aspectos destacados pelos especialistas e pela literatura, a UNESCO debate sobre aumento do uso de IA em sistemas judiciais em todo o mundo, criando mais questões éticas a serem

exploradas[44]. Em algumas situações, profissionais debatem que a IA presumivelmente poderia avaliar casos e aplicar justiça de uma maneira melhor, mais rápida e eficiente do que um juiz, porém é ético utilizar o recurso para esse fim? É um assunto que precisa ser debatido e desmistificado por atores da triple hélice. Portanto, as fornecedoras de soluções de IA e as empresas sabem da relevância da ética e do uso da informação, porém possuem dificuldades em como exercer a ética, também atualmente com a vigência da LGPD. Por exemplo, a LGPD aborda o seguinte aspecto: "Art. 13.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas." Logo, além da ética na indústria, também se debate muito sobre os padrões éticos na pesquisa, o que inclui o debate da ética na IA, o que também está relacionado ao problema Falta de entendimento de como utilizar os algoritmos de IA para criar pesquisas alinhadas com as necessidades da academia e das empresas da seção 4.11.
Por exemplo, a União Europeia divulgou, em 2019, um guia com Diretrizes Éticas para a Inteligência Artificial Confiável. Entre os princípios éticos mencionados no guia europeu[45] estão a prevenção de dados, a explicabilidade, a justiça e o respeito pela autonomia humana. A explicação sobre cada um dos princípios pode ser encontrada detalhada no guia. Além disso, o guia traz exigências como robustez técnica e segurança, bem-estar ambiental e social, diversidade, não discriminação e justiça, privacidade e governança de dados e outros três. Todas estas exigências podem servir de base para indústrias regularem o uso correto da Inteligência Artificial, facilitando o exercício da ética.

De forma geral, na EBIA, um dos eixos transversais é a Legislação, regulação e uso ético da IA, logo um dos objetivos estratégicos é "Contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis." Ou seja, a EBIA está focada na criação de padrões éticos de IA, por exemplo, com a criação de comitês. Além disso, a EBIA tem uma ação ética de: Estimular a produção de IA ética financiando projetos de pesquisa que visem aplicar soluções éticas, principalmente nos campos de equidade/ não-discriminação (fairness), responsabilidade/ prestação de contas (accountability) e transparência (transparency)". Ou melhor, a EBIA aborda a importância de aspectos éticos na pesquisa, por isso o direcionamento do investimento para projetos de pesquisa nesse sentido. Além da EBIA, o Decreto nº 8.771/2016, Política de Dados Abertos do Poder Executivo Federal, destaca a importância do desenvolvimento

de diretrizes sobre como utilizar os dados abertas de forma ética. Logo, além de iniciativas no mundo, o Brasil está investindo para promover a ética em soluções de IA.

Complementarmente, em relação às normas técnicas do grupo de IA, destacaram-se duas normas em desenvolvimento: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines (ISO/IEC AWI 5259-3 – Estágio 20.00) e Information technology — Artificial intelligence — Overview of ethical and societal concerns (ISO/IEC DTR 24368 – Estágio 30.60). Como as normas técnicas estão em desenvolvimento, os seus escopos ainda não estão totalmente definidos, porém a ISO/IEC AWI 5259-3 que faz parte da série 5259 pretende expor os requisitos e as diretrizes para o gerenciamento de qualidade de dados relacionados ao uso de IA.

Dessa forma, podem entrar requisitos éticos para o desenvolvimento e o uso de IA, quais dados podem ser acessados e por quem. De forma geral, a norma em desenvolvimento atende parcialmente o problema porque estabelece diretrizes para o gerenciamento de dados provenientes da IA, podendo ser inserida uma visão crítica e ética do uso de dados. Existe outra norma em desenvolvimento que está relacionada ao problema da ética, Information technology — Artificial intelligence — Overview of ethical and societal concerns (ISO/IEC DTR 24368 - Estágio 30.60), cujo escopo poderá incluir um panorama sobre os âmbitos éticos e sociais relacionados ao uso de IA.

Com base nisso, a norma se relaciona com o problema, uma vez que analisa o uso ético e sociológico dos dados. Os especialistas podem ajudar no desenvolvimento das normas técnicas, visto que as duas normas técnicas, quando combinadas, atendem totalmente ao problema. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de entendimento dos aspectos éticos da utilização de algoritmos de IA e do uso dos dados			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWI 5259-3	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines	Estágio 20.00	Incluir nas normas um panorama em relação a aspectos éticos e sociais nas soluções de IA
ISO/IEC DTR 24368	Information technology — Artificial intelligence — Overview of ethical and societal concerns	Estágio 30.60	

4.14 Falta de conhecimento mínimo e treinamento sobre as soluções de IA (8 – 5º*)

No workshop, os especialistas participantes relataram a falta de um conhecimento mínimo e treinamento sobre as soluções de IA para garantir que o usuário final possa flexibilizar as soluções para o seu determinado interesse, independente de conhecimento prévio sobre o assunto.
Por exemplo, os especialistas citaram a importância da capacitação de colaboradores nas empresas para identificar oportunidades de uso da IA; a relevância do estabelecimento de modelos de treinamento apropriados; a necessidade de conhecimento de experiências motivadoras.

Em consonância com o que foi debatido pelos especialistas no workshop, as grandes empresas, como a Google, e grandes instituições de ensino, como Harvard, têm apontado a necessidade do treinamento em relação à AI. Por isso, a Google criou o programa "Learn With Google AI" para que todos possam aprender com experts na área[46]. No programa, é possível encontrar informações e exercícios a fim de ajudar o desenvolvimento de habilidade e projetos[47]. Já, a Harvard fornece diversos cursos online técnicos e não técnicos sobre o assunto, que podem ser aplicados em diferentes setores[48].

Além dos conhecimentos técnicos a serem desenvolvidos pelos colaboradores, em relação aoprincípio de accountability na EBIA, há uma ênfase em treinamentos: "(ii) a adoção de medidas para aumentar a conscientização interna sobre a necessidade dessa conformidade, inclusive por meio de orientações e treinamentos em toda a empresa". Mesmo que a ênfase não seja em treinamento em algoritmos, é muito importante os colaboradores treinarem e apresentarem sobre a responsabilidade de soluções de IA, visto que, para a escolha de uma solução, eles precisarão levar em consideração esses aspectos.

Além desse aspecto, um dos eixos verticais da EBIA é a Força de Trabalho e Capacitação, visto que serão e são desenvolvidas "iniciativas para capacitar a força de trabalho, em geral, que desenvolvam habilidades para o futuro do trabalho, como investimento em educação ao longo da vida e habilidades digitais." A EBIA está bem relacionada ao problema destacado no workshop. Particularmente, uma das ações estratégicas em destaque sobre força de trabalho e capacitação: "Estimular que as empresas e os órgãos públicos implementem programa de treinamento contínuo da sua força de trabalho voltado às novas tecnologias." Logo, com base nesses destaques, o treinamento dos colaboradores é um objetivo prioritário da EBIA e precisa ser discutido junto aos especialistas para que seja desenvolvidas as melhores soluções possíveis com o auxílio de normas e da literatura.

Complementarmente, no que tange à normalização internacional sobre o assunto, a primeira norma em destaque sobre o assunto é uma norma em desenvolvimento, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology (ISO/IEC DIS 22989 – Estágio 40.99), que apresenta os principais conceitos e terminologias relacionados ao uso de IA. A norma em questão é muito importante porque apresenta conceitos e vocabulários relacionados à IA podendo servir de guia para os colaboradores das empresas em treinamentos.

Dessa maneira, a norma auxilia no entendimento claro do que está sendo tratado em relação à IA e pode ajudar os colaboradores a aprimorarem seus conhecimentos sobre IA. Além da norma sobre vocabulários relacionada à IA, também há uma norma relacionada à Big Data: Information technology — Big data — Overview and vocabulary (ISO/IEC 20546:2019 – Estágio 60.60). A norma fornece um conjunto de termos e definições necessários para promover uma melhor comunicação e compreensão desta área, abrangendo uma base terminológica para padrões relacionados a big data. Além disso, a ISO/IEC 20546:2019 fornece uma visão geral conceitual do campo de big data, seu relacionamento com outras áreas técnicas e esforços de padrões e os conceitos atribuídos a big data que não são novos para big data. De forma geral, os colaboradores necessitam entender conceitos relacionados à IA e à big data para conseguirem ter uma visão geral das melhores soluções de IA.

Outrossim, a terceira norma analisada já está publicada, Information technology — Artificial intelligence (AI) — Use cases (ISO/IEC TR 24030:2021 – Estágio 90.92). A norma fornece uma coleção de casos de uso representativos de aplicativos de IA em uma variedade de aplicações em diversos setores. Como a norma aborda casos em que a IA foi utilizada para solução de problemas, esses casos podem servir como literatura de referência para as empresas, demonstrando as diferentes aplicações da tecnologia.

Logo, os colaboradores podem fazer treinamento com base nesses casos, aprendendo como utilizar a tecnologia da melhor forma possível. Conforme os aspectos destacados em relação às normas técnicas, as duas normas técnicas analisadas para o problema em questão, quando combinadas, podem trazer uma visão geral da solução do problema. Caso necessário, pode-se desenvolver uma norma relacionada aos treinamentos propriamente ditos com o apoio dos especialistas direcionados à necessidade e à demanda de mercado.

Problema: Falta de conhecimento mínimo e treinamento sobre as soluções de IA

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 22989	Information technology — Artificial intelligence — Artificial intelligence concepts and terminology	Estágio 40.99	Incluir normas que abranjam treinamentos específicos para o desenvolvimento de soluções de IA em diversos contextos.
ISO/IEC 20546:2019	Information technology — Big data — Overview and vocabulary	Estágio 60.60	
ISO/IEC TR 24030:2021	Information technology — Artificial intelligence (AI) — Use cases	Estágio 90.92	

No que tange ao grupo de Inteligência Artificial, a Figura 1 resume as principais recomendações de ações a serem avaliadas pelos especialistas a fim de que as normas sejam desenvolvidas de forma alinhada.

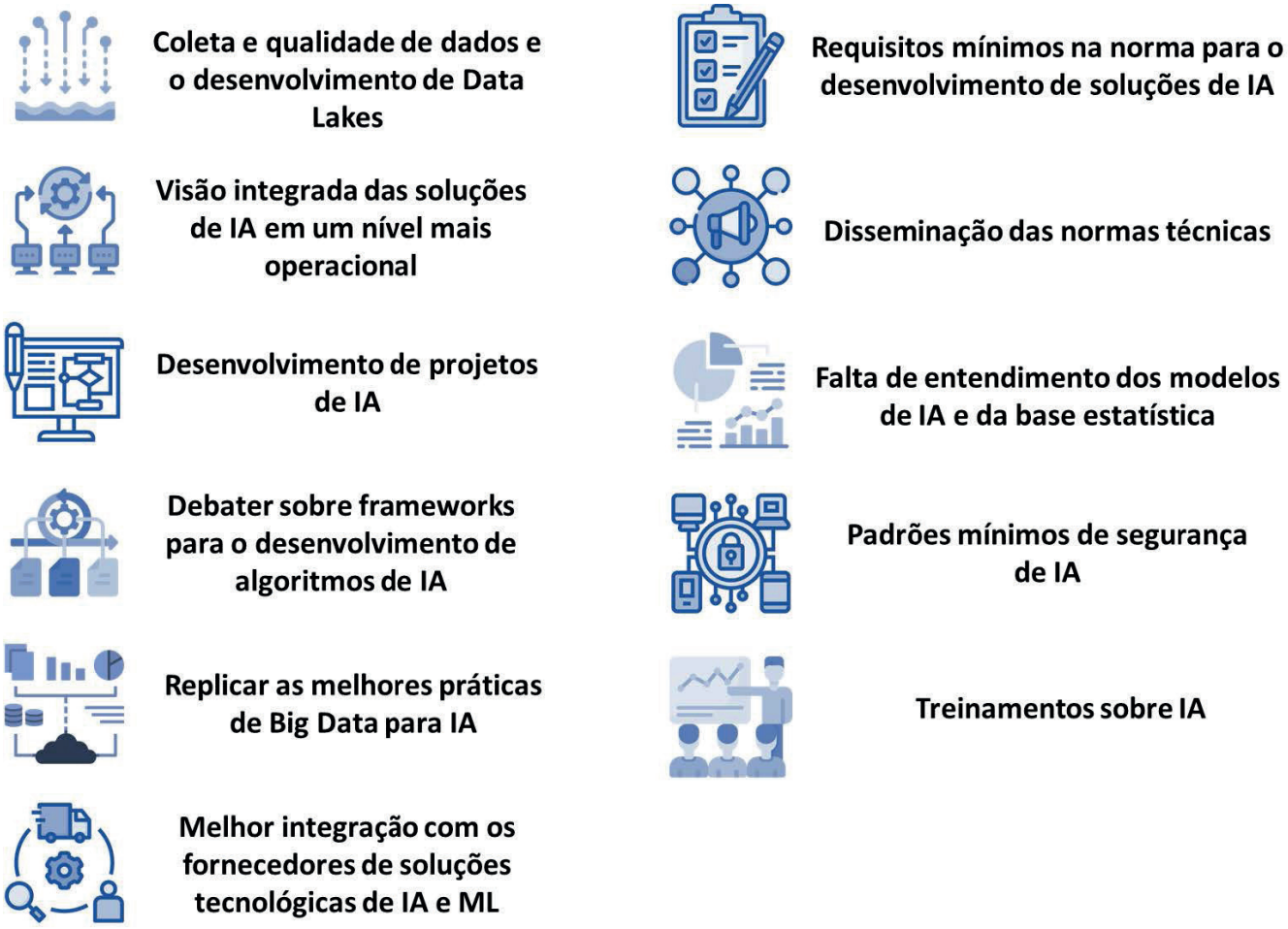

Figura 1 - Tópicos para debate entre os especialistas de IA

5 Grupo de Segurança da Informação, Cibersegurança e Proteção da Privacidade (ISO/IEC/JTC1/SC27)

5.1 Escopo

O objetivo do grupo de trabalho ISO/IEC/JTC1/SC27 é o desenvolvimento de normas técnicas para a proteção da informação e das tecnologias da informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar os aspectos de segurança e privacidade. A seguir serão detalhados os problemas referentes ao workshop de cibersegurança.

5.2 Falta de conhecimento sobre as normas de cibersegurança (18 – 1°)

No decorrer do workshop, os especialistas relataram que as indústrias sofrem com a falta de conhecimento sobre as normas técnicas de cibersegurança para a escolha das soluções tecnológicas da Indústria 4.0 que são mais adequadas aos seus contextos e como essas normas técnicas de cibersegurança podem ser aplicadas em conjunto ou, até mesmo, como as normas técnicas de cibersegurança influenciam em outras normas técnicas de adoção de tecnologias da transformação digital, por exemplo, as normas de cibersegurança aplicadas à IA. Em relação a esses aspectos, os especialistas discutiram sobre: a necessidade de ampliação do conhecimento sobre as normas técnicas, sua aplicabilidade e relacionamento com normas de áreas afins; sobre a apresentação das normas como aplicativos a fim de agilizar sua adoção e propiciar uma disseminação rápida; e sobre a inclusão de aspectos relacionados à segurança de dados a normas já utilizadas pelas indústrias.

Consequentemente, os especialistas abordaram a necessidade de facilitar o acesso a normas técnicas e de promover o conhecimento de cibersegurança em normas já utilizadas pela indústria. Outrossim, esses aspectos também são destacados na Automação Industrial[49]: "no mundo da TA (Tecnologia da Automação), a questão da segurança de dados é relativamente nova, mas podemos afirmar que, a segurança da informação, em qualquer nível de automação, já é uma barreira a implantação e ao crescimento dos sistemas para a Indústria 4.0." Para que as indústrias possam implementar sistemas de cibersegurança na automação industrial visando alcançar níveis de maturidade mais avançado da Indústria 4.0, as indústrias

necessitam gerenciar os riscos; desenvolver o capital humano focado em cibersegurança; entender como utilizar as tecnologias digitais e quais são os procedimentos mais adequados; e, sempre que possível, testar e monitorar os sistemas e os dispositivos de automação e fazer o rastreio periodicamente.

Particularmente, um ótimo exemplo de estudo, entendimento e explicação de normas técnicas e da arquitetura e como elas devem ser utilizadas em determin do contexto está no guia com Princípios e práticas de cibersegurança em dispositivos médicos[50]. O guia tem como objetivo fornecer boas práticas e informações para garantir a segurança cibernética para todos os dispositivos médicos brasileiros. Entre as normas citadas estão: AAMI TIR57:2016, IEC TR 80001-2-2 - Estágio 90.92, IEC TR 80001-2-8 - Estágio 10.99, ISO 14971:2019 - Estágio 60.60, a família ISO 27000 e recursos publicados pelo National Institute Standards and Technologies (NIST). As normas citadas são muitas vezes aplicadas em consonância para potencializar seus resultados. Além disso, o estudo pode ser utilizado como modelo, se os especialistas acharem adequado, para o desenvolvimento de treinamentos em outras áreas do conhecimento, propiciando, assim, a disseminação do conhecimento, visto que demonstra como as normas técnicas podem ser aplicadas conjuntamente em um contexto específico. Consequentemente, a ampliação do contexto é fundamental a fim de propiciar um ambiente integrativo de cooperação para geração e transferência de conhecimento. Além desses aspectos, há também a LGPD, que aborda a proteção de dados pessoais. O capítulo VII aborda da segurança e das boas práticas que também precisam ser conhecidas pelas empresas para que elas possam atender aos requisitos de segurança identificados, aos padrões adequados e a aspectos de governança. Como a vigência de algumas partes iniciou há pouco tempo, é ainda novo para a maioria das empresas, principalmente para empresas de pequeno e médio porte que não tem um setor responsável pela LGPD. Entretanto, é muito importante que as indústrias cruzem as informações das normas técnicas internacionais com a LGPD a fim de verificar se as normas técnicas estão adequadas com a LGPD.

Logo, segundo destacados pelos especialistas e a literatura, é difícil para as indústrias e as fornecedoras de tecnologias entenderem as normas técnicas, a sua aplicabilidade, o relacionamento e complementação com outras normas técnicas. Além disso, as indústrias têm dificuldadeem saber de qual agente normalizador seguir a norma e por quê. Por isso, a presença de especialistas é tão importante na discussão.

Outrossim, em relação às normas específicas, destaca-se, como exemplo, a norma Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 e ISO/IEC 20000-1 (ISO/IEC 27013:2021 - Estágio 60.60), publicada em 2021. A norma se concentra na

implementação integrada de um sistema de gerenciamento de segurança da informação (ISMS) conforme especificado na ISO / IEC 27001 e um sistema de gerenciamento de serviço (SMS) conforme especificado na ISO / IEC 20000-1. Na prática, a ISO / IEC 27001 e a ISO / IEC 20000-1 também podem ser integradas a outros padrões de sistema de gestão, como ISO 9001 e ISO 14001. Portanto, a norma apresenta um exemplo de integração entre duas normas de cibersegurança, que pode ser utilizado como modelo a se seguir para outros contextos.

De forma geral, a norma traz diretrizes e pontos de cuidado ao integrar duas normas no caso a ISO/IEC 27001 e ISO/IEC 20000-1ICS, a partir dele sugere-se uma montagem de um documento padrão para integração de outras normas do mesmo estilo. Com base no uso dessa norma, os especialistas podem ajudar a montar outras integrações de normas, facilitando, assim, o conhecimento sobre as normas a serem debatidas. Além dessa norma, uma norma que foca em conhecimento é a Information technology — Security techniques — Competence requirements for information security management systems professionals (ISO/IEC 27021:2017 - Estágio 60.60), que já foi publicada em 2017 e especifica os requisitos de competência para profissionais que lideram ou estão envolvidos no estabelecimento, implementação, manutenção e melhoria contínua de um ou mais processos de sistema de gestão de segurança da informação em conformidade com a ISO / IEC 27001. A norma apresenta diversas competências que os profissionais devem ter: liderança, comunicação, estratégia de negócios, gestão de riscos e gestão de fornecedores, visto que a falta de conhecimento das normas técnicas também pode ser mitigada pelo desenvolvimento das equipes em geral. A norma fornece também detalhes sobre competências em relação à segurança da informação, planejamento de segurança da operação, operação da segurança da informação, entre outros, ou seja, resolver parcialmente o problema apresentado.

Outrossim, a norma poderia incluir alguns detalhes em relação à cibersegurança. Além dessas duas normas técnicas já publicadas pelos assuntos, destaca-se a série IT security techniques — Competence requirements for information security testers and evaluators (ISO/IEC 19896), também com normas técnicas já publicadas. A primeira norma da série, ISO / IEC 19896-1: 2018 - Estágio 60.60 define termos e estabelece um conjunto organizado de conceitos e relações para compreender os requisitos de competência para especialistas em avaliação e teste de conformidade de garantia de segurança da informação, estabelecendo assim uma base para o entendimento compartilhado dos conceitos e princípios centrais para o Série ISO / IEC 19896 em suas comunidades de usuários. Ele fornece informações fundamentais para os usuários da série ISO / IEC 19896. Considerando o problema apresentado, a norma pode ajudar na criação do aplicativo que contenha os conceitos das normas técnicas porque os profissionais vão ter desenvolvido as competências

necessárias para tal. Ademais, a norma explica alguns elementos da competência, entre eles, destacam-se o conhecimento, habilidades, experiências e educação, inclusive a norma traz um framework que descreve as competências requeridas. Já, a parte dois da série (ISO/IEC 19896-2:2018 - Estágio 60.60) fornece os requisitos mínimos para os requisitos de conhecimento, habilidades e eficácia de indivíduos que executam atividades de teste para um esquema de conformidade usando ISO / IEC 19790 e ISO / IEC 24759.

Nessa norma, há o detalhamento do conhecimento em normas técnicas, em programas de validação e em requisitos presentes em outras normas técnicas. Dessa forma, essa norma também apresenta uma integração com outras normas que é fundamental para o desenvolvimento de competências dos colaboradores assim como a norma ISO/IEC 27013:2021 já destacada. Outrossim, a parte 3 da série (ISO/IEC 19896-3:2018 - Estágio 60.60) fornece os requisitos especializados para demonstrar a competência dos indivíduos na realização de avaliações de segurança de produtos de TI de acordo com a ISO / IEC 15408 (todas as partes) e ISO / IEC 18045. Em específico em relação à integração com outras normas, a ISO/IEC 19896-3:2018 faz uma análise do conhecimento das outras normas técnicas e uma avaliação das habilidades fundamentais presentes nas outras normas. Assim, a série ISO/IEC 19896 apresenta relações com diversas normas que são difíceis de serem analisadas, e os especialistas podem utilizar essas normas técnicas para entender como integrar as normas para o desenvolvimento de conhecimento e também a série apresenta normas técnicas que integram outras normas que podem ser utilizadas para criação de normas ou série de normas mais específicas de cibersegurança. Consequentemente, tendo em vista os elementos citados, mesmo que o público-alvo seja outro, a série ISO/IEC 19896 apresentada, pode ser utilizado para aumentar o conhecimento das normas, porque traz diversos exemplos de integração de normas, inclusive os profissionais que são o público-alvo da norma podem ajudar no desenvolvimento dos aplicativos sobre o tema.

Além das normas técnicas supracitadas que podem auxiliar parcialmente o problema, destacase também a série ISO/IEC TS 23532 publicada em 2021. A primeira norma da série, Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408 (ISO/IEC TS 23532- 1:2021 - Estágio 60.60), complementa e suplementa os procedimentos e requisitos gerais encontrados na ISO / IEC 17025: 2017 - Estágio 60.60 para laboratórios que realizam avaliações com base na série ISO / IEC 15408 - Estágio 90.92 e ISO / IEC 18045 - Estágio 90.92. Já, a parte 2 da norma, Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 2: Testing for ISO/IEC 19790 (ISO/IEC TS 23532-2:2021 - Estágio

60.60) complementa e suplementa os procedimentos e requisitos gerais encontrados na ISO / IEC 17025: 2017 - Estágio 60.60 para laboratórios que realizam testes com base na ISO / IEC 19790 - Estágio 90.92 e ISO / IEC 24759 - Estágio 90.92. Ou seja, as normas técnicas mostram como a integração das diversas normas é importante no contexto da cibersegurança em um contexto específico, assim como outros casos apresentados nesta seção. Considerando esses aspectos, embora todas essas normas técnicas já estejam publicadas e não solucionem totalmente o problema, os especialistas poderiam trabalhar a integração das normas técnicas no contexto industrial ao invés do contexto laboratorial, apresentado nas duas normas da série ISO/IEC TS 23532.

Dessa forma, as normas de série podem ser utilizadas como base assim como as outras citadas na análise para o problema. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de conhecimento sobre as normas de cibersegurança

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27013:2021	Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 e ISO/IEC 20000-1	Estágio 60.60	Incluir nas normas aspectos relacionados à integração das normas técnicas de cibersegurança no contexto industrial
ISO/IEC 27021:2017	Information technology — Security techniques — Competence requirements for information security management systems professionals	Estágio 60.60	
Série ISO/IEC 19896: 2018	IT security techniques — Competence requirements for information security testers and evaluators (ISO/IEC 19896)	Estágio 60.60	
ISO/IEC TS 23532-1:2021	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security	Estágio 60.60	
ISO/IEC TS 23532-2:2021	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security	Estágio 60.60	

5.3 Falta de conhecimento sobre os principais conceitos de cibersegurança (2 – 8º)

Complementar à discussão anteriores, segundo os especialistas, as indústrias e as fornecedoras não conhecem as normas técnicas de cibersegurança e sentem dificuldades de aplicar os conceitos e as normas de segurança já consolidadas na literatura no ambiente industrial. Ou seja, os especialistas destacaram que a necessidade da disseminação das normas técnicas e dos conceitos que as normas trazem para o contexto industrial.

De forma geral, primeiramente, as empresas precisam identificar ativos relacionados ameaçados por questões de segurança cibernética dentro dos contextos de Indústria 4.0 e Internet das Coisas Industrial[51], que está relacionado também ao problema 5.8 do relatório. Para depois, as indústrias possam: definir das vulnerabilidades intrínsecas dos sistemas que comprometem a sua segurança; analisar as ameaças cibernéticas que afetam os sistemas; avaliar e gerenciar os riscos associados aos ataques cibernéticos; planejar e acionar, quando necessário, as contramedidas para lidar com questões de segurança cibernética[52]. Dessa forma, considerando esses aspectos, é necessário exista conjunto mínimo de padrões de cibersegurança, e ele seja disseminado nas indústrias, propiciando, assim, a transferência de conhecimento sobre o assunto e aumentando o entendimento de conceitos básicos.

Além da compreensão sobre os conceitos básicos de cibersegurança, é importante que os profissionais entendam como aplicá-lo, por isso estudos de caso sobre aplicação das normas técnicas de cibersegurança são fundamentais. Um exemplo de aplicação de estudo e aplicação de normas relacionadas à cibersegurança é apresentado no artigo “Framework de Cibersegurança da informação no Setor de Automóvel”[53]. Ao verificar que o guia existente para a aplicação de cibersegurança era insuficiente e as normas atuais não abrangiam inteiramente as necessidades do setor, o autor propõem a criação de um framework e explica como as normas técnicas existentes podem auxiliar em cada etapa do processo. O artigo explica todos os estágios de criação (como implementação, validação e planejamento) e argumenta os motivos da escolha de cada norma, o que pode servir de exemplo para as empresas e fornecedoras de tecnologia para a criação de frameworks ou, até mesmo, diretrizes que abordem o assunto. Em suma, com base nessas reflexões, as indústrias e as fornecedoras de soluções tecnológicas necessitam entender como aplicar as normas de cibersegurança e segurança no ambiente industrial além de compreender como o portfólio de normas sobre o tema e as soluções disponíveis no mercado.

Outrossim, no que concerne às normas, destaca-se a norma de Cybersecurity education and training (ISO/IEC AWI TR 27109 – Estágio 20.00), que está em desenvolvimento e foi abordada na seção 5.4. Uma vez que a norma está em

desenvolvimento em uma fase inicial, o escopo não está definido, porém ela tratará sobre conceitos que envolvam educação e treinamento de cibersegurança. Considerando isso, os especialistas podem debater sobre oportunidades de incluir na norma ou criar uma série a partir dessa norma com intuito de incluir uma seção de treinamento sobre normas técnicas. Acredita-se que, futuramente, a norma poderá resolver o problema de forma parcial, porque os colaboradores, as fornecedoras e as indústrias ainda precisão entender as normas de conceitos básicos, entre elas, a ISO/IEC TS 27100:2020, que será explicada a seguir.

Isto posto, é importante citar uma norma que já está publicada: Information technology — Cybersecurity — Overview and concepts (ISO/IEC TS 27100:2020 - Estágio 60.60). Essa norma descreve a segurança cibernética e os conceitos relevantes, incluindo como ela está relacionada e difere da segurança da informação; estabelece o contexto da cibersegurança; porém, não cobre todos os termos e definições aplicáveis à segurança cibernética; e não limita outros padrões na definição de novos termos de uso relacionados à segurança cibernética. Logo, essa norma pode ser utilizada para solucionar parcialmente o problema destacado pelos especialistas, porque aborda os principais conceitos que precisam ser aprendidos pelos colaboradores e gestores. Esses conceitos básicos são primordiais para a solidificação do conhecimento em cibersegurança e posterior avanço para conceitos mais complexos sobre o tema.

De forma conjunta, as duas normas técnicas citadas podem ajudar na resolução do problema. No entanto, o apoio dos especialistas é essencial para a norma em desenvolvimento seja direcionada a necessidades industriais. E, se a discussão com especialistas evidenciar que os termos presentes na norma ISO/IEC TS 27100:2020 não são suficientes para um bom entendimento da cibersegurança no ambiente industrial, existem diversas normas publicadas e em desenvolvimento que tratam do assunto de segurança no grupo prioritário analisado.

Entre elas, destacam-se: Information technology — Security techniques — Security assurance framework — Part 1: Introduction and concepts (ISO/IEC TR 15443-1:2012 – Estágio 90.93) ; IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements (ISO/IEC 19896-1:2018 – Estágio 60.60); Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2021 and ISO/IEC 18045:2021; IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts (ISO/IEC 24760-1:2019 – Estágio 60.60); Information technology — Security techniques — Network security — Part 1: Overview and concepts (ISO/IEC 27033- 1:2015 – Estágio 90.93); Information technology — Security techniques — Application security — Part 1: Overview and concepts (ISO/IEC 27034-1:2011 – Estágio 90.93). Logo, existem muitas oportunidades para a resolução do problema.

Problema: Falta de conhecimento sobre os principais conceitos de cibersegurança

Normas técnicas que podem atender ao problema

Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC AWI TR 27109	Cybersecurity education and training	Estágio 20.00	Incluir e esclarecer nas normas os principais conceitos de cibersegurança
ISO/IEC TS 27100:2020	Information technology — Cybersecurity — Overview and concepts	Estágio 60.60	
ISO/IEC TR 15443-1:2012	Information technology — Security techniques — Security assurance framework — Part 1: Introduction and concepts	Estágio 90.93	
ISO/IEC 19896-1:2018	IT security techniques — Competence requirements for information security testers and evaluators — Part 1:I ntroduction, concepts and general requirements	Estágio 60.60	
ISO/IEC 24760-1:2019	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts	Estágio 60.60	
ISO/IEC 27033-1:2015	Information technology — Security techni-ques — Network security — Part 1: Overview and concepts	Estágio 90.93	
ISO/IEC 27034-1:2011	Information technology — Security techni-ques— Application security — Part 1: Overview and concepts	Estágio 90.93	

5.4 Falta de conhecimento sobre padrões mínimos de comunicação e integração (13 – 2°)

Durante o workshop, os especialistas relataram que as indústrias e as fornecedoras de tecnologias digitais da Indústria 4.0 desconhecem normas técnicas sobre a integração e padrões mínimos de comunicação com segurança, confiabilidade e qualidade a fim de que a cibersegurança seja integrada. De acordo com os especialistas, existe necessidade de padronização de comunicação para integração (principalmente, em relação aos equipamentos e sistemas legados) e dos métodos utilizados para comunicação industrial, promovendo, assim, a automação industrial e como a cibersegurança pode ser inserida nesses aspectos.

Ademais, os especialistas também discutiram sobre as melhorias da segurança e a necessidade de padronização dos equipamentos e softwares em sistemas para que a cibersegurança seja um pré-requisito em relação a sua aplicação. Além desses aspectos, discutiram também alguns outros problemas: a necessidade de padronização para a transmissão e integração segura de dados entre os controladores lógico programáveis (CLPs) e dispositivos Internet das Coisas (IoT) para que seja possível iniciar a integração vertical e a melhoria da tomada de decisão das indústrias de forma segura, criando, assim, um padrão de segurança para acesso remoto a máquinas industriais. Por exemplo, segundo a uma empresa de tecnologia[54] que é focada em automação industrial, "a grande dificuldade no acesso remoto está em viabilizar que um determinado IP e Porta de um CLP, instalado na máquina ou chão de fábrica esteja acessível remotamente.

Esse tipo de configuração para permitir o acesso remoto ao CLP costuma ser um mecanismo de fácil configuração, mas pouco seguro. Pela falta de segurança, a indústria normalmente não aceita que um IP de um CLP seja acessado remotamente". Considerando esses aspectos, a indústria necessita de uma norma para acessar remotamente de forma mais segura, logo as normas técnicas são uma alternativa para que os fornecedores de soluções tecnológicas de indústria 4.0 possam entregar produtos e/ou serviços que satisfazem os requisitos de qualidade presentes na norma. Complementarmente, a natureza específica dos sistemas industriais é um dos fatores que dificulta o uso de sistemas de comunicação existentes, já que muitos deles não foram concebidos para este fim. Fatores como a confiabilidade das informações e o tempo de envio e recebimento são essenciais a fim de manter o nível de precisão e agilidade de processos indústrias, em especial aqueles que são considerados críticos[55]. Por exemplo, o protocolo Modbus foi inicialmente desenvolvido para uso interno da sua desenvolvedora. Atualmente, ele sofreu modificações e é aberto para utilização em qualquer indústria. Além disso, sensores de rede, responsáveis por interceptar o tráfego de entrada e saída em redes industriais também são importantes, também podem ser utilizados para detectar anomalias e ataques cibernéticos.

Portanto, as indústrias e as fornecedoras de soluções tecnológicas necessitam compreender quais são as melhores práticas de segurança para a integração de dados, sistemas e tecnologias com intuito de mitigar os riscos de incidentes de segurança e maximizar os resultados operacionais da indústria. Em alguns casos, as indústrias realizam processos que favorecerem a interoperabilidade, porém desfavorecem a segurança dos dados dos clientes. Em relação a esse aspecto da interoperabilidade, a LGPD aborda o seguinte tema: "Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista

especialmente a necessidade e a transparência." Ou melhor, as indústrias, os fornecedores de tecnologias e os especialistas devem estar cientes dos padrões mínimos de interoperabilidade que são exigidos a fim de mitigar os riscos e propiciar o ambiente seguro com base na LGPD.

Ademais, no que tange às normas técnicas relacionadas ao problema, existem algumas normas publicadas e em desenvolvimento sobre o assunto. Entre elas, ressalta-se a norma Cybersecurity — IoT security and privacy – Guidelines (ISO/IEC DIS 27400 - Estágio 40.60), que está em desenvolvimento. A norma fornece diretrizes sobre riscos, princípios e controles para segurança e privacidade de soluções de IoT. Além da norma tratar sobre os conceitos de IoT, detalhando as principais características dos sistemas IoT e os principais riscos dos sistemas IoT, existem controles de segurança e privacidade. A partir dessa perspectiva, ao utilizar essa norma, as diretrizes de risco e cibersegurança pode ser maximizada com a intenção de melhorar o desenvolvimento dos projetos e a parte operacional, facilitando integrações seguras entre os componentes do projeto. Portanto, a norma resolver parcialmente o problema, e, além de norma de IoT, seriam necessárias normas para sensores e CLPs, por exemplo.

Como, muitas vezes, os serviços de cibersegurança e as soluções tecnológicas da Indústria 4.0 são fornecidos por empresas diferentes, salienta-se a série ISO/IEC 27036 de Cybersecurity — Supplier relationships. Essa série possui normas que já foram publicadas e estão em desenvolvimento, apresentando normas técnicas tanto para clientes quanto para fornecedores. A primeira norma publicada da série, Cybersecurity — Supplier relationships — Part 1: Overview and concepts (ISO/IEC 27036-1:2021 – Estágio 60.60), fornece uma visão geral da orientação destinada a ajudar as organizações a proteger suas informações e sistemas de informação dentro do contexto de relacionamentos com fornecedores. Dessa forma, a primeira norma mostra uma visão geral das outras normas além de mostrar os riscos de segurança da informação e como manejar esses riscos ao longo da cadeia de suprimentos, visto que, em alguns casos, as empresas precisam integrar as informações com seus fornecedores de forma segura, garantindo, assim, padrões mínimos de integração internos e externos da empresa.

Outrossim, Cybersecurity — Supplier relationships — Part 2: Requirements (ISO/IEC DIS 27036-2 - Estágio 40.60), a segunda norma de série especifica os requisitos fundamentais de segurança da informação para definir, implementar, operar, monitorar, revisar, manter e melhorar os relacionamentos com fornecedores e adquirentes. Esses requisitos cobrem qualquer aquisição e fornecimento de produtos e serviços, como fabricação ou montagem, aquisição de processos de negócios, componentes de software e hardware, aquisição de processos de conhecimento, Build-Operate-Transfer e serviços de computação em nuvem.
Dessa forma, essa norma é fundamental

para a escolha dos fornecedores de solução tecnológica mais segura, o que inclui um processo de planejamento, processo de seleção, gestão e finalização do processo além de incluir alguns processos técnicos necessários. Além das duas partes já citadas da série ISO/IEC CD 27036, existem também a Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security (ISO/IEC CD 27036 – Estágio 90.92) fornece adquirentes e fornecedores de produtos e serviços na cadeia de suprimentos de tecnologia da informação e comunicação (TIC) com orientação sobre: visibilidade e gerenciamento dos riscos de segurança da informação e integração dos processos e práticas de segurança da informação aos processos de ciclo de vida do sistema e software, descritos na ISO / IEC 15288 e ISO / IEC 12207, ao mesmo tempo que dá suporte aos controles de segurança da informação, descritos na ISO / IEC 27002. Com base nesses aspectos, essas normas de fornecedores poderiam servir como exemplo para que os especialistas consigam enxergar como aplicar a integração tanto dentro quanto fora da indústria de forma segura, maximizando o uso de dados.

Além disso, se é seguro escolher um serviço de computação em nuvem ou não, e quais são os requisitos de segurança que os fornecedores devem ter para prover o serviço. Outrossim, como a série de normas técnicas resolve parcialmente o problema apresentado, são necessárias normas mais técnicas para inserir a cibersegurança em padrões mínimos de comunicação dos mais diversos dispositivos. Logo, a discussão dos especialistas é essencial para que as normas possam convergir a uma solução viável e alinhada às necessidades e aos requisitos presentes na LGPD. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de conhecimento sobre padrões mínimos de comunicação e integração			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 27400	Cybersecurity — IoT security and privacy – Guidelines	Estágio 40.60	Incluir nas normas os padrões mínimos de comunicação e comunicação dentro e fora da indústria de forma segura
ISO/IEC 27036-1:2021	Cybersecurity — Supplier relationships — Part 1: Overview and concepts	Estágio 60.60	
ISO/IEC DIS 27036-2	Cybersecurity — Supplier relationships — Part 2: Requirements	Estágio 40.60	
ISO/IEC CD 27036-3	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	Estágio 90.92	

5.5 Falta de profissionais qualificados em cibersegurança (12 – 3º)

Conforme os especialistas do workshop, as indústrias e fornecedoras de tecnologia sofrem com dificuldade em ter profissionais qualificados, para realizar treinamentos e atuar na cultura da empresa e dos colaboradores para uma cultura orientada à cibersegurança além de não estar claro qual padrão ético que estes profissionais devem seguir. Durante o workshop, os especialistas salientaram os seguintes problemas: a necessidade de profissionais qualificados em redes de automação focados em cibersegurança; a importância de um treinamento coerente de pessoal específico para cada área de atuação para a cibersegurança; a relevância de uma mudança cultural focada em cibersegurança e padronização de ética e conduta aos dados disponibilizados a fim de promover a cibersegurança.

As ameaças à segurança estão sempre mudando, e os tipos de ataques mudam diariamente[56]. Portanto, sem treinamento contínuo e apropriado, os colaboradores podem ser vítimas de um novo ataque que, de outra forma, poderiam ter sido notado[57]. Sendo assim, o treinamento deve ser contínuo atendendo antigos e novos colaboradores para que eles possam tomar a melhor atitude quando tiverem um incidente de segurança, e as normas podem ajudar nesse aspecto. Outrossim, a conscientização sobre a segurança cibernética e o treinamento em habilidades cibernéticas são extremamente importantes e desafiadoras no contexto empresarial[58]. Entretanto, as técnicas e respostas de prevenção são abrangentes, mas só são eficazes se usadas de forma correta[59] [60]. Consequentemente, a norma, além de trazer aspectos relevantes, poderia abordar como tornar a apresentação do assunto mais complexo de forma simples, diminuindo, assim, a dificuldade de assimilação e maximizando o aprendizado dos colaboradores para que eles tomem a melhor atitude em relação à segurança. Por exemplo, uma das soluções encontradas para o treinamento de pessoal na prefeitura do município de Esteio, no Rio Grande do Sul, foi a gamificação[61].

A gamificação consiste no uso de jogos para ensinar ou reforçar conteúdos que não são tipicamente apresentados neste formato. O projeto teve a intenção de fornecer treinamento aos funcionários, sensibilizá-los à importância da cibersegurança e apresentar conceitos da LGPD. Foi utilizada a plataforma Hacker Rangers, desenvolvida especificamente para esta finalidade. Após a experiência, 90% dos funcionários afirmaram ter conhecimentos bons ou excelentes sobre cibersegurança e capacidade para aplicá-los. Sendo assim, de acordo com os especialistas do workshop, treinamento, profissionais qualificados e uma equipe orientada a uma cultura de segurança são os pilares que as indústrias necessitam desenvolver para alcançar um nível de segurança adequado tanto em relação a seus dados, dados de clientes e de fornecedores. Portanto, aspectos éticos também entram em questão e quais as condutas que devem ser seguidas, assim como destacado nos itens 4.12 e 4.13 da análise do workshop de IA.

Adicionalmente, no que concerne às normas já publicadas e em desenvolvimento, destaca-se a norma Cybersecurity education and training (ISO/IEC AWI TR 27109 – Estágio 20.00). Como o escopo ainda não está definido, acredita-se que a norma trará de temas relacionados à educação e ao treinamento em relação à cibersegurança. Dependendo de como for construída a norma em desenvolvimento, a sua criação pode ajudar as indústrias a implementarem e qualificarem seus colaboradores para cibersegurança, mitigando, assim, os incidentes de cibersegurança.

Outrossim, os especialistas podem trabalhar e suportar o desenvolvimento dessa norma com intuito de colocar em debate as questões de cibersegurança, refletindo, assim, os principais problemas

enfrentados pela indústria em relação à falta de profissionais qualificados. Dessa maneira, em um primeiro momento, o problema pode ser parcialmente resolvido pela norma, porém é necessária a discussão sobre o assunto junto com os especialistas para estimular aspectos de cibersegurança na indústria. Ademais, em relação a competências mais complexas, sugerese a discussão das normas apresentadas no item 5.2 sobre as competências (série ISO/IEC 19896 - Estágio 60.60 e norma ISO/IEC TS 23532-1 - Estágio 60.60). Entretanto, sugere-se isso para um segundo momento, porque, de acordo com os especialistas, um treinamento básico é necessário dentro das indústrias. Ademais, em relação aos aspectos éticos, há algumas normas presentes em outros grupos, como o de Inteligência Artificial (Information technology — Artificial intelligence — Overview of ethical and societal concerns - ISO/IEC DTR 24368 - Estágio 30.60), que podem ser utilizadas para o desenvolvimento de uma norma em relação aos aspectos éticos da cibersegurança, já discutida na seção 4.13. Logo, a presença de especialistas é essencial para explorar a norma de IA em um contexto de cibersegurança, porém é importante o desenvolvimento de normas relação a outras tecnologias da Indústria 4.0.

Consequentemente, com base na análise das discussões dos especialistas, literatura e normas, entende-se que os especialistas poderiam refletir acerca das normas técnicas em desenvolvimento
que se referem a treinamento simples e complexos em cibersegurança, uma vez que a presença deles é fundamental para uma discussão mais aprofundada em relação aos problemas. Dessa forma, é possível alinhar as expectativas da indústria com as normas técnicas em desenvolvimento e as normas de outros grupos que podem ser articuladas e reescritas para contextos de cibersegurança. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de profissionais qualificados em cibersegurança			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
	Cybersecurity education and training (ISO/IEC AWI TR 27109 – Estágio 20.00).		
Série ISO/IEC19896	IT security techniques — Competence requirements for information security testers and evaluators (ISO/IEC 19896)	Estágio 60.60	Incluir normas técnicas em desenvolvimento que se referem a treinamento simples e complexos em cibersegurança
ISO/IEC TS 23532-1:2021	Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories	Estágio 60.60	
ISO/IEC DTR 24368	Information technology — Artificial intelligence — Overview of ethical and societal concerns	Estágio 30.60	

5.6 Falta de entendimento dos principais benefícios da cibersegurança e normas para terceirização da cibersegurança (9 – 4º)

De acordo com os especialistas presentes no workshop de cibersegurança, as indústrias têm dificuldade em entender os principais benefícios da cibersegurança e como elas podem avaliar que os dados e as informações estão seguras o suficiente, visto que os benefícios da cibersegurança são intangíveis, e as empresas, normalmente, contratam fornecedoras de soluções de cibersegurança (firewall, backup e antivírus) além da fornecedora terceirizada ajudar no desenvolvimento da política de cibersegurança em empresas de pequeno e médio porte.

De forma geral, os especialistas discutiram sobre a necessidade de avaliação do custo-benefício e impacto da Cibersegurança; a padronização e ampliação do uso de avaliação de cibersegurança; e a terceirização da gestão de segurança cibernética. Em relação a terceirização de gestão de segurança cibernética, muitas empresas buscam essas fornecedoras terceirizadas para proteger seus dados e rede industrial. E as fornecedoras terceirização ficam responsáveis pela instalação de firewall,

antivírus e backup; criação de um VPN interno; e elaboração de política de cibersegurança. Dessa forma, a indústria fica responsável por um pagamento de uma mensalidade para receber todos esses serviços. Conforme os especialistas discutiram, normas técnicas em relação a esses aspectos precisam ser discutidas para que o serviço prestado tenha um nível adequado. Complementarmente, existem diversos benefícios da adoção de soluções de cibersegurança. Entre eles, destacam-se os seguintes[62]: proteção redes e dados contra acesso não autorizado; melhoria da segurança da informação e gestão da continuidade dos negócios; maior confiança das partes interessadas em relação à segurança da informação; sistemas de credenciais da empresa aprimoradas com os controles de segurança corretos em vigor; tempos de recuperação mais rápidos em caso de violação. Considerando esses benefícios, mesmo que, em alguns casos, o custo de implementação das soluções pareça não ter retorno, a segurança dos dados da indústria, dos clientes e fornecedores é o principal ativo da empresa, logo ela deve se preocupar com esses aspectos.

A dificuldade de visualizar os benefícios da cibersegurança em um primeiro momento é difícil não só para indústrias como também para governos e pessoas físicas. No entanto, quando é detectado um ataque cibernético, os prejuízos podem ser bem maiores. Segundo um artigo sobre a percepção da cibersegurança[63], os custos associados ao cibercrime podem ser divididos em três grupos: defesa, diretos e indiretos. Os custos de defesa são aqueles que englobam a instalação de antivírus, e sensores de rede. Já os custos diretos incluem o ressarcimento de valores roubados e possível troca de equipamentos. Por fim, os custos indiretos são exemplificados pelo custo para restaurar a confiança dos clientes na empresa e nos sistemas utilizados (o que pode levar à perda de receita) e perda de contratos e oportunidades. Consequentemente, mesmo que a cibersegurança não gere receita diretamente, quando há uma estrutura bem definida de cibersegurança, alguns custos podem ser reduzidos. Consequentemente, as indústrias necessitam avaliar o custo-benefício da adoção da regulação que elas devem seguir além de analisar se o padrão de segurança está adequado em relação aos dados e aos ambientes onde a empresa está inserida. Complementarmente, as indústrias devem avaliar se esses problemas podem ser resolvidos por fornecedores de cibersegurança externos a empresa.

Na LGPD, há um capítulo que fala sobre fiscalização. O § 7° do artigo Art. 52 aborda a questão dos vazamentos: “os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo”. Dessa forma, dependendo de quais dados forem o alvo do vazamento podem gerar multas, advertências, suspensão do uso do banco de

tatos, proibição das atividades. Por isso, indústrias, especialistas e fornecedoras de tecnologias devem estar a par da legislação vigente no país.

No que concerne às normas técnicas, existe a série Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Framework for the specification of evaluation methods and activities (ISO/IEC 15408 - Estágio 90.92), que está em desenvolvimento. A parte 1 da ISO / IEC 15408 (Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model que foi publicada em 2019 está sendo revisa com o seguinte nome Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model) estabelece os conceitos e princípios gerais de avaliação de segurança de TI e especifica o modelo geral de avaliação dado por várias partes da Norma Internacional que, em sua totalidade, deve ser usado como base para a avaliação das propriedades de segurança de Produtos de TI.

Com base no framework, as indústrias podem fazer uma avaliação do uso de cibersegurança, visto que apresenta o conceito central de uma Meta de Avaliação (TOE); o contexto da avaliação; e descreve o público ao qual os critérios de avaliação são dirigidos. Dessa forma, os especialistas podem ajudar a desenvolver as metas de avaliação dependendo da necessidade das indústrias nacionais com base nos principais benefícios do uso da cibersegurança. Além dessa primeira norma da série, destaca-se a quarta norma (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Framework for the specification of evaluation methods and activities - ISO/IEC DIS 15408-4 - Estágio 50.00). A quarta norma da série poderá auxiliar na avaliação interna da empresa, onde ela será possível avaliar seus próprios padrões e, a partir disso, poderá permitir a avaliação dos problemas e o encontro da solução que poderá prover dos fornecedores externos da empresa.

Ou seja, essa norma pode auxiliar no encontro dos padrões internos da empresa, oferecendo a oportunidade de comparação entre os problemas e os principais benefícios, e ao ter o padrão interno estabelecido será mais fácil encontrar fornecedores capazes de atender a demanda. Logo, a norma poderá ser complementar e poderá atender parcialmente o problema identificado, uma vez que mostra padrões de segurança pré-definidos.

Além disso, com base na opinião dos especialistas, como as normas técnicas estão em construção, é possível a inserção de temas pertinentes com base nos principais pontos destacados no relatório. Logo, recomenda-se a presença dos especialistas para que seja possível discutir e aprofundar os principais aspectos sobre a falta de entendimento dos principais benefícios da cibersegurança. Considerando a questão de fornecedores, é importante também abordar a série de normas (ISO/IEC 27036) discutidas no

item 5.4 sobre orientação destinada a auxiliar as organizações na proteção de suas informações e sistemas de informação dentro do contexto do relacionamento com o fornecedor. Entretanto, nesse contexto, precisaria ser discutida normas em relação ao fornecimento de soluções de cibersegurança. A partir disso, os especialistas podem adicionar uma nova norma à série que discute justamente a questão do relacionamento entre o cliente e o fornecedor de soluções de cibersegurança.

Com base nessa análise sobre o problema, há muito o que ser discutido pelos especialistas sobre o tema e como a cibersegurança pode ser um benefício para as indústrias além de discutir meios de diminuir o custo estratégico e operacional da cibersegurança.

Dessa forma, é uma pauta de extrema relevância no ambiente de normalização nacional e internacional. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de entendimento dos principais benefícios da cibersegurança e normas

Normas técnicas que podem atender ao problema

Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 15408–1	ISO / IEC 15408 (Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	Estágio 90.92	Incluir normas sobre diretrizes e frameworks que incluam os benefícios e aspectos de ter-ceirização da cibersegurança, incluindo, por exemplo, relacionamento entre clientes e fornecedores no contexto da cibersegurança
ISO/IEC DIS 15408-4	Information security, cybersecurity and privacy protection —Evaluation criteria for IT security — Framework for the specification of evaluation methods and activities	Estágio 50.00	
ISO/IEC 27036-1:2021	Cybersecurity — Supplier relationships — Part 1: Overview and concepts	Estágio 60.60	
ISO/IEC DIS 27036-2	Cybersecurity — Supplier relationships — Part 2: Requirements	Estágio 40.60	
ISO/IEC CD 27036-3	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply	Estágio 90.92	

5.7 Falta de entendimento para promover integração de forma segura (8 – 5º)

De acordo com os especialistas presentes no workshop, as indústrias e fornecedoras de tecnologias necessitam ter entendimento igual em relação às normas técnicas para promover a integração do uso das tecnologias de forma segura e confiável. Entre os aspectos discutidos pelos entrevistados, destacam-se os seguintes: a necessidade de uma recomendação de um nível mínimo de conhecimento (certificado de segurança) entre consumidores e fabricantes para interlocução, inclusive os especialistas discutiram a necessidade de integração com fornecedores e clientes como potencial risco por falta de auditoria e de definição de certificação.

No mercado, existem algumas cerificações de cibersegurança. Por exemplo, "o CompTIA Cybersecurity Analyst (CySA +) é uma certificação da força de trabalho de TI que aplica análises comportamentais a redes e dispositivos para prevenir, detectar e combater ameaças de segurança cibernética por meio de monitoramento contínuo da segurança."[64] Essa certificação está relacionada a outros problemas já discutidos no relatório nas seções 5.3, 5.4 e 5.5 porque está relacionada à certificação da força de trabalho. Além dessa certificação, existem outras certificações relacionados ao nível básico, como a de Fundamentos de Segurança do Microsoft Technology Associate (MTA) cuja base é a compreensão de princípios de segurança além de aspectos de rede e segurança de software e como o Certificado de Segurança de Sistemas (SSCO) cujo foco é em segurança e infraestrutura de TI[65]. De forma geral, há muitas certificações para profissionais, e os clientes podem requerer o atendimento por uma profissional que seja certificado. Como não há uma convergência em relação a qual certificação deve ser usada em contextos específicos e muitas das certificações focam em aspectos de TI, os especialistas relataram a necessidade de desenvolvimento de normas técnicas direcionadas a certificações de cibersegurança tanto em relação a empresas quanto a pessoas capacitadas em cibersegurança.

Uma certificação que ateste requisitos mínimos de qualidade para a cibersegurança é uma realidade na União Europeia, como apresenta o artigo "Cibersegurança na União Europeia e os Desafios para sua Eficácia"[66]. Segundo a autora, o Parlamento Europeu e Conselho aprovou, em 2019, a criação de uma certificação que compreende as regras de funcionamento, a forma como o trabalho é desenvolvido, a estrutura organizacional e outros aspectos relativos à cibersegurança. Para conceder a certificação, serão avaliados aspectos como: o âmbito de aplicação, o nível previsto de garantia, os critérios e métodos de avaliação entre outros aspectos.

Esta iniciativa deve servir de exemplo para a criação de uma certificação brasileira, mas pode ser utilizada atualmente por indústrias e fornecedoras de tecnologia como parâmetro para avaliação.

No contexto brasileiro, é necessário que as indústrias conheçam em profundidade a LGPD a fim de alinhar o uso e a adoção das tecnologias da indústria 4.0 de forma integrada com base nos requisitos dispostos na lei. Com base nesses aspectos explorados no workshop, as indústrias têm dificuldades em compreender quais são os padrões tecnológicos de segurança adotados pelas fornecedoras de soluções tecnológicas da Indústria 4.0 e qual é o nível básico de certificação de segurança que a fornecedora e seus colaboradores devem ter.

Considerando a análise de normas técnicas específicas, em relação aos fornecedores, salienta-se a série ISO/IEC 27036 de Cybersecurity — Supplier relationship (ISO/IEC 27036-1:2021 – Estágio 60.60) que possui normas publicadas e em desenvolvimento. A série já foi discutida no item 5.4 desse relatório, porque trata de uma visão geral, conceitos importantes, requisitos, diretrizes de comunicação segura e diretrizes para uso de serviços de computação em nuvem. No entanto, embora a série discorra sobre esses diversos itens, os especialistas, se acharem necessário, podem discutir a criação de uma possível norma relacionada à certificação dos fornecedores, se acharem necessário, ou, até mesmo, um framework que ajude na escolha de fornecedoras que tenham a cibersegurança como elemento principal da sua solução. Dessa forma, a indústria poderá utilizar a norma para aprimorar o seu processo de decisão direcionado à cibersegurança e, quando as fornecedoras de tecnologias e as empresas utilizarem essa série de normas técnicas, poderão maximizar os seus resultados com um melhor relacionamento com os fornecedores. Escolhendo, consequentemente, a fornecedora com a solução tecnológica de cibersegurança mais adequada aos desafios enfrentados pela empresa.

Além da série relacionada a fornecedores, também há série Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Framework for the specification of evaluation methods and activities (ISO/IEC DIS 15408) que também já foi discutida anteriormente. Dessa série, destaca-se, principalmente, a parte 4 da série, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities (ISO/IEC FDIS 15408-4 – Estágio 50.00). Essa norma define os requisitos de garantia da série ISO / IEC 15408, incluindo os componentes de garantia individuais a partir dos quais os níveis de garantia de avaliação e outros pacotes contidos na ISO / IEC 15408-5 são compostos, e os critérios para avaliação de Perfis de Proteção (PPs), Configurações de PP, Módulos de PP e Metas de Segurança (STs).

Portanto, é importante ressaltar a junção das partes 4 e 5 para se ter um maior entendimento de como aplicar a norma no contexto de avaliação de sistemas integrados, por exemplo, pois a norma Information security, cybersecurity and privacy protection — Evaluation criteria

for IT security — Part 5: Pre-defined packages of security requirements (ISO/IEC FDIS 15408-5- Estágio 50.00) abrange os pacotes de segurança pré-definidos, que podem ser definidos para a integração. A utilização das normas técnicas da série permite que a empresa tenha noção de suas operações e possa fazer avaliações internas de sua segurança e suas tecnologias, dando a opção de que a empresa possa entender seus próprios padrões para buscar fornecedores que se encaixam. Ademais, é importante salientar que a parte de fornecedores também encaixaria a série de normas já citadas (ISO/IEC DIS 15408), visto que, além de realizar uma avaliação interna, as empresas deveriam realizar uma avaliação externa.

No entanto, as indústrias devem buscar também por certificações. Ou melhor, de forma geral, as normas técnicas analisadas não abordam a parte de certificações, ficaria a cargo da empresa a escolha do mais adequado para si. Além disso, há possibilidade de desenvolver normas para certificações como já salientado, porém é importante ressaltar a união do uso das séries já pode trazer inúmeros benefícios para as empresas que estão enfrentando o problema.

Consequentemente, a discussão dos especialistas sobre o tema é primordial para a criação de normas técnicas que possam suportar o desenvolvimento de certificações das empresas, das fornecedoras de tecnologias da Indústria 4.0 e dos profissionais das áreas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas

Problema: Falta de entendimento para promover integração de forma segura			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27036-1:2021	Cybersecurity — Supplier relationships — Part 1: Overview and concepts	Estágio 60.60	Incluir normas para promover a segurança, incluindo aspectos de certificações, avaliações de cibersegurança, diretrizes de cibersegurança
ISO/IEC DIS 27036-2	Cybersecurity — Supplier relationships — Part 2: Requirements	Estágio 40.60	
ISO/IEC CD 27036-3	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	Estágio 90.92	
ISO/IEC FDIS 15408-4	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 4	Estágio 50.00	
ISO/IEC FDIS 15408-5	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 5	Estágio 50.00	

5.8 Necessidade de definição de requisitos mínimos de governança de cibersegurança (5 – 6º)

Durante os workshops, os especialistas discutiram sobre a necessidade de que os projetos de soluções tecnológicas da Indústria 4.0 envolvam aspectos de cibersegurança. Os projetos necessitam que requisitos mínimos de governança sejam atendidos pelas empresas para que elas consigam prover segurança e confiabilidade nos dados internos e nos clientes. Outrossim, os especialistas discutiram sobre a necessidade de padronização dos processos governança em termos de procedimentos e atualizações necessárias em relação à cibersegurança e a necessidade de definição dos processos

de governança para questões específicas, como ataques de hackers e/ou vazamento de informações e dados de clientes.

Dessa maneira, os especialistas enfatizaram os aspectos de governança da cibersegurança. A norma ISO / IEC 27001 define governança da cibersegurança como, "o sistema pelo qual uma organização dirige e controla a governança de segurança, especifica a estrutura de responsabilidade e fornece supervisão para garantir que os riscos sejam adequadamente mitigados, enquanto a administração garante que os controles sejam implementados para mitigar os riscos. " Com base nessa definição, a governança da cibersegurança é muito importante para diversos setores da economia e para manter o funcionamento de aspectos críticos de segurança. Por isso, o governo investe na cibersegurança de tratamento de água e de smart grids[67] para que a entrega de serviços seja feita de forma segura à sociedade. Outrossim, outro aspecto de suma relevância tanto no meio acadêmico quanto no meio industrial é que a Governança da Cibersegurança é um conceito relativamente novo e muito relevante, a ideia de avaliar a eficácia da implementação da Governança da Segurança Cibernética ainda é muito debatida e pesquisada[68]. Logo, como discutido pelos especialistas no workshop, a criação de normas nesse sentido pode auxiliar e direcionar o desenvolvimento de soluções de governança de cibersegurança viáveis e padronizadas para as empresas, as fornecedoras de soluções tecnológicas, o governo e a sociedade.

As indústrias em geral têm um desafio bem grande em relação à cibersegurança. A obtenção de provas de ataques hackers ou a responsabilização por vazamentos de dados é um desafio no Brasil não só para as empresas como ta bém para a polícia[69]. Após a decisão em 2010 de não aderir à Convenção de Budapeste, que contém diretrizes relacionadas ao direito processual penal para crimes cibernéticos, a legislação brasileira tem sido lenta para definir padrões e limites para o uso do ambiente virtual. Atualmente, investigadores possuem dificuldade para obter acesso aos Log de Dados (registro de eventos de um sistema computacional) e Internet Protocols (identificação de dispositivos), pois, muitas vezes, eles estão em posse de empresas privadas ou em países com os quais não há grande cooperação no assunto. Portanto, o Brasil ainda tem muito a avançar neste âmbito a fim de definir padrões de governança e procedimentos úteis para resolução de problemas. Entretanto, mesmo que exista algumas dificuldades internacionais em relação à cibersegurança, o Brasil tem avançado na criação de leias internas sobre o assunto, a LGPD.

Nela, há uma seção de boas práticas relacionadas à Governança. No artigo 50, existe o inciso: "demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento

desta Lei." Ou seja, indústrias, governos e universidades podem ser solicitados a demonstrarem se o programa de governança construído está sendo efetivo. Logo, é muito importante a intersecção da LGPD com as outras normas de governança para que possam ser construídos planos de governança alinhados a necessidades das empresas com base em requisitos mínimos da LGPD e das normas técnicas internacionais. Logo, as indústrias e as fornecedoras de soluções de cibersegurança necessitam criar uma estrutura de governança robusta o suficiente para mitigar possíveis incidentes de segurança contra as empresas. Por isso, o desenvolvimento de um padrão de governança é essencial para que as empresas possam desenvolver seus processos focadas em resultados operacionais, mitigando os possíveis incidentes de segurança.

No que concerne às normas técnicas específicas, a Information security, cybersecurity and privacy protection — Governance of information security (ISO/IEC 27014:2020 – Estágio 60.60), que foi publicada em 2020, fornece orientação sobre conceitos, objetivos e processos para a governança da segurança da informação, por meio dos quais as organizações podem avaliar, direcionar, monitorar e comunicar os processos relacionados à segurança da informação dentro da organização. O público-alvo desta norma é: corpo diretivo e alta administração; aqueles que são responsáveis por avaliar, dirigir e monitorar um sistema de gestão de segurança da informação (SGSI) baseado na ISO / IEC 27001; os responsáveis pela gestão da segurança da informação.

Dessa forma, é possível observar que já há uma norma relacionada à governança da segurança da informação que aborda sobre outras normas relacionadas à governança e gestão, governança da segurança da informação propriamente dita e requisitos dos especialistas e cenários de governança. Logo, com essa norma que pode solucionar parcialmente o problema destacado na seção, os especialistas já poderiam começar uma discussão sobre os requisitos de governança da cibersegurança, visto que a norma apresenta soluções para segurança em geral, algumas especificidades para cibersegurança precisariam ser debatidas, juntamente com os aspectos da LGPD. Alinhando, assim, a normalização internacional com a legislação nacional.

A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Necessidade de definição de requisitos mínimos de governança de cibersegurança			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27014:2020	Information security, cybersecurity and privacy protection — Governance of informationsecurity	Estágio 60.60	Incluir nas normas requisitos de governança de cibersegurança, expandindo as normas pré-existentes

5.9 Cibersegurança em dispositivos IoT (5 – 7°)

No decorrer do workshop, os especialistas relataram que as indústrias e as fornecedores de tecnologia da Indústria 4.0 possuem dificuldades em propiciar a segurança dos dados na implementação de dispositivos IoT em diversos contextos. Embora esse seja um tema também presente no workshop de interoperabilidade, apresentou-se em destaque no de cibersegurança, já que, segundo os especialistas e a Deloitte[70], por exemplo, as soluções de IoT oferecem novas maneiras para as empresas e as indústrias criarem valor, porém a conectividade constante e o compartilhamento de dados também criam oportunidades para o comprometimento das informações que podem aumentar o número de incidentes de cibersegurança. Isto posto, as empresas estão buscando novas maneiras de mitigar os riscos cibernéticos em dispositivos IoT.

Muitas vezes, as empresas compram os dispositivos IoT de fornecedoras que já dispõem intrinsicamente de mecanismos de cibersegurança com intuito de diminuir os riscos e aumentar a segurança dos equipamentos. Outrossim, como a estrutura do IoT é complexa, os padrões e protocolos precisam ser modificados para que seja possível a criação de um ambiente que proporcione a troca de dados de forma segura[71]. Logo, o desenvolvimento de normas que possam ajudar

no desenvolvimento de uma arquitetura IoT padronizada que inclua modelos de dados, interfaces e protocolo, por exemplo[72]. Por fim, o uso da IoT agilizou imensamente os processos produtivos uma vez que possibilitou a captura de informações e transmissão para tomadas de decisão em tempo real. O grande desafio da cibersegurança é garantir a confidencialidade, integridade e disponibilidade dessas informações. Para isso, é preciso primeiramente avaliar as vulnerabilidades dos protocolos utilizados e entender como é feita a transmissão de informações[73]. A partir disso, é possível definir softwares e outras ferramentas adequadas ao tipo de produção que irão garantir a segurança dos espaços virtuais.

No Brasil, em relação à segurança em IoT, o MCTI lançou ações estratégicas de IoT e a ação 31 busca "fomentar o uso de plataformas abertas, padronizadas e seguras para implantação de soluções IoT nos ambientes priorizados, priorizando soluções que se valham de protocolos e interfaces de comunicação padronizados por órgãos reconhecidos." Ou seja, o governo direciona na estratégia para que a informação esteja em um ambiente padronizado e seguro, mas também apresenta o foco na interoperabilidade. Além disso, existem diversos objetivos catalisadores referentes a aspectos: Regulatório, Segurança e Privacidade[74]. Entre os objetivos, destaca-se: "incentivar a adoção de padrões internacionais na temática de segurança da informação pela iniciativa privada."

Esse objetivo está relacionado ao que os especialistas e a literatura discutem sobre o problema. De forma geral, com base nessa análise, as indústrias e as fornecedoras de soluções tecnológicas precisam entender quais são os mecanismos de segurança, as melhores práticas, as diretrizes em relação à segurança de dispositivos IoT e de seus dados. Além disso, os especialistas destacaram que casos de uso podem facilitar esses processos e uma regulamentação bem estrutura também.

Em relação às normas da intersecção entre Cibersegurança e IoT, destacam-se as seguintes normas que estão em desenvolvimento: Cybersecurity — IoT security and privacy — Guidelines (ISO/IEC DIS 27400 – Estágio 40.60); Cybersecurity — IoT security and privacy — Device baseline requirements (ISO/IEC CD 27402.2 – Estágio 30.60); Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics (ISO/IEC WD 27403.6 – Estágio 20.20). A norma ISO/IEC DIS 27400 já foi discutida no item 5.3 do relatório e trata sobre diretrizes sobre riscos, princípios e controles para segurança e privacidade de soluções de IoT.

Desse modo, a norma pode ser utilizada para identificar as principais características dos sistemas IoT e ainda auxilia na parte de mapeamento das fontes de risco, inclusive aborda questões de controle de segurança e privacidade no contexto do IoT. Como as outras duas normas (ISO/IEC CD 27402.2 - Estágio 30.60 e ISO/IEC WD 27403.6 - Estágio 20.20) estão em fase de desenvolvimento de um estágio a priori da norma citada, as duas normas não têm

um escopo pré-definido. No entanto, é uma oportunidade de trabalho junto as especialistas para que eles ajudem a definir quais são os requisitos básicos de segurança e de privacidade do dispositivo IoT, por exemplo. Além desse dispositivo, os especialistas podem discutir em relação ao uso de CLP e sensores, por exemplo. A partir dessas normas, os especialistas podem construir um arcabouço para aprimorar os aspectos de cibersegurança em dispositivos IoT, diminuindo, assim, os riscos de perda de informação dos clientes, dos fornecedores e das suas linhas de produção.

Como os dispositivos IoT estão conectados à Internet, uma das normas interessantes nesse tipo de situação é a norma geral, Information technology — Security techniques — Guidelines for cybersecurity (ISO/IEC CD 27032.3 – Estágio 30.20), que foi publicada em 2012 e está em desenvolvimento novamente. A norma fornece orientação para melhorar o estado da segurança cibernética, destacando os aspectos exclusivos dessa atividade e suas dependências de outros domínios de segurança, em particular: segurança da informação, segurança de rede, segurança da internet, e proteção de infraestrutura de informação crítica (CIIP). Sendo assim, a ISO/IEC CD 27032.3 pode ajudar na resolução do problema evidenciado nessa seção porque traz aspectos importantes de segurança da informação, de rede e de Internet. Com base nas análises das normas em desenvolvimento e publicadas, é importante ressaltar que os especialistas têm oportunidades de criar soluções viáveis para o problema de cibersegurança nos dispositivos IoT além de discutir aspectos relacionados ao Plano Nacional de Internet das Coisas. Além disso, é recomendado realizar um trabalho em conjunto entre os grupos de cibersegurança e IoT para que as normas sejam pensadas direcionadas à necessidade da indústria e das fornecedoras de soluções de IoT.

Entretanto, também é necessária a discussão do assunto em relação a outras tecnologias da Indústria 4.0, como IA (discutido na seção 4.12) e gêmeos digitais. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Cibersegurança em dispositivos IoT			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC DIS 27400	Cybersecurity — IoT security and privacy — Guidelines	Estágio 40.60	Incluir nas normas diretrizes, checklists e frameworks em relação à cibersegurança em dispositivos IoT direcionadas à indústria, clientes e fornecedores de tecnologias
ISO/IEC CD 27402.2	Cybersecurity — IoT security and privacy — Device baseline requirements	Estágio 30.60	
ISO/IEC WD 27403.6	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	Estágio 20.20	
ISO/IEC CD 27032.3	Information technology — Security techniques — Guidelines for cybersecurity	Estágio 30.20	

Em relação ao grupo de Cibersegurança, a Figura 2 sumariza os principais problemas destacados que podem ser debatidos pelos especialistas com intuito de que as normas sejam desenvolvidas de forma alinhada.

Figura 2 - Tópicos para debate entre os especialistas de Cibersegurança

6 Grupo de Internet das coisas e Gêmeos digitais (ISO/IEC JTC 1/SC 41)

6.1 Escopo

O grupo de Internet das coisas e gêmeos digitais (ISO/IEC JTC 1/SC 41) tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin, além de fornecer orientação a entidades que desenvolvem aplicativos relacionados. Neste workshop também foram debatidos com os especialistas os problemas no contexto da interoperabilidade, que é um dos pilares para alcançar os gêmeos digitais. A seguir serão detalhados os problemas apontados pelos especialistas.

6.2 Dificuldade na integração dos softwares e hardwares de diversos fornecedores (17-1º)

Segundo os especialistas, as indústrias têm dificuldade em realizar a integração dos softwares e dos hardwares de diversos fabricantes para a coleta de dados e promover a interoperabilidade. Durante o workshop, os especialistas debateram sobre alguns problemas, por exemplo: diferentes versões de softwares para cada controlador industrial; necessidade de integração entre sistemas da empresa na nuvem a fim de garantir a segurança e facilidade de acesso à informação, porém alguns especialistas também relataram dificuldade para armazenamento dos dados em nuvem já que as empresas não conseguem integrar rede de tecnologias da automação (TA) com TI; necessidade de padronização a fim de que seja realizada a integração entre equipamentos.

É importante destacar que a desconexão entre profissionais de TI e de TA é uma das barreiras no desenvolvimento e na adoção de soluções IoT na indústria que foi apontado no relatório do aprofundamento de verticais do Estudo de IoT, que foi base para o desenvolvimento do Plano Nacional de IoT[75]. Além disso, os mesmos problemas são relatados por fornecedores de soluções tecnológicas, visto que "as integrações são complexas e cheias de desafios, uma vez que podem ocorrer entre soluções estruturadas, de diferentes provedores, de diferentes épocas, com plataformas distintas, com tecnologias distintas, usando protocolos distintos, repleta de restrições, limitações, problemas, separadas geograficamente dentro e fora do escopo da organização."[76] Dessa forma, como, em muitos casos, a indústria possui equipamentos de diferentes gerações tecnológicas, há

essa dificuldade de integração entre os softwares e hardwares utilizados.

Além dessas dificuldades de integração, os especialistas discutiram as dificuldades em relação às Application Programming Interface (APIs). No workshop, enfatizaram-se os seguintes problemas: a necessidade de padronização de APIs de sistemas e Enterprise Resource Planning (ERPs) para integração dos dados e a necessidade de atualizações constantes de APIs a cada novo release de um software, por exemplo, uma nova versão do sistema ERP utilizado na empresa. Em relação a esse aspecto, APIs integradas com ERP que as indústrias utilizam para gerenciar os dados da empresa podem ser suscetíveis a algumas falhas operacionais, porque, por meio da API, pode haver problemas de cibersegurança[77]. Logo, as normas podem ajudar as indústrias a implementarem APIs com menos falhas operacionais e de cibersegurança, propiciando, assim, a continuidade do negócio e mitigando os possíveis riscos associados ao uso de API para o acesso de serviços.

Além da questão de conhecer recursos para realizar a coleta, exportação e padronização de dados, as empresas e fornecedoras de tecnologia precisam ter em mente que diferentes alternativas podem acarretar maior ou menor consumo de recursos como memória e energia. Alguns exemplos de sistemas utilizados são[78]: Key-value based, em que os dados são tratados como chaves e valores em arquivos e Markup scheme based, que usa tags para modelar os dados e permite o uso de mecanismos de troca de dados e linguagens de marcação para armazenamento e transferência de dados. Logo, como existem muitos recursos para integrar os dados, as indústrias têm dificuldades em escolher qual é o melhor. De forma geral, com base no que foi discutido com os especialistas e evidenciado na literatura, as indústrias sofrem com diversas barreiras, entre elas a falta de padronização dos softwares, falta de mão de obra especializada, uso de diferentes versões dos softwares que dificultam a interoperabilidade e a integração, falta de uma cultura de integração, dificuldade em utilizar uma estrutura de rede que integre equipamentos e máquinas, uso do gerenciamento da exceção para que as mensagens sejam enviadas e recebidas entre aplicativos independentes e necessidade de atualização constante das APIs.

Em relação a normas, há a série ISO/IEC21823, Internet of things (IoT) — Interoperability for IoT systems, em que todas as normas já foram publicadas. A norma ISO / IEC 29182-1: 2013 (Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework – Estágio 60.60) fornece uma visão geral das características de uma rede de sensores e a organização das entidades que compõem essa rede. Ele também descreve os requisitos gerais que são identificados para redes de sensores. Desse modo, as indústrias podem utilizar o framework para aprimorar a interoperabilidade na utilização de sistemas IoT, visto que a norma abrange aspectos como: requisitos de

interoperabilidade para características de IoT e framework para sistemas IoT interoperáveis com base na arquitetura de referência IoT. Com base nessa norma, os especialistas podem ajudar na criação de outras normas que contenham informações além dos sistemas IoT. Ademais, é importante os especialistas discutirem o tema em relação às ações estratégicos do Plano Nacional de Internet das Coisas, que tem algumas ações estruturantes com foco em Infraestrutura, Conectividade e Interoperabilidade.

Entre os objetivos, destacam-se os seguintes itens: "Incentivar e apoiar a adoção de IoT no que diz respeito à interoperabilidade." e "Consolidar boas práticas relacionadas com IoT que favoreçam interoperabilidade."[79] Logo, a discussão da normalização internacional também deve ser em relação a esses aspectos estratégicos presente no Plano Nacional para que exista o alinhamento entre as normas nacionais e internacionais. Além disso, é fundamental ressaltar que esses objetivos também permeiam os outros problemas de IoT destacados neste relatório.

Já, a segunda norma da série, Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability (ISO / IEC 21823-2: 2020 – Estágio 60.60), especifica uma estrutura e requisitos para interoperabilidade de transporte, a fim de permitir a construção de sistemas de IoT com troca de informações, conectividade ponto a ponto e comunicação contínua entre diferentes sistemas de IoT e entre entidades dentro de um sistema IoT. Na norma, são especificados: modelo de conectividade de rede e interfaces entre sistemas IoT; modelo de conectividade de rede e interfaces em um sistema IoT; interfaces de rede entre diferentes sistemas IoT; elementos de rede para suporte de conectividade de rede. Ademais, a norma apresenta elementos visuais para que os especialistas possam discutir como aplicar em casos mais gerais de interoperabilidade, possibilitando, consequentemente, o alinhamento entre as necessidades da indústria e o desenvolvimento das normas.

Outrossim, a terceira norma da série, Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability (ISO/IEC 21823-3:2021 - Estágio 60.60), fornece os conceitos básicos para interoperabilidade semântica de sistemas IoT, conforme descrito no modelo de faceta da ISO / IEC 21823-1, incluindo: requisitos das ontologias principais para interoperabilidade semântica; melhores práticas e orientação sobre como usar ontologias e desenvolver aplicativos específicos de domínio, incluindo a necessidade de permitir a extensibilidade e a conexão com ontologias externas; casos de uso e cenários de serviço que apresentam necessidades e requisitos de interoperabilidade semântica. Como a norma apresenta exemplos e casos de uso, facilita a utilização em outros contextos, porque, com base nos exemplos apresentados, pode-se observar como a integração pode ser realizada de outra forma. No relatório do aprofundamento

de verticais, que foi base para o desenvolvimento do Plano Nacional de IoT, também existem diversos exemplos de aplicação de tecnologias IoT com algumas descrições para o setor industrial para gestão de estoque, monitoramento de barragens, manutenção preditiva, engenharia de produção, integração da planta produtiva, explicando como as camadas estão relacionadas de forma sintética[80].

Além dos exemplos relacionados à indústria, existem outros relatórios que abrangem, por exemplo, a área de saúde (monitoramento de condições dos pacientes com diabetes; diagnóstico descentralizado; identificação e controle de epidemias, entre outros)[81] e área rural (monitoramento do microclima, gestão de pragas, monitoramento da saúde animal, entre outros)[82]. Consequentemente, os especialistas podem debater sobre casos de usos do problema presentes tanto na normalização internacional quanto nos relatórios de IoT do governo.

As normas analisadas até o momento para o problema evidenciado têm foco em IoT e conseguem resolver parcialmente o problema. Como o problema não envolve somente tecnologias IoT, destaca-se também a seguinte norma: Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7: Interoperability guidelines (ISO/IEC 29182- 7:2015 – Estágio 60.60), que já foi publicada e é a sétima parte da série ISO/IEC 29182. A norma fornece uma visão geral e diretrizes para alcançar a interoperabilidade entre os serviços de rede de sensores e entidades relacionadas em uma rede de sensores heterogênea. Além de exemplos relacionados dos dispositivos IoT, as normas apresentam casos de interoperabilidade em sensores. A norma tem como principal foco fornecer uma visão geral e diretrizes para alcançar a interoperabilidade entre os serviços, o que está consonância com o problema das indústrias em realizar a integração de softwares e hardwares. Entretanto, como discutido anteriormente, os especialistas precisam discutir muito sobre o tema para conseguirem ter uma visão geral da situação, incluindo aspectos técnicos e gerenciais, embora a norma já apresente uma visão geral que facilite esse processo.

Entretanto, embora existam diversas normas sobre a interoperabilidade de sistemas IoT e de sensores, seria interessante os especialistas discutirem algumas partes mais técnicas de integração de hardware e software, utilizando as normas supracitadas como exemplo. Além disso, é fundamental que os especialistas discutam também em relação as APIs e como podem criar normas para melhorar o seu funcionamento, diminuindo, consequentemente, as falhas que podem ser ocasionados.

Com base nessas primeiras análises, os especialistas têm diversas oportunidades para a solução do problema que é fundamental para a adoção de tecnologias digitas da Indústria 4.0, orientadas também pelo Plano Nacional de IoT. A tabela abaixo apresenta um resumo das normas que podem atender ao problema

apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Dificuldade na integração dos softwares e hardwares de diversos fornecedores

Normas técnicas que podem atender ao problema

Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO / IEC 29182-1: 2013	(Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework –	Estágio 60.60	Incluir nas normas diretrizes e frameworks para técnicas de integração de hardware ISO / IEC e software
ISO / IEC 21823-2: 2020	Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability	Estágio 60.60	
ISO/IEC 21823- 3:2021	Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability	Estágio 60.60	
ISO/IEC 29182-7:2015	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7: Interoperability guidelines	Estágio 60.60	

6.3 Diversidade de protocolos e padrões de comunicação (14 – 2º)

No decorrer do workshop, os especialistas destacaram que os protocolos e padrões de comunicação são os mais diversos no ambiente industrial, e as indústrias e as fornecedoras de tecnologias digitais da Indústria 4.0 têm dificuldades em entender quais protocolos elas podem e/ou devem utilizar para realizar a troca de informação de forma correta e segura, propiciando, assim, a interoperabilidade. Os especialistas enfatizaram que buscam a uniformização dos protocolos de comunicação e de diferentes fabricantes e visam a padronização dos protocolos com intuito de que eles sejam capazes de trocar mensagens de forma correta e segura. No ambiente IoT, existem diversos protocolos de comunicação, porém foi necessária a criação de novos protocolos, o que pode dificultar a interoperabilidade e comunicação[83].

Dessa forma, as arquiteturas de comunicação são as mais diversas e é importante que as indústrias escolham da melhor forma possível com base na análise das vantagens e desvantagens de cada um para permitir um incremento na interoperabilidade e na segurança[84]. Como existem muitos protocolos que permitem a troca de informações, é difícil realizar a escolha correta e assertiva para cada caso específico, logo os especialistas indicaram que as normas poderiam ajudar nesse sentido. Essa necessidade evidenciada pelos especialistas também está presente como uma das ações estratégicas do Plano Nacional de Internet das Coisas: "fomentar o uso de plataformas abertas, padronizadas e seguras para implantação de soluções IoT nos ambientes priorizados, priorizando soluções que se valham de protocolos e interfaces de comunicação padronizados por órgãos reconhecidos."[85] Em outro documento do Estudo IoT que consolida os resultados das entrevistas e pesquisa[86], há o seguinte desafio em relação ao desenvolvimento de IoT: "O estímulo à adoção de padrões abertos tanto em termos de conectividade de dispositivos quanto de redes, por meio dos quais se avança rumo à interoperabilidade global". Logo, o problema destacado no workshop pelos especialistas está bastante evidenciado no contexto de IoT.

Complementarmente, com o desenvolvimento acelerado da IoT nos últimos anos, é possível notar o desenvolvimento de objetos para esta tecnologia provenientes de diversos fabricantes. Com isso, a padronização de protocolos se tornou um grande desafio para as empresas[87]. Por exemplo, um dos protocolos mais amplamente difundidos é o Padrão IEEE 802.15.4, que permite interconexões para comunicação com baixo consumo e complexidade. Ele também fornece uma base para a adição de outros protocolos em camadas superiores.

Diversos outros protocolos, como Zigbee (mais utilizado para serviços de segurança e novos dispositivos) e Thread (utilizado em Smart homes) utilizam o IEEE 802.15.4 como base. Isto posto, existem diversos protocolos e padrões de comunicação

que as indústrias podem utilizar para propiciar a interoperabilidade, o que foi evidenciado pelos especialistas, literatura e Plano Nacional de IoT e documentos correlatos. Com base nesses aspectos, de forma geral, o problema relatado é que as indústrias e as fornecedoras de tecnologias da Indústrias 4.0 estão buscando padrões de integração com vários protocolos, e as indústrias e fornecedoras também discutem muito o uso de padrões abertos para facilitar a integração da tecnologia.

Ademais, no que tange às normas, há série Internet of things (IoT) — Interoperability for IoT systems (ISO/IEC21823 – Estágio 60.60), que foi discutida também na seção 6.2, acredita-se que a norma atenda parcialmente o problema, uma vez que aborda uma visão geral de interoperabilidade, permitindo, de certa forma, o desenvolvimento de padrões de comunicação. Nesse caso, como a série traz uma perspectiva de protocolos mais geral relacionado à interoperabilidade de sistemas IoT, pode ser utilizado de exemplo pelos especialistas para eles criarem padrões e protocolos que promovam a troca de informação mais segura no ambiente industrial. Entretanto, ainda falta a análise de protocolos e padrões de comunicações na adoção de outras tecnologias da Indústria 4.0.

Nesse sentido, existe também a série Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) (ISO/IEC 29182), também já parcialmente discutida na Seção 6.2. A primeira norma da série, Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements (ISO / IEC 29182-1: 2013 – Estágio 60.60), fornece uma visão geral das características de uma rede de sensores e a organização das entidades que compõem essa rede. Novamente, percebe-se que os especialistas precisam partir de uma visão geral para que eles possam utilizar protocolos e padrões de comunicação para que consigam discutir as melhores opções a serem utilizadas em contextos diversos. No entanto, ainda não está clara com essa norma quais diretrizes que precisam ser seguidas, visto que a primeira parte contempla parcialmente o problema apresentado por proporcionar uma visão geral do problema destacado na seção.

Desse modo, novamente, como na seção 6.2, destaca-se a sétima parte da série (Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7: Interoperability guidelines - ISO / IEC 29182-7: 2015 – Estágio 60.60) que fornece uma visão geral e diretrizes para alcançar a interoperabilidade entre os serviços de rede de sensores e entidades relacionadas em uma rede de sensores heterogênea. O problema apresentado é contemplado parcialmente pela sétima parte da série, uma vez que ela expõe diretrizes para a interoperabilidade de sistemas que utilizam sensores. Ela também estabelece padrões para integração, que podem servir de base para as indústrias

e fornecedoras de tecnologia solucionarem seus problemas. Ou melhor, a norma explora dois tópicos: visão geral da interoperabilidade entre redes de sensores heterogêneas e diretrizes para interoperabilidade entre redes de sensores heterogêneas. Portanto, a presença de especialistas é essencial nesse contexto para que sejam discutidos aspectos relacionados à dificuldade pela diversidade de protocolos de comunicação. Com ajuda dos especialistas, é possível direcionar as normas e/ou adicionar uma norma na série a fim de ajudar na uniformização dos protocolos e padrões utilizados na indústria.

Com base na análise das duas séries, observou-se que as normas, principalmente as duas séries, podem trazer benefícios para as empresas porque através delas as indústrias conseguem entender conceitos de forma geral, porém ainda atendem de forma parcial o problema. Logo, seria necessária uma maior especificidade técnica, por exemplo, as normas publicadas e em desenvolvimento do grupo prioritário de Redes Industriais (IEC/TC65/SC65C) – discutido na Nota Técnica C - poderiam ajudar nessas questões. Em relação a padrões e protocolos de comunicação, as normas do grupo têm avançado em perfis de comunicação de redes sem fio e modelos de coexistência das redes sem fio. Dessa forma, os especialistas devem entender de tópicos além dos relacionados aos grupos prioritários que trabalham diretamente, uma vez que os grupos de normalização estão altamente relacionados, como demonstrado nas notas técnicas anteriores. Além disso, é importante que, com o auxílio dos especialistas, as indústrias possam compreender como elas podem aumentar a interoperabilidade sem prejuízo nos processos já existentes e possam usufruir dos benefícios de protocolos para criar um ambiente de automação industrial. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Diversidade de protocolos e padrões de comunicação			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 21823	Internet of things (IoT) — Interoperability for IoT systems	Estágio 60.60	Incluir nas normas diretrizes e framewoks para promover a interoperabilidade que envolvem a diversidade de protocolos e padrões de comunicação
ISO/IEC 29182-1: 2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 1	Estágio 60.60	
ISO / IEC 29182-7: 2015	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7	Estágio 60.60	

6.4 Cibersegurança em dispositivos IoT para interoperabilidade (6 -3°)

Além de ser destacado o tema na seção 5.8 no workshop sobre cibersegurança, o tema também foi debatido no workshop de interoperabilidade. De acordo com os especialistas presentes nos workshops, as indústrias têm dificuldade em promover a segurança no uso de dispositivos IoT, porque elas utilizam muitos componentes inseguros, inclusive os especialistas do workshop de interoperabilidade enfatizaram que existem problemas em relação ao gerenciamento de backups. Entre os tópicos debatidos pelos especialistas, destacam-se: uso de componentes inseguros, não industriais e/ou obsoletos nos ambientes industriais; gerenciamento de backups na área de TA não realizado pelas ferramentas da TI adequadas e seguras; uso de sistemas legados embarcados sem documentação, sem backups e sem possibilidade de acesso externo.

Com base nessas constatações, evidencia-se que a área de automação industrial necessita investir em backups. Como existem muitas mudanças em configurações de PLCs, por exemplo, e algumas mudanças não ocorrem tão bem e podem desencadear paradas inesperadas nas linhas de produção. Logo, se a empresa tem backups, é possível ter uma gestão de automação industrial de forma

ativa com intuito de manter um ritmo de produção mais otimizado[88]. Além disso, muitas indústrias buscam serviços de computação na nuvem na automação industrial para informações que precisam de backup e rastreio[89]. Assim, adquirem um IaaS (Infrastructure-as-a-Service) que é composto por máquinas virtuais e backups, logo, quando adquirem o serviço, também adquirem o serviço de cibersegurança[90], que foi discutido na seção 4.5. Também se evidencia que muitas pequenas e médias empresas acabam contratando um serviço mensal com fornecedores de soluções de cibersegurança para garantirem que seus backups, antivírus e firewall estejam funcionando adequadamente, uma vez que apresentam diversos componentes inseguros no ambiente industrial.

A questão dos componentes é também debatida no Plano Nacional de IoT com os seguintes itens: "Revisão do processo de importação de componentes eletrônicos e insumos para a pesquisa necessários aos dispositivos e soluções de IoT." e "Promover os padrões brasileiros de soluções para conectividade em IoT como referências para padrões internacionais, de modo a estimular economias de escala para os componentes das soluções."[91] Dessa forma, conforme os itens do plano, mesmo que eles não foquem explicitamente em cibersegurança, é possível observar que o objetivo também é utilizar/desenvolver componentes mais seguros e que estejam dentro dos padrões internacionais e desenvolver padrões nacionais, o que também está relacionado ao problema da seção 6.3. Ademais, as pesquisas sobre os componentes são primordiais para o desenvolvimento de novos dispositivos que possivelmente serão mais seguros que os anteriores. Além desses aspectos, em relação a ações estratégicas de Regulação, Segurança e Privacidade, destaca-se a seguinte ação: "Incentivar a criação de sistema de certificação creditatória de segurança da informação em dispositivos em Internet das Coisas, baseada em modelo de autorregulação voluntária pela iniciativa privada."[92] Esta ação está bastante relacionada com a segurança no ambiente IoT, logo há uma convergência entre ações para a criação de componentes e dispositivos seguros com base em padrões internacionais para o desenvolvimento de padrões nacionais seguros. Com base nesses aspectos, é importante destacar que os problemas evidenciados pelos especialistas também estão presentes no Plano Nacional de IoT.

Além dos aspectos destacados pelos especialistas e discutidos no Plano Nacional de IoT sobre a segurança, o uso da IoT acarretou o aumento do volume de dados pessoais que são compartilhados entre dispositivos, criando uma demanda por soluções de segurança capaz de proteger diversos tipos de dispositivos. A tecnologia de Blockchain também é muito utilizada por empresas atualmente, no entanto poucas têm consciência de que é possível utilizá-la para proteção de IoT[93]. A ideia é que através de um sistema de DHT (distributed hash table) seja possível compartilhar apenas partes

necessárias de arquivos, e não a sua integridade. A Blockchain é então usada de forma a gerenciar onde esses dados estão distribuídos e quem tem acesso a eles. Dessa forma, Blockchain é outra tecnologia da Indústria 4.0 que pode ajudar na segurança de dados das indústrias e das cadeias de suprimentos. Com base nos aspectos destacados, de forma geral, pode-se observar que as indústrias e as fornecedoras de tecnologias de transformação digital estão com dificuldades em garantir a interoperabilidade do sistema, visto que, em alguns casos, são utilizados componentes inseguros.

Complementarmente, em relação a normas, destacam-se normas que já foram publicadas: Information technology — Security techniques — Information security risk management (ISO/IEC 27005:2018 – Estágio 90.92 – será substituída por uma norma que está em desenvolvimento que está no estágio 40.20) e Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016 – Estágio 90.92) e normas que estão em desenvolvimento Cybersecurity — IoT security and privacy — Guidelines (ISO/IEC DIS 27400 – Estágio 40.60) e Cybersecurity — IoT security and privacy — Device baseline requirements (ISO/IEC CD 27402.2 – Estágio 30.60). Além dessas normas, como foi discutida a questão do blockchain para a segurança, adicionou-se uma reflexão sobre a seguinte norma já publicada: Internet of Things (IoT) —- Integration of IoT and DLT/blockchain: Use cases (ISO/IEC TR 30176:2021 – Estágio 60.60).

A norma publicada ISO/IEC 27005:2018 fornece diretrizes para a gestão de riscos de segurança da informação. A norma é aplicável a todos os tipos de organizações (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos) que pretendem gerenciar riscos que podem comprometer a segurança da informação da organização. De forma geral, a norma explora o âmbito que diz respeito à gestão de riscos para segurança da informação de sistemas, inclusive os IoT. Com a norma, é possível realizar a identificação, análise e avaliação dos riscos associados no uso de dispositivos IoT, sistemas legados e automação industrial. Além disso, a norma aborda sobre o tratamento do risco, o que inclui modificações do risco, retenção do risco, por exemplo, inclusive a norma aborda identificação e avaliação de ativos e avaliação de impacto com exemplos. Logo, as indústrias e fornecedoras podem utilizar alguns conceitos apresentados para melhorar a cibersegurança na automação industrial, porque a norma aborda diversos pontos que podem ser utilizadas por elas. Entretanto, mesmo que a norma aborde diversos aspectos das soluções, a norma soluciona apenas parcialmente o problema pois contempla apenas a parte dos requisitos de gestão de risco, não abordando a questão de interoperabilidade e backups, por exemplo.

A outra norma já publicada (ISO/IEC 27004:2016- Estágio 90.20) fornece diretrizes destinadas a auxiliar as organizações

na avaliação do desempenho da segurança da informação e a eficácia de um sistema de gestão da segurança da informação. Ou melhor, as indústrias podem verificar se o sistema de segurança delas está funcionando adequadamente, auxiliando parcialmente na resolução do problema destacado na seção. É importante ressaltar que a norma apresenta conceitos relacionados ao monitoramento, medição, análise e avaliação para sistemas. Com base nessas informações, as indústrias e fornecedoras de soluções tecnológicas podem aperfeiçoar e aumentar a interoperabilidade dos sistemas, otimizando, assim, a automação industrial. A norma aborda a questão da segurança, trazendo em seus anexos: um modelo de medição de segurança da informação e exemplos de construção de medição de segurança da informação, logo a norma está focada em segurança da informação, que é primordial no ambiente industrial, porém não aborda tanto os temas de backup, sensores e IoT.

Em relação à cibersegurança de sistemas IoT, no que tange às normas, a seção 5.8 já destacou as seguintes normas: Cybersecurity — IoT security and privacy — Guidelines (ISO/IEC DIS 27400 - Estágio 40.60); Cybersecurity — IoT security and privacy — Device baseline requirements (ISO/IEC CD 27402.2 - Estágio 30.60); Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics (ISO/IEC WD 27403.6 - Estágio 20.20). Nessa nova geração de tecnologias para a indústria 4.0, é importante se preocupar com a segurança dos dispositivos. Além disso, no ambiente industrial, há dispositivos de várias gerações tecnológicas, logo alguns dispositivos são mais seguros e outro menos. Com base nessas normas com foco em IoT, poder-se-ia obter uma base para tornar outros dispositivos mais seguros e desenvolver novas normas ou série nesse sentido, porque é importante, principalmente, nesses casos, a construção de normas sobre diretrizes e requisitos básicos, como as normas referentes a IoT.

A outra norma já publicada (ISO/IEC 27004:2016 - Estágio 90.20) fornece diretrizes destinadas a auxiliar as organizações na avaliação do desempenho da segurança da informação e a eficácia de um sistema de gestão da segurança da informação. Ou melhor, as indústrias podem verificar se o sistema de segurança delas está funcionando adequadamente, auxiliando parcialmente na resolução do problema destacado na seção.

É importante ressaltar que a norma apresenta conceitos relacionados ao monitoramento, medição, análise e avaliação para sistemas. Com base nessas informações, as indústrias e fornecedoras de soluções tecnológicas podem aperfeiçoar e aumentar a interoperabilidade dos sistemas, otimizando, assim, a automação industrial. A norma aborda a questão da segurança, trazendo em seus anexos: um modelo de medição de segurança da informação e exemplos de construção de medição de segurança da informação, logo a norma está focada em segurança da informação, que é primordial no ambiente industrial, porém não aborda

tanto os temas de backup, sensores e IoT.

No tange à tecnologia Blockchain, a ISO/IEC TR 30176:2021 (Estágio 60.60) identifica e coleta casos de uso para a integração do DLT/blockchain em sistemas, aplicativos e/ou serviços de IoT. Os casos de uso apresentados neste documento usam o modelo de caso de uso de IoT. Os casos apresentados na norma são referentes à agricultura, a serviços financeiros, a serviços de hipotecas de bem móveis, à distribuição de energias e a pagamentos automáticos de estacionamento.

Para cada um dos casos apresentados na norma, são discutidos, entre outros aspectos, segurança de dados, privacidade e confiabilidade. Logo, os especialistas podem discutir como a cibersegurança está sendo aplicada nesses casos e como pode ser expandida em outros casos e/ou indústrias que adotam as tecnologias blockchain e IoT. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Cibersegurança em dispositivos IoT para interoperabilidade			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management	Estágio 90.92	Incluir nas normas diretrizes, checklists e frameworks em relação à cibersegurança em dispositivos IoT direcionadas à indústria, clientes e fornecedores de tecnologias para promover a interoperabilidade
ISO/IEC 27004:2016	Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	Estágio 90.92	
ISO/IEC DIS 27400	Cybersecurity — IoT security and privacy — Guidelines	Estágio 40.60	
ISO/IEC CD 27402.2	Cybersecurity — IoT security and privacy — Device baseline requirements	Estágio 30.60	
ISO/IEC TR 30176:2021	Internet of Things (IoT) —- Integration of IoT and DLT/blockchain: Use cases	Estágio 60.60	
ISO/IEC DIS 27400	Cybersecurity — IoT security and privacy — Guidelines	Estágio 40.60	
ISO/IEC CD 27402.2	Cybersecurity — IoT security and privacy — Device baseline requirements	Estágio 30.60	
ISO/IEC WD 27403.6	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	Estágio 20.20	

6.5 Dificuldades em relação a dados para interoperabilidade (4 – 4º*)

Durante o workshop, os especialistas destacaram que as indústrias possuem dificuldades relacionadas ao uso de dados: como realizar a coleta de dados, quais são os dados necessários e quem é o requisitante de dados. De forma geral, os especialistas enfatizaram os seguintes relacionados ao tema: padronização dos sistemas de coleta e exportação de dados; adoção de um orquestrador para gerenciar os dados; dificuldade em padronizar os diversos tipos de dados; e necessidade de padronização no armazenamento dos dados. Isso posto, discutiu-se muito a necessidade de desenvolvimento de normas relacionadas aos dados para promover a interoperabilidade.

Em suma, a interoperabilidade de dados é um desafio para indústrias, visto que podem gerar interrupções de trabalho, prejudicar a colaboração de parceiros e aumentar o retrabalho[94]. No setor da construção civil, por exemplo, a Autodesk investiu na parceria com outras empresas para desenvolver APIs antes mesmo de utilizar a computação de nuvens[95]. Entretanto, as empresas citam, em alguns casos, o desenvolvimento de padrões de dados abertos, a criação de ambientes comuns de dados e o uso da computação na nuvem para o gerenciamento de dados[96]. Por exemplo, o problema de interoperabilidade de dados está presente em diversas indústrias: dados espaciais a geográficos[97] e dados da saúde[98] além de diversos setores da indústria de transformação. Complementarmente, o entendimento sobre o IoT em cidades, saúde, área rural e indústrias são prioritários conforme o estudo de IoT no Brasil[99]. Por exemplo, o setor industrial é um dos mais afetados no que se refere à questão de interoperabilidade e integração de sistemas relacionados à IoT, pois é um setor em que o desenvolvimento da tecnologia se deu de forma muito acelerada, resultando em uma grande variedade de objetos disponíveis provenientes de diversos fabricantes. Uma das soluções encontradas por empresas é a adoção de um sistema Publish/Subscribe[100], que viabiliza a integração e troca de informações entre agentes de dados.

Além disso, o protocolo MQTT (em inglês, Message Queuing Telemetry Transport) pode ser aplicado para o transporte das mensagens que carregam o conteúdo de carga útil ou payload (termo em inglês conhecido na área de comunicação para transmissão de dados). Por fim, mesmo que já existam diversas soluções no mercado, é importante ressaltar as indústrias e as empresas de fornecedoras de solução tecnológica têm dificuldade em coletar, exportar e padronizar os mais diversos tipos de dados, os especialistas destacaram que é um problema de diversos setores, como agricultura, saúde e manutenção das fábricas, o que converge com o que foi apontado pelos Estudos de IoT do Plano Nacional de IoT e pela literatura. Outrossim, em relação à análise de normas sobre o assunto, há a norma Internet of Things (IoT) — Requirements of IoT data exchange platform for various

IoT services (ISO/IEC 30161:2020 – Estágio 60.60) que já foi publicada sobre o assunto. A norma especifica requisitos para uma plataforma de troca de dados de IoT para vários serviços nas áreas de tecnologia de: os componentes de middleware de redes de comunicação, permitindo a coexistência de serviços de IoT com o legado; o desempenho dos pontos finais nas redes de comunicação entre a IoT e os serviços legados, entre outros.

A norma soluciona parcialmente o problema uma vez que estabelece as diretrizes para a troca de dados utilizando a IoT, porém outras indústrias podem buscar alternativas além do uso do IoT que precisam ser debatidas. Com base na norma de IoT, as empresas e as fornecedoras de soluções tecnológicas podem utilizar essas diretrizes como base para coletar, exportar e padronizar as informações necessárias, aprimorando, assim, a interoperabilidade. No entanto, é importante cada indústria conversar com fornecedores de tecnologias IoT para ver qual é a melhor soluções desejada. A norma traz alguns exemplos de caso de uso e como devem ser operadas as IoT, porém não esgota as possibilidades.

Além das normas do grupo de IoT e Gêmeos Digitais, os especialistas poderiam debater sobre as normas do Dados industriais (ISO/TC184/SC4) – discutido na Nota Técnica C - que apresenta algumas normas relacionadas a dados no ambiente de manufatura. Por exemplo, está sendo construída a série ISO 23247 que foca em sistemas de automação e integração com foco em Gêmeos Digitais. A série ISO 23247 define uma estrutura para apoiar a criação de gêmeos digitais de elementos de manufatura observáveis, incluindo pessoal, equipamentos, materiais, processos de manufatura, instalações, ambiente, produtos e documentos de suporte. Os escopos das quatro partes desta série são:

- ISO 23247-1: Princípios e requisitos gerais para o desenvolvimento de gêmeos digitais na manufatura - Estágio 60.60;

- ISO 23247-2: Arquitetura de referência com visões funcionais - Estágio 60.60;

- ISO 23247-3: Lista de atributos básicos de informação para os elementos de manufatura observáveis - Estágio 60.60;

- ISO 23247-4: Requisitos técnicos para troca de informações entre entidades dentro da arquitetura de referência - Estágio 60.60.

A primeira norma da série já foi publicada (Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles - ISO 23247-1:2021 - Estágio 60.60) fornece uma visão geral e princípios gerais de uma estrutura de gêmeos digitais para fabricação, incluindo: termos e definições; requisitos da estrutura de gêmeos digitais para fabricação. Dessa forma, os especialistas podem discutir o uso da norma em outros contextos e com outras tecnologias. Por fim, eles podem criar

uma série de normas com base nessas discussões. Além das atividades do ISO/IEC JTC 1 SC42 que foram discutidas durante o workshop, destacamos as atividades do ISO/TC184/SC4 e IEC/TC65/WG24.

Dessa forma, recomenda-se a avaliação técnica das diferentes propostas para normalização do conceito do gêmeo digital a fim de alinhar um posicionamento brasileiro. Com base nessas perspectivas, de forma geral, recomenda- se que os especialistas tenham uma visão geral das normas do grupo de IoT junto com as de dados industriais que podem ser fundamentais para a resolução dos problemas. Além disso, os problemas de dados também foram discutidos no workshop de IA. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de integração e comunicação para a troca de dados

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 30161:2020	Internet of Things (IoT) — Requirements of IoT data exchange platform for various IoT services	Estágio 60.60	Incluir nas normas uma visão geral das normas relacionadas a dados e a dispositivos IoT para resolução de problemas de interoperabilidade
ISO 23247 -1:2021	Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles	Estágio 60.60	
ISO 23247-2	Reference architecture with functional views	Estágio 60.60	
ISO 23247-3	List of basic information attributes for observable manufacture elements	Estágio 60.60	
ISO 23247-4	Technical requirements for exchanging information between entities within the reference architecture	Estágio 60.60	

6.6 Dificuldade do entendimento de conceito IoT (4 – 4º*)

De acordo com os especialistas, as indústrias, em alguns casos, têm dificuldade de entender o uso do conceito de IoT fora do contexto, logo as indústrias tendem a generalizar o uso desse conceito. Os especialistas citaram os seguintes problemas: dificuldades em relação à semântica de informações não padronizadas e uso do termo IoT fora de contexto; generalização do uso, das soluções e do conceito IoT/ Industrial Internet of things (IIoT); falta de uma padronização de quais informações mínimas precisam ser disponibilizadas por dispositivo e ou sistema para considerar que é IoT.

Dessa maneira, com base na visão dos especialistas, o conceito de IoT e IIoT não está bem disseminado na indústria, e as fornecedoras de solução IoT podem ajudar nesse sentido, visto que, muitas vezes, as indústrias compram a solução de IoT pronta com as fornecedoras de tecnologia. Assim, as fornecedoras de IoT implementam a tecnologia, realizam treinamento com colaboradores e gestores e fazem um contrato mensal com as indústrias, principalmente as indústrias de pequeno e médio porte, para que elas entendam o conceito de IoT e como utilizar a tecnologia de forma adequada.

No entanto, é importante destacar que, embora não exista um consenso sobre a padronização e universalização dos termos relacionados a IoT e IIoT, existem muitos materiais para referência com o intuito de abordar os conceitos e práticas mais amplamente difundidas acerca do tema. Por exemplo, o livro "A Internet das Coisas"[101] que aborda os principais temas relacionados à tecnologia e faz um panorama da sua utilização no Brasil e aponta os pontos positivos e negativos da sua adoção. Este tipo de material pode servir de base para empresas e fornecedoras de tecnologia uma vez que o vocabulário utilizado busca ser coerente com o uso cotidiano e intuitivo. Portanto, além das normas sobre o assunto que serão discutidas posteriormente, existem outros materiais que as indústrias e as fornecedoras podem utilizar para ajudar no alinhamento dos termos utilizados e na comunicação clara e precisa. Considerando esses aspectos, os especialistas evidenciaram que as indústrias e as fornecedoras de tecnologias de IoT buscam padronizar os termos de uso sobre IoT e IIoT a fim de facilitar a comunicação entre as partes.

Com relação a normas sobre o problema evidenciado pelos especialistas no workshop, há uma norma publicada em 2021: Information technology — Internet of Things (IoT) — Vocabulary (ISO/IEC 20924:2021 - Estágio 60.60). A norma oferece uma definição de IoT junto com um conjunto de termos e definições importantes correlatas. A norma é uma base terminológica para a IoT que aborda os temos geral e alguns termos específicos de IoT. Com o uso dessa norma, é possível que as indústrias e as fornecedoras de tecnologia consigam explorar o conceito de IoT e IIoT de uma forma mais adequada. Além dessa norma de

vocabulário, existem também a norma de casos de uso, Information technology — Internet of things (IoT) use cases (ISO/IEC TR 22417:2017 - Estágio 60.60), que foi publicada em 2017. A norma identifica cenários de IoT e casos de uso com base em aplicativos e requisitos do mundo real. Os casos de uso fornecem um contexto prático para considerações sobre interoperabilidade e padrões com base na experiência do usuário. A apresentação de casos para o uso de IoT, feita nessa norma, dialoga com o problema apresentado, uma vez que direciona o uso correto da tecnologia, evitando assim seu uso fora de contexto e a generalização do uso, conforme relatado no problema. No entanto, a norma não aborda a questão de padronização de temos apresentada no problema, como a norma ISO/IEC TR 22417:2017. Logo, para uma solução completa, é importante o uso das normas em conjunto e o debate do especialista sobre o assunto. No entanto, se os especialistas acharem necessário, é interessante a discussão sobre o tema, visto que existem outros materiais que podem ajudar na comunicação entre as partes.

Entretanto, há oportunidade de explorar a dificuldade do entendimento de conceito IoT de forma mais ampla, adicionando problemas de vocabulário e terminologia envolvendo sensores. Por exemplo, quando o problema de interoperabilidade envolver questões referentes ao uso de sensores, a norma publicada Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 2: Vocabulary and terminology (ISO/IEC 29182-2:2013 - Estágio 60.60) pode ser utilizada para resolver o problema apresentado. A norma tem como objetivo facilitar o desenvolvimento de padrões Internacionais em redes de sensores e apresenta termos e definições para conceitos selecionados relevantes para o campo das redes de sensores.

Como a norma tem como objetivo elucidar o vocabulário e as terminologias essenciais para o uso da tecnologia de sensores juntamente com a norma de vocabulário de IoT propriamente dita, as duas normas conversam de tal forma que auxiliam no entendimento de conceitos complexos. A adequada compreensão destes conceitos poderá auxiliar na padronização correta de termos nas indústrias e fornecedoras de soluções tecnológicas de IoT e de sensores.

Consequentemente, em problemas mais complexos, as três normas citadas, quando combinadas, promovem a solução completa do problema apresentado na seção com foco em IoT e sensores. Contudo, os especialistas necessitam discutir dependendo da complexidade do problema e do contexto que está inserido para que a comunicação entre cliente e fornecedores seja a mais clara e transparente possível. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Falta de integração e comunicação para a troca de dados			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 20924:2021	Information technology — Internet of Things (IoT) — Vocabulary	Estágio 60.60	Incluir nas normas conceitos e vocabulários para padronização correta do conceito IoT
ISO/IEC TR 22417:2017	Information technology — Internet of things (IoT) use cases	Estágio 60.60	
ISO/IEC 29182-2:2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 2: Vocabulary and terminology	Estágio 60.60	

6.7 Falta de documentação de sistemas legados e protocolos proprietários (3-5°)

Os especialistas discutiram que as indústrias têm dificuldade em relação a documento dos sistemas legados e de protocolos proprietários que dificultam o acesso à informação necessária, prejudicando a interoperabilidade do sistema. Foram discutidos diversos tópicos, por exemplo: o atendimento de sistemas legados com baixo ou nenhum tipo de documentação; dificuldades no acesso a documentações de protocolos proprietários com acesso restrito; diversos problemas com sistemas embarcados legados que afetam a interoperabilidade do sistema como um todo.

A empresa Totvs[102] debateu o tema também em uma publicação. A fornecedora tecnologia abordou que os sistemas legados são um desafio para empresas, uma vez que não conversam bem com os novos recursos disponíveis no mercado e destaca a falta de escalabilidade e de conhecimento sobre os sistemas. Nesse caso, a documentação certa poderia ajudar na falta de conhecimento, porém a falta de documentação prejudica ainda mais a situação. Com intuito de resolver o problema, alguns pesquisadores[103] criaram um Guia de Elicitação de Requisitos para Sistemas Embarcados (GERSE) que

ajuda a melhorar a captura e organização dos requisitos do sistema embarcado além de debaterem sobre o template Volere, que é utilizada para organizar os requisitos de software e pode incluir a documentação e treinamento do usuário em sistemas embarcados. Com base nessas análises, já existem algumas soluções que podem ser utilizadas, porém os especialistas necessitam debater sobre a necessidade de normas sobre o assunto. Por exemplo, uma das soluções apontadas na literatura é o uso de sistemas legados em plataformas como CLP e SCADA[104].

Esses sistemas já possuem grande parte das informações necessárias disponíveis, facilitando sua incorporação. Essa facilidade se deve, em parte, ao fato dos sistemas estarem conectados com a computação em nuvem através de um gateway ("porta de entrada" para troca de informações"). Além disso, essas plataformas são essenciais para adoção do sistemas MES (manufacturing execution system) e ERP, que são utilizados na integração vertical, promovendo a integração de dados, aproximando os dados de gestão e produção e melhorando a tomada de decisão da empresa. A integração vertical é um dos princípios fundamentais da Indústria 4.0, uma vez que considera a integração de sistemas de informação de diferentes níveis hierárquicos em uma empresa para apoiar a tomada de decisões com fluxos de dados em tempo real[105]. Por fim, os especialistas ressaltaram que a falta de uma documentação adequada acarreta diversos problemas em relação aos sistemas legados, ao acesso externo, às informações e aos protocolos proprietários.

Em relação à normalização internacional no contexto da Indústria 4.0, a norma publicada Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013 - Estágio 90.93) pode auxiliar na solução do problema, já que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto da organização.

Esta norma é um primeiro passo para resolução do problema, visto que resolver parcialmente o problema abordado, inclusive o a norma já foi discutida na seção 5.2 do relatório sobre a falta de conhecimento em normas de cibersegurança. A falta de documentação das empresas dialoga com a norma apresentada, pois ela especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão. Entretanto, os especialistas necessitam discutir sobre os principais problemas em relação aos sistemas legados e ao uso de plataformas. Logo, é necessário um aprofundamento sobre o assunto e abordar diretrizes de como usar sistemas sem documentação e como criar documentações para sistemas que faltam documentação, por exemplo.

Além dessas normas, a literatura[106] discute sobre o uso de ISO 27002 nesse caso de sistemas embarcados. Os autores

discutem que os padrões de segurança da informação da norma ISO/IEC 27002 são basicamente salvaguardas para evitar e neutralizar riscos de segurança relacionados a software. Antes de mais nada, é essencial destacar que estrutura dos padrões ISO 27002 apresenta cláusulas de controle de segurança que definem os controles e objetivos de controle relativos à necessidade de proteger disponibilidade, integridade e confidencialidade das informações[107]. Além disso, é um padrão reconhecido internacionalmente projetado em torno de um grupo de controles de segurança inter-relacionados, apresentados para resolver as dificuldades de Sistemas Embarcados[108].

De forma geral, este padrão está explicitamente preocupado com a segurança de todas as formas de informação e é igualmente benéfico para todos os tipos e tamanhos de organizações que lidam e dependem de informações[109]. Dessa forma, considerando a análise dos especialistas, das normas e da literatura, é crucial que os especialistas debatam sobre assunto a fim de conseguir analisar uma forma de mitigar o problema que as indústrias enfrentam, visto que as normas citadas podem ajudar a solucionar o problema destacado na seção.

Problema: Falta de documentação de sistemas legados e protocolos proprietários

Normas técnicas que podem atender ao problema

Número	Título	Desenvolvimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	Estágio 90.93	Incluir nas normas diretrizes e checklist sobre documentação de sistemas legados

6.8 Necessidade de modernização dos equipamentos para a transformação digital (1-6º)

No workshop realizado, os especialistas discutiram que as indústrias precisam modernizar seus equipamentos para o uso das tecnologias da Indústria 4.0, e as fornecedoras de tecnologia possuem um papel fundamental nessa transição, principalmente em relação a pequenas e médias empresas. Os especialistas exemplificaram que é preciso padronizar o Retrofitting 4.0 e definir de requisitos mínimos para Gateways e digitalização. O retrofit é um processo que tem como objetivo a modernização de um produto ou equipamento[110]. Como as indústrias possuem diversas eras tecnológicas no chão de fábrica, elas precisam criar mecanismos para modernizar os equipamentos e linhas de produção. Ademais, alguns pesquisadores[111] já apresentaram uma estrutura de retroffiting para indústria 4.0, porém necessitariam ser realizados mais testes a fim de validar a estrutura.

Logo, como destaque, os especialistas esperam que as normas possam ajudar a criar uma estrutura sólida, coesa e adequada de retrofitting a fim de que as indústrias possam modernizar a linha de produção. Além da dificuldade com o custo dos equipamentos e da obtenção do Know-how de como utilizá-los, restrições quanto aos sistemas computacionais disponíveis e o consumo de energia são fatores que impactam as indústrias na tentativa de implementar a IoT em seus processos. Uma das soluções sendo estudadas é a adoção de uma infraestrutura de virtualização[112], que pode assumir funções como o tratamento de pacotes sem a necessidade de objetos conectados. Isso se torna viável a partir da virtualização do nó de acesso, o que segundo o estudo não causa atrasos significativos na comunicação e não acomete outras funções da rede. Dessa forma, é possível a modernização de equipamento. Considerando os aspectos evidenciados por especialistas e pela literatura, as indústrias têm dificuldades em utilizar seus equipamentos antigos na transformação digital, por isso elas buscam a reforma de equipamentos com intuito de propiciar a adoção das tecnologias da Indústria 4.0 no chão de fábrica.

Para auxiliar na resolução do problema, identificaram-se duas normas: a série Information technology — Electronic Discovery (ISO/IEC 27050 - Estágio 60.60) e, principalmente, a quarta parte da série Information technology — Electronic discovery — Part 4: Technical readiness (ISO/IEC 27050-4 - Estágio 60.60) que já estão publicadas. De forma geral, a descoberta eletrônica é o processo de descobrir informações armazenadas eletronicamente (ESI) ou dados pertinentes por uma ou mais partes envolvidas em uma investigação ou litígio, ou processo semelhante. A Information technology — Electronic discovery — Part 1: Overview and concepts (ISO/IEC 27050-1:2019 - Estágio 60.60) fornece uma visão geral da descoberta eletrônica. Além disso, define os termos relacionados e descreve

os conceitos, incluindo, mas não se limitando a identificação, preservação, coleta, processamento, revisão, análise e produção de ESI. O documento também identifica outros padrões relevantes (por exemplo, ISO / IEC 27037) e como eles se relacionam e interagem com as atividades de descoberta eletrônica. Sendo assim, a norma é importante para os especialistas pois traz alguns conceitos técnicos de descoberta eletrônica que podem ser utilizadas nas indústrias que desejam modernizam a fábrica, resolvendo, assim, parcialmente o problema apresentado pelos especialistas no workshop.

Já, a ISO/IEC 27050-4:2021 fornece orientação sobre como uma organização pode planejar, preparar e implementar a descoberta eletrônica do ponto de vista da tecnologia e dos processos. O documento fornece orientação sobre medidas proativas que podem ajudar a permitir a detecção e processos eletrônicos eficazes e apropriados. A quarta norma da série está alinhada com o problema destacado na seção, já que fornece orientações para o planejamento, preparação e implementação de equipamentos específicos. As orientações podem ajudar as empresas a decidir os melhores equipamentos e máquinas para cada situação e necessidade, resolvendo, consequentemente, parcialmente o problema destacado na seção. No entanto, cada indústria precisa avaliar conforme a sua necessidade a fim de que os equipamentos sejam modernizados da melhor forma possível.

Com base nisso e como as normas solucionam parcialmente o problema, é importante que os especialistas, as indústrias e as fornecedoras de tecnologias leiam toda a série a fim de que o entendimento de modernização seja generalizado, melhorando, consequentemente, os resultados que as indústrias podem alcançar.

Logo, os especialistas, além de discutir alguns aspectos técnicos já abrangidos pela norma, também necessitam abordar alguns aspectos de gestão sobre ela, auxiliando, assim, uma transição mais favorável para a transformação digital. A tabela abaixo apresenta um resumo das normas que podem atender ao problema apresentado pelos especialistas, assim como a principal recomendação de ação para o grupo de trabalho da ABNT, com base no apontado pelos especialistas.

Problema: Necessidade de modernização dos equipamentos para a transformação digital			
Normas técnicas que podem atender ao problema			
Número	Título	Desenvol-vimento	Recomendação de ação baseada na avaliação dos especialistas
ISO/IEC 27050-1:2019	Information technology — Electronic discovery — Part 1: Overview and concepts	Estágio 60.60	Incluir normas sobre modernização de equipamentos e de aspectos de gestão para a transformação digital.
ISO/IEC 27050-4	Information technology — Electronic discovery — Part 4: Technical readiness	Estágio 60.60	

Com base na análise discorrida sobre os problemas enfrentados pelo grupo de IoT, a Figura 3 sumariza os principais problemas destacados que podem ser debatidos pelos especialistas com intuito de que as normas sejam desenvolvidas de forma alinhada.

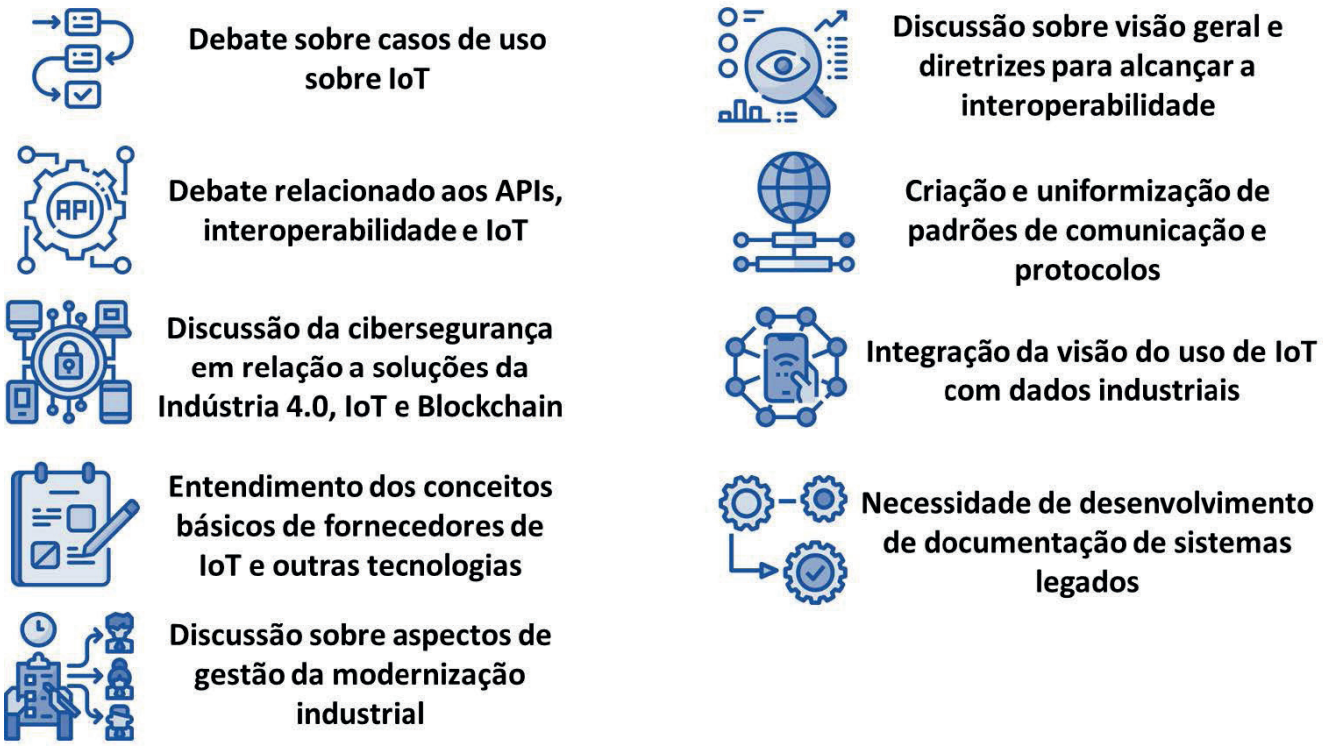

Figura 3 - Tópicos para debate entre os especialistas de Internet das Coisas

7 Conclusões Gerais

Foi possível observar através do estudo que muitos dos problemas levantados pelos especialistas estão alinhados com as normas em desenvolvimento, porém, como estas estão justamente "em desenvolvimento", precisam de uma atuação ativa dos especialistas para que sejam desenvolvidas com foco na resolução dos problemas apresentados. Ainda, foi possível observar nos workshops uma grande disposição dos especialistas em participar dos grupos de discussão através da ABNT. Assim, estes workshops abrem o caminho para que a ABNT possa posicionar o Brasil nos debates internacionais de normas contando com o suporte dos muitos especialistas existentes no país nos assuntos referentes à indústria 4.0.

A seguir são resumidos alguns dos principais pontos trazidos ao longo da análise deste relatório:

- Em relação à Inteligência Artificial, destacaram-se 13 problemas. Além disso, foram analisadas 32 normas publicadas e em desenvolvimento de Inteligência Artificial que podem ajudar a solucionar os problemas das indústrias e fornecedoras de tecnologia através de uma matriz de correlação entre os problemas e as normas. Identificou-se a necessidade de desenvolvimento e melhoria de normas, visto que muitas normas desse grupo estão em desenvolvimento e necessitam serem aprofundadas para cobrirem totalmente os problemas destacados pelos participantes do workshop de normalização brasileira de IA. Por exemplo, o grupo também trata sobre normas de Big Data, algumas normas de Big Data podem expandir seu escopo para a resolução de problemas de IA. Além disso, também se observou a intersecção dos problemas com outros grupos, como de Cibersegurança (por exemplo, o problema Falta de um padrão mínimo de segurança em IA). Dessa forma, os especialistas podem discutir sobre diversos temas integrados, mesmo sendo membros de comitês distintos.

- No que se refere à Cibersegurança, foram destacados 8 problemas. E 40 normas publicadas e em desenvolvimento foram analisadas em relação à cibersegurança e, quando necessário, foram analisadas outras normas do mesmo grupo que contém cerca de 290 publicadas e em desenvolvimento, que foi fundado em 1989. Com base na análise, verificou-se que muitas das normas sobre cibersegurança para a resolução dos problemas estão em desenvolvimento, conforme também destacado nos problemas referentes à IA. Por isso, há uma oportunidade de debate sobre quais os problemas que as normas solucionarão e se serão necessárias mais normas ou uma readaptação das já existentes. Um dos problemas destacado é o Falta de profissionais qualificados

em cibersegurança que pode afetar a adoção das tecnologias da indústria 4.0 em um futuro próximos, e, conforme o relatório Profissões Emergentes na Era Digital113, a curto prazo, seriam necessários mais de 7.000 profissionais com essa formação. Logo, há oportunidades para o aprimoramento das normas para que os profissionais conheçam o sistema.

- No que concerne ao grupo prioritários Internet das Coisas e Gêmeos Digitais e Interoperabilidade, foram evidenciados 7 problemas. Ademais, foram analisadas 40 normas publicadas e em desenvolvimento sobre Internet das Coisas e Gêmeos digitais a fim de verificar se as normas solucionavam os problemas das indústrias e das fornecedoras de tecnologia. Como o workshop abordou o tema interoperabilidade, foi realizada análises de normas sobre outras tecnologias da Indústria 4.0, como sensores (para uma futura integração vertical) e Blockchain (para garantir a cibersegurança). Isto posto, a visão dos especialistas é essencial para que se possa obter vantagens dos usos das tecnológicas de forma integrada e direcionada para a resolução de problemas. Muitas vezes, quando se implementa uma norma, pode ser resolvido mais de um problema detalhado pelos especialistas. Por exemplo, a Cibersegurança em dispositivos IoT que foi citado nos itens 5.8 e 6.4.

- Mesmo que haja um grupo de Cibersegurança, o tópico foi abordado em todos os workshops, demonstrando a necessidade de desenvolvimento de normas sobre o tópico em questão em diferentes tecnologias da Indústria 4.0, como Inteligência Artificial, Machine Learning e Internet das Coisas. Além disso, destaca-se a necessidade de alinhamento entre as normas e a Lei Geral de Proteção de Dados (LGPD). Dessa forma, é importante relacionar as normas de Inteligência Artificial e Internet das Coisas com as de Cibersegurança para que os grupos prioritários de transformação digital e/ou comitês desenvolvam normas que estejam relacionadas a necessidades da indústria como um todo e possam refletir a necessidade futura dessas indústrias. [113]

8 Apêndice A

Estágio	Subestágio						
				90 Decisão			
	00 Cadastro	20 Início da principal ação	60 Conclusão da principal ação	92 Repita uma fase anterior	93 Repita fase atual	98 Abandono	99 Continuar
00 Estágio preliminar	00,00 Proposta para um novo projeto recebida	00,20 Proposta paraum novo projeto em revisão	00,60 Fechamento da revisão			00,98 Proposta para uma novo projeto abandonada	00,99 Aprovação de uma nova votação p/ um projeto
10 Estágio da proposta	10,00 Proposta para um novo projeto registrada	10,20 Nova votação do projeto iniciada	10,60 Votação fechada	10,96 Retorno da proposta p/ o submitente com definições		10,98 Novo projeto rejeitado	10,99 Aprovação para o novo projeto
20 Estágio preparatório	20,00 Novo projeto registrado no programa de trabalho (TC/SC)	20,20 Rascunho de trabalho (WD) do estudo iniciado	20,60 Fechamento do período de observações			20,98 Projeto deletado	20,99 WD aprovado para registro como CD
30 Estágio de comitê	30,00 Estágio do comitê (CD) registrado	30,20 CD estudo/votação iniciado(a)	30,60 Fechamento da votação/do período de comentários	30,92 CD remetidos ao grupo de trabalho		30,98 Projeto deletado	30,99 CD aprovado para registro como DIS
40 Estágio de investigação	40,00 DIS registrado	40,20 Votação do DIS iniciada: 12 semanas	40,60 Fechamento da votação	40,92 Circulação do relatório completo: DIS remetido p/ TC ou SC	40,93 Circulação do relatório completo: decisão para novo votação DIS	40,98 Projeto deletado	40,99 Circulação do relatório completo: DIS aprovada p/ registro como FDIS
50 Estágio de aprovação	50,00 Texto final recebido ou FDIS registrado para aprovação formal	50,20 Prova enviada p/ secretaria ou votação do FDIS iniciada: 8 semanas	50,60 Fechamento da votação. Prova devolvida por secretariado	50,92 FDIS ou prova remetido de volta para TC ou SC		50,98 Projeto deletado	50,99 FDIS ou prova aprovado para publicação
60 Estágio de publicação	60,00 Norma Internacional Padrão em publicação		60,60 Norma Internacional Padrão Publicado				
90 Estágio de revisão		90,20 Norma Internacional Padrão em período de revisão	90,60 Fechamento da revisão	90,92 Norma Internacional Padrão a ser revisada	90,93 Norma Internacional Padrão Confirmada		90,99 Suspensão da Norma Internacional Padrão proposta por TC ou SC
95 Estágio de suspensão		95,20 Votação de suspensão iniciada	95,60 Fechamento da votação	95,92 Decisão de não suspender a norma internacional padrão			95,99 Supensão da Norma Internacional Padrão

9 Apêndice B

Além do cruzamento entre os problemas e as normas[114], realizou o cruzamento dos problemas com alguns relatórios, artigos e normas brasileiras sobre o assunto (Estratégia Brasileira de Inteligência Artificial; Plano Nacional de Internet das Coisas; Lei Geral de Proteção de Dados Pessoais). A tabela a seguir apresenta a lista de referências utilizadas.

Autoria	Ano	Título
McKinsey & Company.	2021	Succeeding in the AI supply-chain revolution
BENZIDIA, Smail; MAKAOUI, Naouel; BENTAHAR,	2021	The impact of big data analytics and artificial intelligence on green supply chain process integration and hospital environmental performance
BORGES, Aline FS et al.	2021	The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions.
PTI, Redação.	2021	AIOps: um novo modelo de gerenciar TI e os negócios.
Towards data Science.	2021	The Role of Cloud Computing in Artificial Intelligence
Datacamp.	2021	How To Manage AI Projects Effectively.
TRUBY, Jon et al.	2021	A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications.
Google AI.	2021	Responsible AI practices.
EBIA.	2021	Estratégia Brasileira de Inteligência Artificial. Relatório de Acompanhamento.
NAIK, Umesh Parameshwar et al.	2021	Implementation of YOLOv4 Algorithm for Multiple Object Detection in Image and Video Dataset using Deep Learning...
MAKAROV, Vladimir A. et al.	2021	Best practices for artificial intelligence in life sciences research.
MEINDL, Benjamin et al.	2021	The four smarts of Industry 4.0: Evolution of ten years of research and future perspectives.

Autoria	Ano	Título
RUDNER, Tim GJ; TONER, Helen.	2021	Key Concepts in AI Safety: An Overview.
OLIVEIRA, Vânia Filipa Moreira Queirós de.	2021	Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação
UNESCO.	2021	Artificial Intelligence: examples of ethical dilemmas.
Google AI.	2021	Learn from ML Experts at Google.
DE MEDEIROS, Luciano Frontino; JUNIOR, Armando Kolbe; MOSER, Alvino.	2021	Uma Inteligência Artificial Ensinando sobre Inteligência Artificial: Relato de Experiência.
Automação Industrial.	2021	A segurança de dados na Indústria 4.0. 2021
HI Tecnologia.	2021	Industria 4.0 - Acesso remoto (Parte I): comunicação com CLP utilizando celular.
Security Intelligence.	2021	How to Include Cybersecurity Training in Employee Onboarding
World Scholarship Forum.	2021	10 melhores certificações de cibersegurança do mundo
HENRIQUES, Filipe José Delgado.	2021	FRAMEWORK DE CIBERSEGURANÇA DA INFORMAÇÃO NO SETOR AUTOMÓVEL.
Autodesk.	2021	Todos juntos: a interoperabilidade de dados e a revolução na colaboração.
VASCONCELLOS, Matheus Dos Santos.	2021	Análise e coleta de dados utilizando internet das coisas para integração de aplicações distribuidas
DA CRUZ, Fabio Batista; MALUF, Marcio Nassif; CICHACZEWSKI, Ederson.	2021	IOT computação na nuvem: o aproveitamento de sistemas legados para industria 4.0.
TABIM, Verônica Maurer; AYALA, Néstor Fabián; FRANK, Alejandro G.	2021	Implementing Vertical Integration in the Industry 4.0 Journey: Which Factors Influence the Process of Information Systems adoption?
NEO, Giz, SENAI.	2021	Profissões Emergentes na Era Digital: Oportunidades e desafios na qualificação profissional para uma recuperação verde.
GARCIA, Ana Cristina Bicharra et al.	2020	Inteligência artificial para sistemas colaborativos

Autoria	Ano	Título
MIT Sloan Management.	2020	Artificial Intelligence and Business Strategy.
ALLEN, Michael.	2020	Inteligência Artificial em redes corporativas
Advian.	2020	What is Edge AI?
IBM.	2020	A Inteligência Artificial de hoje: dados, treinamentos e inferência.
Analytics Diamag.	2020	How To Choose The Best Machine Learning Algorithm For A Particular Problem?
Future Processing.	2020	Project management of AI Projects.
Algorithma.	2020	Why you need an AI framework.
HU, Wu-Chih et al.	2020	Optimal route planning system for logistics vehicles based on artificial intelligence.
IGNÁCIO, Lucas Vinicio Ribeiro et al.	2020	O uso de inteligência artificial para a previsão do preço do petróleo
PEIXOTO, Fabiano Hartmann; COUTINHO, Marina de Alencar Araripe.	2020	Marina de Alencar Araripe. Inteligência Artificial e Regulação.
CEN-CENELEC Focus Group	2020	Road Map on Artificial Intelligence (AI)
Harvard.	2020	Artificial Intelligence Couse
ANVISA.	2020	Princípios e práticas de cibersegurança em dispositivos médicos.
BARBOZA, Rafael Menezes.	2020	Monitoramento voltado à cibersegurança em sistemas industriais.
BSI.	2020	Cybersecurity.
CompTIA Cya+.	2020	CÓDIGO DO EXAME CS0-002

Autoria	Ano	Título
HERMENEGILDO, Gabriella França.	2020	Cibersegurança na União Europeia e os Desafios para a sua Eficácia: Perspetivas, Panorama Estratégico e Instrumentos Jurídicos
Delloite.	2020	Cyber risk in an Internet of Things world.
BOLETA, Roberta Teles et al.	2020	A INTERNET DAS COISAS (IoT): COMPREENSÃO E APLICAÇÃO NO CONTEXTO DA INDÚSTRIA 4.0.
MCTI.	2020	Ações Estratégicas.
Rotta et al.	2020	Protocolos de comunicação para ambientes de Internet das coisas
Venturus.	2020	Protocolos Industriais no Cenário IoT
MCTI.	2020	Frente 4 - Relatório de Entrevistas e Pesquisas - Fase I
Automação Industrial.	2020	Cloud Computing na Automação Industrial.
Ministério da Saúde.	2020	Rede Nacional de Dados em Saúde – RNDS
BUKHARI, Sahar; ISLAM, Muhammad Hasan.	2020	Security of Embedded Systems Using “ISO 27002” Standards.
JR, Edson Amaro et al.	2020	Utilização de Inteligência Artificial em Saúde
AIRES, Clayton Silva França; ALMEIDA, G. J.; SILVEIRA, Sidioney Onézio.	2019	Inteligência Artificial na Gestão de Estoque.
ZHAO, Xuejing et al.	2019	Research and application based on the swarm intelligence algorithm and artificial intelligence for wind farm decision system.
FRAZÃO, Ana.	2019	Quais devem ser os parâmetros éticos e jurídicos para a utilização da inteligência artificial.
MOREIRA, CÁSSIO DOS SANTOS; PEREIRA, Fagner Coin.	2019	Gamificação como solução de treinamento em cibersegurança na prefeitura municipal de Esteio/RS.
Consistem	2019	6 coisas que você deve saber sobre a integração de ERP com APIs.

Autoria	Ano	Título
Totvs.	2019	Saiba o que é sistema legado e como modernizar a sua empresa.
Werner et al.	2019	Retrofitting, um caminho lean para indústria 4.0
NARGESIAN, Fatemeh et al	2019	Data lake management: challenges and opportunities
IBM	2019	Data Lake
McKinsey Digital.	2018	Why digital strategies fail
PRATES, Marcelo; AVELAR, Pedro; LAMB, Luis C.	2018	On quantifying and understanding the role of ethics in AI research: A historical account of flagship conferences and journals.
JIN, Ge et al.	2018	Game based cybersecurity training for high school students
BELLI, Luca et al.	2018	Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas...
LU, Yang; DA XU, Li. I	2018	Internet of Things (IoT) cybersecurity research: A review of current research topics
LEZZI, Marianna; LAZOI, Mariangela; CORALLO, Angelo.	2018	Cybersecurity for Industry 4.0 in the current literature: A reference framework
MCTI.	2018	Relatório 9ª. Relatório final do estudo.
MAGRANI, Eduardo.	2018	A internet das coisas
MATTOS, Diogo MF; VELLOSO, Pedro B.; DUARTE, Otto Carlos MB.	2018	Uma infraestrutura Ágil e efetiva de virtualização de funções de rede para a internet das coisas
Medium.	2017	How to Build an AI Sandbox.
PARDINI, Daniel Jardim; HEINISCH, Astrid Maria Carneiro; PARREIRAS, Fernando Silva	2017	Cyber security governance and management for smart grids in Brazilian energy utilities
MCTI.	2017	Produto 7D: Aprofundamento de verticais – Indústrias.

Autoria	Ano	Título
Totvs.	2017	As dificuldades da integração entre soluções.
MCTI.	2017	Produto 7B: Aprofundamento de Verticais – Saúde
ROTTA, Giovanni; CHARÃO, Andrea; DANTAS, Mario.	2017	Um estudo sobre protocolos de comunicação para ambientes de internet das coisas.
CHICARINO, V. R. et al.	2017	Uso de blockchain para privacidade e segurança em internet das coisas.
SCHREIBER, Isabela Franco.	2017	A relação entre o retrofit e a satisfação do usuário: Estudo de caso em uma empresa do Vale dos Sinos
HENDRIX, Maurice; ALSHERBAZ, Ali; VICTORIA, Bloom.	2017	Game based cyber security training: are serious games suitable for cyber security training?
CORREIA, Pedro Miguel Ribeiro Alves; DA SILVA SANTOS, Susana Isabel;	2016	Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas...
DE BRUIN, Rossouw; VON SOLMS, S. H.	2016	Cybersecurity Governance: How can we measure it?.
SANTOS, Bruno P. et al.	2016	Internet das coisas: da teoria à prática
NAGARAJAN, Ajay et al.	2012	Exploring game design for cybersecurity training.
OSSADA, Jaime Cazuhiro et al.	2012	GERSE: Guia de Elicitação de Requisitos para Sistemas Embarcados.
MIN, Hokey.	2010	Artificial intelligence in supply chain management: theory and applications.
BECCENERI, José Carlos.	2008	Meta-heurísticas e Otimização Combinatória: Aplicações em Problemas Ambientais.
CASANOVA, Marco Antonio et al.	2005	Integração e interoperabilidade entre fontes de dados geográficos.
LECHETA, Edson Martins.	2004	Algoritmos genéticos para planejamento em inteligência artificial
SUCUPIRA, Igor Ribeiro.	2004	Métodos heurísticos genéricos: metaheurísticas e hiper-heurísticas.

Autoria	Ano	Título
NEO, Giz, SENAI. Profissões Emergentes na Era Digital: Oportunidades e desafios na qualificação profissional para uma recuperação	2021	Profissões Emergentes na Era Digital: Oportunidades e desafios na qualificação profissional para uma recuperação verde.

Para auxiliar o aprofundamento dos problemas, também foram conduzidas algumas entrevistas com especialistas sobre o assunto na Tabela 2.

Descrição da empresa	Cargo dos entrevistados
Startup especializada em IoT e IA para gestão da produção.	COO e Líder de Projetos e Pessoas
Startup especializada em IoT e IA para Gestão de manutenção. Foi adquirida em 2021 por um grande grupo nacional do setor de máquinas e equipamentos.	CEO e Líder de Vendas
Empresa de pequeno porte especializada em projetos de segurança de TI.	CEO e COO
Empresa de grande porte responsável por sistemas de pagamento	Desenvolvedor Sênior
Startup que oferece soluções de IA para grandes empresas	CEO
Startup que oferece soluções de IA para grandes empresas	CEO e Professor Universitário
Universidade federal	Técnico em LGPD

10 Notas e Referências

[1] A análise das normas foi realizada em dezembro de 2021.

[2] IBM. Data Lake. 2019. Disponível em: https://www.ibm.com/br-pt/analytics/data-lake

[3] NARGESIAN, Fatemeh et al. Data lake management: challenges and opportunities. Proceedings of the VLDB Endowment, v. 12, n.12, p. 1986-1989, 2019.

[4] JR, Edson Amaro et al. Utilização de Inteligência Artificial em Saúde. 2020. Disponível em: https://www.nic.br/media/docs/publicacoes/6/20200908170853/panorama_setorial_ano-xii_n_2_Ano%20XII%20-%20N.%202%20-%20inteligencia_artificial_e_saude.pdf

[5] BENZIDIA, Smail; MAKAOUI, Naouel; BENTAHAR, Omar. The impact of big data analytics and artificial intelligence on green supplychain process integration and hospital environmental performance. Technological Forecasting and Social Change, v. 165, p. 120557, 2021.

[6] GARCIA, Ana Cristina Bicharra et al. Inteligência artificial para sistemas colaborativos. Disponível em: https://sistemascolaborativos.uniriotec.br/wp-content/uploads/sites/18/2019/06/SC-cap16-inteligenciaartificial.pdf

[7] BORGES, Aline FS et al. The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions. International Journal of Information Management, v. 57, p. 102225, 2021.

[8] MIT Sloan Management. Artificial Intelligence and Business Strategy. Disponível em: https://sloanreview.mit.edu/big-ideas/artificial-intelligence-business-strategy/

[9] ALLEN, Michael. Inteligência Artificial em redes corporativas. 2020. Disponível em: https://www.infranewstelecom.com.br/inteligencia-artificial-nas-redes-corporativas/

[10] PTI, Redação. AIOps: um novo modelo de gerenciar TI e os negócios. 2021. Disponível em: https://www.profissionaisti.com.br/aiops-um-novo-modelo-de-gerenciar-ti-e-os-negocios/

[11] Advian. What is Edge AI? Disponível em: https://www.advian.fi/en/what-is-edge-ai

[12] Towards data Science. The Role of Cloud Computing in Artificial Intelligence. 2021. Disponível em: https://towardsdatascience.com/the-role-of-cloud-computing-in-artificial-intelligence-507ffd68ca46

[13] Towards data Science. The Role of Cloud Computing in Artificial Intelligence. 2021. Disponível em: https://towardsdatascience.com/the-role-of-cloud-computing-in-artificial-intelligence-507ffd68ca46

[14] IBM. A Inteligência Artificial de hoje: dados, treinamentos e inferência. 2020. Disponível em: https://www.ibm.com/blogs/systems/br-pt/2020/01/a-inteligencia-artificial-hoje-dados-treinamento-e-inferencia/?utm_medium=OSocial&utm_source=Blog&utm_content=000038HA&utm_term=10003252&utm_id=storage-matters&cm_mmc=OSocial_Blog-_-Systems_Systems+-+Infrastructure-_-LA_IBR-_-storage-matters&cm_mmca1=000038HA&cm_mmca2=10003252

[15] Datacamp. How To Manage AI Projects Effectively. 2021. Disponível em: https://www.datacamp.com/community/blog/how-tomanage-ai-projects-effectively

[16] Datacamp. How To Manage AI Projects Effectively. 2021. Disponível em: https://www.datacamp.com/community/blog/how-tomanage-ai-projects-effectively

[17] Analytics Diamag. How To Choose The Best Machine Learning Algorithm For A Particular Problem? 2020. Disponível em:https://analyticsindiamag.com/how-to-choose-the-best-machine-learning-algorithm-for-a-particular-problem/

[18] Medium. How to Build an AI Sandbox. 2017. Disponível em: https://medium.com/the-business-of-ai/how-to-build-an-ai-sandbox-3a95e9507379

[19] TRUBY, Jon et al. A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications. European Journal of Risk Regulation,p. 1-29, 2021. Disponível em: https://www.

cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D

[20] Google AI. Responsible AI practices. Disponível em: https://ai.google/responsibilities/responsible-ai-practices/

[21] Algorithma. Why you need an AI framework. 2020. Disponível em: https://algorithmia.com/blog/ai-framework

[22] Algorithma. Why you need an AI framework. 2020. Disponível em: https://algorithmia.com/blog/ai-framework

[23] EBIA. Estratégia Brasileira de Inteligência Articial. Relatório de Acompanhamento. 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia_relatorio-de-acompanhamento-2021.pdf

[24] AIRES, Clayton Silva França; ALMEIDA, G. J.; SILVEIRA, Sidioney Onézio. Inteligência Artificial na Gestão de Estoque. Fateclog, v. 1,p. 1-7, 2019.

[25] MIN, Hokey. Artificial intelligence in supply chain management: theory and applications. International Journal of Logistics: Research and Applications, v. 13, n. 1, p. 13-39, 2010.

[26] ZHAO, Xuejing et al. Research and application based on the swarm intelligence algorithm and artificial intelligence for wind farm decision system. Renewable energy, v. 134, p. 681-697, 2019.

[27] NAIK, Umesh Parameshwar et al. Implementation of YOLOv4 Algorithm for Multiple Object Detection in Image and Video Dataset using Deep Learning and Artificial Intelligence for Urban Traffic Video Surveillance Application. In: 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT). IEEE, 2021. p. 1-6.

[28] LECHETA, Edson Martins. Algoritmos genéticos para planejamento em inteligência artificial. 2004. Disponível em: https://www.acervodigital.ufpr.br/bitstream/handle/1884/25440/D%20-%20LECHETA%2c%20EDSON%20MARTINS.pdf?sequence=1&isAllowed=y

[29] SUCUPIRA, Igor Ribeiro. Métodos heurísticos genéricos: metaheurísticas e hiper-heurísticas. USP: São Paulo, v. 32, 2004.

[30] BECCENERI, José Carlos. Meta-heurísticas e Otimização Combinatória: Aplicações em Problemas Ambientais. INPE, Sao José dos Campos, 2008.

[31] HU, Wu-Chih et al. Optimal route planning system for logistics vehicles based on artificial intelligence. Journal of Internet Technology, v. 21, n. 3, p. 757-764, 2020.

[32] IGNÁCIO, Lucas Vinicio Ribeiro et al. O uso de inteligência artificial para a previsão do preço do petróleo. Disponível em: http://ww.revistaespacios.com/a17v38n24/a17v38n24p03.pdf

[33] MAKAROV, Vladimir A. et al. Best practices for artificial intelligence in life sciences research. Drug Discovery Today, 2021.

[34] MAKAROV, Vladimir A. et al. Best practices for artificial intelligence in life sciences research. Drug Discovery Today, 2021.

[35] MEINDL, Benjamin et al. The four smarts of Industry 4.0: Evolution of ten years of research and future perspectives. Technological Forecasting and Social Change, v. 168, p. 120784, 2021.

[36] PEIXOTO, Fabiano Hartmann; COUTINHO, Marina de Alencar Araripe. Inteligência Artificial e Regulação. Revista Em Tempo, v. 19, n. 1, 2020. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3129

[37] RUDNER, Tim GJ; TONER, Helen. Key Concepts in AI Safety: An Overview. 2021. Disponível em: https://cset.georgetown.edu/publication/key-concepts-in-ai-safety-an-overview/

[38] RUDNER, Tim GJ; TONER, Helen. Key Concepts in AI Safety: An Overview. 2021. Disponível em: https://cset.georgetown.edu/publication/key-concepts-in-ai-safety-an-overview/

[39] OLIVEIRA, Vânia Filipa Moreira Queirós de. Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. 2021. Tese de Doutorado. Disponível em: https://run.unl.pt/bitstream/10362/117660/1/TGI0405.pdf

[40] Análise realizada em dezembro de 2021.

[41] Road Map on Artificial Intelligence (AI). Disponível em: https://standict.eu/sites/default/files/2021-03/CEN-CLC_FGR_RoadMapAI.pdf

[42] PRATES, Marcelo; AVELAR, Pedro; LAMB, Luis C. On quantifying and understanding the role of ethics in AI research: A historical account of flagship conferences and journals. arXiv preprint arXiv:1809.08328, 2018.

[43] PRATES, Marcelo; AVELAR, Pedro; LAMB, Luis C. On quantifying and understanding the role of ethics in AI research: A historical account of flagship conferences and journals. arXiv preprint arXiv:1809.08328, 2018.

[44] UNESCO. Artificial Intelligence: examples of ethical dilemmas. Disponível em: https://en.unesco.org/artificial-intelligence/ethics/cases

[45] FRAZÃO, Ana. Quais devem ser os parâmetros éticos e jurídicos para a utilização da inteligência artificial. 2019. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-10-28-Quais_devem_ser_os_parametros_eticos_e_juridicos_para_a_utilizacao_da_inteligencia_artificial_As_respostas_oferecidas_pelas_recentes_Diretrizes_da_Uniao_Europeia_para_a_inteligencia_artificial_confiavel.pdf

[46] Google AI. Learn from ML Experts at Google. Disponível em: https://ai.google/education/

[47] Google AI. Learn from ML Experts at Google. Disponível em: https://ai.google/education/

[48] Harvard. Disponível em: https://pll.harvard.edu/subject/artificial-intelligence

[49] Automação Industrial. A segurança de dados na Indústria 4.0. 2021. Disponível em: https://www.automacaoindustrial.info/seguranca-de-dados-na-industria-4-0/

[50] ANVISA. Princípios e práticas de cibersegurança em dispositivos médicos. 2020. Disponível em: https://www.gov.br/anvisa/ptbr/assuntos/noticias-anvisa/2020/saiba-mais-sobre-ciberseguranca-em-dispositivos-medicos/guia-38.pdf

[51] LEZZI, Marianna; LAZOI, Mariangela; CORALLO, Angelo. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, v. 103, p. 97-110, 2018.

[52] LEZZI, Marianna; LAZOI, Mariangela; CORALLO, Angelo. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, v. 103, p. 97-110, 2018.

[53] HENRIQUES, Filipe José Delgado. FRAMEWORK DE CIBERSEGURANÇA DA INFORMAÇÃO NO SETOR AUTOMÓVEL. 2021. Tese de Doutorado. Disponível em: https://iconline.ipleiria.pt/bitstream/10400.8/5590/1/Relatorio_FilipeHenriques_com_corre%c3%a7%c3%b5es_formais.pdf

[54] HI Tecnologia. Industria 4.0 - Acesso remoto (Parte I): comunicação com CLP utilizando celular. 2021. Disponível em: https://www.hitecnologia.com.br/blog/industria-4.0-acesso-remoto-parte-i-comunica%C3%A7%C3%A3o-com-clp-utilizando-celular/

[56] Security Intelligence. How to Include Cybersecurity Training in Employee Onboarding. 2021. Disponível em: https://securityintelligence.com/articles/how-include-cybersecurity-training-employee-onboarding/

[57] Security Intelligence. How to Include Cybersecurity Training in Employee Onboarding. 2021. Disponível em: https://securityintelligence.com/articles/how-include-cybersecurity-training-employee-onboarding/

[58] NAGARAJAN, Ajay et al. Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, 2012. p. 256-262.

[59] NAGARAJAN, Ajay et al. Exploring game design for cybersecurity training. In: 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). IEEE, 2012. p. 256-262.

[60] HENDRIX, Maurice; AL-SHERBAZ, Ali; VICTORIA, Bloom. Game based cyber security training: are serious games suitable for cyber security training?. International Journal of Serious Games, v. 3, n. 1, 2016.

[61] MOREIRA, CÁSSIO DOS SANTOS; PEREIRA, Fagner Coin. GAMIFICAÇÃO COMO SOLUÇÃO DE TREINAMENTO EM CIBERSEGURANÇA

NA PREFEITURA MUNICIPAL DE ESTEIO/RS. PROJETOS E RELATÓRIOS DE ESTÁGIOS, v. 1, n. 1, p. 1-64, 2019. Disponível em: http://raam.alcidesmaya.com.br/index.php/projetos/article/view/63/61

[62] BSI. Cybersecurity. Disponível em: https://www.bsigroup.com/en-GB/Cyber-Security/

[63] CORREIA, Pedro Miguel Ribeiro Alves; DA SILVA SANTOS, Susana Isabel; DE FARIA BILHIM, João Abreu. Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio. Revista da FAE, v. 19, n. 2, p. 22-37, 2016. Disponível em: https://revistafae.fae.edu/revistafae/article/view/98

[64] CompTIA CySA+. CÓDIGO DO EXAME CS0-002. Disponível em: https://www.comptia.org/pt/certificacoes/cybersecurity-analyst

[65] World Scholarship Forum. 10 melhores certificações de cibersegurança do mundo | 2021 Disponível em: https://worldscholarshipforum. com/pt/cybersecurity-certifications/

[66] HERMENEGILDO, Gabriella França. Cibersegurança na União Europeia e os Desafios para a sua Eficácia: Perspetivas, Panorama Estratégico e Instrumentos Jurídicos. 2020. Disponível em: https://repositorioaberto.up.pt/bitstream/10216/131092/2/434117.pdf

[67] PARDINI, Daniel Jardim; HEINISCH, Astrid Maria Carneiro; PARREIRAS, Fernando Silva. Cyber security governance and management for smart grids in Brazilian energy utilities. JISTEM-Journal of Information Systems and Technology Management, v. 14, p. 385-400, 2017.

[68] DE BRUIN, Rossouw; VON SOLMS, S. H. Cybersecurity Governance: How can we measure it?. In: 2016 IST-Africa Week Conference. IEEE, 2016. p. 1-9.

[69] BELLI, Luca et al. Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. FGV Direito Rio, 2018. Disponível em: https://www.gobernanzainternet.org/livro_portugues/gobernanza_y_regulaciones_de_internet_en_america_latina_pt.pdf

[70] Deloitte. Cyber risk in an Internet of Things world. Disponível em: https://www2.deloitte.com/us/en/pages/technology-mediaand-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html

[71] LU, Yang; DA XU, Li. Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, v. 6, n. 2, p. 2103-2115, 2018.

[72] LU, Yang; DA XU, Li. Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, v. 6, n. 2, p. 2103-2115, 2018.

[73] BOLETA, Roberta Teles et al. A INTERNET DAS COISAS (IoT): COMPREENSÃO E APLICAÇÃO NO CONTEXTO DA INDÚSTRIA 4.0. In: V Encontro de Iniciação Científica e Tecnológica-EnICT (ISSN: 2526-6772). 2020. Disponível em: https://arq.ifsp.edu.br/eventos/index.php/enict/5EnICT/paper/viewFile/491/295

[74] MCTI. Ações Estratégicas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-dascoisas-acoes

[75] MCTI. Produto 7D: Aprofundamento de verticais – Indústrias. 2017. Disponível em: https://www.gov.br/mcti/pt-br/acompanheo-mcti/transformacaodigital/arquivosinternetdascoisas/fase3_7d_relatorio-de-aprofundamento-das-verticais-industria.pdf

[76] Totvs. IMASTERS. As dificuldades da integração entre soluções. 2017. Disponível em: https://imasters.com.br/desenvolvimento/as-dificuldades-da-integracao-entre-solucoes

[77] Consistem. 6 coisas que você deve saber sobre a integração de ERP com APIs. 2019. Disponível em: https://blog.consistem.com.br/6-coisas-sobre-integracao-de-erp-com-apis/

[78] SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016. Disponível em: http://35.238.111.86:8080/jspui/bitstream/123456789/329/1/Santos_Bruno_Internet%20das%20coisas.pdf

[79] MCTI. Ações estratégicas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-dascoisas-acoes

[80] MCTI. Produto 7D: Aprofundamento de verticais

– Indústrias. 2017. Disponível em: https://www.gov.br/mcti/pt-br/acompanheo-mcti/transformacaodigital/arquivosinternetdascoisas/fase3_7d_relatorio-de-aprofundamento-das-verticais-industria.pdf

[81] MCTI. Produto 7B: Aprofundamento de Verticais – Saúde. 2017. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-omcti/transformacaodigital/arquivosinternetdascoisas/fase3_7b_relatorio-de-aprofundamento-das-verticais-saude.pdf

[82] MCTI. Produto 7C: Aprofundamento de Verticais – Rural. 2017. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-omcti/transformacaodigital/arquivosinternetdascoisas/fase3_7c_relatorio-de-aprofundamento-das-verticais-rural.pdf

[83] Rotta et al. Protocolos de comunicação para ambientes de Internet das coisas Disponível em: https://infranewstelecom.com.br/protocolos-de-comunicacao-para-ambientes-de-internet-das-coisas/

[84] Venturus. Protocolos Industriais no Cenário IoT. 2020. Disponível em: https://www.venturus.org.br/protocolos-industriais-no-cenario-iot/

[85] MCTI. Ações estratégicas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-dascoisas-acoes

[86] MCTI. Frente 4 - Relatório de Entrevistas e Pesquisas - Fase I Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-omcti/transformacaodigital/arquivosinternetdascoisas/fase1_4a_entrevistas-e-pesquisas-documento-principal.pdf

[87] ROTTA, Giovanni; CHARÃO, Andrea; DANTAS, Mario. Um estudo sobre protocolos de comunicação para ambientes de internet das coisas. In: Anais da XVII Escola Regional de Alto Desempenho do Estado do Rio Grande do Sul. SBC, 2017. Disponível em: https://sol.sbc.org.br/index.php/eradrs/article/view/2984/2946

[88] Brasil Logic Sistemas. Gestão de mudanças na automação industrial: melhor controle, maior produtividade. Disponível em: http://www.blsistemas.com.br/gestao-de-mudancas-na-automacao-industrial-melhor-controle-maior-produtividade/

[89] Automação Industrial. Cloud Computing na Automação Industrial. Disponível em: https://www.automacaoindustrial.info/cloudcomputing-na-automacao-industrial/

[90] Automação Industrial. Cloud Computing na Automação Industrial. Disponível em: https://www.automacaoindustrial.info/cloudcomputing-na-automacao-industrial/

[91] MCTI. Ações estratégicas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-dascoisas-acoes

[92] MCTI. Ações estratégicas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/nternet-dascoisas-acoes

[93] CHICARINO, V. R. et al. Uso de blockchain para privacidade e segurança em internet das coisas. Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, v. 28, 2017. Disponível em: https://www.researchgate.net/profile/Vanessa-Rocha-Leandro-Chicarino/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas/links/5a3b92aaaca272774f9baf5a/Uso-de-Blockchain-para-Privacidade-e-Seguranca-em-Internetdas-Coisas.pdf

[94] Autodesk. Todos juntos: a interoperabilidade de dados e a revolução na colaboração. 2021. Disponível em: https://redshift.autodesk.com.br/interoperabilidade-de-dados/

[95] Autodesk. Todos juntos: a interoperabilidade de dados e a revolução na colaboração. 2021. Disponível em: https://redshift.autodesk.com.br/interoperabilidade-de-dados/

[96] Autodesk. Todos juntos: a interoperabilidade de dados e a revolução na colaboração. 2021. Disponível em: https://redshift.autodesk.com.br/interoperabilidade-de-dados/

[97] CASANOVA, Marco Antonio et al. Integração e interoperabilidade entre fontes de dados geográficos. CASANOVA, MA et al. Banco de dados geográficos. Curitiba: Mundogeo, p. 315-352, 2005.

[98] Ministério da Saúde. Rede Nacional de Dados em Saúde – RNDS. Disponível em: https://www.gov.br/saude/pt-br/assuntos/rnds

[99] MCTI. Relatório 9ª. Relatório final do estudo. 2018. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/

arquivosinternetdascoisas/fase3_9a_relatorio-final-do-estudo.pdf

[100] VASCONCELLOS, Matheus Dos Santos. Análise e coleta de dados utilizando internet das coisas para integração de aplicações distribuidas. 2021. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/231878/001133496.pdf?sequence=1&isAllowed=y

[101] MAGRANI, Eduardo. A internet das coisas. Editora FGV, 2018. Disponível em: https://books.google.com.br/books?hl=pt-

[102] Totvs. Saiba o que é sistema legado e como modernizar a sua empresa. 2019. Disponível em: https://www.totvs.com/blog/negocios/saiba-o-que-e-sistema-legado-e-como-modernizar-a-sua-empresa/

[103] OSSADA, Jaime Cazuhiro et al. GERSE: Guia de Elicitação de Requisitos para Sistemas Embarcados. In: WER. 2012.

[104] DA CRUZ, Fabio Batista; MALUF, Marcio Nassif; CICHACZEWSKI, Ederson. IOT computação na nuvem: o aproveitamento de sistemas legados para industria 4.0. Caderno Progressus, v. 1, n. 2, p. 49-64, 2021. Disponível em: https://cadernosuninter.com/index.php/progressus/article/view/1993

[105] TABIM, Verônica Maurer; AYALA, Néstor Fabián; FRANK, Alejandro G. Implementing Vertical Integration in the Industry 4.0 Journey: Which Factors Influence the Process of Information Systems Adoption?. Information Systems Frontiers, p. 1-18, 2021.

[106] BUKHARI, Sahar; ISLAM, Muhammad Hasan. Security of Embedded Systems Using “ISO 27002” Standards.

[107] BUKHARI, Sahar; ISLAM, Muhammad Hasan. Security of Embedded Systems Using “ISO 27002” Standards.

[108] BUKHARI, Sahar; ISLAM, Muhammad Hasan. Security of Embedded Systems Using “ISO 27002” Standards.

[109] BUKHARI, Sahar; ISLAM, Muhammad Hasan. Security of Embedded Systems Using “ISO 27002” Standards.

[110] SCHREIBER, Isabela Franco. A relação entre o retrofit e a satisfação do usuário: Estudo de caso em uma empresa do Vale dos Sinos. 2017.

[111] Werner et al. RETROFITTING, UM CAMINHO LEAN PARA A INDÚSTRIA 4.0. 2019. Disponível em: http://www.abepro.org.br/biblioteca/TN_STO_294_1661_38384.pdf

[112] MATTOS, Diogo MF; VELLOSO, Pedro B.; DUARTE, Otto Carlos MB. Uma infraestrutura Ágil e efetiva de virtualização de funções de rede para a internet das coisas. In: Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2018. Disponível em: https://sol.sbc.org.br/index.php/sbrc/article/view/2474/2438

[113] NEO, Giz, SENAI. Profissões Emergentes na Era Digital: Oportunidades e desafios na qualificação profissional para uma recuperação verde. 2021. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/b7/5a/b75af326-9c36-49e7-b298-1b9f0a3d4938/estudo_profissoes_emergentes_-_giz_ufrgs_e_senai.pdf

[114] A análise das normas técnicas foi realizada em dezembro de 2021.

Núcleo de Engenharia Organizacional

Departamento de Engenharia de Produção e Transportes

Universidade Federal do Rio Grande do Sul

Av. Osvaldo Aranha, 99 - 5º andar

90035-190 - Porto Alegre - RS - Brasil

Fone: +55 51 3308.3490

E-mail: neo@producao.ufrgs.br

www.ufrgs.br/neo

NEO
NÚCLEO DE ENGENHARIA ORGANIZACIONAL | UFRGS

UFRGS ENGENHARIA DE PRODUÇÃO

UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL