



Análise dos grupos prioritários de normalização internacional no contexto da Indústria 4.0

O Centro de Gestão e Estudos Estratégicos (CGEE) edita publicações sobre diversas temáticas que impactam a agenda do Sistema Nacional de Ciência, Tecnologia e Inovação (SNCTI).

As edições são alinhadas à missão institucional do Centro de subsidiar os processos de tomada de decisão em temas relacionados à ciência, tecnologia e inovação, por meio de estudos em prospecção e avaliação estratégica baseados em ampla articulação com especialistas e instituições do SNCTI.

As publicações trazem resultados de alguns dos principais trabalhos desenvolvidos pelo Centro, dentro de abordagens, como produção de alimentos, formação de recursos humanos, sustentabilidade e energia. Todas estão disponíveis gratuitamente para download.

A instituição também produz, semestralmente, a revista Parcerias Estratégicas, que apresenta contribuições de atores do SNCTI para o fortalecimento da área no País.

Você está recebendo uma dessas publicações, mas pode ter acesso a todo o acervo do Centro pelo nosso site: <http://www.cgEE.org.br>.

Boa leitura!

Análise dos grupos prioritários de normalização internacional no contexto da Indústria 4.0

Centro de Gestão e Estudos Estratégicos (CGEE)

Diretor-presidente

Marcio de Miranda Santos

Diretores

Luiz Arnaldo Pereira da Cunha Junior

Regina Maria Silverio

Edição / Rafael Souza - Contexto Gráfico

Capa / Contexto Gráfico

Apoio técnico ao projeto/Tatiana Farias Ramos

Coordenação da Comunicação Integrada

Jean Marcel da Silva Campos

C389a

Análise dos grupos prioritários de normalização internacional no contexto da Indústria 4.0. Nota Técnica. Brasília, DF: Centro de Gestão e Estudos Estratégicos, 2021.

210 p.

ISBN 978-65-5775-031-5

1. Indústria 4.0. 2. Desenvolvimento tecnológico. 3. Inteligência Artificial.
4. Transformação Digital. 5. Brasil. I. CGEE. II. Título.

004.896:67 (81)

Centro de Gestão e Estudos Estratégicos (CGEE), SCS Qd. 9, Torre C, 4º andar, Ed. Parque Cidade Corporate, CEP: 70308-200 - Brasília, DF, Telefone: (61) 3424 9600, <http://www.cgee.org.br>, @CGEE_oficial

Referência bibliográfica: CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS- CGEE. Análise dos grupos prioritários de normalização internacional no contexto da Indústria 4.0. Nota Técnica. Brasília, DF: Centro de Gestão e Estudos Estratégicos, 2021. 210 p.

Esta publicação é parte integrante das atividades desenvolvidas no âmbito do 2º Contrato de Gestão CGEE – 21º Termo Aditivo/Ação: Apoio Técnico à Gestão Estratégica do SNCTI /Projeto: Subsídios para as Câmaras 4.0, inclusive quanto aos seus impactos na transformação digital no Brasil - 53.05.52.03/MCTI/2020.

Todos os direitos reservados pelo Centro de Gestão e Estudos Estratégicos (CGEE). Os textos contidos nesta publicação poderão ser reproduzidos, armazenados ou transmitidos, desde que citada a fonte.

Análise dos grupos prioritários de normalização internacional no contexto da Indústria 4.0

Supervisão

Luiz Arnaldo Pereira da Cunha Júnior

Equipe técnica do CGEE

Lucas Varjão Motta (Líder o projeto)

Caroline Nascimento Pereira

Larissa Gabrielle Vieira de Sousa

Roberta Andrade Cestari Capelotto

Verena Hitner Barros

Consultor

Néstor Fabián Ayala

Sumário

Apresentação	7
1 Inteligência Artificial e 5G	11
1.1 Sumário executivo	11
1.1.1 Foco do estudo	11
1.1.2 Abordagem metodológica.....	11
1.1.3 Resultados.....	11
1.2 Introdução.....	12
1.2.1 Conteúdo deste relatório	12
1.2.2 Grupos para o desenvolvimento de normas.....	12
1.3 Metodologia	16
1.4 Grupos Inteligência Artificial (ISO/IEC/JTC1/SC42)	17
1.4.1 Escopo.....	17
1.4.2 <i>Status quo</i>	17
1.4.3 Mapa mental de relação do grupo de Inteligência Artificial com outros grupos	18
1.4.4 Tendências	20
1.4.5 Relevância.....	26
1.5 Grupo de aprendizado de máquina para redes do futuro, incluindo 5G (ITU/T/FG/5GML).....	28
1.5.1 Escopo.....	28
1.5.2 Status quo.....	28
1.5.3 Mapa mental de relação com outros grupos.....	30
1.5.4 Tendências	32
1.5.5 Relevância	35
1.6 Conclusões da nota técnica sobre Inteligência Artificial.....	38
1.7 Conclusões gerais da análise dos grupos prioritários.....	39
2 Segurança e cibersegurança	43
2.1 Sumário executivo	43
2.1.1 Foco do estudo	43
2.1.2 Abordagem metodológica.....	43
2.1.3 Resultados.....	43
2.2 Introdução.....	44
2.2.1 Conteúdo deste relatório	44
2.2.2 Grupos para o desenvolvimento de normas.....	45
2.3 Metodologia	48
2.4 Grupos de segurança de máquinas (ISO/TC 199).....	49
2.4.1 Escopo.....	49
2.4.2 <i>Status quo</i>	50
2.4.3 Mapa mental da relação do grupo Segurança de Máquinas com outros grupos	52
2.4.4 Tendências	54
2.4.5 Relevância	57
2.5 Grupo de segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27)	61
2.5.1 Escopo.....	61
2.5.2 <i>Status quo</i>	61
2.5.3 Mapa mental de relação com outros grupos.....	66
2.5.4 Tendências	69
2.5.5 Relevância	75
2.6 Segurança para medição e controle dos processos industriais (IEC/TC65/WG10).....	80
2.6.1 Escopo.....	80
2.6.2 Status quo.....	80

2.6.3	Mapa mental de relação com outros grupos.....	81
2.6.4	Tendências.....	83
2.6.5	Relevância.....	93
2.7	Conclusões da nota técnica sobre Segurança e Cibersegurança.....	100
2.8	Conclusões Gerais.....	101
3	Redes industriais e interoperabilidade.....	105
3.1	Sumário executivo.....	105
3.1.1	Foco do estudo.....	105
3.1.2	Abordagem metodológica.....	105
3.1.3	Resultados.....	105
3.2	Introdução.....	107
3.2.1	Conteúdo deste relatório.....	107
3.2.2	Grupos para o desenvolvimento de normas.....	108
3.3	Metodologia.....	111
3.4	Grupos de redes industriais (IEC/TC65/SC65C).....	112
3.4.1	Escopo.....	112
3.4.2	<i>Status quo</i>	112
3.4.3	Mapa mental de relação com outros grupos.....	115
3.4.4	Tendências.....	117
3.4.5	Relevância.....	123
3.5	Grupo Fábrica Digital (IEC/TC65/WG16).....	125
3.5.1	Escopo.....	125
3.5.2	<i>Status quo</i>	125
3.5.3	Mapa mental de relação com outros grupos.....	127
3.5.4	Tendências.....	129
3.5.5	Relevância.....	131
3.6	Grupo Internet das coisas e gêmeos digitais} (ISO/IEC JTC 1/SC 41).....	133
3.6.1	Escopo.....	133
3.6.2	<i>Status quo</i>	133
3.6.3	Tendências.....	140
3.6.4	Relevância.....	147
3.7	Grupo Dados industriais (ISO/TC184/SC4).....	154
3.7.1	Escopo.....	154
3.7.2	<i>Status quo</i>	154
3.7.3	Mapa mental de relação com outros grupos.....	161
3.7.4	Tendências.....	164
3.7.5	Relevância.....	170
3.8	Grupo Robótica (ISO/TC299).....	174
3.8.1	Escopo.....	174
3.8.2	<i>Status quo</i>	174
3.8.3	Mapa mental de relação da Robótica com outros grupos.....	181
3.8.4	Tendências.....	184
3.8.5	Relevância.....	187
3.9	Conclusões do grupo redes industriais e Interoperabilidade.....	190
3.10	Conclusões Gerais do estudo dos grupos prioritários.....	191
	Siglas encontradas nesta publicação.....	192
	Lista de Figuras.....	194
	Lista de Tabelas.....	197

Apresentação

Este estudo é proveniente do projeto **Subsídios para a Câmara Brasileira da Indústria 4.0**, uma iniciativa da Câmara da Indústria 4.0. A coordenação da Câmara é feita pelo Ministério da Economia (ME) e pelo Ministério da Ciência, Tecnologia e Inovações (MCTI), com a participação de atores do setor público e de representantes dos setores industriais e da academia.

O projeto busca elaborar estudos estratégicos a fim de acelerar a transformação digital na indústria brasileira, por meio de proposições de ações para impulsionar as atividades da Câmara, contribuindo para o aprimoramento e para a produção de políticas públicas. A adoção de tecnologias 4.0 pelo setor industrial é tema prioritário, porém permeado por múltiplos desafios para sua implementação.

Entre os desafios do setor industrial brasileiro elencados pela Câmara da Indústria 4.0 estão as necessidades de:

- Aumentar a competitividade e a produtividade das empresas brasileiras por meio da Indústria 4.0;
- Melhorar a inserção do Brasil nas cadeias globais de valor;
- Introduzir o uso de tecnologias da Indústria 4.0 nas pequenas e médias empresas;
- Garantir instrumentos para que soluções de base tecnológica, *startups* e integradoras possam ser ofertadas e disponibilizadas diretamente às empresas;
- Assegurar estabilidade e volume de recursos a custo adequado para a implementação de iniciativas para a Indústria 4.0;
- Identificar e desenvolver soluções para a Indústria 4.0 adequadas às empresas do parque produtivo brasileiro; e
- Evitar a sobreposição de esforços individuais de instituições públicas e privadas e pulverização de recursos para solucionar necessidades e demandas da Indústria 4.0 no Brasil.

O Centro de Gestão e Estudos Estratégicos (CGEE) vem oferecendo contribuições à Câmara da Indústria 4.0, fornecendo subsídios para superar os entraves observados pelos membros e buscando facilitar a formulação de iniciativas voltadas para a adoção de tecnologias 4.0 pela indústria brasileira. Por meio de estudos estratégicos, o CGEE espera aumentar o conhecimento dos atores sobre as necessidades do setor, bem como promover os incrementos necessários para o futuro.

Desse modo, O CGEE e a Câmara da Indústria 4.0 esperam, com este conteúdo, contribuir para o melhoramento do cenário do setor industrial brasileiro, promovendo maior produtividade, competitividade e desenvolvimento econômico.

Luiz Arnaldo Pereira da Cunha Junior

Diretor do CGEE

Inteligência Artificial e 5G

1 Inteligência Artificial e 5G

1.1 Sumário executivo

1.1.1 Foco do estudo

A presente nota técnica analisa o contexto da Inteligência Artificial e *Machine Learning* na normalização internacional sobre a Indústria 4.0. O estudo tem como tema central a normalização em relação à transformação digital e à Indústria 4.0 e analisa a relevância das normas em relação a aplicações de Inteligência Artificial e *Machine learning* no contexto da Indústria 4.0. Para tanto, são analisados dois grupos prioritários: (i) Inteligência Artificial (ISO/IEC/JTC1/SC42) e (ii) Aprendizado de máquina para redes do futuro, incluindo 5G (ITU/T/FG/5GML).

1.1.2 Abordagem metodológica

O relatório utiliza uma abordagem mista que combina a análise das normas/regulações, de relatórios, de empresas em relação aos grupos prioritários estudados, além de fazer uma análise sobre estudos anteriores do tema. Complementarmente, utilizou-se uma análise de conteúdo e o desenvolvimento de figuras para facilitar a compreensão do tema.

1.1.3 Resultados

O relatório apresenta diversos resultados:

- As normas de Inteligência Artificial são essenciais para que se possa desenvolver seu uso em diversas indústrias com o foco no desenvolvimento de Indústria 4.0, visto que é uma tecnologia que propicia que as empresas possam garantir vantagem competitiva frente a seus concorrentes, gerando benefícios econômicos.
- As normas apresentam informações relevantes que explicam o vocabulário básico para aplicação de Inteligência Artificial, *roadmaps* que facilitam a implementação da tecnologia em empresas de diversos setores, *frameworks* que possibilitam uma visão geral da aplicação do tema. Dessa forma, as normas podem ajudar empresas que já implementam a tecnologia a atingir resultados ainda melhores e empresas que desejam implementá-la.
- A Inteligência Artificial é um tema extremamente relevante e possui diversas conexões com outros grupos prioritários que visam o desenvolvimento de normalizações para aplicação da Indústria 4.0. Consequentemente, é importante um entendimento claro de quais são os principais aspectos da Inteligência Artificial, uma vez que as empresas podem usar a tecnologia em consonância com outros prioritários.

- Outro aspecto importante é que as normas têm um enfoque no gerenciamento de riscos do uso da tecnologia, propiciando que as empresas entendam como gerenciar o seu risco e possibilitando uma análise geral do uso da tecnologia. Além disso, é importante avaliar o desempenho do uso da tecnologia, com critérios claros e controles de avaliação.

1.2 Introdução

O projeto tem como objetivo geral o desenvolvimento de um estudo detalhado das discussões, propostas e tendências nos principais fóruns internacionais de normalização com foco na Indústria 4.0, facilitando a compreensão de empresas e entidades nacionais da relevância dos mesmo para o desenvolvimento da transformação digital da indústria brasileira. As três notas técnicas que compõem o estudo global analisam dez grupos prioritários, previamente definidos pelo Grupo de Trabalho “Regulação, Normalização Técnica e Infraestrutura para Normalização” da Câmara Brasileira da Indústria 4.0, com intuito de expor e explicar o estado atual do trabalho normativo, bem como propostas em discussão. Os temas abordados pelas três notas técnicas são:

Nota técnica A: **Inteligência artificial e 5G**

Nota técnica B: **Segurança e cibersegurança**

Nota técnica C: **Redes industriais e interoperabilidade**

1.2.1 Conteúdo deste relatório

O relatório contempla dois grupos prioritários, seu escopo de atuação, *status quo* das normas publicadas, relacionamento com outros grupos prioritários, tendências de normalização para os próximos anos e relevância dos grupos para o Brasil. Os grupos prioritários abordados no relatório são:

1. Inteligência Artificial (ISO/IEC/JTC1/SC42)
2. Aprendizado de máquina para redes do futuro, incluindo 5G (ITU/T/FG/5GML)

1.2.2 Grupos para o desenvolvimento de normas

Os grupos prioritários são comissões de estudo sobre temas específicos que têm como objetivo desenvolver normalizações sobre assuntos relevantes no desenvolvimento nacional em nível mundial. Dessa forma, os grupos prioritários são essenciais para as empresas que se baseiam no desenvolvimento de produtos e serviços. De modo geral, a participação nessas comissões é aberta a qualquer parte interessada. O Brasil possui participação em alguns grupos. É importante salientar que o País pode ser um membro P, que é mais atuante e participativo, e membro O, que é mais observador.

Complementando esses aspectos dos grupos, é imprescindível entender a que instituições de normalização eles estão associados. Por exemplo, nesse relatório, são a ISO, a IEC e a ITU. A Organização Internacional de Normalização (ISO), que desenvolve normas e relatórios técnicos

quando há necessidade de mercado. Para tanto, as normas 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 a um objetivo de crescimento, a Secretaria da ISO suporta o desenvolvimento das normas.

Embora a ISO seja muito relevante, a *International Electrotechnical Commission* (IEC) é a organização mundial que prepara e publica normas internacionais para as áreas elétrica, eletrônica e tecnologias relacionadas, complementando as normas da ISO. Logo, publicações são feitas para a aplicação em fábricas e em outros ambientes. É importante salientar que o desenvolvimento de normas é feito por meio do Comitê Nacional da IEC de cada país. Além da ISO e da IEC, a ITU engloba a padronização da área de Telecomunicações da União Internacional de Telecomunicações (ITU) (*International Telecommunication Union*), focada também no desenvolvimento de normas. Com base nessas informações, a ITU é focada na parte de telecomunicações enquanto a IEC aborda temas de eletroeletrônica. De forma geral, a ISO aborda os temas não abordados pelos comitês anteriores. Conseqüentemente, as três se complementam as normas entre si, desenvolvendo novas normalização para suportar as empresas. Em suma, elas podem ser consideradas “federações” que congregam os organismos de normalização nacionais (sendo permitida a participação de uma entidade por país, a qual pode ser membro de diversas entidades). A maior diferença entre eles é o fato de que a representação na ISO e IEC são feitas por organismos de normalização, enquanto na ITU a participação é realizada pelos governos, uma vez que apresenta um caráter mais estratégico.

Em relação a 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);
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 International 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 das etapas se encontra no Apêndice A. Já as tipologias de documento podem ser normas internacionais, porém também abordam outros documentos, como Technical Specification (TS), Public Available Specification (PAS) e Technical Report (TR).

1.2.2.1 Coordenação

A participação na normalização internacional requer um bom nível de coordenação dos trabalhos e participações. A atual nota busca mostrar as relações entre os grupos prioritários para facilitar e agilizar o processo de normalização com o enfoque na coordenação. Quando um certo grau de coordenação e gestão for alcançado entre os atores que participarão das diferentes discussões de normalização, maiores serão os ganhos para a indústria brasileira. Além disso, em busca de uma coordenação eficiente, ágil e eficaz, abordam-se conceitos que facilitam o entendimento do vocabulário de Indústria 4.0, que são lacunas destacadas nas próximas notas técnicas.

1.2.2.2 Visão estratégica

É crítico desenvolver e implementar uma visão estratégica da participação na normalização internacional para a Indústria 4.0. Este relatório aborda uma visão estratégica ao acrescentar discussões importantes de diversos atores da Indústria 4.0, tanto em relação à análise das normas quanto à relevância. Aborda, conseqüentemente, aspectos de governança de gestão, uma vez que aponta aplicações práticas da implementação de tecnologias em diversos contextos, promovendo, assim, um entendimento estratégico sobre o assunto. Em alguns grupos prioritários, quando necessário, são destacadas as diferenças estratégicas dos países a fim de identificar a sua relevância.

1.2.2.3 Recursos

Este relatório aborda perspectivas relacionadas aos recursos humanos competentes a fim de desempenhar determinadas funções da Indústria 4.0. Além disso, o relatório abrange informações pertinentes acerca das necessidades do desenvolvimento de capacidades dos usuários, dos desenvolvedores e dos colaboradores da Indústria 4.0. Logo, é possível entender como cada ator pode ajudar ao desenvolvimento da transformação digital na indústria brasileira, destacando os principais conhecimentos que são necessários para tal finalidade.

1.2.2.4 Capacitação

Este relatório apresenta embasamento das principais normas internacionais que podem ser utilizadas para desenvolver as capacidades e os conhecimentos dos colaboradores, capacitando atores do governo das empresas e das universidades. Com base em uma visão holística, o relatório abrange tópicos importantes que diferentes membros de uma instituição necessitam desenvolver para conseguirem alcançar os objetivos organizacionais de implementação das tecnologias da Indústria 4.0.

1.2.2.5 Priorização

É necessário priorizar os temas, setores e atividades em que é válido envolver-se ativamente, decidir aqueles que serão acompanhados e também aqueles em que não é prioritário o envolvimento. Respondendo a tal necessidade, com base na análise completa das normas e da relevância dos grupos prioritários, este relatório prioriza os principais assuntos que devem ser considerados para a normalização, mostrando a relevância de cada grupo prioritário, tanto para o mundo quanto para o Brasil. Complementarmente, o relatório traz exemplos mundiais do uso das tecnologias para o desenvolvimento da Indústria 4.0, ampliando o número de países que foram citados nas próximas notas técnicas, mostrando a relevância da atuação de alguns países e como as suas ações e melhores práticas apresentaram resultados positivos. Com base no benchmarking Internacional, é possível entender como o Brasil está posicionado em comparação a outros países no uso de tecnologias para a Indústria 4.0. Ademais, o relatório apresenta como o Brasil e suas empresas são destaque Internacional no uso de tecnologias, abordando as ações, as legislações desenvolvidas e os principais atores que interagem para o desenvolvimento de uma indústria brasileira mais avançada.

Nesse sentido, o atual relatório agrega valor em relação à diferença de desenvolvimento de alguns setores em relação aos outros e como o uso de algumas tecnologias está mais avançado nesses setores, mostrando aplicações e seus resultados em diversas áreas. Além desses aspectos, o relatório aborda, quando possível, algumas previsões da literatura para o uso de tecnologias, os empregos que podem ser gerados e o desenvolvimento de ações nos próximos anos, expondo os benefícios esperados para o futuro.

Algumas definições da Indústria 4.0 e do uso de tecnologias necessitavam de esclarecimento, visto que a literatura não convergia para uma definição comum, o que dificultava o entendimento de conceitos-chave para a convergência e gestão de estratégias sobre o desenvolvimento dessa indústria Indústria 4.0 no País. Considerando tal perspectiva, foram destacadas, ao longo do relatório, algumas definições importantes para a adoção de tecnologias, propiciando o conhecimento necessário para o entendimento completo dos temas abordados com base na normalização. Favoreceu-se, então, a compreensão das principais definições, promovendo a disseminação do conhecimento sobre o tema e aprofundando, quando necessário, elementos e definições que baseiam a adoção das tecnologias.

Internet das coisas, sensores inteligentes, inteligência artificial, computação em nuvem e robótica avançada, são importantes para o desenvolvimento da Indústria 4.0. Este relatório conseguiu abranger detalhadamente as principais tecnologias para tal desenvolvimento, além de destacar alguns dos principais órgãos técnicos que são tratados como grupos prioritários. Nesse sentido, o atual relatório abrange uma análise detalhada dos grupos Rede Industrial, Fábrica Digital e Dados Industriais. Assim, esta terceira nota técnica abrange considerações importantes a respeito da implementação de tecnologia para o desenvolvimento da Indústria 4.0.

1.3 Metodologia

A partir da análise das normas dos grupos prioritários e de relatórios, artigos e sites oficiais relacionados, foram debatidos cinco principais tópicos para cada um dos grupos prioritários. São eles:

- (i) Escopo: aborda o escopo e algumas das principais definições do grupo prioritário;
- (ii) *Status quo*: apresenta as principais normas do grupo prioritário, mostrando o que foi realizado no passado até o que foi publicado em 2021;
- (iii) Mapa mental: facilita o posicionamento do grupo prioritário em relação a outros grupos e tópicos relacionados a ele;
- (iv) Tendências: aborda as tendências normativas a serem publicadas pelos grupos prioritários nos próximos anos, detalhando quais normas estão em desenvolvimento;
- (v) Relevância: aborda as principais aplicações dos temas relacionados ao grupo prioritário estudado, sua importância mundial e no Brasil.

Para facilitar a compreensão de como foi realizada cada etapa da análise dos grupos, consolidou-se o detalhamento das etapas na Tabela 1.

Tabela 1 - Detalhamento da metodologia para o conteúdo do Relatório

Etapas	Metodologia
(i) Escopo	Realizou-se por meio da análise de conteúdo das normas.
(ii) Status quo	Realizou-se por meio da análise de conteúdo das normas publicadas selecionadas em uma análise temporal e prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ¹
(iii) Mapa mental	Realizou-se por meio da análise de conteúdo das normas, de entrevistas e de análise dos <i>Laisons</i> presentes nos sites dos grupos prioritários. ²
(iv) Tendências	Realizou-se por meio da análise de conteúdo das normas em desenvolvimento selecionadas em uma análise temporal e

¹ As normas foram analisadas em maio, junho e julho de 2021.

² A relações foram desenvolvidas nos meses de maio, junho e julho de 2021.

	prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ³
(v) Relevância	Realizou-se por meio da análise de conteúdo de relatórios de consultorias, de artigos e de sites oficiais a fim de se destacar as primeiras aplicações, a importância mundial e importância no Brasil. ⁴

Além das análises dos grupos prioritários, ao final do relatório apresenta-se uma avaliação das principais lições aprendidas com base nos temas desenvolvidos pelos grupos. A partir disso, foi possível a realização de uma série de abstrações dos temas tratados pelos grupos prioritários, obtendo percepções do desenvolvimento de diversas estruturas normativas internacionais e nacionais e como elas, em conjunto, podem alavancar a Indústria 4.0 nas empresas brasileiras. Portanto, a reflexão das lições aprendidas proporciona discussões relevantes quanto ao uso de tecnologias da Indústria 4.0 para o desenvolvimento de uma indústria nacional mais tecnológica, que acompanhe as normalizações internacionais sobre o assunto.

1.4 Grupos Inteligência Artificial (ISO/IEC/JTC1/SC42)

1.4.1 Escopo

A proposta do grupo de Inteligência Artificial (IA) é elaborar normas baseadas nos 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.

Conforme definido nas normas, a IA pode ser entendida como o ramo da ciência dedicado ao desenvolvimento de sistemas de processamento de dados que executam funções normalmente associadas à inteligência humana, como raciocínio, aprendizagem e autoaperfeiçoamento (**ISO/IEC 2382:2015**). Além do conceito do IA, outros conceitos importantes para a aplicação das tecnologias são *machine learning* e *Big Data*. Entende-se *machine learning* como o processo que usa algoritmos em vez de codificação processual, permitindo aprender a partir de dados existentes para prever resultados futuros (**ISO/IEC 38505-1:2017**). Conforme a **ISO/IEC 20546:2019**, entende-se como que o termo *Big Data* implica conjuntos de dados que são extensos em volume, velocidade, variedade e/ou variabilidade, que requerem uma tecnologia escalonável para armazenamento, manipulação, gerenciamento e análise eficientes.

1.4.2 Status quo

O grupo prioritário iniciou com foco em *Big Data*, criando padrões de arquitetura para uso de *Big Data* em casos de uso e o desenvolvimento de *roadmaps* para facilitar a sua aplicação na indústria. Ou seja, o grupo prioritário em Inteligência Artificial apresentou inicialmente um

³ As normas foram analisadas em maio, junho e julho de 2021. Algumas normas foram revisadas entre 16 e 20 de agosto de 2021.

foco em dados. Além disso, o grupo desenvolveu normas com vocabulários-base sobre o tema (por exemplo, o que consta na norma **ISO/IEC 20546:2019**), além de frameworks na **ISO/IEC TR 20547-1:2020** que descrevem o processo de como um usuário pode aplicar big data a um problema específico.

Muitas vezes, as empresas têm receio de utilizar a IA, porque acreditam que o sistema da empresa pode se tornar mais vulnerável devido aos riscos associados à sua implementação. Logo, a norma **ISO/IEC TR 24028:2020** foi desenvolvida a fim de propiciar um embasamento referente a tópicos relacionados à confiabilidade em sistemas de IA; armadilhas de engenharia e ameaças e riscos típicos associados aos sistemas de IA, juntamente a possíveis técnicas e métodos de mitigação; abordagens para avaliar e alcançar a disponibilidade, resiliência, confiabilidade, precisão, proteção e privacidade dos sistemas de IA. Portanto, considerando essas perspectivas, também é importante entender como a IA pode ser utilizada. Por isso, a **ISO/IEC TR 24030:2021** emerge como uma norma fundamental, visto que fornece uma coleção de casos de IA.

Assim, as normas publicadas pelo grupo Inteligência Artificial (ISO/IEC/JTC1/SC42) estão consolidadas na Tabela 2.

Tabela 2 - Normas do grupo de Inteligência Artificial

Norma	Escopo
ISO/IEC 20546:2019	Fornecer uma base terminológica para padrões relacionados à big data.
ISO/IEC TR 24028:2020	Abrange a confiabilidade em sistemas de IA.
ISO/IEC TR 20547-1:2020	Aborda um <i>framework</i> de aplicação de <i>Big Data</i> .
ISO/IEC TR 24030:2021	Fornecer uma coleção de casos de uso representativos de IA.

1.4.3 Mapa mental de relação do grupo de Inteligência Artificial com outros grupos

A Figura 1 apresenta a relação do grupo Inteligência Artificial (ISO/IEC/JTC1/SC42) com outros que abordam o tema. À direita, em azul-escuro, estão os grupos prioritários diretamente citados neste relatório e que se relacionam com o grupo prioritário de Inteligência Artificial. São eles:

- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO/IEC e em cooperação com outros comitês técnicos da ISO e IEC.
- **Rede Industrial** – O escopo do grupo prioritário sobre a rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como

para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.

- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas 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.
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir como proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo prioritário tem o intuito de fornecer orientação a entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido e em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais, Segurança de rede e sistema.
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas de *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.
- **Robótica** – O escopo do grupo prioritário de robótica é sua padronização, excluindo brinquedos e aplicações militares.

À esquerda, em amarelo, estão outros grupos não analisados no relatório, mas encontram-se relacionados ao assunto, segundo as análises realizadas. Cada um deles está explicado a seguir:

- **Automação de sistemas e integração:** Padronização na área de sistemas de automação e sua integração para projeto, *sourcing*, fabricação, produção e entrega, suporte, manutenção e descarte de produtos e seus serviços associados.
- **Gerenciamento de riscos:** Padronização na área de gestão de risco.
- **Blockchain and distributed ledger Technologies:** Padronização de tecnologias de *blockchain* e tecnologias de razão distribuída.
- **Smart Manufacturing:** Para fornecer coordenação e aconselhamento no domínio da manufatura inteligente a fim de harmonizar e avançar nas atividades de manufatura inteligente na IEC e outros SDO.

- **Medição, controle e automação de processos industriais:** Preparar padrões internacionais de sistemas e elementos usados para medição, controle e automação de processos industriais. Busca-se coordenar as atividades de padronização que afetam a integração de componentes e funções em tais sistemas, incluindo aspectos de proteção e segurança.
- **Engenharia de software e sistemas:** Padronização de processos, ferramentas de suporte e tecnologias de suporte à engenharia de produtos e sistemas de software.
- **Tecnologia da informação:** Ambiente de desenvolvimento de padrões onde especialistas se reúnem a fim de desenvolver padrões mundiais de Tecnologia da Informação e Comunicação (TIC) para aplicações de negócios e de consumo.

Já em vermelho, acima e abaixo dos outros tópicos, estão os principais conceitos relacionados à transformação digital na Indústria, que também estão interconectados com a inteligência artificial.

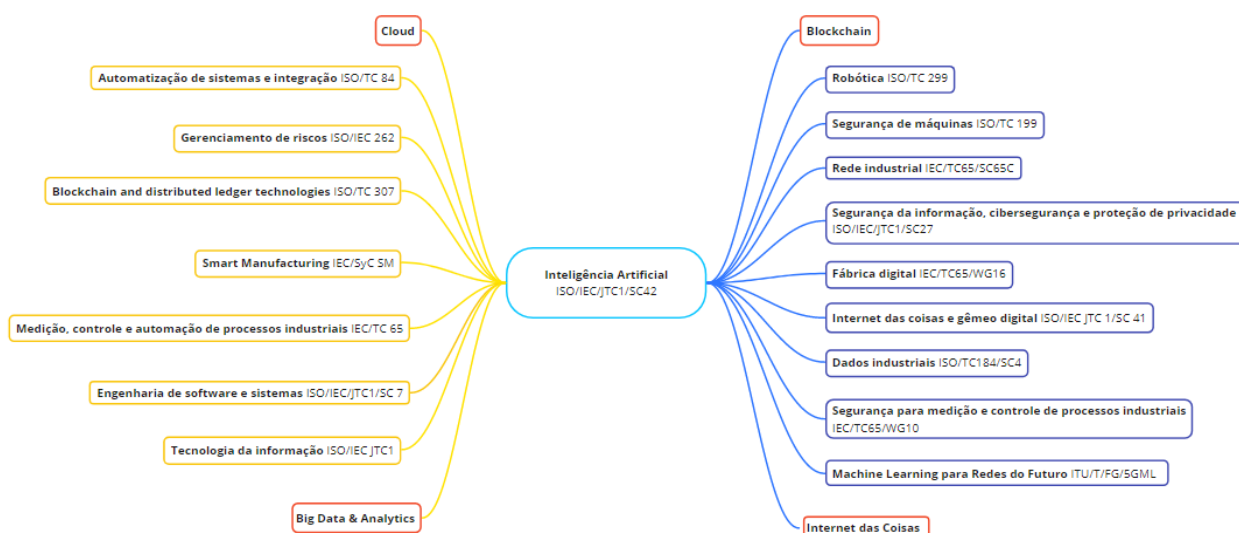


Figura 1 - Mapa mental da relação do grupo de Inteligência Artificial com outros grupos

1.4.4 Tendências

Com base nas normas em desenvolvimento do grupo prioritário, as principais tendências destacadas em relação à IA são:

1.4.4.1 Implicações de governança do uso de inteligência artificial pelas organizações (ISO/IEC DIS 38507)

O escopo da **ISO/IEC DIS 38507** é fornecer orientação para o corpo diretivo de uma organização que está usando ou considerando o uso de inteligência artificial. Atualmente, tal norma se encontra no estágio próximo à votação (estágio 40,60)⁵. Ela é capaz de fornecer um

⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/56641.html>

padrão consultivo de alto nível baseado em princípios. Além de fornecer ampla orientação sobre o papel de um órgão regulador, incentiva as organizações a usar padrões apropriados para sustentar sua governança de tecnologia da informação, incluindo o uso de inteligência artificial.

Conforme apontado pela norma, a IA é um sistema definido pelo poder de computação, escalabilidade, rede, dispositivos conectados e interfaces, junto a grandes quantidades de dados. Assim, a IA deve ser entendida como se referindo a toda uma família de tecnologias e métodos, e não a qualquer tecnologia, método ou aplicação específica. Os seguintes conceitos de IA são apontados como muito relevantes pela norma:

Uso de IA: é definido como desenvolvimento e aplicação de um sistema de IA em qualquer parte de seu ciclo de vida a fim de cumprir objetivos e criar valor para a organização. Isso inclui relacionamentos com qualquer parte que forneça ou use tais sistemas.

Implicações de governança do uso de IA: o uso de IA traz novos riscos e responsabilidades que devem ser tratados pelas organizações que a utilizam. IA não é inerentemente "boa" ou "má", "justa" ou "tendenciosa", "ética" ou "antiética", embora seu uso possa ser ou possa parecer ser. O propósito, a ética e outras diretrizes da organização são refletidos, formal ou informalmente, em suas políticas.

Assim, a ISO/IEC DIS 38507 examina as políticas de governança e organizacionais e sua aplicação e fornece orientação para adaptá-las ao uso de IA. Os elementos operacionais das políticas são implementados por meio da gestão. A ISO/IEC DIS 38507 se refere também a outros padrões para obter detalhes sobre tópicos relacionados, incluindo responsabilidade social, confiabilidade (como gerenciamento de risco, gerenciamento de preconceito e qualidade) e gerenciamento de conformidade.

1.4.4.2 Framework de gerenciamento do processo para análise de *big data* (ISO/IEC DIS 24668:2020)

O framework de gerenciamento do processo para análise de big data, que está sendo desenvolvido na norma **ISO/IEC DIS 24668:2020**, fornece subsídios para o desenvolvimento de processos com o objetivo de alavancar efetivamente a análise de *big data* em toda a organização, independentemente do setor ou indústria. Atualmente, a norma está na fase de registro Rascunho de Padrão Internacional (estágio 40,00)⁶. A norma apresenta um framework direcionado ao gerenciamento de processos para análises de big data com suas várias categorias de processos levadas em consideração, juntamente a suas interconectividades, descrevendo processos para adquirir, descrever, armazenar e processar dados em um nível de organização que fornece serviços analíticos de *Big Data*.

Para facilitar a compreensão, a norma divide o framework em cinco categorias de processos essenciais: (i) Engajamento de Partes Interessadas Organizacionais; (ii) Processos de Desenvolvimento de Competências; (iii) Processos de Gerenciamento de Dados; (iv) Processos de Desenvolvimento de *Analytics*; e (v) Processos de Integração de Tecnologia. Todos eles estão na base da infraestrutura de tecnologia e são guiados pela cultura e estratégia de liderança organizacional. Cada um dos processos essenciais está dividido em categorias que são detalhadas em tabelas para fornecer subsídios suficientes às empresas que desejam

⁶ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78368.html>

utilizá-lo. Além disso, há sugestões de indicadores de capacidade do processo, facilitando, assim, o gerenciamento do processo para análise da dados.

1.4.4.3 Visão geral de abordagens computacionais para sistemas de IA (ISO/IEC TR 24372:2021)

A norma **ISO/IEC TR 24372:2021** 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; e b) principais algoritmos e abordagens em sistemas de IA, referenciando os casos de uso da **ISO/IEC TR 24030**⁷, publicada em maio de 2021. A visão geral de abordagens computacionais em sistemas de IA inclui *machine learning* e métodos de aprendizagem não automática. Para refletir os métodos mais modernos usados em IA, a norma:

- Fornece uma descrição geral das abordagens computacionais em sistemas de IA;
- Aborda as principais características dos sistemas de IA;
- Fornece uma taxonomia geral de abordagens computacionais;
- Discute algoritmos selecionados usados em sistemas de IA.

Ao fornecer uma visão geral das diferentes tecnologias usadas por sistemas de IA, ISO/IEC TR 24372:2021 tem a intenção de fornecer suporte ao entendimento das características e abordagens computacionais usadas em IA.

1.4.4.4 Viés de sistemas de IA e tomada de decisão suportada por IA (ISO/IEC PRF TR 24027)

Os sistemas de IA que aprendem padrões a partir dos dados e podem refletir os vieses existentes da sociedade. É importante salientar que os vieses em sistemas de IA podem ser introduzidos como resultado de deficiências estruturais no projeto do sistema ou de vieses cognitivos humanos. Tais fatores significam que as implantações de tecnologias de IA podem perpetuar ou ampliar as perspectivas existentes ou até mesmo criá-las. O viés em sistemas de IA é uma área ativa de pesquisa. Logo, a norma **ISO/IEC PRF TR 24027** (atualmente no estágio *Final Draft*, 50,00)⁸ articula as práticas atuais para detectar e tratar vieses em sistemas de IA ou na tomada de decisão auxiliada por IA, independentemente da fonte. A norma abrange os seguintes aspectos:

- relação entre vieses e imparcialidade;
- fontes potenciais de vieses para especificar a natureza da tendência potencial;
- avaliação de vieses e imparcialidade por meio de métricas;
- abordar o viés por meio de estratégias de tratamento.

⁷ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77610.html>

⁸ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77607.html>

1.4.4.5 Gerenciamento de riscos em IA (ISO/IEC CD 23894.2)

Considera-se que gerenciamento de risco é a identificação, avaliação e priorização de riscos (ISO 31000:2018), seguidas pela aplicação de recursos com intuito de minimizar, monitorar e controlar a probabilidade não intencional de eventos ocorrerem. A norma **ISO/IEC CD 23894.2** (atualmente no estágio 30,00 – rascunho)⁹ fornece diretrizes sobre como as organizações que desenvolvem, produzem, implantam e usam produtos, sistemas e serviços que utilizam IA podem gerenciar riscos especificamente relacionados à IA. A norma apresenta uma tabela que analisa a relação do gerenciamento de risco e o ciclo de vida do sistema de IA.

A norma apresenta um *framework* com intuito de auxiliar a organização na integração do gerenciamento de risco em atividades e funções específicas em relação à IA. O *framework* é baseado em vários objetivos que suportam a gestão de risco, tais como: imparcialidade, segurança, privacidade, robustez, transparência, *accountability*, entre outros. Além disso, são avaliadas as principais fontes de risco em relação ao nível de automação, complexidade do ambiente, problemas de sistema de engenharia, problemas de *hardware*, maturidade tecnológica, riscos relacionados à *machine learning* etc.

1.4.4.6 Avaliação do desempenho da classificação de *machine learning* (ISO/IEC TS 4213:2021)

A norma **ISO/IEC DTS 4213:2021**¹⁰ (atualmente no estágio 30.60, fechada para votação/período de comentários) especifica metodologias para medir o desempenho de classificação de modelos, sistemas e algoritmos de aprendizado de máquina. Na norma, são explicados alguns termos e definições, como em relação à classificação, parâmetros, falso negativo, falso positivos, entre outros. A norma desenvolveu um processo generalizado para avaliação de desempenho de classificação de *machine learning*, que é dividido em cinco etapas: (i) Definir as tarefas para avaliação; (ii) Especificar as métricas; (iii) Conduzir a avaliação; (iv) Coletar e analisar dados; e (v) Gerar resultados de avaliação. Complementarmente a esse processo, a norma delimitou critérios de controle na avaliação de desempenho de classificação de *machine learning*, uma vez que, ao se avaliar o desempenho da classificação de *machine learning*, os aspectos metodológicos devem ser controlados com intuito de garantir a relevância, legitimidade e extensibilidade. Portanto, cuidados especiais e adicionais devem ser tomados em avaliações comparativas de vários modelos de classificação de *machine learning*, algoritmos ou sistemas para garantir que nenhuma abordagem seja favorecida em relação a outra.

⁹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77304.html>

¹⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/79799.html>

A Tabela 3 resume as normas em desenvolvimento no grupo Inteligência Artificial (ISO/IEC/JTC1/SC42):

Tabela 3 - Normas em relação a tendências do grupo de Inteligência Artificial

Norma	Escopo
ISO/IEC DIS 38507	Orienta sobre as implicações de governança do uso de inteligência artificial pelas organizações.
ISO/IEC WD 24668:2020	Estabelece um framework de gerenciamento do processo para análise de big data.
ISO/IEC TR 24372:2021	Promove uma visão geral de abordagens computacionais para sistemas de IA.
ISO/IEC 24027:20XX	Identifica perspectivas de sistemas de IA e comporta a tomada de decisão suportada por IA.
ISO/IEC CD 23894.2	Oferece subsídios para o gerenciamento de riscos em IA.
ISO/IEC TS 4213:2021	Promove a avaliação do desempenho da classificação de <i>machine learning</i> .

A fim de complementar as informações da Tabela 3, a Figura 2 sumariza as informações referentes ao escopo, *status quo* e tendências do grupo Inteligência Artificial (ISO/IEC/JTC1/SC42).

Inteligência artificial

ISO/IEC/JTC1/SC42

Escopo

Servir como proponente de programas de padronização de Inteligência Artificial
Fornecer orientações aos comitês que desenvolvem aplicações em IA

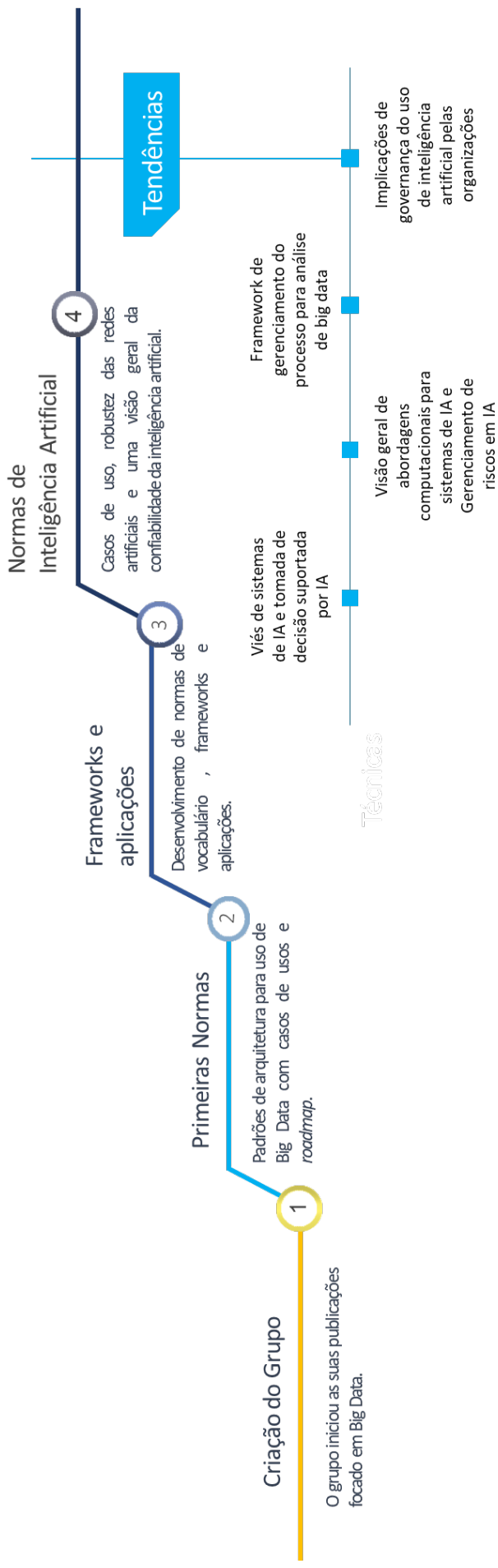


Figura 2 - Consolidação da análise do grupo de Inteligência Artificial

1.4.5 Relevância

A IA é uma das tecnologias-base para a transformação digital. Por isso, existem diversas oportunidades de aplicação tanto na indústria quanto no setor de serviços, visto que soluções baseadas em *Big Data* e inteligência artificial oferecem suporte a decisões. Algumas das principais aplicações da IA são (STEFANINI GROUP, 2020): (i) *chatbots* (atendimento ao cliente de um robô que reproduz o comportamento humano); (ii) aplicações de gestão (ferramenta para tomada de decisão de gestores); (iii) assistente pessoal (por exemplo, a Siri da Apple, que reconhece os comandos de voz e realiza as funções); (iv) mecanismo de segurança digital (*internet banking* utiliza IA para a identificação de tentativas de ataques ou fraudes); (v) previsões (realiza previsões de comportamento humano ou máquinas); (vi) vendas e marketing (melhora a qualidade do cliente); e (vii) ensino (atendimento complementar do aluno 24h enquanto o professor não estiver on-line).

O uso de IA apresenta benefícios financeiros e é uma tecnologia utilizada mundialmente para recuperação econômica e geração de empregos. De acordo com um recente estudo da McKinsey & Company (MCKINSEY & COMPANY, 2020a), alguns entrevistados apontam que **20 por cento ou mais dos ganhos de suas organizações** antes de juros e impostos (EBIT) estão relacionados à IA. Portanto, essas empresas planejam investir ainda mais em IA em resposta à pandemia de Covid-19. Complementarmente aos quesitos financeiros, o uso de tecnologias de IA pode impactar nos empregos de diversos países, ocasionando, assim, um impacto socioeconômico. Conforme o WEF (WORLD ECONOMIC FORUM - WEF, 2020), com base em dados de 20 economias (incluindo a do Brasil), de todos os novos empregos gerados nestes países, 1,38% serão relacionados a Dados, Inteligência Artificial (IA), Engenharia de software e *Cloud Computing*. O WEF aponta também que a probabilidade da IA ser adotada por vários setores da economia até 2025 é de 78%, com destaque para os setores de Comunicações Digitais e Tecnologia da Informação, com 95%, e de serviços financeiros, com 90%.

Por outro lado, os governos precisam criar condições para as empresas utilizarem a IA como vantagem competitiva. O Brasil se destaca por alguns pontos principais: o desenvolvimento de uma estratégia nacional de inteligência artificial, novos laboratórios de pesquisa e desenvolvimento na área e a presença de startups de IA. Em abril de 2021, o Brasil publicou a Estratégia Brasileira de Inteligência Artificial. O documento orientará as políticas para o desenvolvimento de IA no Brasil (BRASIL, 2021a).

A Estratégia Brasileira de Inteligência Artificial tem como objetivos: contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis; promover investimentos sustentados em pesquisa e desenvolvimento em IA; remover barreiras à inovação em IA; capacitar e formar profissionais para o ecossistema da IA; estimular a inovação e o desenvolvimento da IA brasileira em ambiente internacional; e promover ambiente de cooperação entre os entes públicos e privados, a indústria e os centros de pesquisas para o desenvolvimento da Inteligência Artificial (BRASIL, 2021a).

Ações complementares a essa estratégia foram criadas pelo governo, e o Brasil está se tornando um *hub* de inovação na área de IA. Ele e outros grandes países latino-americanos estão financiando a inovação em IA. O governo brasileiro anunciou recentemente a criação de uma rede de pesquisa e oito laboratórios para o desenvolvimento de IA (VENTURE BEAT - VB, 2020). Todas essas ações propiciam a criação de um ambiente que possibilita o

desenvolvimento industrial e empresarial com base no uso de tecnologias da Indústria 4.0, principalmente a IA.

Além disso, as *startups* de IA são capazes de redefinir indústrias (CB INSIGHTS, 2021). Hoje, 14% das *startups* no Brasil utilizam inteligência artificial para criar seu modelo de negócios ou se diferenciar de seus concorrentes (MCKINSEY & COMPANY, 2020b). Por sua vez, 37% das *startups* utilizam *analytics* e *big data* para o mesmo fim (MCKINSEY & COMPANY, 2020b), que são também foco do grupo de prioritário. Ainda que as startups exibam um desenvolvimento avançado individualmente na utilização de tecnologias de Indústria 4.0 (principalmente a IA), a criação de ecossistemas de inovação de startups é uma estratégia utilizada para o desenvolvimento de ideias, conceitos, produtos e processos voltados a empresas que contratam algumas startups com intuito de desenvolver a transformação digital e ingressar numa Jornada 4.0 (REDE RS INDÚSTRIA 4.0., 2021).

Tendo como base a perspectiva atual em relação à geração de empregos, conforme a Microsoft Data Science (MICROSOFT DATA SCIENCE, s.d.), o Brasil possui mais de 440 mil trabalhadores na área de análise de dados, *machine learning* e AI. Até 2025, é estimado que sejam adicionados mais de 880 mil empregos nessa área. É importante salientar que a geração de empregos é bastante importante para economia, visto que há tanto a geração de riqueza do País quanto o desenvolvimento econômico dos trabalhadores, possibilitando, assim, uma melhoria na qualidade de vida.

A Figura 3 consolida questões relevantes do grupo prioritário, esquematizando as aplicações da IA e a relevância dela no Brasil e no mundo.

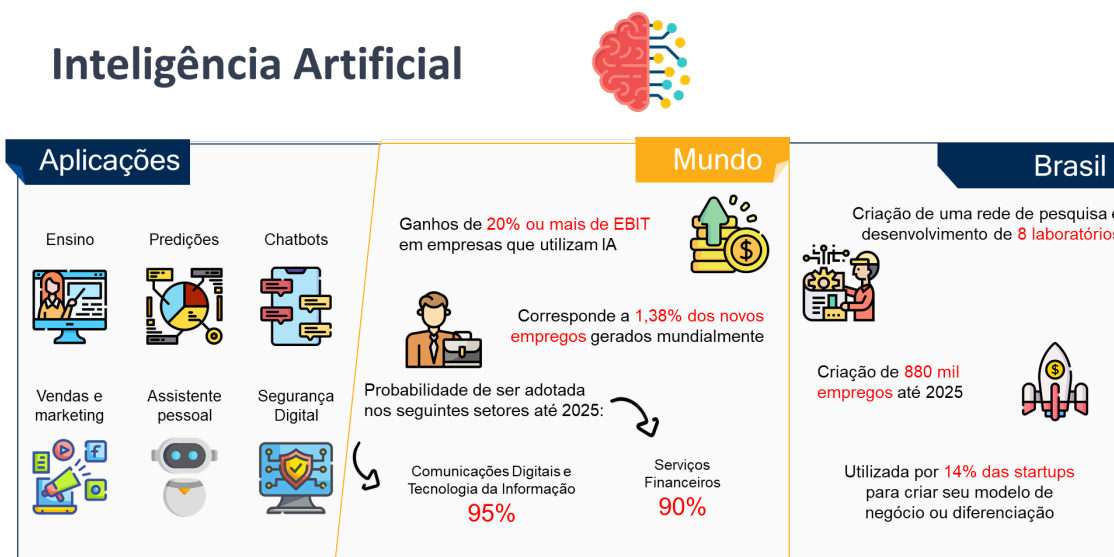


Figura 3 - Infográfico da Relevância para o Grupo de Inteligência Artificial

1.5 Grupo de aprendizado de máquina para redes do futuro, incluindo 5G (ITU/T/FG/5GML)

1.5.1 Escopo

O grupo Aprendizado de máquina para redes do futuro, incluindo 5G (**ITU/T/FG/5GML**), tem por objetivo a elaboração de especificações técnicas para *machine learning* e redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.

Para entendimento das normas do grupo, é importante compreender os seguintes conceitos:

- **Network function:** As funções de rede incluem, mas não estão limitadas a funcionalidades de nó de rede, por exemplo, gerenciamento de sessão, gerenciamento de mobilidade e funções de transporte, cujo comportamento funcional e interfaces são definidos. As funções de rede podem ser implementadas em um hardware dedicado ou como funções de software virtualizadas.
- **Machine learning (ML):** Processos que permitem que os sistemas computacionais entendam os dados e gerem conhecimento a partir deles, sem necessariamente serem programados explicitamente. Aprendizado de máquina supervisionado e aprendizado de máquina não supervisionado são dois exemplos de tipos de aprendizado de máquina.
- **Machine learning model:** modelo criado aplicando técnicas de aprendizado de máquina a dados. Um modelo de aprendizagem de máquina é usado para gerar previsões (por exemplo, regressão, classificação, agrupamento) em novos dados (não treinados). Um modelo de aprendizado de máquina pode ser encapsulado na forma de um software (por exemplo, máquina virtual, contêiner) ou em um componente de hardware (por exemplo, dispositivo IoT).

1.5.2 Status quo

A norma **ITU-T FG-ML5G-ARC5G** define uma arquitetura unificada para o *machine learning* na quinta geração (5G) e, no futuro, redes. Um conjunto abrangente de requisitos (arquitetônicos) é apresentado na norma, o que propicia construções de arquitetura específica. Com base nelas, um pipeline lógico de ML (junto aos requisitos derivados e suas realizações em vários tipos de arquiteturas) é discutido. Por fim, são listados na norma os principais problemas arquitetônicos enfrentados pela integração desse tipo de ML em redes futuras em constante evolução.

ITU-T Y.3172 especifica um framework arquitetônico para aprendizado de máquina em redes futuras, incluindo *International Mobile Telecommunications (IMT) 2020*. Um conjunto de requisitos arquitetônicos é apresentado, mostrando os componentes necessários para satisfazê-los. ITU-T Y.3172 também descreve um framework arquitetônico para a integração em redes futuras e aborda diretrizes para a aplicação do framework em uma variedade de redes subjacentes específicas da tecnologia.

ITU-T Y.3170-series analisa casos de uso de *machine learning* em redes futuras, incluindo IMT-2020, e apresenta em um formato unificado, fornecendo descrições de casos de uso, e indica o conjunto básico de requisitos possíveis para cada um. Na Tabela 4, são apresentados exemplos de alguns casos.

Tabela 4 - Casos de uso de machine learning em redes futuras

Casos de Uso	Definições
Redes cognitivas heterogêneas e SON baseado em ML	<p>Uma rede IMT-2020 fornece serviços para suportar diversos requisitos, usando funções instanciadas conforme o recomendado. As redes atuais são flexíveis e dependem muito de automação e virtualização do que as redes auto-organizadas (SON).</p> <p>Os requisitos em redes futuras não serão apenas altas taxas de dados e baixa latência, mas devem ser inteligentes para manter todos os requisitos de uma empresa de telecomunicações continuamente e de forma otimizada. Conseqüentemente, requer-se a intervenção de conceitos e algoritmos de inteligência artificial e aprendizado de máquina.</p> <p>Uma solução SON baseada em ML monitora alarmes de rede e indicadores-chave de desempenho (KPIs), além de tomar as medidas adequadas para limpar os alarmes, aprimorar os KPIs da rede ou fornecer recomendações de design de rede sem intervenção humana.</p>
Gerenciamento de recursos de rádio para divisão de rede (RRM-NS)	<p>A alocação de recursos de rádio é baseada em QoS por fluxo ou portadora de rádio perfil. Um dos principais desafios com futuras redes e implantação de rede é o fatiamento, que busca garantir o desempenho em termos de largura de banda dedicada mínima com alta confiabilidade, garantindo a utilização eficiente dos recursos de rádio.</p> <p>É fundamental que as redes habilitadas para ML apoiem a coleta contínua de dados para atualizar os modelos de previsão, com intuito de melhorar em tempo real a precisão e eficácia da previsão de modelos.</p>
Automação de operação de rede ponta a ponta - Projeto de serviço	<p>Os serviços da indústria vertical implicam uma ampla gama de requisitos de serviço. Por exemplo, uma rede de banda larga de alto rendimento é necessária para satisfazer os requisitos de serviço de diagnóstico remoto. ML pode fornecer soluções para design de serviço ágil e design de rede automatizado. ML também pode fornecer soluções automatizadas, escalonáveis e personalizadas para design de rede e, conseqüentemente, pode encurtar o tempo de entrega.</p>

ITU-T Y.3173 descreve uma estrutura para avaliar os níveis de inteligência do futuro em redes que incluem o IMT-2020. Logo, tem-se a tendência de desenvolvimento de inteligência de rede, de métodos de avaliação dos níveis de inteligência da rede e de visão arquitetônica para avaliar os níveis de inteligência. Os apêndices descrevem e detalham a relação entre a estrutura descrita nessa recomendação e trabalho correspondente em outras normas ou órgãos da indústria, bem como a aplicação do método para avaliar os níveis de inteligência da rede em casos de uso representativo.

ITU-T Y.3174 fornece uma estrutura para manipulação de dados para permitir o ML em futuras redes, incluindo IMT-2020. O escopo dessa recomendação inclui: antecedentes e motivações; requisitos de alto nível de tratamento de dados e modelos de dados; estrutura para tratamento de dados para permitir o ML em redes futuras, incluindo IMT-2020; diretrizes e exemplos para o uso da estrutura em redes futuras, incluindo IMT-2020.

A Tabela 5 sumariza as principais normas de machine learning para redes do futuro.

Tabela 5 - Normas do grupo de Machine Learning para Redes do futuro

Norma	Escopo
ITU-T FG-ML5G-ARC5G	Arquitetura unificada para aprendizado de máquina em redes 5G e futuras redes.
ITU-T Y.3172	Framework arquitetônico para <i>machine learning</i> em redes futuras, incluindo IMT-2020.
ITU-T Y.3170-series	<i>Machine learning</i> no futuro em redes, incluindo IMT-2020: casos de uso.
ITU-T Y.3173	<i>Framework</i> para avaliar os níveis de inteligência de futuras redes, incluindo IMT-2020.
ITU-T Y.3174	<i>Framework</i> para manipulação de dados a fim de permitir o aprendizado de máquinas em redes futuras, incluindo IMT-2020.

1.5.3 Mapa mental de relação com outros grupos

A Figura 4 ilustra as relações existentes com outros grupos que abordam o tema *machine learning para Redes do Futuro*. Foram listados à direita, em azul-escuro, os grupos prioritários que abordam tópicos de *machine learning*. Eles estão explicados abaixo:

- **Inteligência Artificial** – A proposta do grupo de IA é criar normas para subsidiar o desenvolvimento de programas de padronização, além de fornecer orientações aos comitês para o desenvolvimento de aplicações.
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO/IEC e em cooperação com outros comitês técnicos da ISO e IEC.
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como

para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.

- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas para a proteção da informação e das tecnologias da informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar questões de segurança e privacidade.
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de *framework* da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir de proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, tem o intuito de fornecer orientação a entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais – Segurança de rede e sistema.
- **Robótica** – O escopo do grupo prioritário de Robótica é a padronização no campo de robótica, excluindo brinquedos e aplicações militares.

Em amarelo, estão representados os grupos não classificados como prioritários, mas que apresentam elementos que se conectam ao grupo em destaque. Tais grupos estão listados a seguir:

- **Automatização de sistemas e integração:** Padronização na área de sistemas de automação e sua integração para projeto, *sourcing*, fabricação, produção e entrega, suporte, manutenção e descarte de produtos e seus serviços associados.
- **Gerenciamento e intercâmbio de dados:** Padrões para gerenciamento de dados dentro e entre ambientes de sistemas de informação locais e distribuídos. Fornece tecnologias capacitadoras para promover a harmonização dos recursos de gerenciamento de dados em áreas específicas do setor.
- **Dispositivos e integração em sistemas empresariais:** Padronização na área de sistemas de automação e sua integração para projeto, *sourcing*, fabricação, produção e entrega, suporte, manutenção e descarte de produtos e seus serviços associados.

- **Tecnologia da informação:** Ambiente de desenvolvimento de padrões onde especialistas se reúnem para desenvolver padrões mundiais de Tecnologia da Informação e Comunicação (TIC) para aplicações de negócios e de consumo.
- **Medição, controle e automação de processos industriais:** Preparar padrões internacionais para sistemas e elementos usados para medição, controle e automação de processos industriais. Para coordenar as atividades de padronização que afetam a integração de componentes e funções em tais sistemas, incluindo aspectos de proteção e segurança.
- **Engenharia de software e sistemas:** Padronização de processos, ferramentas de suporte e tecnologias de suporte à engenharia de produtos e sistemas de software.
- **Técnicas de identificação automática e captura de dados:** Padronização de formatos de dados, sintaxe de dados, estruturas de dados, codificação de dados e tecnologias para o processo de identificação automática e captura de dados e de dispositivos utilizados em aplicativos interindustriais e intercâmbios de negócios internacionais e para aplicativos móveis.

Em vermelho, acima e abaixo dos demais, estão os grupos conectados à transformação digital na Indústria, que também estão interconectados com o *machine learning* para redes do futuro.



Figura 4 - Mapa mental de relação do grupo de machine learning para Redes do Futuro com outros grupos

1.5.4 Tendências

1.5.4.1 ITU AI/ML no desafio 5G (ITU, 2020)

Atualmente, o grupo Aprendizado de máquina para redes do futuro, incluindo 5G (ITU/T/FG/5GML), não desenvolve novas normas. Porém, a IA e ML estão mudando o modo como as redes de comunicação são administradas. Muitas empresas do setor de tecnologia estão explorando como fazer o melhor uso da IA/ML. Portanto, é um momento oportuno para reunir a comunidade técnica e as partes interessadas a fim de inovar e resolver problemas

relevantes em 5G usando AI/ML. Com base nisso, a ITU está conduzindo um Desafio ITU AI/ML 5G global sobre o tema *Como aplicar a arquitetura ML em redes 5G*. Os participantes são desafiados a resolver problemas do mundo real, com base em tecnologias padronizadas desenvolvidas para ML em redes 5G. As equipes são desafiadas a habilitar, criar, treinar e implantar modelos de ML, de modo que os participantes adquiram experiência prática em AI/ML em áreas relevantes para 5G.

Por fim, a Figura 5 sumariza a evolução do grupo *Aprendizado de máquina para redes do futuro*, incluindo 5G (ITU/T/FG/5GML).

ML para redes do futuro (5G)

ISO/TC 184/SC 4

Escopo

Elaborar especificações técnicas para aprendizado de máquina (ML) para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados

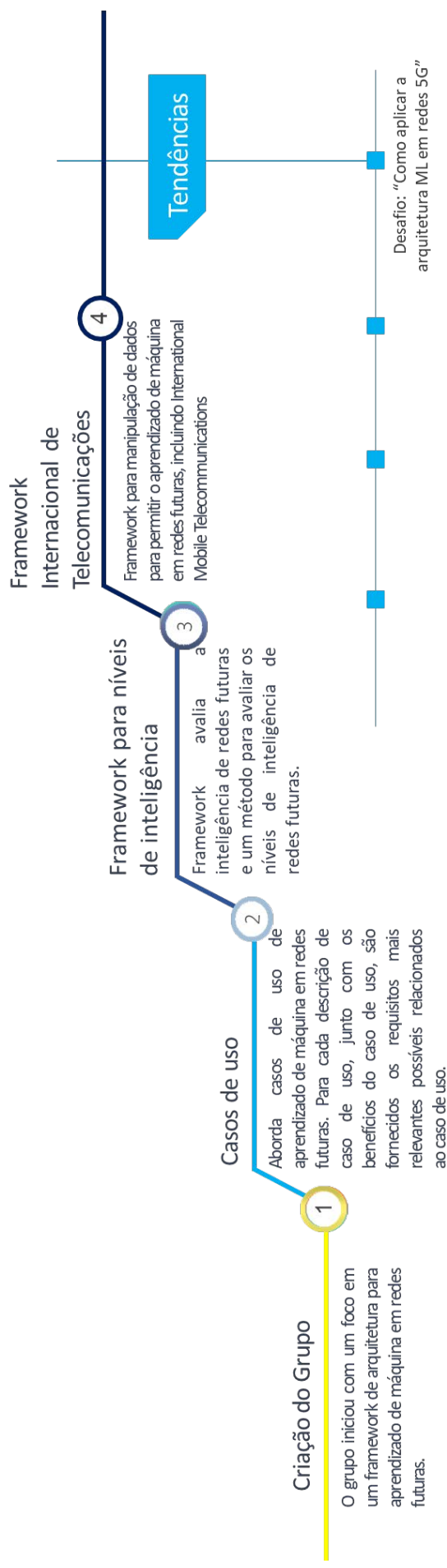


Figura 5- Consolidação da análise do Grupo de ML para Redes do Futuro

1.5.5 Relevância

O aprendizado de máquina ou *machine learning*, como é conhecido mundialmente, surgiu do fenômeno conhecido como *Big Data* (JORDAN; MITCHELL, 2015). Com a aumento da quantidade de dados gerados pelos dispositivos eletrônicos modernos, surgiu a necessidade de analisar essas informações de maneira mais eficiente. O *machine learning* é um tipo específico de inteligência artificial que automatiza a análise de dados. Esse método tem como objetivo permitir que sistemas possam aprender a partir de dados existentes, identificar padrões e tomar decisões com pouca ou nenhuma intervenção humana. O *machine learning* é um processo iterativo, o que significa que o sistema é capaz de adaptar suas decisões à medida que recebe novos dados. Isso é a base da tecnologia usada para desenvolver carros autônomos ou para a distribuição de anúncios e recomendações em redes sociais, por exemplo. Bancos e instituições financeiras usam essa tecnologia para detecção de fraudes e de novas oportunidades de investimento; profissionais da área da saúde podem usar dados sobre os pacientes para identificar tendências na sua saúde, diagnosticar doenças mais rapidamente e prescrever o tratamento com maior eficácia para cada paciente; varejistas são capazes de recomendar produtos de forma personalizada, baseados nos hábitos de compra dos clientes; dados sobre tráfego são usados para reduzir congestionamentos por meio da modelagem dos tempos semafóricos; empresas de aviação civil e transportadoras analisam dados para otimizar as rotas de transporte.

No entanto, o foco do grupo ITU/T/FG/5GML não é somente o ML. Ao integrar o ML à tecnologia 5G, as estações inteligentes serão capazes de tomar decisões por si mesmas, e os dispositivos móveis serão capazes de se adaptar dinamicamente com base nos dados aprendidos (DEEPSIG, 2021). Isso melhorará a eficiência, latência e confiabilidade dos aplicativos de rede. Ademais, com todo o potencial de uso de ML e IA para integração com redes 5G, as indústrias já estão trabalhando para inovar com 5G. Algumas das principais inovações incluem (DEEPSIG, 2021):

- Esportes: 5G fornecerá recursos de visualização avançados, como visualização em 3D e várias visualizações em perspectiva de um jogo ao vivo.
- Realidade virtual sem fio (VR): Com o 5G, os usuários poderão desfrutar do conteúdo de VR em qualquer lugar e a qualquer hora.
- Realidade aumentada (AR): 5G fornecerá serviços realistas de AR, como zoológicos virtuais.
- Apresentações ao vivo: 5G fornecerá performances ao vivo de altíssima qualidade a partir de dispositivos sem fio.
- Streaming de jogos: os jogos serão processados na nuvem via 5G e transmitidos enquanto permitem a entrada de outras pessoas.
- Cantos on-line: Muitas pessoas poderão cantar juntos, on-line, usando os recursos 5G.

- Carros autônomos: essa tecnologia exigirá potência de computação que só pode ser obtida por meio de redes 5G e IA, pois os mapas 3D das cidades são carregados nos veículos em tempo real, o tráfego é atualizado e as atualizações de software são enviadas.
- Casa sem fio: alguns dos primeiros dispositivos 5G incluirão pontos de acesso sem fio para toda a casa.
- Scanners de baixo consumo de energia, como determinados equipamentos agrícolas, caixas eletrônicas, equipamentos médicos e maquinário pesado de controle remoto: esses itens não precisam de uma conexão constante e, portanto, serão capazes de funcionar na mesma bateria por 10 anos, embora enviem periodicamente dados. Técnicos com habilidades especializadas serão capazes de operar máquinas de qualquer lugar do mundo.
- Segurança pública e infraestrutura: cidades e outros municípios poderão operar de forma mais eficiente usando redes 5G. As empresas de serviços públicos poderão rastrear o uso remotamente, os sensores podem notificar os departamentos de obras públicas quando os drenos inundam ou as luzes da rua queimam e os municípios poderão instalar câmeras de vigilância de forma rápida e econômica.
- Saúde: telemedicina, recuperação remota, fisioterapia via RA, cirurgia de precisão e até cirurgia remota são todas as possibilidades. Os hospitais poderão criar redes de sensores para monitorar os pacientes, os médicos poderão prescrever pílulas inteligentes para monitorar a conformidade e as seguradoras poderão monitorar os assinantes para determinar os tratamentos e processos apropriados.

Embora existam muitas complexidades inerentes à adoção de redes 5G, uma maneira pela qual a indústria está lidando com essas complexidades é integrando inteligência artificial às redes. Quando a Ericsson entrevistou os tomadores de decisão de 132 empresas de celular em todo o mundo, mais de 50% disseram que esperavam integrar IA em suas redes 5G até o final de 2020. Atualmente, o Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) consultou 350 executivos de diferentes países (Brasil, China, Estados Unidos, Índia e Reino Unido). O estudo da IEEE, entidade profissional setorial de alcance mundial, mostrou quais as tecnologias usadas pelos CIO e CTO pesquisados tiveram sua adoção acelerada com a pandemia: mais da metade (55%) dos entrevistados aceleraram a adoção da computação em nuvem; 52% aceleraram a adoção de 5G; 51% têm IA e *machine learning* acelerada; 42% adotaram IoT; 35% realidade aumentada e virtual; além de tecnologias de videoconferência (35%) (CIO FROM DIG, 2020; INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, 2021). O foco principal da integração de IA com 5G é reduzir despesas de capital, otimizar o desempenho da rede e criar novas receitas (DEEPSIG, 2021). Além disso, 55% dos tomadores de decisão afirmaram que a IA já está sendo usada para melhorar o atendimento

ao cliente e aprimorar a experiência do cliente, melhorando a qualidade da rede e oferecendo serviços personalizados (DEEPSIG, 2021). 70% acreditam que o uso de IA no planejamento de rede é o melhor método para recuperar os investimentos feitos na mudança de redes para 5G (DEEPSIG, 2021). 64% dos respondentes da pesquisa concentrarão seus esforços de IA no gerenciamento de desempenho de rede (DEEPSIG, 2021). Segundo uma pesquisa recente da Qualcomm, além de gerar uma receita de US\$ 13,2 trilhões até 2035, o 5G ajudará a criar cerca de 22 milhões de empregos até o mesmo ano (SIMPLE, 2020).

No Brasil, existem algumas iniciativas de empresas que se destacam (INFORCHANNEL, 2020):

- NEC Brasil, empresa japonesa de tecnologia: acredita que a importância da colaboração em relação ao 5G é estratégica, a adoção do 5G em conjunto com outras tecnologias, IoT, Inteligência Artificial e *Big Data* é a tendência do futuro, pois revolucionará a sociedade.
- Vivo no Brasil: o 5G pode aumentar a capacidade com o uso de sensores e dispositivos, porque a empresa já possui uma colaboração com a Vale no uso de veículos autônomos, que podem usar IA e ML;
- Amdocs: a união de redes de dados e inteligência que auxilia no monitoramento, coleta e análise de dados de forma inteligente. A rede 5G possui regras diferenciadas e monitoramento intenso que apoia a extração de dados. Um desafio é organizar a intensa produção de dados.
- Weg (BENETTI, 2020; 2021): concluiu diversos testes para implementação do 5G na fábrica de Jaraguá do Sul. Os robôs utilizam o 5G para otimizar as suas rotas. A empresa possui parcerias com associações (Agência Nacional de Telecomunicações e Agência Brasileira de Desenvolvimento Industrial) para regulamentar as redes 5G no Brasil. O 5G foi utilizado em conjunto com a IA para verificar se os colaboradores estavam utilizando máscaras.

Concluindo, a Figura 6 sumariza algumas aplicações de ML para redes do futuro e aborda sua importância mundial e brasileira.

ML para redes do futuro (5G)

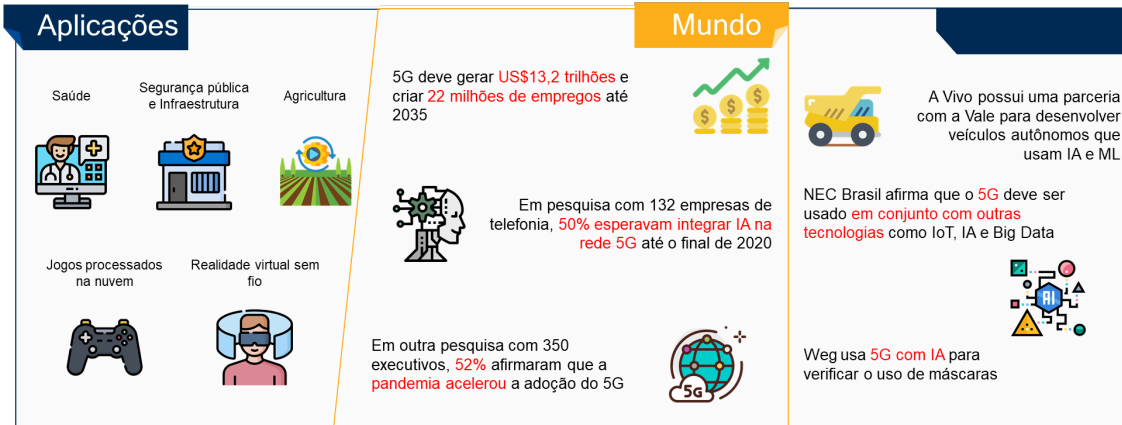
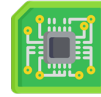


Figura 6 - Infográfico da Relevância para o Grupo de ML para redes do futuro (5G)

1.6 Conclusões da nota técnica sobre Inteligência Artificial

A IA pode ser aplicada nos mais diversos contextos e nas mais diversas indústrias, como em saúde, agricultura e segurança pública. Portanto, é imprescindível que as empresas entendam como é realizado o seu uso com apoio das normas que estabelecem critérios claros, *roadmaps*, *frameworks* que propiciam que as empresas usem a tecnologia da melhor forma possível em diversos setores. Dessa forma, as normas que envolvem IA e ML podem ajudar as empresas a impulsionar seus resultados econômicos, gerando também empregos. Mundialmente, os resultados já são bastante expressivos e tendem a crescer, porque o uso de IA e ML são vantajosos. No Brasil, as empresas possuem muitas oportunidades em relação à implementação das tecnologias, principalmente para startups. Além disso, grandes empresas se beneficiam desse desenvolvimento, visto que, normalmente, possuem investimento para desenvolver a inovação. Por isso, o relatório destacou casos de sucesso do uso da tecnologia no país. Além dos casos de sucesso, os centros de pesquisa e a geração de empregos também são destaque, logo toda a sociedade é beneficiada, já que, além de inovar, as empresas geram novos empregos para esses cargos tecnológicos (GIZ, SENAI, NEO-UFRGS, 2021 p. 39).

A normalização da IA e ML para redes do futuro traz uma nova perspectiva para uso das tecnologias, visto que as normas abordam casos de usos que podem auxiliar empresas que já estão implementando a tecnologia e as que desejam implementá-la. Dessa forma, as normas conseguem aproximar com exemplos como as empresas podem utilizar a tecnologia a fim de alcançar os resultados desejados. Com isso, elas podem suportar o desenvolvimento da Indústria 4.0 no País. Por exemplo, a norma de governança de IA pode suportar a LGPD, visto que a LGPD determina que as decisões tomadas por uma IA sejam transparentes. Portanto, as decisões podem ser auditáveis, e as metodologias de auditoria a serem desenvolvidas devem se basear nas tendências das normas.

Complementarmente, as empresas que ainda não aderiram ao uso de tecnologias podem usar o *benchmarking* com diversas outras que já estão usando as tecnologias. Além de resultados econômicos que são mundialmente destacados em casos de sucesso, em relação ao Covid-19,

as tecnologias implementadas que utilizam IA, ML e 5G propiciam maior segurança ao colaborador, uma vez que, com análise de imagens, é possível alertar quem está sem máscara para que todos estejam seguros e saudáveis. Com o uso das tecnologias destacadas no relatório, é possível uma melhora no ambiente de trabalho, propiciando melhorias na saúde do trabalhador.

1.7 Conclusões gerais da análise dos grupos prioritários

Como conclusão, são apresentados alguns pontos de lições aprendidas ao longo do estudo das dez normas consideradas prioritárias pelo grupo de trabalho da Câmara da Indústria 4.0.

Complementariedade dos grupos: Mesmo que os grupos de trabalho desenvolvam normas específicas do tema, as normas e os grupos prioritários se relacionam. Portanto, é imprescindível o entendimento do contexto que as normas estão inseridas para facilitar o processo decisório das empresas. Nesse sentido, as empresas necessitam ter uma visão clara do que desejam com o uso das tecnologias para que as normas possam auxiliar na potencialização dos resultados. Além disso, em muitas normas há casos de uso para que as empresas possam se identificar ou não.

Desenvolvimento nacional com base no desenvolvimento internacional: o Brasil já possui diversas empresas que implementam as mais diferentes tecnologias com objetivos diversos. No entanto, quando o Brasil não possui empresas que estão adotando as tecnologias, pode se espelhar em países mais avançados. Para isso, é essencial a realização do *benchmarking* internacional. Porém, são imprescindíveis avaliações claras e a definições de diretrizes e objetivos tanto do país quanto das empresas que querem implementar tecnologias de Indústria 4.0.

Entendimento base das tecnologias, do vocabulário, dos casos de usos e do *framework* facilitam o uso da tecnologia e a integração dos dados nas empresas: muitas informações que constam nas normas podem ajudar as empresas a se desenvolverem e adotarem tecnologias da transformação digital, visto que os conhecimentos que as normas propiciam são amplos e precisos. Portanto, as empresas devem reestruturar os seus processos digitais com base no conhecimento desenvolvido, e o uso das normas pode facilitar esse processo complexo.

Visão integrativa do uso de tecnologias pode apoiar os resultados da empresa: as empresas devem desenvolver uma visão abrangente do uso das tecnologias e como elas podem ser usadas em conjunto para maximizar os resultados das empresas. Muitas vezes, as tecnologias apresentam objetivos e funções únicas e, quando são utilizadas em conjunto, facilitam os processos das empresas. Com o uso das normas, é possível integrar tecnologias.

Segurança e cibersegurança

2 Segurança e cibersegurança

2.1 Sumário executivo

2.1.1 Foco do estudo

Esta nota técnica faz parte de um grupo de outros três trabalhos correlatos desenvolvidos pelo CGEE a pedido da Câmara da Indústria 4.0, com o objetivo de analisar dez grupos considerados prioritários para a normalização no contexto da Indústria 4.0. A presente nota técnica analisa o contexto da **Segurança e Cibersegurança** na normalização internacional sobre a Indústria 4.0. O estudo tem como tema central a normalização em relação à transformação digital e à Indústria 4.0 e analisa a relevância das normas em relação a aplicações de segurança no contexto da Indústria 4.0. Para tanto, são analisados três grupos prioritários: (i) Segurança de máquinas (ISO/TC 199); (ii) Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27); (iii) Segurança para medição e controle de processos industriais (IEC/TC65/WG10).

2.1.2 Abordagem metodológica

O relatório utiliza uma abordagem mista que combina a análise das normas/regulações, de relatórios, de empresas em relação aos grupos prioritários estudados. Além de fazer uma análise sobre estudos anteriores do tema. Complementarmente, utilizou-se uma análise de conteúdo e o desenvolvimento de figuras para facilitar a compreensão do tema.

2.1.3 Resultados

O relatório apresenta diversos resultados:

- As normas de segurança de máquinas têm por objetivo padronizar conceitos e princípios gerais de segurança, permitindo, assim, que as empresas possam utilizar as normas no cotidiano. Como consequência, as normas propiciam a empresas um alicerce seguro. Por exemplo, em relação à Indústria 4.0, as normas contribuem especificando requisitos para um sistema integrado de manufatura. Complementarmente, na segurança de máquinas, o uso de veículos autônomos está normatizado a fim de mitigar os riscos associados ao uso de inteligência artificial. Além disso, a segurança de máquinas está associada ao uso de robôs colaborativos, entendendo o processo de interação homem-máquina.
- As normas de segurança da informação, cibersegurança e proteção de privacidade explicam a importância de esquemas e de uso de assinatura digital e os métodos de criptografia autenticada. Além disso, as normas abordam a segurança de sistemas biométricos e como se realiza a gestão da segurança da informação. Os critérios de

avaliação de segurança de TI; segurança e privacidade de dispositivos IoT; competências para profissionais de sistemas de gestão de segurança da informação; e diretrizes de implementação de tecnologias, que são tendências para os próximos anos. Além dessas particularidades, é essencial que as empresas foquem em prevenção da cibersegurança, visto que há diversas normas que podem se apoiar nisso, além de entender como é o ciclo de vida de produção inteligente, como o uso de Inteligência artificial, por exemplo. Complementarmente, destaca-se a Lei Geral de Proteção de Dados, que o Brasil criou com base nas normas europeias.

- Em relação a questões de segurança de medição, as normas abordam as diretrizes de avaliação de conformidade de segurança. Logo, as empresas podem usá-las em conjunto com tecnologias para verificar se estão em conformidade com as necessidades do negócio. Outra questão importante das normas é a definição de diferentes níveis de segurança. As empresas podem planejá-los quando utilizam alguma tecnologia da Indústria 4.0. Além disso, as normas abordam uma esquematização de recursos de segurança utilizados na automação industrial, auxiliando as empresas que desejam automatizar seus processos e utilizar tecnologias da Indústria 4.0.

2.2 Introdução

Este projeto tem como objetivo geral o desenvolvimento de um estudo detalhado das discussões, propostas e tendências nos principais fóruns internacionais de normalização com foco na Indústria 4.0, facilitando a compreensão de empresas e entidades nacionais de sua relevância para o desenvolvimento e transformação digital da indústria brasileira. As três notas técnicas que compõem o estudo global analisam dez grupos prioritários previamente definidos pelo Grupo de Trabalho “Regulação, Normalização Técnica e Infraestrutura para Normalização” da Câmara Brasileira da Indústria 4.0, com intuito de expor e explicar o estado atual do trabalho normativo, bem como propostas em discussão. Os temas abordados pelas três notas técnicas são:

Nota técnica A: **Inteligência artificial e 5G;**

Nota técnica B: **Segurança e cibersegurança;**

Nota técnica C: **Redes industriais e interoperabilidade.**

2.2.1 Conteúdo deste relatório

O relatório contempla três grupos prioritários, seu escopo de atuação, *status quo* das normas publicadas, relacionamento com outros grupos prioritários, tendências de normalização para os próximos anos e relevância dos grupos para o Brasil. Os grupos prioritários abordados no relatório são:

1. Segurança de máquinas (ISO/TC 199);
2. Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27);
3. Segurança para medição e controle de processos industriais (IEC/TC65/WG10).

2.2.2 Grupos para o desenvolvimento de normas

Os grupos prioritários são Comissões de Estudo sobre temas específicos que têm como objetivo desenvolver normalizações sobre assuntos relevantes no desenvolvimento nacional em nível mundial. Logo, os grupos prioritários são essenciais para as empresas que se baseiam para o desenvolvimento de produtos e serviços. De modo geral, a participação nessas comissões é aberta a qualquer parte interessada. O Brasil, em alguns grupos, possui participação. É importante salientar que o País pode ser um membro P, que é mais atuante e participativo, e membro O, que é mais observador.

Complementando essas especificidades dos grupos, é imprescindível entender a que instituições de normalização eles estão associados. Por exemplo, nesse relatório, são a ISO, a IEC e a ITU. A ISO é a Organização Internacional de Normalização que desenvolve normas e relatórios técnicos quando há necessidade de mercado. Para tal, as normas 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. A fim de que as necessidades estejam alinhadas e direcionadas para um objetivo de crescimento, a Secretaria da ISO desenvolve as normas.

Embora a ISO seja muito relevante, 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. Dessa maneira, eles fazem publicações para a aplicação em fábricas e em diversos ambientes. É importante salientar que o desenvolvimento de normas é feito por meio do Comitê Nacional da IEC de cada país. Além da ISO e da IEC, a ITU aborda a padronização da área de Telecomunicações do ITU - União Internacional de Telecomunicações (*International Telecommunication Union*), focada também no desenvolvimento de normas. Com base nessas informações, a ITU é focada na parte de telecomunicações, enquanto a IEC aborda temas de eletroeletrônica. De forma geral, a ISO trabalha com os temas não abordados pelos comitês anteriores. Consequentemente, as três se complementam entre si, desenvolvendo novas normalizações para suportar as empresas. Em suma, elas podem ser consideradas “federações” que congregam os organismos de normalização nacionais de cada país, sendo permitida a participação de uma entidade por país, a qual pode ser membro de diversas entidades). A maior diferença entre eles é o fato de que a representação na ISO e IEC é feita por organismos de normalização, enquanto na ITU a participação é realizada pelos governos, uma vez que apresenta caráter mais estratégico.

Em relação a normas da ISO, é importante entender alguns tópicos 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);
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 International 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 das etapas se encontra no Apêndice A. Em relação a tipologias de documentos da ISO, podem ser normas internacionais, porém também aborda outros documentos, tais como *Technical Specification* (TS), *Public Available Specification* (PAS) e *Technical Report* (TR).

2.2.2.1 Coordenação

A participação na normalização internacional requer um bom nível de coordenação dos trabalhos e participações. A atual nota busca mostrar as relações entre os grupos prioritários para facilitar e agilizar o processo de normalização com o enfoque na coordenação. Quando um certo grau de coordenação e gestão for alcançado entre os atores que participarão das diferentes discussões de normalização, maiores serão os ganhos para a indústria brasileira. Além disso, em busca de uma coordenação eficiente, ágil e eficaz, são abordados conceitos que facilitam o entendimento do vocabulário de Indústria 4.0.

2.2.2.2 Visão estratégica

É crítico desenvolver e implementar uma visão estratégica da participação na normalização internacional para a Indústria 4.0. Este relatório aborda uma visão estratégica ao adicionar elementos importantes de diversos atores da Indústria 4.0 tanto na análise das normas quanto na relevância. Aborda-se, conseqüentemente, aspectos de governança de gestão, pois aponta aplicações práticas da implementação de tecnologias em diversos contextos, promovendo, assim, um entendimento estratégico sobre o assunto. Em alguns grupos prioritários, quando necessário, são destacadas as diferenças estratégicas dos países com intuito de identificar a sua relevância.

2.2.2.3 Recursos

Desenvolver normas e participar ativamente desse desenvolvimento custa recursos importantes. Este relatório aborda questões relacionadas aos recursos humanos competentes para desempenhar determinadas funções da Indústria 4.0. Além disso, o relatório abrange

informações pertinentes a respeito das necessidades do desenvolvimento de capacidades dos usuários, dos desenvolvedores e dos colaboradores da Indústria 4.0. Assim, é possível entender como cada ator pode ajudar ao desenvolvimento da transformação digital na indústria brasileira, destacando os principais conhecimentos que são necessários para este fim.

2.2.2.4 Capacitação

A capacitação de recursos humanos para a participação nas atividades de normalização internacional é um dos principais desafios nacionais. Este relatório traz embasamento das principais normas internacionais que podem ser utilizadas para desenvolver as capacidades e os conhecimentos dos colaboradores, capacitando atores do governo, das empresas e das universidades. Com base em uma visão holística, o relatório abrange aspectos importantes que diferentes membros de uma instituição necessitam desenvolver para conseguirem alcançar os objetivos organizacionais de implementação das tecnologias da Indústria 4.0.

2.2.2.5 Priorização

É necessário priorizar os temas, setores e atividades em que vale a pena se envolver ativamente, até com certa liderança, decidir quem serão acompanhados e também aqueles para os quais não é prioritário se envolver. Respondendo a tal necessidade, este relatório prioriza, com base na análise completa das normas e da relevância dos grupos prioritários, os principais assuntos que devem ser considerados para a normalização, mostrando a relevância de cada grupo prioritário, tanto para o Brasil quanto para o mundo. Complementarmente, o relatório traz exemplos mundiais do uso das tecnologias para o desenvolvimento da Indústria 4.0, ampliando o número de países demonstrando a relevância da atuação de alguns países e como as suas ações e melhores práticas apresentaram resultados positivos. Com base no benchmarking Internacional, é possível entender como o Brasil está posicionado quanto aos outros países no uso de tecnologias da Indústria 4.0. Além disso, o relatório apresenta como as empresas que operam no País são destaques internacionais no uso de tecnologias, abordando as ações das empresas, as legislações desenvolvidas e os principais atores que interagem para o desenvolvimento de uma indústria mais avançada.

Ademais, o relatório agrega valor em relação à diferença de desenvolvimento de alguns setores em comparação aos outros, e como o uso de algumas tecnologias está propiciando avanços nesses setores, mostrando aplicações e seus resultados em diversas áreas. Além do mais, o relatório aborda algumas previsões da literatura para o uso de tecnologias, os empregos que podem ser gerados e o desenvolvimento de ações nos próximos anos, expondo os benefícios esperados para o futuro.

Algumas definições da Indústria 4.0 e do uso de tecnologias necessitavam de esclarecimento, visto que a literatura não convergia para uma definição comum, o que dificultava o entendimento de conceitos-chave para a convergência e gestão de estratégias sobre o desenvolvimento da Indústria 4.0 no País. Considerando esse aspecto, foram destacadas, ao longo do relatório, algumas definições importantes para a adoção de tecnologias, propiciando o conhecimento necessário para o entendimento completo dos temas abordados com base na normalização. Favoreceu-se, assim, a compreensão das principais definições, promovendo a disseminação do conhecimento sobre o tema e aprofundando, quando necessário, alguns elementos principais e definições que baseiam a adoção das tecnologias.

2.3 Metodologia

A partir da análise de conteúdo das normas dos grupos prioritários e de relatórios, artigos e sites oficiais relacionados, foram debatidos cinco principais tópicos para cada um dos grupos:

- (i) Escopo: aborda o escopo e algumas das principais definições do grupo prioritário;
- (ii) Status quo: apresenta as principais normas do grupo prioritário, mostrando o que foi realizado no passado até o que foi publicado em 2021;
- (iii) Mapa mental: facilita o posicionamento do grupo prioritário em relação a outros grupos e tópicos relacionados a ele;
- (iv) Tendências: aborda as tendências normativas a serem publicadas pelos grupos prioritários nos próximos anos, detalhando quais normas estão em desenvolvimento atualmente;
- (v) Relevância: aborda as principais aplicações dos temas relacionados ao grupo prioritário estudado, sua importância mundial e no Brasil.

Para facilitar a compreensão de como foi realizada cada etapa da análise dos grupos prioritários, consolidou-se o detalhamento das etapas na Tabela 6.

Tabela 6 - Detalhamento da metodologia para o conteúdo do Relatório

Etapas	Metodologia
(vi) Escopo	Realizou-se por meio da análise de conteúdo das normas.
(vii) Status quo	Realizou-se por meio da análise de conteúdo das <i>normas publicadas</i> selecionadas por meio de uma análise temporal e prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ¹¹
(viii) Mapa mental	Realizou-se por meio da análise de conteúdo das normas, de entrevistas e de análise dos <i>Laisons</i> presentes nos sites dos grupos prioritários. ¹²
(ix) Tendências	Realizou-se por meio da análise de conteúdo das <i>normas em desenvolvimento</i> selecionadas por meio de uma análise temporal e prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ¹³
(x) Relevância	Realizou-se por meio da análise de conteúdo de relatórios de consultorias, de artigos e de sites oficiais a fim de se destacar as primeiras aplicações, a importância mundial e importância no Brasil. ¹⁴

¹¹ As normas foram analisadas em maio, junho e julho de 2021.

¹² As relações foram desenvolvidas nos meses de maio, junho e julho de 2021.

¹³ As normas foram analisadas em maio, junho e julho de 2021. Algumas normas foram revisadas na semana de 16 a 20 de agosto de 2021.

Além das análises dos grupos prioritários, ao final do relatório, apresenta-se uma avaliação das principais lições aprendidas com base nos temas desenvolvidos pelos grupos. A partir disso, foi possível a realização de uma série de abstrações dos temas tratados pelos grupos prioritários, obtendo percepções do desenvolvimento de diversas estruturas normativas internacionais e nacionais, e como elas, em conjunto, podem alavancar a Indústria 4.0 nas empresas brasileiras. Portanto, a reflexão das lições aprendidas discute questões relevantes do uso de tecnologias da Indústria 4.0 para o desenvolvimento de uma indústria nacional mais tecnológica que acompanha as normalizações internacionais sobre o assunto.

2.4 Grupos de segurança de máquinas (ISO/TC 199)

2.4.1 Escopo

O grupo prioritário de segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas, incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura da ISO e IEC, e em cooperação com outros comitês técnicos destas entidades.

Dentro das normas deste grupo, os principais termos são:

- I. **Medida de proteção:** medidas destinadas a alcançar a redução de risco, as medidas de proteção podem ser implementadas:
 - pelo *designer* (design inerentemente seguro, medidas de proteção e medidas de proteção complementares, informações para uso) e
 - pelo *usuário* (organização: procedimentos de trabalho seguros, supervisão, sistemas de autorização de trabalho; fornecimento e uso de salvaguardas adicionais; uso de equipamento de proteção individual; treinamento).
 - II. **Safeguarding:** medida de proteção usando salvaguardas para proteger as pessoas dos perigos que não podem ser razoavelmente suprimidos ou riscos que não podem ser suficientemente limitados por medidas de projeto inerentemente seguras.
 - III. **Procedimento de trabalho seguro:** procedimento especificado que visa reduzir a possibilidade de lesões durante a execução de uma tarefa atribuída.
 - IV. **Medida de design inerentemente segura:** medida de proteção que elimina perigos ou reduz os riscos associados a perigos, alterando o projeto ou as características operacionais da máquina sem o uso de guardas ou dispositivo de proteção.
 - V. **Sistema de manufatura integrado (IMS):** grupo de máquinas trabalhando juntas de forma coordenada, ligadas por um sistema de manuseio de materiais, interconectadas por controles (ou seja, controles IMS), com a finalidade de fabricação, tratamento, movimento ou embalagem de peças ou conjuntos discretos.
-

2.4.2 Status quo

O grupo prioritário de segurança de máquinas iniciou com normas cujo foco se voltava à integração de sistemas de manufatura, desenvolvendo, assim, requerimentos básicos de segurança de máquinas e de desenho de novas máquinas. Entre as normas desenvolvidas pelo grupo relacionadas à Indústria 4.0, destaca-se a **ISO 11161:2007**, que especifica os requisitos de segurança para sistemas de manufatura integrados (IMS), os quais incorporam duas ou mais máquinas interconectadas para aplicações específicas, como fabricação ou montagem de componentes. A norma fornece requisitos e recomendações para o projeto seguro, proteção e informações para o uso de tais IMS.

Posteriormente, o grupo prioritário desenvolveu alguns documentos relacionados à segurança do sistema de controle (princípios gerais e validação) e uma série de normas para dispositivos de proteção sensíveis à pressão. Por exemplo, a **ISO 13849-1** fornece requisitos de segurança e orientação sobre os princípios para o projeto e integração de partes relacionadas à segurança de sistemas de controle (SRP/CS), incluindo o projeto de software. Já a **ISO 13849-2** especifica os procedimentos e condições a serem seguidos para a validação por análise e teste das funções de segurança especificadas, da categoria alcançada e do nível de desempenho alcançado com base nos requisitos de segurança de um sistema de controle projetado de acordo com a ISO 13849-1.

Atualmente, o grupo atua com foco no desenvolvimento de normas de sistema de suporte de proteção que estão relacionados com **ISO 12100** (avaliação de riscos e redução de riscos para o desenho de máquinas) e com a **ISO 11161** (principalmente em relação a requisitos básicos de sistema de manufatura). ISO12100 especifica a terminologia básica, os princípios e uma metodologia para alcançar a segurança no projeto de máquinas. Ademais, a norma especifica os princípios de avaliação e redução de risco para ajudar os projetistas a alcançar este objetivo. Tais princípios são baseados no conhecimento e na experiência do projeto, uso, incidentes, acidentes e riscos associados às máquinas. De forma geral, são fornecidas orientações sobre a documentação e verificação do processo de avaliação e redução de riscos.

Complementarmente, a norma **ISO/TR 22053:2021** tem por objetivo o desenho e a integração de sistema de suporte de proteção, mostrando a aplicação dos termos utilizados em outras normas, com a norma ISO 12100. Em todo caso, é importante entender a definição de *sistema de suporte de proteção (SSS)*, que abrange a redução de risco complementar/medido de proteção para permitir a seleção pelo uso de meios de autenticação. Um sistema de suporte de proteção é usado em conjunto com guardas e dispositivos de proteção. Trata-se de um sistema de suporte de proteção ativa, isto é, um modo solicitado quando a autorização atende aos requisitos para a tarefa a ser executada. Consequentemente, o sistema de suporte afeta todos os modos de operação que requerem tarefas em zonas de perigo, incluindo, por exemplo, ajuste, configuração, ensino e solução de problemas. O SSS utiliza alguns dispositivos, entre eles, o *elemento de identificação*, que se refere a todas as unidades lógicas e seus equipamentos periféricos, mas exclui o banco de dados.

Na norma **ISO/TR 22100-1:2021**, há um fluxograma para o processo de avaliação e mitigação do risco que pode ser usado pelas empresas. Aliás, nessa mesma norma são propostos outros fluxogramas e *frameworks* que podem ser utilizados pelos designers de máquinas para prover equipamentos mais tecnológicos e seguros aos *smart workers*.

Como a segurança dos trabalhadores pode ser comprometida quando há inserção de *machine learning* e inteligência artificial em máquinas, o grupo desenvolve normas que englobam as principais implicações do seu uso, uma vez que o sistema pode usar *machine learning* para melhorar a performance da máquina e executar as tarefas. Conforme a **ISO/TR 22100-5:2021**, o uso de IA no setor de máquinas é recomendado para as seguintes aplicações: controle de qualidade, otimização do processo, monitoramento de falhas e manutenção preditiva. Dessa forma, é importante ressaltar que o grupo de segurança de máquinas está intimamente relacionado ao grupo de Inteligência Artificial.

Além da implementação de IA, a Indústria 4.0 propõe a utilização de AGVs (*Automated Guided Vehicle* – veículos autônomos). É importante avaliar as implicações de segurança quando o AGV opera em um espaço não delimitado por um perímetro de segurança e ocorre otimização de rotas do AGV baseada em aplicações de IA. Nessa situação, o AGV introduz novos perigos no ambiente de trabalho e aumentam-se os riscos de acidentes, uma vez que o AGV pode criar rotas na planta, as quais podem ser próximas aos locais de trabalho dos operadores. Para tanto, é necessária uma análise dos riscos, e algumas normas ISO podem servir de apoio. A **ISO/TR 22100-5:2021** pode ajudar no processo de implementação de AGV com IA nas fábricas, visto que sumariza as principais etapas de avaliação e mitigação de riscos conforme a ISO 12100 para AGV com e sem o uso da IA.

Assim, as normas já publicadas pelo grupo prioritário de segurança de máquinas (ISO/TC 199) e que possuem relação direta com a Indústria 4.0 são apresentadas na Tabela 7.

Tabela 7- Normas do grupo de Segurança de Máquinas

Norma	Escopo
ISO 11161:2007	Requisitos de segurança para sistemas de manufatura integrados (IMS).
ISO 13849-1	Requisitos de segurança e orientação para o projeto e integração de partes relacionadas à segurança de sistemas de controle.
ISO 13849-2	Procedimentos e condições a serem seguidos para a validação por análise e teste das funções de segurança.
ISO12100	Terminologia básica, os princípios e uma metodologia para alcançar a segurança no projeto de máquinas.
ISO/TR 22053:2021	Desenho e integração de sistema de suporte de proteção (SSS).
ISO/TR 22100-1:2021	Processo de avaliação e mitigação do risco.
ISO/TR 22100-5:2021	Inteligência artificial no setor de máquinas.

2.4.3 Mapa mental da relação do grupo Segurança de Máquinas com outros grupos

Para complementar a análise do grupo prioritário, desenvolveu-se um mapa mental para facilitar a análise das relações entre os grupos prioritários, tecnologias e outros grupos existentes na Figura 7. À direita, em azul mais escuro, estão os grupos prioritários analisados neste relatório, que se relacionam com a segurança das máquinas e que estão listados abaixo:

- **Inteligência Artificial** – A proposta do grupo de inteligência artificial é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA.
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas para a proteção da informação e das tecnologias da informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar elementos de segurança e privacidade.
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo a definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. Tem como objetivo servir de proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo prioritário tem o objetivo de fornecer orientação a entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido e em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais e segurança de rede e sistema.
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.
- **Robótica** - O escopo do grupo prioritário de robótica é a padronização no campo de robótica, excluindo brinquedos e aplicações militares.

À esquerda, em amarelo, estão os grupos que não são analisados diretamente neste relatório, mas estão relacionados ao assunto. Pode-se perceber que tais grupos dizem respeito ao trabalho efetivo em indústrias e a discussões que permeiam esse âmbito. São eles:

- **Aspectos eletroeletrônicos:** Padronização no campo da aplicação de equipamentos e sistemas eletrotécnicos de máquinas (incluindo um grupo de máquinas trabalhando em conjunto de maneira coordenada, excluindo aspectos de sistemas de nível superior) não portáteis à mão durante o trabalho, mas que podem incluir equipamentos móveis.
- **Medição do processo industrial, controle e automação:** Preparar padrões internacionais para sistemas e elementos usados para medição, controle e automação de processos industriais, a fim de coordenar as atividades de padronização que afetam a integração de componentes e funções em tais sistemas, incluindo proteção e segurança.
- **Segurança:** Padronização de conceitos básicos e princípios gerais para segurança, incorporando terminologia, metodologia, proteções e dispositivos.
- **Ruído:** Normalização na área de máquinas e equipamentos utilizados em canteiros de obras, incluindo: máquinas de concreto, fundação, de processamento de agregados, máquinas e equipamentos de construção e manutenção de estradas, máquinas de perfuração de túnel (TBMs) e de e equipamentos associados.

Já em vermelho, acima e abaixo dos outros tópicos, pontuam-se os fatores relacionados à Indústria 4.0, que também tem a ver com a segurança das máquinas.

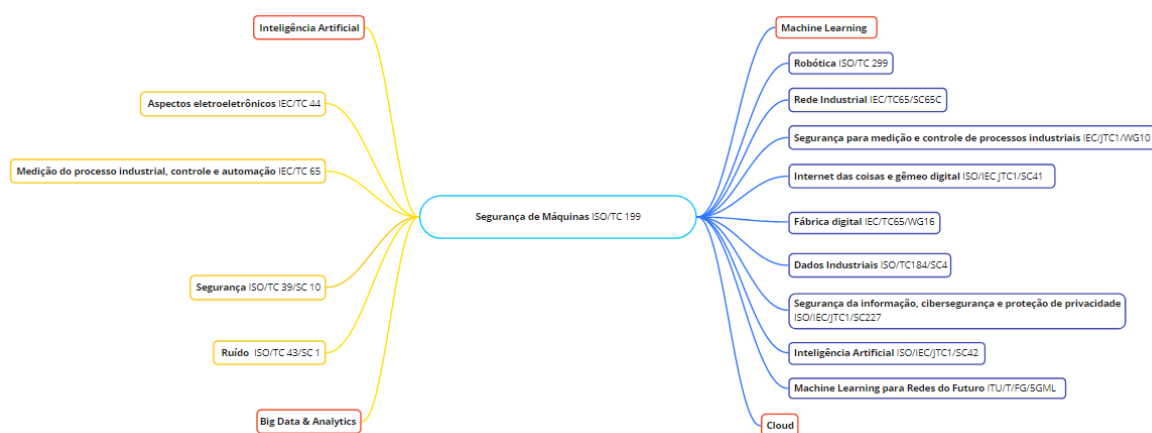


Figura 7 - Mapa mental de relação do grupo de Segurança de Máquinas com outros

2.4.4 Tendências

2.4.4.1 Dados de segurança mecânica para contatos físicos entre máquinas em movimento ou partes móveis de máquinas e pessoas (ISO/DIS 21260)

A **ISO/DIS 21260** (que está na fase 40,98)¹⁵ abrange limites para contatos físicos entre a máquina ou partes da máquina e humanos causados pelo movimento da máquina como parte de seu uso pretendido ou uso indevido previsível. A ISO aborda todos os tipos de máquinas que são projetadas para funcionar, nas quais as pessoas têm permissão para estarem presentes e a máquina pode fazer contato físico com elas. Além disso, a norma abrange interações que são intencionais ou não intencionais. A norma contempla diversos fluxogramas que explicam uma visão geral da avaliação de risco/redução de risco (ISO 12100), que analisam pontos e contato da interação homem-máquina e a classificação dos contatos e que abordam os componentes de transferência de energia durante o contato. Tal norma é importante no contexto da Indústria 4.0, dado o avanço nas automações dos processos e o incremento da interação homem-máquina, inclusive com a possibilidade de utilização de robôs colaborativos

2.4.4.2 Dispositivos de intertravamento associados às proteções - Princípios para projeto e seleção (ISO/DIS 14119)

A norma **ISO/DIS 14119** (que está em desenvolvimento na fase 40,60 e foi publicada uma versão em 2013)¹⁶ especifica os princípios para o projeto e seleção – independentemente da natureza da fonte de energia – de dispositivos de intertravamento associados a proteções, e fornece orientação de medidas para minimizar a possibilidade de anulação de dispositivos de intertravamento de maneira razoavelmente previsível. A norma ISO/DIS 14119 aborda as partes das proteções que atuam nos dispositivos de intertravamento e princípios para o projeto, seleção e aplicação de dispositivos e sistemas de intertravamento de chave com segredo para aplicações de máquinas, independentemente do tipo de energia usada para controlá-los ou que eles controlam. Além da ISO/DIS 14119, a norma **ISO 14120** especifica os requisitos gerais para o projeto e construção de proteções fornecidas principalmente para proteger as pessoas de riscos mecânicos. Por isso, as normas devem ser implementadas juntas. Consequentemente, o processamento do sinal do dispositivo de intertravamento para parar a máquina e evitar uma inicialização inesperada é tratado na **ISO 13849-1** ou **IEC 62061: 2015**. Tais normas são importantes no contexto da Indústria 4.0, dado o avanço nas automações dos processos e o incremento da interação homem-máquina, inclusive com a possibilidade de utilização de robôs colaborativos.

¹⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/70298.html>

¹⁶ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/75942.html>

2.4.4.3 Posicionamento de salvaguardas com respeito à abordagem do corpo humano e a velocidades (ISO/CD 13855:2021)

A ISO/CD 13855:2021 (que está na fase de desenvolvimento 30,60 e foi publicada uma primeira versão em 2010)¹⁷ estabelece o posicionamento de salvaguardas com respeito à abordagem do corpo humano ou de suas partes, especificando parâmetros com base em valores para sua abordagem e fornece uma metodologia para determinar as distâncias mínimas da zona de detecção. Os valores para velocidades de abordagem (velocidade de caminhada e movimento do membro superior) são testados ao longo do tempo e comprovados na experiência prática. A norma fornece também orientação para abordagens típicas.

2.4.4.4 Integração de máquinas em um sistema (IMS) – Requisitos básicos (ISO/CD 11161:201)

A revisão da ISO/CD 11161:2019 (cujas versões são de 2007 e 2010 e está na fase 30,20)¹⁸ especifica os requisitos de segurança para a integração de máquinas em um sistema, fornecendo requisitos e recomendações para um design, proteção e segurança para o uso de um IMS. No contexto da ISO/WD 11161:2019, o termo sistema se refere a um maquinário integrado que também pode colaborar com outros domínios dentro da(s) cadeia(s) de abastecimento de uma empresa. Entretanto, a fim de realizar uma avaliação de risco adequada, os seguintes parâmetros básicos de IMS devem ser definidos: funcionalidades; limites; interfaces entre as diferentes partes do IMS.

Assim, as normas de tendências do grupo Segurança de máquinas (ISO/TC 199) que possuem alguma relação com a Indústria 4.0 são consolidadas na Tabela 8.

Tabela 8 - Normas referentes a tendências do grupo de Segurança de Máquinas

Norma	Escopo
ISO/DIS 21260	Dados de segurança mecânica para contatos físicos entre máquinas em movimento ou partes móveis de máquinas e pessoas.
ISO/DIS 14119	Dispositivos de intertravamento associados às proteções – Princípios para projeto e seleção.
ISO/CD 13855:2021	Posicionamento de salvaguardas com respeito à abordagem do corpo humano.
ISO/WD 11161:2019	Integração de máquinas em um sistema – Requisitos básicos.

Para complementar as informações da Tabela 8, a Figura 8 sumariza as informações referentes ao escopo, *status quo* e tendências do grupo.

¹⁷ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/80590.html>

¹⁸ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/79368.html>

Segurança de máquinas

ISO/TC 199

Escopo

Padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC Guia 51 e em cooperação com outros comitês técnicos da ISO e IEC.

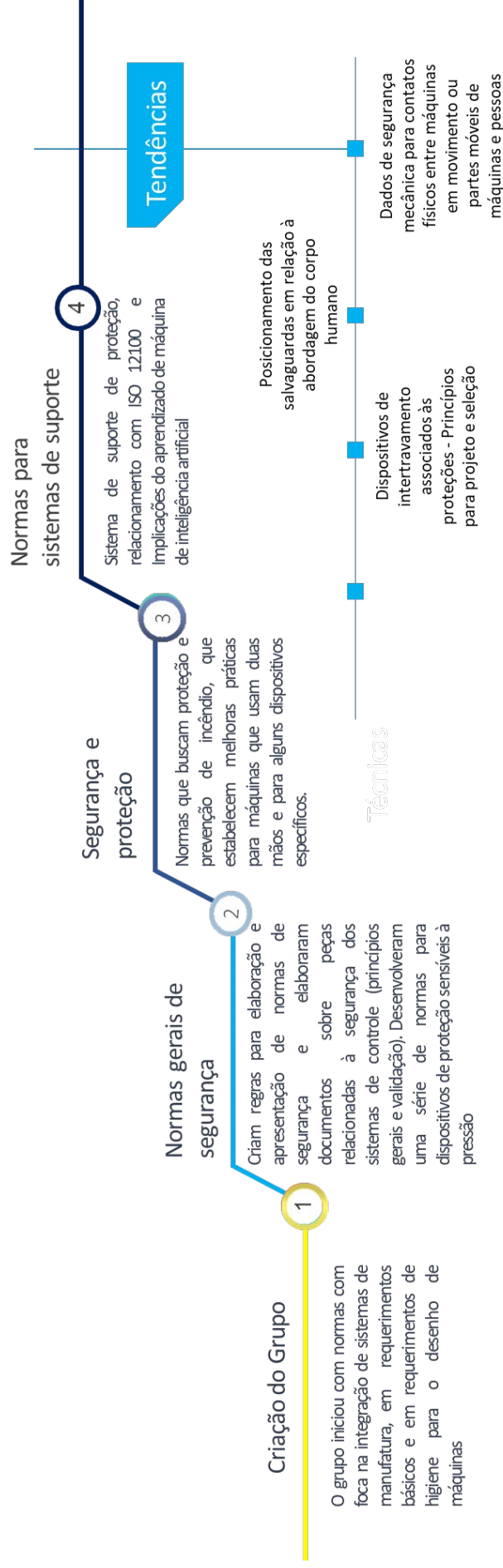


Figura 8 - Consolidação da análise do grupo de Segurança de Máquinas

2.4.5 Relevância

As possibilidades de aplicação de tecnologias da Indústria 4.0 para a segurança do trabalho são as mais diversas (IACO, 2019). Dentre elas, destaca-se o uso de sensores e componentes que estão conectados por meio de Internet das Coisas (IoT) a fim de se realizar o controle automatizado e em tempo real, possibilitando o envio de informações de segurança. Complementarmente, alguns dispositivos podem ser usados para controlar acessos a áreas que são potencialmente perigosas, em que as máquinas não apresentam todos os mecanismos. Além de evitar o acesso a alguns locais perigosos, o uso de robôs pode facilitar o acesso a locais perigosos em vez dos operadores (TECHPLUS, s.d.). Os robôs também podem ser usados para a execução de atividades perigosas ou pesadas para os trabalhadores. As ações e movimentos dos trabalhadores e das máquinas podem ser monitoradas por câmeras de segurança que podem ser usadas em conjuntos com softwares que fazem a coleta e a análise dos dados dos processos com intuito de otimizar a segurança do trabalhador pelo uso de máquinas mais seguras, conforme as normas da ISO. Outro tema importante de ser destacado é a organização dos dados relacionados à saúde do trabalhador, pois eles podem ser usados de entrada no desenvolvimento de novos mecanismos de segurança em máquinas, facilitando, conseqüentemente, o desenho das máquinas e auxiliando na gestão dos riscos.

Para futuras tendências, o foco deve ser a coleta e análise das conseqüências potenciais do uso, as tecnologias que impulsionam a Indústria 4.0 (Big Data, Internet das coisas, sistemas ciberfísicos, rede robótico-colaborativa de computadores, inteligência artificial e simulação) em termos de organização do trabalho, quadro regulamentar e legislativo de saúde e segurança ocupacional (OHS - *Occupational Health and Safety*), sistemas de gestão de OHS e sistemas de gestão de risco ocupacional (BADRI; BOUDREAU-TRUDEL; SOUISSI, 2018).

1 – Organização do trabalho: A Indústria 4.0 aumenta a interação entre o conteúdo do trabalho (variedade, ciclo, habilidades, incertezas, exposição etc.), organização (programação da equipe, horas extras, ordens urgentes etc.), gestão (responsabilidades, comunicação, funções, relações, resolução de problemas etc.) e outros fatores organizacionais (promoção e aumentos salariais, segurança no emprego, valor social do trabalho etc.).

2 – Quadro Legislativo e regulatório: A atual legislação e regulamentação de OHS é, em grande parte, resultado de pesquisas e recomendações de especialistas feitas após acidentes industriais graves.

3 – Sistemas de Gestão de OHS: Estruturas de gerenciamento de OHS foram desenvolvidas para orientar as práticas no setor de negócios (OHSAS 18001, CSA Z1000-06, Z1002-12 etc.). Deve-se notar que a inspiração para tais estruturas veio principalmente do conceito de qualidade total.

4 – Gestão de Riscos Ocupacionais: O gerenciamento de riscos de SSO, incluindo as fases de identificação, análise e avaliação, pode ser visto como uma ferramenta de tomada de decisão usada para melhorar a antecipação de riscos que são conhecidos e provavelmente têm um impacto sobre as metas de negócios e controles já implementados.

A Figura 9 resume o uso de algumas tecnologias da Indústria 4.0 e aspectos centrais de OHS.

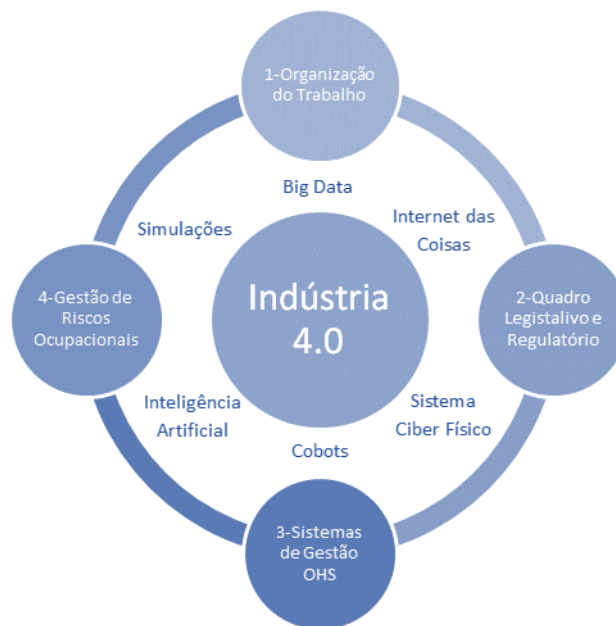


Figura 9 - Categorias tecnológicas da Indústria 4.0 e aspectos de OHS

Klumpp *et al.* (2019) propuseram um modelo para a tomada de decisão colaborativa em interação homem-máquina. Ao desenvolver um sistema que requer interação entre humanos e máquinas autônomas, os desenvolvedores devem decidir por uma das opções para cada caso de uso, com intuito de maximizar a experiência do usuário (KLUMPP *et al.*, 2019), mitigando os riscos relacionados ao uso de robôs. No entanto, muitos profissionais não sabem como usar robôs e outras tecnologias. Portanto, para os próximos anos, será necessário o investimento em treinamentos a fim de que se possa aproveitar o alto rendimento das máquinas em conformidade com os requisitos de segurança. Alguns autores já propuseram um sistema de treinamento de *smart workers*, é baseado também no uso de tecnologias da Indústria 4.0 (*process mining* e realidade virtual). Os resultados mostraram que o sistema proposto é competitivo em relação às alternativas tradicionais já utilizadas pelas empresas (ROLDÁN *et al.*, 2019). Complementarmente, as avaliações dos treinados são melhores em termos de demanda mental, percepção, aprendizagem, resultados e desempenho (ROLDÁN *et al.*, 2019). Como consequência, o uso de tecnologias da Indústria 4.0 pode favorecer os treinamentos de uso de máquinas inteligentes no ambiente industrial, o que potencializa a interação humano-máquina para uma tomada de decisão segura.

No Brasil (SERCON, 2019), os profissionais de saúde e segurança do trabalho da Indústria 4.0 precisam desempenhar funções além das exigências legais requisitadas. Os profissionais necessitam agir como gestores cujo objetivo é o bem-estar e a saúde dos trabalhadores. Portanto, há a necessidade de redefinição de processos, visto que há um crescimento na relação entre o homem e máquina. O uso de tecnologias pode ajudar os profissionais da saúde e segurança do trabalho, pois diversas ferramentas podem ser utilizadas para monitorar os

indicadores e avaliar o cumprimento da legislação trabalhista. O uso de sensores, câmeras inteligentes e softwares pode ser útil para esses profissionais. O governo brasileiro criou o eSocial com intuito de facilitar o envio de informações ao governo por meio de um sistema único, informatizado, que permite a conexão com diversos órgãos de controle e fiscalização. O eSocial faz parte da política de monitoramento de dados, que é fundamental para a Indústria 4.0, e as informações serão essenciais para o desenvolvimento de ações de saúde e segurança da informação nos próximos anos.

O Brasil também possui, desde 1978, uma Comissão Interna de Prevenção de Acidentes (Cipa) responsável pela prevenção de acidentes e doenças decorrentes do trabalho, que é instituída a partir de Normas Regulamentadoras (NR). Desde então, elas vêm sofrendo diversas alterações, visando adequarem-se aos avanços das relações de trabalho. A **NR 05**, que tem como foco a segurança do trabalho, foi revisitada em 2019, quando foi introduzida a possibilidade de treinamentos nas modalidades semipresencial e Ensino a Distância (EaD), possibilitando o uso da tecnologia para treinamentos com profissionais que estejam em outros países. Dessa forma, as NR já iniciaram a inclusão de tecnologias (BRASIL, 2021b).

Entre as normas em destaque, a **NR 17** tem como objeto de estudo a segurança no tocante a questões de ergonomia. Cerca de 172.000 acidentes e adoecimentos relacionados aos temas abordados na norma foram registrados no Brasil entre janeiro de 2016 e dezembro de 2020, sendo 27 fatais (BRASIL, 2021c). É importante salientar que a NR 17 já regula o contexto industrial e, com avanço do uso de tecnologias, torna-se muito pertinente. Como o uso de tecnologias exige que os trabalhadores sejam mais treinados e qualificados no ambiente de trabalho, isso pode ser um fator que pode interferir positivamente no número de acidentes (INDUSTRIAL 4.0., 2019). De forma geral, uma fábrica inteligente deve ser segura para seus trabalhadores. Assim como as NR 05 e NR17, outras NR podem ser beneficiadas pela utilização de tecnologias associadas à Indústria 4.0. Nesse sentido, a Tabela 9 apresenta cada uma das normas regulamentadoras e seus objetivos para o entendimento de como é possível aplicar na Indústria 4.0.

Tabela 9 - Normas Regulamentadoras, de Segurança de Máquinas objetivos e exemplos de aplicações na Indústria 4.0

Norma Regulamentadora	Principal assunto abordado	Objetivo Principal	Objetivos Específicos
Número 05	Comissão Interna de Prevenção de Acidentes.	Fortalecer a atuação da Comissão Interna de Prevenção de Acidentes na prevenção de acidentes e doenças relacionadas ao trabalho, aumentando a segurança jurídica na aplicação da norma.	Acompanhar a evolução tecnológica e as mudanças no contexto das relações de trabalho; buscar a simplificação e desburocratização da norma. Indústria 4.0: desenvolvimento de treinamentos a distância.
Número 17	Ergonomia	Adaptar as condições de trabalho às características psicofisiológicas dos trabalhadores.	Definir uma etapa de avaliação ergonômica preliminar, visando dar maior efetividade à implementação de medidas; priorizar um ciclo contínuo de identificação, avaliação e prevenção de riscos no ambiente de trabalho; Buscar a simplificação e desburocratização da norma. Indústria 4.0: desenvolvimento de treinamentos a distância.

Número 19	Explosivos	Reduzir a exposição de trabalhadores, sem a devida proteção, aos perigos decorrentes do trabalho com explosivos.	Reduzir as ocorrências de acidentes e doenças ocupacionais relativos ao setor de explosivos; harmonizar a NR 19 com as demais normas regulamentadoras; atualizar e ajustar a redação da NR 19. Indústria 4.0: fábricas não tripuladas.
Número 30	Segurança e Saúde no Trabalho Aquaviário	Implementar um sistema de gestão abrangente dos riscos ocupacionais no trabalho aquaviário.	Reduzir o número de acidentes; ajustar campo de aplicação e objetivo da norma; estender o campo de aplicação da norma para todos os trabalhadores do setor; ajustar comandos normativos em face da detecção de problemas. Indústria 4.0: Shipbuilding 4.0 com foco em segurança.
Número 37	Segurança e Saúde em Plataformas de Petróleo	Estabelecer uma gestão eficiente e eficaz da segurança e saúde no trabalho a bordo de plataformas de petróleo.	Harmonizar o texto da NR 37 com as novas disposições de gerenciamento de riscos ocupacionais e com as demais normas de SST; criar um capítulo com o Programa de Gerenciamento de Riscos Ocupacionais; reorganizar a estrutura da norma, conferindo-lhe leitura e compreensão mais objetivas, tornando mais fácil sua aplicação. Indústria 4.0: Frameworks de IIoT para segurança confiável em empresas de óleo e gás.

Por fim, foi feito um esquema conceitual dos principais aspectos do Grupo de segurança de máquinas na Figura 10, englobando as aplicações e a importância em nível global.



Figura 10 - Infográfico da Relevância para o Grupo de Segurança de Máquinas

2.5 Grupo de segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27)

2.5.1 Escopo

O objetivo do grupo **ISO/IEC/JTC1/SC27** é o desenvolvimento de normas para a proteção da informação e das tecnologias da informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar questões de segurança e privacidade.

Assim, alguns dos principais conceitos relacionados a tal grupo de normas são:

- **Segurança da informação:** preservação da confidencialidade, integridade e disponibilidade das informações. Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade também podem estar envolvidas.
- **Continuidade da segurança da informação:** processos e procedimentos para garantir a continuidade das operações de segurança da informação.
- **Autenticidade:** propriedade de que uma entidade é o que afirma ser.
- **Não repúdio:** capacidade de comprovar a ocorrência de um evento ou ação reivindicada e suas entidades originais.
- **Confiabilidade:** propriedade de comportamento e resultados pretendidos consistentes.
- **Confidencialidade:** propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.
- **Integridade:** propriedade de precisão e integridade.
- **Disponibilidade:** propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

Conforme o artigo da IEC sobre a *Factory of the Future* (IEC, 2019), a proteção da segurança cibernética segue o caminho da confidencialidade, integridade e disponibilidade (C-I-D), que ainda se aplica a redes de sistemas de informação. No entanto, a fábrica dos sistemas do futuro que integram o espaço físico e o espaço cibernético exige uma prioridade de proteção diferente, que segue o caminho da disponibilidade, integridade e confidencialidade (D-I-C).

2.5.2 Status quo

As normas iniciais do grupo (ISO/IEC/JTC1/SC27) focaram em técnicas de segurança. A **ISO/IEC TR 14516:2002** fornece orientação para o uso e gestão de um Terceiro de Confiança (Trusted Third Party – TTPs), promovendo, assim, uma definição clara das funções básicas e serviços prestados, sua descrição e sua finalidade, e as funções e responsabilidades dos TTP e entidades que utilizam seus serviços. Já a norma **ISO/IEC 7064:2002** abrange um conjunto de sistemas de verificação de caracteres capaz de proteger strings contra erros. As *strings* podem

ser de comprimento fixo ou variável e podem ter conjuntos de caracteres que são: numérico (10 dígitos: 0 a 9); alfabético (26 letras: A a Z); e alfanumérico (letras e dígitos).

É importante salientar que as **normas sobre assinaturas digitais** podem ser divididas em duas linhas, porém existem diversas normas interessantes sobre o tema. O primeiro grupo refere-se a esquemas de assinatura digital para recuperação de mensagens. Por exemplo, a **ISO/IEC 9796-3:2006** é uma norma crucial nesse contexto, visto que uma assinatura digital na troca eletrônica de informações fornece o mesmo tipo de facilidades que são esperadas de uma assinatura manuscrita em correio em papel. Portanto, é aplicável para fornecer autenticação de entidade, autenticação de origem de dados, não repúdio e integridade de dados. Consequentemente, a ISO/IEC 9796-3:2006 especifica mecanismos de assinatura digital dando recuperação parcial ou total da mensagem com o objetivo de reduzir o armazenamento e a sobrecarga de transmissão. Em relação a discussões mais técnicas, a norma ISO/IEC 9796-3:2006 especifica seis esquemas de assinatura digital que fornecem recuperação de dados.

Tanto as normas sobre assinatura digital para recuperação de mensagens quanto as de assinatura digital com apêndice foram sendo desenvolvidas em partes, ao longo dos anos. As normas ISO/IEC 14888-1:2008, ISO/IEC 14888-2:2008 e ISO/IEC 14888-3:2018 abrangem o uso de assinatura digital com apêndice. A norma **ISO/IEC 14888-1: 2008** aborda os princípios gerais e requisitos para assinaturas digitais com apêndice. Já a norma **ISO/IEC 14888-2** endereça assinaturas digitais com base em fatoração inteira, e **ISO/IEC 14888-3** endereça assinaturas digitais com base em logaritmo discreto.

A norma **ISO/IEC 9798-1:2010** abrange um modelo de autenticação e requisitos gerais e restrições para mecanismos de autenticação de entidade que usam técnicas de segurança. Esses mecanismos são usados para corroborar que entidade é reivindicada. Uma entidade a ser autenticada prova sua identidade mostrando seu conhecimento de um segredo. Os mecanismos são definidos como trocas de informações entre entidades e, quando necessário, trocas com terceiros de confiança. A ISO/IEC 9798 é dividida em seis partes. Destaca-se a **parte 2**, que aborda os mecanismos de autenticação de entidade usando algoritmos de criptografia autenticados. Quatro dos mecanismos fornecem autenticação de entidade entre duas, onde nenhum terceiro confiável está envolvido; dois deles são mecanismos para autenticar unilateralmente uma entidade para outra, enquanto os outros dois são mecanismos para autenticação mútua de duas entidades. Já a **parte 3** abrange mecanismos de autenticação de entidade usando assinaturas digitais baseadas em técnicas assimétricas. Uma assinatura digital é usada para verificar a identidade de uma entidade. Dez mecanismos são especificados neste documento. Os primeiros cinco não envolvem terceiros confiáveis on-line, e os cinco últimos utilizam terceiros confiáveis. Resumidamente, a **parte 4** engloba os mecanismos que usam uma função de verificação criptográfica, abordando a codificação da informação. ISO/IEC 9798-5: 2009 (**parte 5**) especifica mecanismos de autenticação de entidade usando técnicas de conhecimento zero. Já, a **parte 6** (ISO/IEC 9798-6: 2010) aborda oito mecanismos de autenticação de entidade com base na transferência manual de dados entre dispositivos de autenticação. Quatro desses mecanismos são versões otimizadas dos mecanismos especificados na ISO/IEC 9798-6: 2005, uma vez que proporcionam mais segurança. Eles podem ser apropriados em uma variedade de circunstâncias em que não há necessidade de uma infraestrutura de chave pública existente, chaves secretas compartilhadas ou senhas. Uma das aplicações ocorre em redes pessoais, nas quais o proprietário de dois dispositivos pessoais capazes de comunicação sem fio deseja que eles realizem um procedimento de

autenticação de entidade como parte do processo de prepará-los para uso na rede. As partes 2 e 3 foram atualizadas em 2019.

A **ISO 11770** abrange técnicas de segurança, principalmente em relação à gerenciamento de chaves. A **parte 1 (ISO/IEC 11770-1: 2010)** define um modelo geral de gerenciamento de chaves independente do uso de qualquer algoritmo criptográfico específico. É importante destacar que ISO/IEC 11770-1: 2010 contém o material necessário para um entendimento básico das partes subsequentes. Entretanto, exemplos do uso de mecanismos de gerenciamento de chaves estão incluídos na ISO 11568. São normas utilizadas de forma complementar. Geralmente a ISO/IEC 11770-1: 2010 aborda automatizados e manuais do gerenciamento de chaves, inclusive sequências de operações que são usadas para obter serviços de gerenciamento de chaves. Complementando as outras normas e a primeira parte, a **parte 2 (ISO/IEC 11770-2:2018)** define mecanismos de estabelecimento de chaves usando técnicas criptográficas simétricas. O documento apresenta três ambientes para o estabelecimento de chaves: Ponto a Ponto, Centro de Distribuição de Chaves (KDC) e o Centro de Tradução de Chaves (KTC). Já a **parte 3 (ISO/IEC 11770-3: 2015)** abrange mecanismos de gerenciamento de chave com base em técnicas criptográficas assimétricas. Ele aborda especificamente o uso de técnicas assimétricas para atingir os seguintes objetivos: (i) estabelecer uma chave secreta compartilhada para uso em uma técnica criptográfica simétrica entre duas entidades A e B por acordo de chave; (ii) estabelecer uma chave secreta compartilhada para uso em uma técnica criptográfica simétrica entre duas entidades A e B por meio de transporte de chave. É essencial destacar que alguns dos mecanismos da ISO/IEC 11770-3: 2015 são baseados nos mecanismos de autenticação correspondentes na ISO/IEC 9798-3.

A **parte 4 (ISO/IEC 11770-4: 2017)** aborda os principais mecanismos de estabelecimento com base em segredos que podem ser prontamente memorizados por um humano (conhecidos como segredos fracos) e que serão escolhidos a partir de um conjunto relativamente pequeno de possibilidades. Além disso, a **parte 5 da norma (ISO/IEC 11770-5:2011)** especifica mecanismos para estabelecer chaves simétricas compartilhadas entre grupos de entidades. Ele define: (i) mecanismos de estabelecimento de chave simétricos baseados em chave para várias entidades com um centro de distribuição de chaves (KDC); e (ii) mecanismos de estabelecimento de chave simétrica baseados em uma estrutura de chave lógica, baseada em árvore geral com recodificação individual e rechaveamento em lote. A **parte 6 (ISO/IEC 11770-6: 2016)** especifica funções de derivação de chave, ou seja, funções se utilizam de informações secretas e outros parâmetros (públicos) como entrada e saída de uma ou mais chaves secretas "derivadas".

A Tabela 10 apresenta a sumarização das outras normas relevantes do grupo Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27). Pode se observar que um número grande de normas relevantes foi publicado em 2020 e 2021, as quais são descritas mais detalhadamente na tabela.

Tabela 10 - Normas do grupo de Segurança da informação, cibersegurança e proteção da privacidade

Norma	Escopo
ISO/IEC TR 14516:2002	Orientação para o uso e gestão de um Terceiro de Confiança.
ISO/IEC 7064:2002	Sistemas de verificação de caracteres capazes de proteger <i>strings</i> .
ISO/IEC 9796-3:2006	Esquemas de assinatura digital para recuperação de mensagens.
ISO/IEC 14888-1:2008, ISO/IEC 14888-2:2008 e ISO/IEC 14888-3:2018	Uso de assinatura digital com apêndice.
ISO/IEC 9798-1:2010 ISO/IEC 9798-2:2019 ISO/IEC 9798-3:2019 ISO/IEC 9798-4:1999 ISO/IEC 9798-5:2009 ISO/IEC 9798-6:2010	Modelo de autenticação com requisitos gerais e mecanismos de autenticação com atualizações.
ISO 11770 ISO/IEC 11770-1:2010 ISO/IEC 11770-2:2018 ISO/IEC 11770-3:2015 ISO/IEC 11770-4:2017 ISO/IEC 11770-5:2011 ISO/IEC 11770-6:2016	Técnicas de segurança e gerenciamento de chaves.
ISO/IEC 13888 ISO/IEC 13888-1:2020 ISO/IEC 13888-2:2010 ISO/IEC 13888-3:2020	<p>A série ISS/IEC 13888 fornece mecanismos de não repúdio para as seguintes fases: geração de evidências; transferência, armazenamento e recuperação de evidências; e verificação de evidências.</p> <p>ISO/IEC 13888-1: 2020 apresenta um modelo geral para as partes subsequentes, especificando mecanismos de não repúdio por meio do uso de técnicas criptográficas.</p> <p>A ISO/IEC 13888-3: 2020 fornece mecanismos para serviços específicos de não repúdio, relacionados à comunicação, usando técnicas criptográficas assimétricas.</p>

ISO/IEC 18032:2020	<p>Teste de números primos.</p> <p>Aborda métodos para gerar e testar números primos, conforme exigido em protocolos e algoritmos criptográficos.</p>
ISO/IEC 19772:2020	<p>Métodos de criptografia autenticada.</p> <p>Abrange cinco métodos para criptografia autenticada com base em: (i) confidencialidade de dados, que permite proteção contra divulgação não autorizada de dados; (ii) integridade dos dados, que permite ao destinatário dos dados verificar se eles não foram modificados; (iii) autenticação da origem dos dados, que permite ao destinatário dos dados verificar a identidade do originador dos dados.</p>
ISO/IEC 19989-1:2020	<p>Avaliação de segurança de sistemas biométricos.</p> <p>Apresenta uma estrutura geral para a avaliação de segurança de sistemas biométricos, incluindo componentes funcionais de segurança estendidos e atividades de avaliação adicionais e orientações/recomendações para um avaliador lidar com essas atividades.</p>
ISO/IEC 19989-2:2020	<p>Avaliação de segurança de sistemas biométricos.</p> <p>Dedicada à avaliação de segurança de desempenho de reconhecimento biométrico aplicada à série ISO/IEC 15408. Fornece requisitos e recomendações para o desenvolvedor e o avaliador para as atividades suplementares sobre desempenho de reconhecimento biométrico especificado na ISO/IEC 19989-1.</p>
ISO/IEC 19989-3:2020	<p>Avaliação de segurança de sistemas biométricos.</p> <p>Dedicada à avaliação de segurança de detecção de ataque de apresentação aplica à série ISO/IEC 15408. Fornece recomendações e requisitos para o desenvolvedor e o avaliador para as atividades suplementares na detecção de ataques de apresentação especificadas na ISO/IEC 19989-1.</p>
ISO/IEC 20547-4:2020	<p>Especifica tópicos de segurança e privacidade aplicáveis à arquitetura de referência de <i>big data</i> (BDRA), incluindo as funções de <i>big data</i>, atividades e componentes funcionais, e também fornece orientação sobre operações de segurança e privacidade para <i>big data</i>.</p>
ISO/IEC 27007:2020	<p>Orienta sobre o gerenciamento de auditoria de sistema de gestão e segurança da informação (SGSI), sobre a realização de auditorias e sobre a competência dos auditores de SGSI, além da orientação contida na ISO 19011.</p>
ISO/IEC 27014:2020	<p>Fornece orientação sobre conceitos, objetivos e processos para a governança da segurança da informação, por meio dos quais as organizações podem avaliar, dirigir, monitorar e comunicar os processos relacionados à segurança da informação na organização.</p>

ISO/IEC 27035-3:2020	Fornecer diretrizes para resposta a incidentes de segurança da informação em operações de segurança de TIC. Em primeiro lugar, o documento aborda diretrizes operacionais das operações de segurança de TIC de uma perspectiva de pessoas, processos e tecnologia. Em seguida, concentra-se na resposta a incidentes de segurança de informações em operações de segurança de TIC, incluindo detecção de incidentes de informações, relatórios, triagem, análise, resposta, contenção, erradicação, recuperação e conclusão.
ISO/IEC TS 27100:2020	Descreve a segurança cibernética e os conceitos relevantes, incluindo como ela é relacionada e diferente da segurança da informação.
ISO/IEC 29184:2020	Privacidade on-line. Especifica os controles que moldam o conteúdo e a estrutura dos avisos de privacidade on-line, bem como o processo de solicitação de consentimento para coletar e processar informações de identificação pessoal (PII) de diretores de PII.
ISO/IEC 23264-1:2021	Abrange as propriedades dos mecanismos criptográficos para dados autênticos. Em particular, define os processos envolvidos nesses mecanismos, as partes participantes e as propriedades criptográficas.
ISO/IEC TS 27006-2:2021	Oferece orientação para organismos que fornecem auditoria e certificação de um sistema de gerenciamento de informações de privacidade (PIMS), de acordo com a ISO/IEC 27701 em combinação com a ISO/IEC 27001, além dos requisitos contidos na ISO/IEC 27006 e ISO/IEC 27701. O objetivo principal é apoiar o credenciamento de organismos que fornecem a certificação PIMS.
ISO/IEC TS 27110:2021	Aborda diretrizes para o desenvolvimento de uma estrutura de segurança cibernética. É aplicável aos criadores de estruturas de segurança cibernética, independentemente do tipo, tamanho ou natureza de suas organizações.

2.5.3 Mapa mental de relação com outros grupos

Para ilustrar as relações entre o grupo Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27) e outros grupos e tecnologias existentes, apresenta-se um mapa mental na Figura 11. Aqueles que possuem relação com o grupo em destaque aparecem na cor azul escuro, à direita, e estão listados abaixo:

- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial (IA) é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA.
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas,

incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO/IEC e em cooperação com outros comitês técnicos da ISO e IEC.

- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo a definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. Tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, seu intuito é de fornecer orientação a entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais – Segurança de rede e sistema.
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.
- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares.

Já os outros grupos existentes que também possuem alguma relação com o grupo em destaque estão à esquerda, em amarelo. São eles:

- **Gerenciamento de sistemas de energia e troca de informações:** Para preparar padrões internacionais para equipamentos de controle de sistemas de energia e sistemas, incluindo EMS (Sistemas de Gerenciamento de Energia), Scada (Controle de Supervisão e Aquisição de Dados), automação de distribuição, teleproteção e troca de informações associadas para informações em tempo real ou não, usado no planejamento, operação e manutenção de sistemas de energia.
- **Gerenciamento de riscos:** Padronização na área de gestão de risco.
- **Blockchain and distributed ledger Technologies:** Padronização de tecnologias de *blockchain* e tecnologias de razão distribuída.
- **Smart Manufacturing:** Para fornecer coordenação e aconselhamento no domínio da Manufatura Inteligente a fim de harmonizar e avançar as atividades de Manufatura Inteligente na IEC e outros SDO.

- **Medição, controle e automação de processos industriais:** Preparar padrões internacionais para sistemas e elementos usados para medição, controle e automação de processos industriais, a fim de coordenar as atividades de padronização que afetam a integração de componentes e funções em tais sistemas, incluindo proteção e segurança.
- **Engenharia de software e sistemas:** Padronização de processos, ferramentas de suporte e tecnologias de suporte à engenharia de produtos e sistemas de software.
- **Tecnologia da informação:** Ambiente de desenvolvimento de padrões, onde especialistas se reúnem para desenvolver padrões mundiais de Tecnologia da Informação e Comunicação (TIC) para aplicações de negócios e de consumo.
- **Gerenciamento e intercâmbio de dados:** Padrões para gerenciamento de dados dentro e entre ambientes de sistemas de informação locais e distribuídos. Fornece tecnologias capacitadoras para promover a harmonização dos recursos de gerenciamento de dados em áreas específicas do setor.
- **Segurança da medição, controle e equipamentos do laboratório:** Preparar padrões de segurança para equipamentos de teste e medição, equipamentos de controle de processos industriais e equipamentos de laboratório onde quer que sejam usados.

Em vermelho, acima e abaixo dos outros tópicos, estão os fatores conectados à transformação digital na Indústria, que também se conectam com Segurança da informação, cibersegurança e proteção de privacidade.

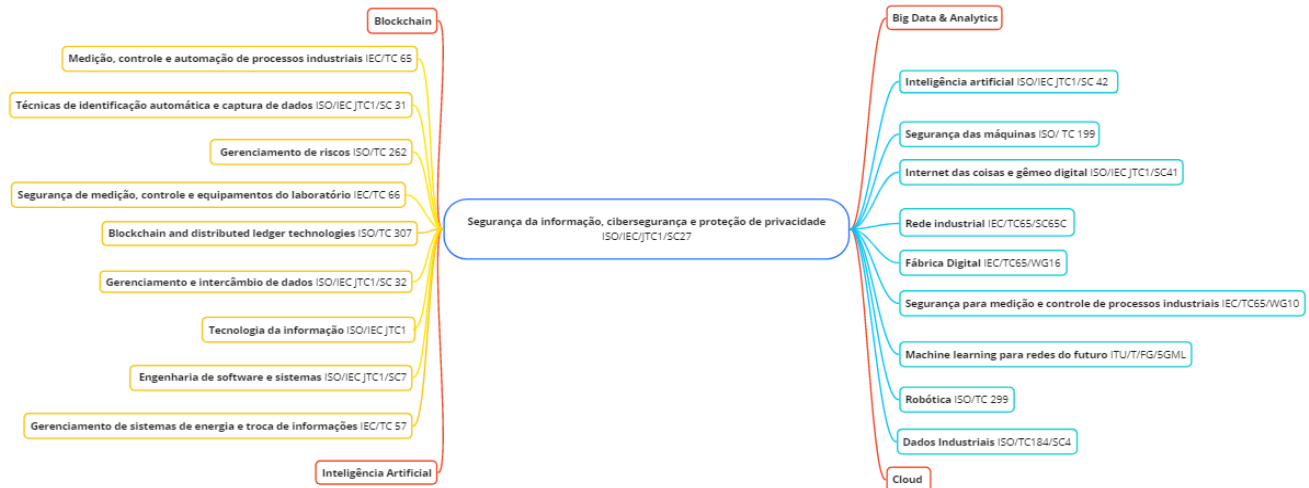


Figura 11 - Mapa mental de relação do grupo de Segurança da informação, cibersegurança e proteção de privacidade com outros grupos

2.5.4 Tendências

2.5.4.1 Segurança da informação, cibersegurança e proteção da privacidade - Critérios de avaliação para segurança de TI (ISO/IEC DIS 15408)

A norma **ISO/IEC DIS 15408-1** (cuja primeira versão foi publicada em 2009, em desenvolvimento no estágio 40,99)¹⁹ estabelece os conceitos e princípios gerais da avaliação da segurança de TI e especifica o modelo geral de avaliação dado por várias partes da norma ISO/IEC 15408 que, em sua totalidade, deve ser usado como base para a avaliação das propriedades de segurança do TOE (*Target of Evaluation*), o contexto da avaliação; e descreve o público ao qual os critérios de avaliação são dirigidos. É fornecida uma introdução aos conceitos básicos de segurança necessários para a avaliação de produtos de TI. A norma ISO/IEC 15408-1: 2009 fornece diretrizes para a especificação de alvos de segurança (ST) e uma descrição da organização dos componentes em todo o modelo. A norma define as várias operações pelas quais os componentes funcionais e de garantia fornecidos na ISO/IEC 15408-2 e ISO/IEC 15408-3 podem ser ajustados por meio do uso de operações permitidas. Já a **ISO/IEC DIS 15408-4** descreve uma estrutura que pode ser usada para derivar as atividades de avaliação de unidades de trabalho da ISO/IEC 18045 e agrupá-las em métodos de avaliação, concatenando em um framework para a especificação de métodos de avaliação e atividades. A norma **ISO/IEC DIS 15408-5** fornece pacotes de garantia de segurança e requisitos funcionais de segurança que foram identificados como úteis para apoiar o uso comum pelas partes interessadas.

2.5.4.2 Cibersegurança - segurança e privacidade de IoT (ISO/IEC DIS 27400)

Com o aumento do número de dispositivos IoT no mundo, os riscos de segurança cibernética e privacidade aumentarão. O baixo custo dos dispositivos e a facilidade de implantação em redes e ecossistemas os tornam alvos fáceis e principais de ataques cibernéticos, especialmente considerando a complexidade e heterogeneidade do ecossistema IoT. Dessa forma, a ISO/IEC DIS 27400²⁰ fornece diretrizes sobre riscos, princípios e controles para segurança e privacidade de soluções de Internet das Coisas (IoT). Além disso, a norma traz algumas definições importantes:

- **Computação em nuvem:** paradigma para permitir o acesso à rede escalável de compartilháveis físicos ou virtuais, além de recursos com provisionamento de autoatendimento e administração sob demanda. Alguns exemplos de recursos incluem servidores, sistemas operacionais, redes, software, aplicativos e equipamento de armazenamento.
- **Dispositivo IoT:** entidade de um sistema IoT que interage e se comunica com o mundo físico por meio de detecção ou atuante.

¹⁹ Status e atualizações da norma podem ser encontrados em: <https://www.iso.org/standard/72891.html>

²⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/44373.html>

- **Plataforma IoT:** infraestrutura que permite a implantação, gerenciamento e operação de dispositivos IoT.
- **Sistema IoT:** sistema que fornece funcionalidades de Internet das Coisas; o sistema IoT inclui dispositivos IoT, gateways IoT, sensores e atuadores.
- **Solução IoT:** um pacote perfeitamente integrado de tecnologias incluindo sensores, gateways e atuadores que podem resolver um problema ou necessidade específica ou podem ser usados para criar funcionalidade adicional em outras soluções IoT.
- **Usuário de IoT:** O usuário IoT é o beneficiário final de um serviço e pode ser categorizado como usuário humano ou usuário digital. Humano é um indivíduo que usa o serviço IoT. Já o digital é um usuário não humano do serviço IoT; pode ser um serviço automatizado agindo em nome de um usuário humano.

O nível de segurança e privacidade exigido para ser fornecido em um sistema ou serviço de IoT é impulsionado principalmente por expectativas ou considerações de risco feitas por usuários de IoT. No entanto, estes podem frequentemente não estar cientes das implicações de segurança das tecnologias. Para qualquer caso de uso, um entendimento profundo dos usuários de IoT e de suas necessidades e requisitos é crucial. Portanto, é imprescindível que os controles de segurança e privacidade sigam um padrão e sejam desenvolvidos para as partes interessadas em um sistema IoT, a fim de ser utilizado por cada parte interessada ao longo do ciclo de vida do sistema.

A **ISO/IEC CD 27402.2** (que está no estágio 30,20)²¹ fornece requisitos básicos para dispositivos IoT e seus fabricantes, a fim de oferecer suporte à segurança das informações e controles de privacidade, especificando um conjunto básico de requisitos de segurança e privacidade (a "Linha de Base") de que um dispositivo IoT precisa ser capaz para que os usuários façam tal determinação. Em muitos casos, os usuários precisarão complementar os requisitos com outros adicionais, apropriados aos riscos de segurança e privacidade de segmentos ou grupos de mercado vertical específicos ou para lidar com ambientes de alto risco. Por exemplo, o fabricante do dispositivo IoT deve realizar uma avaliação de risco para cada modelo, levando em consideração os resultados pretendidos e as necessidades e expectativas das partes interessadas (incluindo efeitos indesejáveis). Logo, o fabricante do dispositivo IoT deve documentar a avaliação de risco.

É importante ressaltar que a **ISO/IEC DIS 27400** traz o ciclo de vida do IoT com intuito de que as empresas entendam como funciona a fim de promover a segurança. Portanto, é imprescindível entender que um serviço IoT apresenta vários ciclos de vida, que podem ser mapeados para as partes interessadas de um sistema IoT. Mais especificamente, um serviço IoT é:

- a) desenvolvido por um desenvolvedor de serviço IoT e desenvolvedor(es) de dispositivo IoT;
- b) fornecido por um provedor de serviços IoT; e
- c) usado por usuários de IoT.

²¹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/80136.html>

Os processos das partes interessadas formam um conjunto de ciclos de vida interdependentes de desenvolvimento de dispositivo, desenvolvimento, prestação de serviço e utilização do serviço. Assim, a Figura 12 mostra esses ciclos de vida e as relações entre eles, identificando os pontos que precisam de atenção.

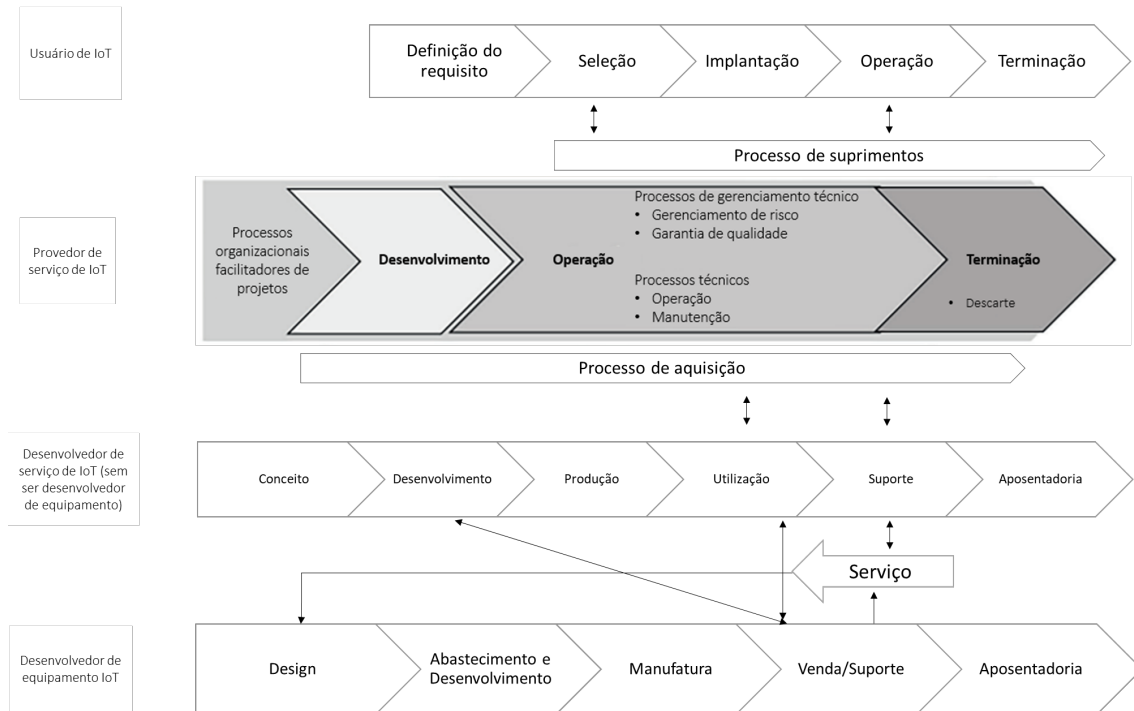


Figura 12 - Ciclo de vida de um serviço IoT para compreensão de pontos de risco

2.5.4.3 Requisitos de competência para profissionais de sistemas de gestão de segurança da informação (ISO/IEC DTS 23532-1.2)

A **ISO/IEC DTS 23532-1.2** (que está na fase 30,99)²² especifica os requisitos de competência para líderes ou 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. Este documento deve ser usado por:

- indivíduos que gostariam de demonstrar sua competência em gestão de segurança da informação profissionais de sistemas (SGSI), ou que queiram compreender e realizar as competências necessárias para trabalhar nesta área, bem como queiram ampliar seus conhecimentos.
- organizações que buscam potenciais candidatos profissionais de SGSI para definir a competência necessária para cargos em funções relacionadas com sistemas de gestão de segurança.

²² Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77199.html>

c) organismos para desenvolver certificação para profissionais que precisam de um corpo de conhecimento (BOK) para fontes de exame.

d) organizações de educação e treinamento, como universidades e instituições vocacionais, cuja finalidade é alinhar seus programas e cursos aos requisitos de competência para profissionais de SGSI.

2.5.4.4 Tecnologia da informação - Segurança e privacidade de *Big Data* - Diretrizes de implementação (ISO/IEC WD 27046)

O objetivo da proposta da **ISO/IEC WD 27046**²³ (que está na fase 20,60) é analisar os desafios e riscos com a implementação de *Big Data* sobre a fatores de segurança e privacidade dos serviços. A proposta abrange desde o ciclo de vida dos dados até ciclos de vida do sistema, fornecendo algumas diretrizes para implementação de segurança e privacidade de *Big Data*, incluindo os seguintes elementos:

1. Como avaliar a segurança e privacidade de *Big Data*;
2. Como implantar medidas de segurança e privacidade de *Big Data*;
3. Como manter a segurança e privacidade de *Big Data*;
4. Como validar e verificar a segurança e privacidade de *Big Data*.

A proposta pode ajudar as partes interessadas a obter segurança e privacidade de *big data* para software e hardware na construção de estrutura de *big data* com segurança, a fim de que provedores e consumidores de dados realizem funções de *big data* com segurança. Complementarmente, a proposta pode ajudar a indústria a melhorar a robustez e eficiência no nível do ecossistema com vistas a melhorar a compatibilidade e interoperação e diversificar as opções de produtos de segurança e privacidade, reduzindo custos.

Assim, as principais normas de tendências do grupo Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27) estão consolidadas na Tabela 11.

Tabela 11 - Normas referentes a tendências do grupo de Segurança da informação

Norma	Escopo
ISO/IEC DIS 15408-1 ISO/IEC 15408-2 ISO/IEC 15408-3 ISO/IEC DIS 15408-4	Avaliação das propriedades de segurança
ISO/IEC DIS 27400	Diretrizes sobre riscos, princípios e controles para segurança e privacidade

²³ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78572.html>

	de soluções de Internet das Coisas.
ISO/IEC 27402	Requisitos básicos de dispositivos IoT e seus fabricantes para oferecer suporte à segurança das informações e controles de privacidade.
ISO/IEC DTS 23532-1.2 ISO/IEC DTS 23532-2.2	Requisitos de competência para líderes ou envolvidos na gestão de segurança da informação.
ISO/IEC NP 27046	Desafios e riscos com a implementação de <i>Big Data</i> em relação a aspectos de segurança e privacidade dos serviços.

Por fim, a Figura 13 resume o escopo, linha do tempo e tendência do grupo Segurança da informação, cibersegurança e proteção da privacidade (ISO/IEC/JTC1/SC27).

Segurança da informação

ISO/IEC/JTC1/SC27

Escopo

O desenvolvimento de normas para a proteção da informação e das TIC; inclui métodos genéricos, técnicas e diretrizes para abordar os aspectos de segurança e privacidade



Figura 13 - Consolidação da análise do grupo de Segurança da Informação

2.5.5 Relevância

No contexto da Indústria 4.0, a cibersegurança possibilita diversos benefícios, entre eles: proteção contra perda de dados; proteção de roubo de senhas e identidade; proteção de sequestro de dados; proteção quanto à manipulação de dados, entre outros (UPPERTOOLS, 2020). Assim, é importante explorar algumas vertentes preventivas sobre a cibersegurança na Indústria 4.0 (Figura 14) (REGIS *et al.*, 2019).

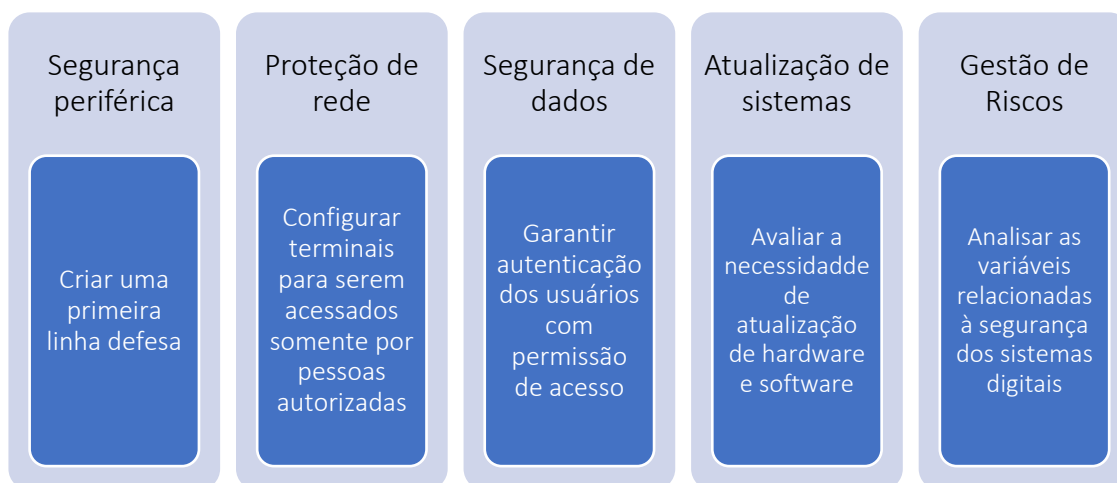


Figura 14 - Aspectos preventivos da cibersegurança na Indústria 4.0

No entanto, existem outras perspectivas que são essenciais na cibersegurança da Indústria 4.0. A Deloitte aborda diversos estágios do ciclo de vida de produção inteligente e quais são as ações de segurança da informação que buscam antecipar e tratar os riscos cibernéticos como bem para integrar proativamente a segurança cibernética na Indústria 4.0. A Tabela 12 explora o ciclo de vida da produção inteligente, seus riscos e objetivos.

Tabela 12 - Ciclo de vida de produção inteligente e risco cibernético (DELOITTE., 2020)

Estágio do ciclo de vida de produção inteligente	Categorização segura, vigilante e resiliente	Ciber-imperativo	Objetivo
Digital supply network	Segura, vigilante e resiliente	Compartilhamento de dados	Garantir a integridade dos sistemas para que dados privados e proprietários não possam ser acessados
	Segura, vigilante e resiliente	Processamento de fornecedor	Manter a confiança quando os processos não puderem ser validados
Smart factory	Vigilante	Saúde e segurança	Garantir a segurança dos funcionários e do meio ambiente
	Vigilante e resiliente	Resiliência/eficiência de produção e processo	Garantir a produção contínua e recuperação de sistemas críticos
	Vigilante e resiliente	Instrumentação e resolução proativa de problemas	Proteger a marca e a reputação da organização
	Segura e resiliente	Operabilidade, confiabilidade e integridade dos sistemas	Apoiar o uso de vários fornecedores e versões de software
	Vigilante e resiliente	Eficiência e redução de custos	Reduzir os custos operacionais e aumentar a flexibilidade com diagnósticos e engenharia de local remoto
	Segura	Regulatório e devida diligência	Garantir a confiabilidade do processo
Connected object	Segura	Design de produto	Empregar ciclo de vida de desenvolvimento de software seguro para produzir um dispositivo funcional e seguro
	Vigilante	Proteção de dados	Manter a segurança dos dados confidenciais ao longo do ciclo de vida dos dados
	Resiliente	Correção de efeitos de ataque	Minimizar os efeitos de um incidente enquanto se restaura rapidamente as operações e a segurança

Além disso, existem outras tecnologias da Indústria 4.0 que podem apoiar a cibersegurança. Os líderes de segurança devem continuar a tratar a IA como tecnologia emergente, adicionando-a como controle experimental e complementar (GARTNER, 2020). A Figura 15 concatena alguns dos principais elementos de IA em todo o programa de segurança crítico (GARTNER, 2020).

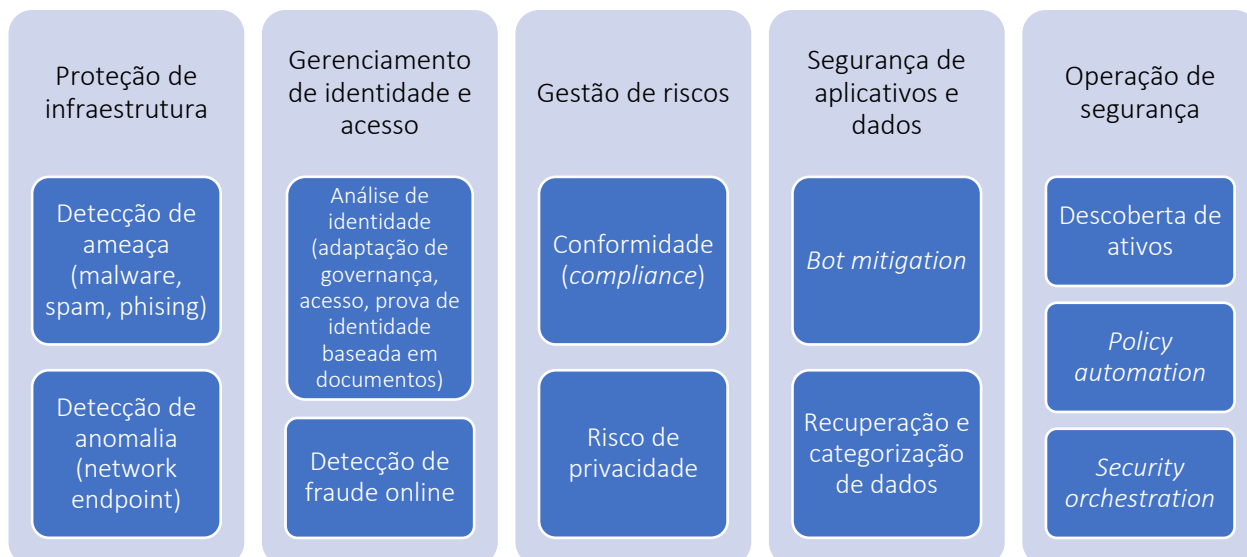


Figura 15 - Principais aspectos de IA em todo o programa de segurança crítico

Embora seja uma tendência positiva, a Indústria 4.0 e a digitalização mais ampla também apresentam novos riscos, devido ao crescimento das ameaças cibernéticas. Entretanto, apenas 13% das empresas percebem totalmente o impacto de seus investimentos digitais. Naturalmente, os hackers veem uma oportunidade na conectividade sem precedentes e, em 2019, os pesquisadores da F-Secure registraram um aumento de três vezes nos ataques cibernéticos em dispositivos IoT (WORLDFIRST, 2020). Além disso, conforme o Global Cybersecurity Index de 2018, Reino Unido, Estados Unidos da América, França, Lituânia, Estônia, Cingapura, Espanha, Malásia, Noruega, Canadá, Austrália etc. apresentaram alto nível de comprometimento com a cibersegurança (ITU, 2018). Em 2018, a legislação de crimes cibernéticos foi bem implementada em todo o mundo. Existe legislação contra crimes cibernéticos (91%) em cerca de 177 países, o que melhora em relação a 2017 (79%). Entretanto, os governos precisam usar as leis como uma estrutura para implementar estratégias que garantam iniciativas governamentais sustentáveis, em conformidade com as autoridades de tecnologia da informação, o que aumenta a segurança cibernética (ITU, 2018). Entretanto, existe muita oportunidade em relação às empresas, visto que 80% dos clientes do Gartner carecem de um processo de planejamento de estratégia de força de trabalho quando se trata de segurança e gerenciamento de riscos (GARTNER, 2020). Para ficar à frente da curva, os líderes devem olhar além da superfície em busca de competências, alinhá-las com as funções apropriadas e aprimorar a força de trabalho para criar uma equipe de segurança ideal, que possa equilibrar a necessidade de administrar e proteger o negócio. Assim, além do país propiciar o arcabouço legal, as empresas precisam engajar seus líderes e seus colaboradores para atingir níveis excelentes de segurança.

De acordo com o Global Cybersecurity Index, o Brasil apresenta médio nível de comprometimento, apresentando oportunidades de melhoria na implementação de gestão estratégica tanto do governo quanto de empresas. Assim como em escala mundial, as empresas brasileiras necessitam repensar suas políticas de segurança de dados (políticas de segurança da interna 4.0) com intuito de envolver tanto empresas quanto pessoas jurídicas, visto que ocorreu um aumento da variedade de dispositivos conectados à rede, o que propicia ataques cibernéticos (SENIOR, 2020). Por exemplo, em 2018, foram detectados cinco links maliciosos por segundo, e 20% dos brasileiros foram potenciais alvos dos ataques (VOITTO, 2020).

Considerando tais números e diversos ataques sofridos por pessoas e empresas, o Brasil criou a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2019a). Nela, estão regulamentando como as empresas deverão tratar dados e informações pessoais, além de estar alinhada às regulações europeias, isto é, Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation) (AUTOMAÇÃO INDUSTRIAL, 2021). A LGPD apresenta regras a respeito da coleta, uso, tratamento e armazenamento de dados, aplicando para dados de pessoas físicas em operações dentro e fora do Brasil (AUTOMAÇÃO INDUSTRIAL, 2021). Complementarmente, a LGPD criou uma Autoridade Nacional de Proteção de dados cuja missão era criar regras setoriais e fiscalizar, começando sua atuação em agosto de 2021 (IND 4.0, 2020). Além disso, a cibersegurança pode ser uma barreira para implementação da integração horizontal, visto que as empresas apresentam uma limitação de acesso a dados dos clientes, das outras áreas funcionais, dos fornecedores, o que dificulta a implementação.

A fim de mitigar os riscos, existe uma série de ações que as empresas brasileiras precisam realizar para estarem alinhadas com a LGPD e com as necessidades das empresas e seus parceiros (ABIMAQ; NEO, 2021). Entre elas, podemos destacar: compreensão da estrutura de dados; auditoria do tratamento de dados; relatório de impacto; implantação de medidas de segurança de dados; obtenção de certificação de auditorias; criação de um plano de comunicação de incidente etc. (AUTOMAÇÃO INDUSTRIAL, 2021). Ademais, é importante entender os desafios que as empresas passam com a digitalização e na indústria. A Tabela 13 sumariza alguns exemplos de desafios e soluções (AUTOMAÇÃO INDUSTRIAL, 2021).

Tabela 13 - Desafios e soluções de segurança na digitalização industrial

Desafio	Solução
Alta capacidade de endereçamento, processamento, baixa latência e novos padrões e protocolo.	IPv6 de endereçamento, computação em nuvem, 5G.
Evolução da segurança da internet devido ao aumento exponencial de pontos de acesso (por exemplo, uso de IoT).	Antivírus (vacinas digitais) na rede, uso da Deep Web (Dark Web), criptografia nativa.
Mudança da internet de um território livre para regulado (não rígido).	Uso de Leis e Marcos Regulatórios.
Convergência de dados, computação em nuvem e interconexão com internet em fábricas (transformação digital).	Aplicar a Técnica de Defesa em Profundidade com uso de algumas normas da ISO/IEC 27001 e 27002 (ISA99).
Infraestrutura de redes de comunicação e camada de IoT na fábrica.	Aplicação técnica de Defesa em Profundidade com base em alguns conceitos ISO/IEC 27001 e 27002 (ISA99) que envolvem criptografia e outros tópicos de comunicação.
Banco de dados de clientes, planejamento, fornecedores, logística que a fábrica tem acesso.	Aplicação da LGPD e todas as premissas da Lei.

Quando a LGPD é aplicada diretamente na indústria, os principais elementos devem ser mitigados: cadeia de valor interconectada (dados dos clientes, fornecedores, *marketing*, *supply chain* e conexão com a Fábrica Digital) e o uso de diversos bancos de dados de interconectados (AUTOMAÇÃO INDUSTRIAL, 2021). Considerando todo o contexto, os Planos de Cibersegurança da Indústria 4.0 devem abranger os seguintes elementos: Política de Segurança Interna; Controle de Acesso e detecção de invasão; Uso de assinaturas digitais; Isolamento de conexão; Monitoramento de sistemas e redes (VOITTO, 2020).

Por fim, a Figura 16 sumariza as principais aplicações de Segurança da Informação e qual sua relevância nacional e mundial.



Figura 16 - Infográfico da Relevância do Grupo de Segurança da Informação

2.6 Segurança para medição e controle dos processos industriais (IEC/TC65/WG10)

2.6.1 Escopo

O grupo **IEC/TC65/WG10** tem por objetivo a definição de normas de segurança para medição e controle de processos industriais, incluindo a segurança de redes e sistemas. Nesse contexto, um *patch* de segurança é uma alteração aplicada a um ativo para corrigir a fraqueza descrita por uma vulnerabilidade. Essa ação corretiva impedirá a exploração bem-sucedida e removerá ou atenuará a capacidade de uma ameaça de explorar uma vulnerabilidade específica.

2.6.2 Status quo

O relatório técnico **IEC TR 62443-2-3: 2015** (segurança para automação industrial e sistemas de controle - Parte 2-3: Gerenciamento de patches no ambiente IACS) descreve os requisitos para proprietários de ativos e fornecedores de produtos de sistema de controle e automação industrial que estabeleceram e agora mantêm um programa de gerenciamento de patches IACS. O relatório técnico IEC TR 62443-2-3: 2015 recomenda um formato definido para a distribuição de informações sobre patches de segurança dos proprietários de ativos para fornecedores de produtos IACS, definindo algumas atividades associadas ao desenvolvimento das informações de *patch* por fornecedores de produtos IACS e auxiliando na implantação e instalação dos *patches* por proprietários de ativos. O relatório técnico IEC TR 62443-2-3: 2015 define também o formato e as atividades de trocas para uso em patches relacionados à segurança. Ademais, outra parte da mesma série é a **IEC 62443-2-4: 2015 + A1: 2017**, que especifica os requisitos para recursos de segurança e provedores de serviços IACS. Em complemento, os provedores de serviços IACS podem ajudar na integração e manutenção de uma solução de automação.

Além das partes já mencionadas da série IEC 62443, a norma da **IEC 62443-4: 2018** (segurança para automação industrial e sistemas de controle - Parte 4-1: Requisitos de ciclo de vida de desenvolvimento de produtos seguros) especifica os requisitos de processo para o desenvolvimento seguro de produtos usados em automação industrial e sistemas de controle. A norma da IEC 62443-4 define as exigências de ciclo de vida de desenvolvimento seguro (SDL) relacionadas à segurança cibernética para produtos destinados ao uso em automação industrial e ambiente de sistemas de controle, e fornece orientação sobre como atender aos requisitos descritos em cada elemento. É importante ressaltar que a descrição do ciclo de vida inclui definição de requisitos de segurança, design seguro, implementação segura (incluindo diretrizes de codificação), verificação e validação, gerenciamento de defeitos, gerenciamento de *patches* e fim da vida útil do produto.

Em todo caso, existem mais partes da série IEC 62443. A norma **IEC 62443-4-2: 2019** (segurança para automação industrial e sistemas de controle - Parte 4-2: Requisitos técnicos de segurança para componentes IACS) fornece requisitos de componentes do sistema de controle técnico (CR) detalhados e associados aos sete requisitos básicos (FR) descritos na IEC TS 62443-1-1, incluindo a definição para níveis de segurança de capacidade do sistema de controle e seus componentes. Conforme definido na IEC TS 62443-1-1, há um total de sete requisitos básicos (FR): (i) controle de identificação e autenticação (IAC); (ii) controle de uso

(UC); (iii) integridade do sistema (SI); (iv) confidencialidade dos dados (DC); (v) fluxo de dados restrito (RDF); (vi) resposta oportuna a eventos (TRE); e (vii) disponibilidade de recursos (RA). Esses sete FR são a base para definir os níveis de capacidade de segurança do sistema de controle. Complementarmente, é importante definir os níveis de capacidade de segurança para o componente do sistema de controle, visto que é a meta e o objetivo da IEC 62443-4-2: 2019.

Na Tabela 14, há o resumo das normas mencionadas.

Tabela 14 - Normas do grupo de Segurança de processos industriais

Norma	Escopo
IEC 62443-2-1 ED2	Requisitos do programa de segurança para proprietários de ativos IACS
IEC 62443-2-2 ED1	Classificações do programa de segurança IACS
IEC 62443-2-4	Diretriz para avaliações de conformidade
IEC 62443-4-2: 2019	Requisitos técnicos de segurança para componentes IACS
IEC TS 62443-1-1	Definição dos requisitos para níveis de segurança de capacidade do sistema de controle e seus componentes

2.6.3 Mapa mental de relação com outros grupos

A Figura 17 apresenta um mapa mental do grupo de Segurança para medição de processos industriais com outros grupos. Os grupos prioritários estão listados em azul-escuro, à direita. Eles estão explicados a seguir:

- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial é criar normas para subsidiar o desenvolvimento de programas de padronização, além de fornecer orientações aos comitês para o desenvolvimento de aplicações.
- **Segurança de máquinas** – O grupo prioritário de segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO/IEC, em cooperação com outros comitês técnicos da ISO e IEC.
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas para a proteção da informação e das tecnologias da

informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar questões de segurança e privacidade.

- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo prioritário tem intuito de fornecer orientação entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido, em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.
- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares.

Já os outros grupos aparecem na cor amarela, à esquerda. Eles não estão diretamente abordados neste relatório, mas apresentam tópicos em comum com o grupo analisado. Eles estão listados abaixo:

- **Smart Manufacturing:** A fim de fornecer coordenação e aconselhamento no domínio da manufatura inteligente para harmonizar e avançar as atividades na IEC e outros SDO.
- **Gerenciamento de sistemas de energia e troca de informações:** Para preparar padrões internacionais para equipamentos de controle de sistemas de energia e sistemas, incluindo EMS (Sistemas de Gerenciamento de Energia), SCADA (Controle de Supervisão e Aquisição de Dados), automação de distribuição, teleproteção e troca de informações associadas para informações em tempo real ou não, usado no planejamento, operação e manutenção de sistemas de energia.
- **Aspectos eletroeletrônicos:** Padronização no campo da aplicação de equipamentos e sistemas eletrotécnicos a máquinas (incluindo um grupo de máquinas trabalhando em conjunto de maneira coordenada, excluindo questões de sistemas de nível superior) não portáteis à mão durante o trabalho, mas que podem incluir equipamentos móveis.
- **Interconexão de equipamentos de troca de tecnologia da informação:** Padronização de sistemas microprocessados, interfaces, protocolos, arquiteturas e meios de interconexão associados para equipamentos e redes de tecnologia da informação a fim de suportar ambientes de computação integrados e distribuídos, sistemas de armazenamento e outros componentes de entrada/saída.

- **Telecomunicações e troca de informações entre sistemas:** Padronização no campo das telecomunicações, tratando da troca de informações entre sistemas abertos, incluindo funções do sistema, procedimentos, parâmetros, bem como as condições de uso.

Os grupos que aparecem em vermelho são aqueles conectados à transformação digital na Indústria 4.0, que também estão interconectados com o grupo em destaque.

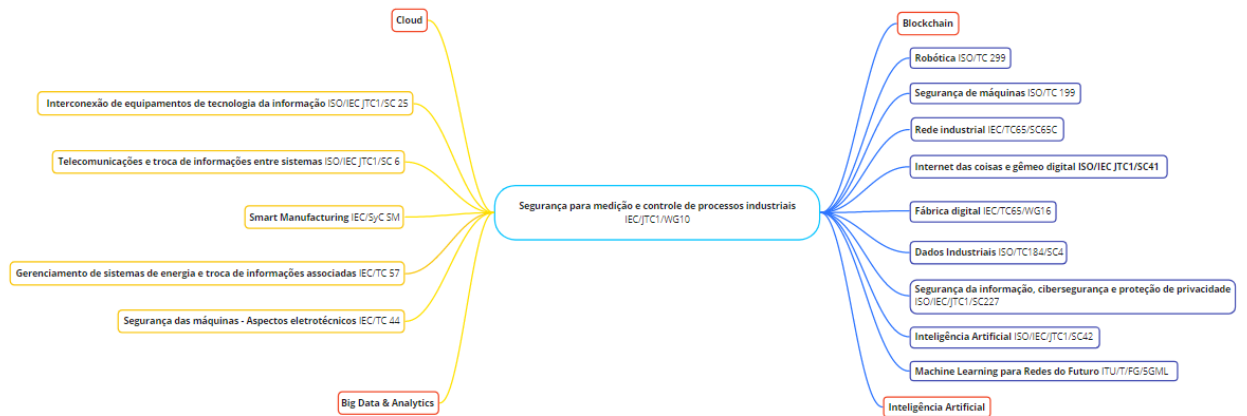


Figura 17 - Mapa mental de relação do grupo de Segurança para medição de processos industriais com outros grupos

2.6.4 Tendências

A Figura 18 ilustra a relação das diferentes partes da **IEC 62443** que foram ou estão sendo desenvolvidas e que serão exploradas nesta seção. É importante ressaltar que há normas mais gerais que focam em políticas e procedimentos, sistemas e componentes. As normas abordam temas complementares de segurança que são importantes para medição dos processos industriais com outros grupos.

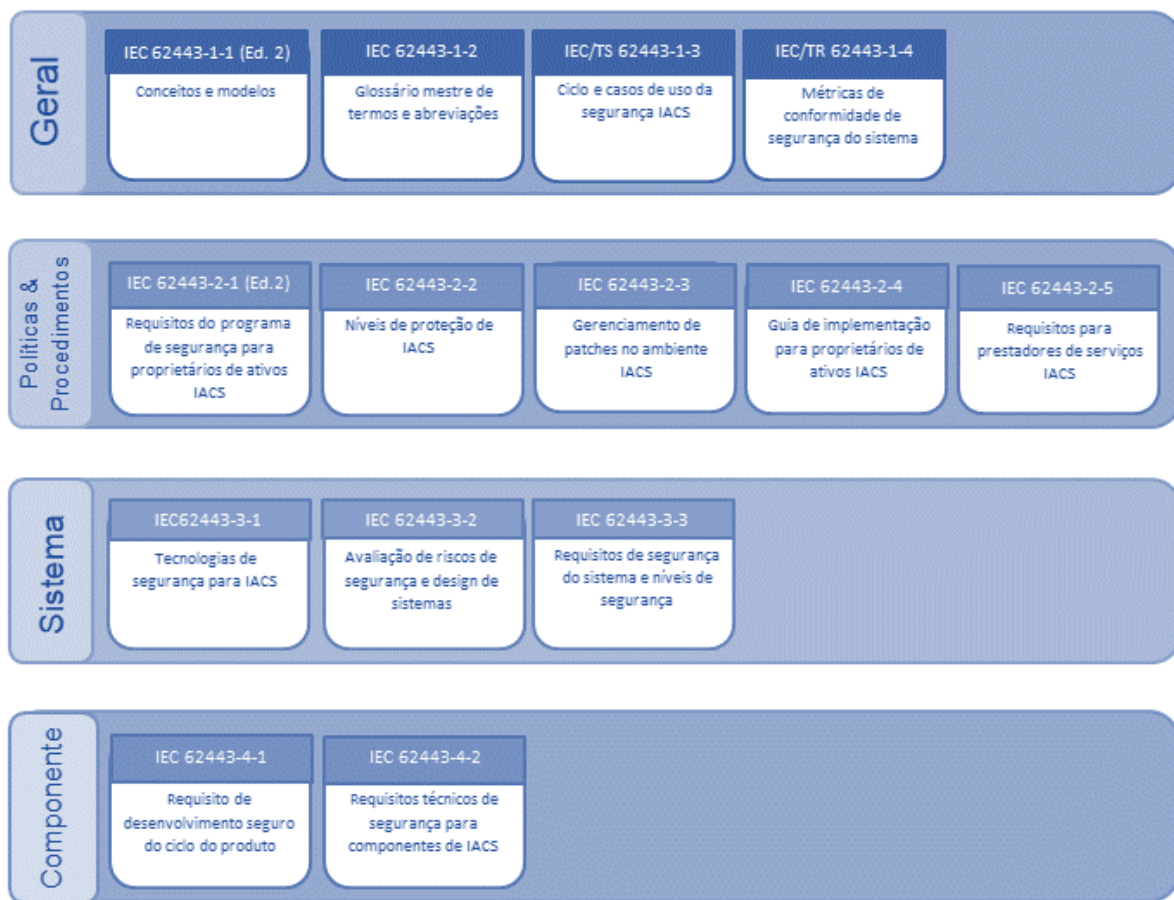


Figura 18 - Consolidação das diferentes partes da IEC 62443

2.6.4.1 Segurança para automação industrial e sistemas de controle - Parte 2-1: Requisitos do programa de segurança para proprietários de ativos IACS (IEC 62443-2-1 ED2)

A norma **IEC 62443-2-1 ED2** (em desenvolvimento – 40,99)²⁴ faz parte da série IEC 62443, que contém requisitos de segurança para proprietários de ativos (SP) de sistema de controle e automação industrial (IACS). As redes do sistema de controle e automação industrial (IACS) geralmente estão abertas por padrão. Sua abertura facilita a coexistência da tecnologia e da interoperabilidade de dispositivos IACS; também exige que as redes IACS estejam protegidas por configuração e arquitetura, ou seja, defendam o limite. Muitas organizações e organismos de normalização recomendam a segmentação das redes de sistemas empresariais a partir de redes em toda a planta, por meio do uso de uma Zona Desmilitarizada Industrial (IDMZ) (CISCO; ROCKWELL AUTOMATION, 2015).

²⁴ Atualizações da norma podem ser encontradas em: <https://bds-bg.org/en/project/show/iec:proj:102021>

Além disso, a norma da IEC 62443-2-1 usa a ampla definição e escopo de o que constitui um IACS, conforme descrito em IEC 62443-1-1. No contexto da IEC 62443-2-1, o proprietário do ativo também inclui o operador do IACS. A norma IEC 62443-2-1 reconhece que a vida útil de um IACS pode ultrapassar vinte anos e que muitos sistemas legados contêm hardware e software que não são mais suportados. Portanto, o SP para um sistema legado pode abordar apenas um subconjunto dos requisitos definidos neste documento. Por exemplo, se o software não for mais compatível, os requisitos de *patch* de segurança não poderão ser atendidos. Do mesmo modo, o software de backup para sistemas mais antigos pode não estar disponível para todos os componentes do IACS. Como resultado, a norma IEC 62443-2-1 reconhece que nem todos os requisitos podem ser atendidos por sistemas legados. Já em situações nas quais requisitos específicos ou subconjuntos de requisitos são aplicáveis, não se pode implementá-los em sistemas legados, de modo que medidas compensatórias devem ser implementadas sempre que possível.

Para entender melhor como os requisitos podem ser alcançados para os mais diversos tipos de softwares e sistemas, a Figura 19 ilustra os recursos de segurança do proprietário do ativo, provedores de serviço e fornecedores de produto de um IACS e seus relacionamentos entre si e com a solução de automação. Particularmente, a solução de automação é uma solução técnica que implementa os recursos funcionais necessários para o IACS. É composto de componentes de hardware e software que foram instalados e configurados para operar no IACS. O IACS é uma combinação da solução de automação e medidas organizacionais necessárias para seu projeto, implantação, operação e manutenção. Alguns dos recursos dependem da aplicação apropriada de manutenção e de integração definidos em IEC 62443-2-4, de e recursos técnicos de segurança definidos em IEC 62443-3-3 e IEC 62443-4-2.

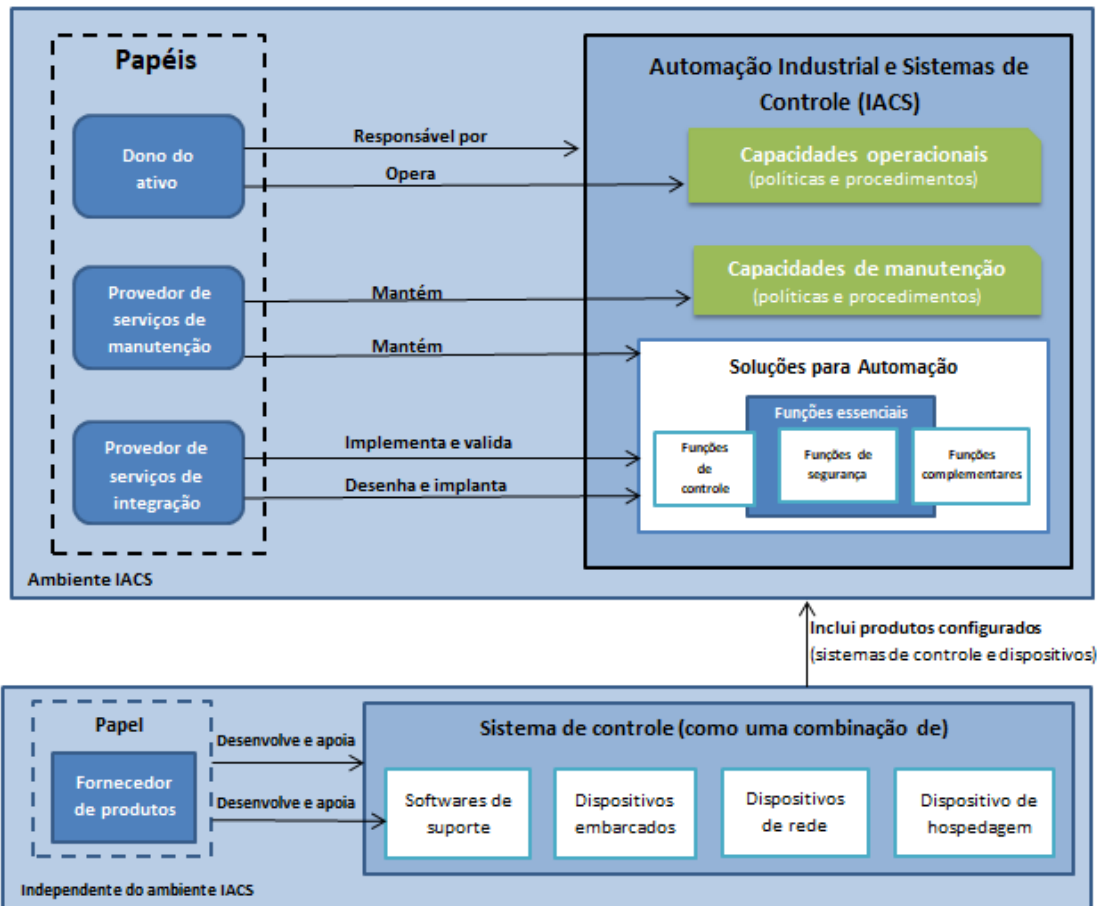


Figura 19 - Esquemática dos recursos de segurança usados na Automação Industrial

Além disso, a norma aborda algumas definições importantes sobre a segurança:

- **Patch:** alteração incremental de software para resolver uma vulnerabilidade de segurança, um bug, um problema de confiabilidade ou operabilidade (atualização) ou adicionar um novo recurso (atualização).
- **Patch de segurança:** patch de software que é relevante para a segurança de um componente de software.
- **Solução de automação:** sistema de controle e qualquer hardware complementar e componentes de software que foram instalados e configurados para operar em um IACS.

Sistema de gerenciamento de segurança (SMS): conjunto de elementos interrelacionados ou interagentes de uma organização para estabelecer políticas e objetivos de segurança e um conjunto de processos sistemáticos a fim de atingir tais objetivos.

- **Programa de segurança (SP):** portfólio de serviços de segurança, incluindo serviços de integração e serviços de manutenção, e suas políticas, procedimentos e produtos associados que são aplicáveis ao IACS.

2.6.4.2 Segurança para automação industrial e sistemas de controle - Parte 2-2: Classificações do programa de segurança IACS (IEC 62443-2-2 ED1)

A norma **IEC 62443-2-2 ED1** (em desenvolvimento no estágio 30,60)²⁵ faz parte da **série ISA/IEC-63443** e especifica uma metodologia para a avaliação da proteção de sistemas de automação e controle industrial em operação, combinando a avaliação de medidas organizacionais e técnicas em um único valor, denominado classificações do programa de segurança (SPR).

A norma IEC 62443-2-2 ED1 aborda a avaliação da proteção da segurança cibernética que pode ser razoavelmente esperada de um esquema de proteção holística para um IACS em operação. A norma inclui uma metodologia para combinar a avaliação das medidas de segurança organizacional e técnica com base em uma estratégia de defesa em profundidade. O resultado é apresentado em valores numéricos e avaliações do programa de segurança (SPR).

Dependendo da sua própria avaliação dos riscos associados às ciberameaças, as organizações podem definir o seu próprio conjunto de valores a partir dos limites das regras, conforme a Figura 20 (exemplo de matrizes para determinação do valor de SPR). Para um determinado valor de SL, os valores de SPR não devem diminuir se a maturidade melhorar, pois a parte do nível de maturidade reflete a confiabilidade da organização para operar os recursos fornecidos pelas medidas de segurança aplicadas à solução de automação.

²⁵ Atualizações da norma podem ser encontradas em: <https://ism.me/en/project/show/iec:proj:102558>

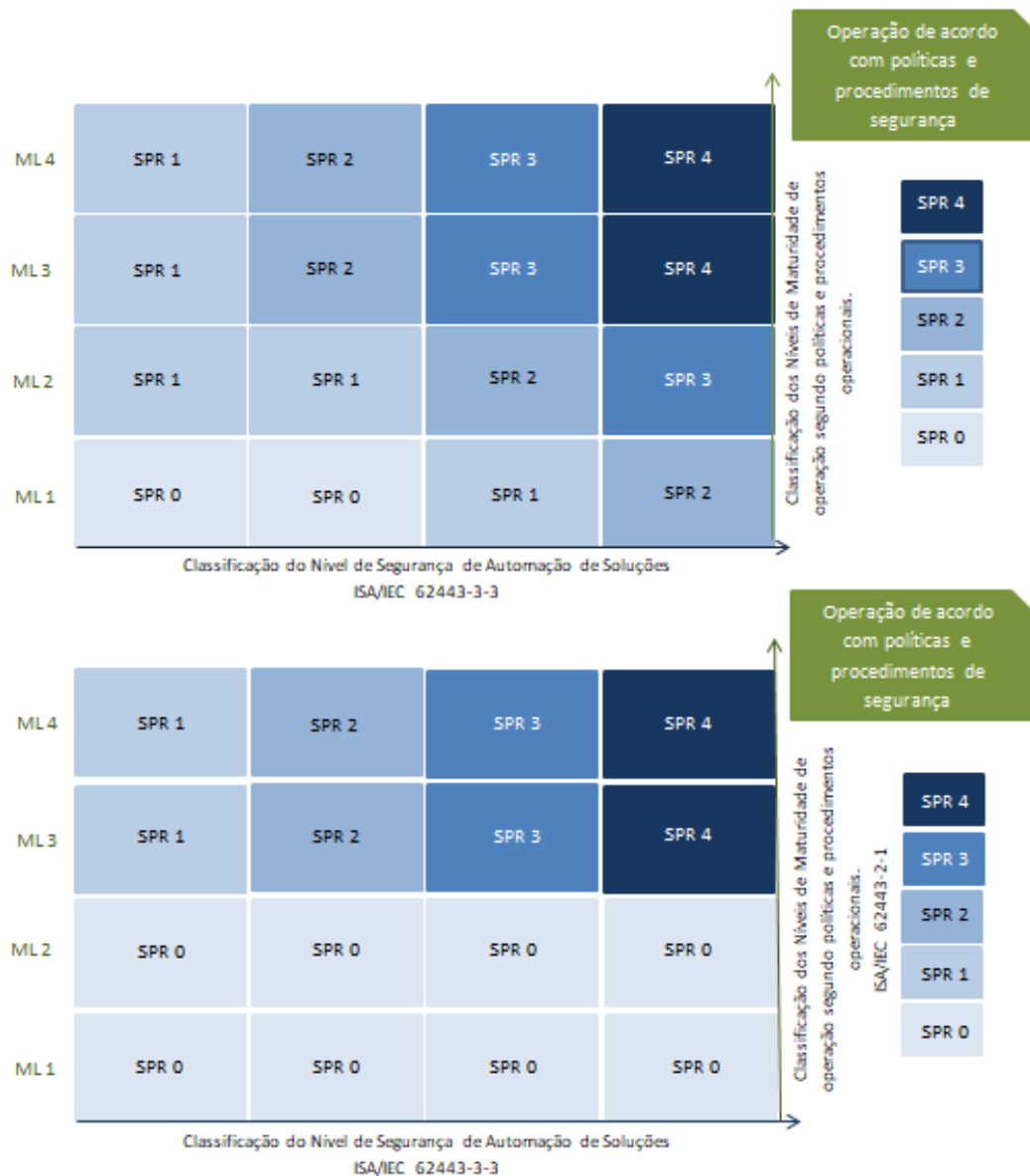


Figura 20- Exemplo de Matrizes para Determinação do valor de SPR

Como as outras normas da série, a IEC 62443-2-2 ED1 aborda alguns termos importantes, como:

- **Medidas de segurança aplicadas à solução de automação:** medidas implementadas com o objetivo de atingir o nível de segurança pretendido. São basicamente medidas técnicas e, eventualmente, contramedidas de compensação técnicas e/ou organizacionais para melhorar as capacidades técnicas dos produtos usados na solução de automação.
- **Sistema de automação e controle industrial (IACS):** coleção hardware e software que podem afetar ou influenciar a operação segura e confiável de um processo industrial.

- **Medidas de segurança organizacional para operação:** medidas de segurança organizacional a serem praticadas durante a operação da solução de automação, a fim de atingir e manter as classificações desejadas do programa de segurança. Além disso, as medidas de segurança organizacional incluem o mantimento das informações utilizadas nas medidas de segurança.
- **Classificação do programa de segurança (SPR):** Classificação da proteção fornecida pelo esquema de proteção holística com base na avaliação: a) das capacidades das medidas de segurança aplicadas à solução de automação; e b) da maturidade para praticar as medidas de segurança organizacionais para operação.

2.6.4.3 Diretriz para avaliações de conformidade (IEC 62443-2-4)

A norma **IEC 62443-2-4** (publicada em 2017)²⁶ especifica os critérios de conformidade, bem como as possíveis evidências de conformidade para cada requisito da IEC 62443-2-4, a serem fornecidos de acordo com o nível de maturidade solicitado, o qual deve ser apresentado pelo requerente para cumprir os respectivos requisitos da IEC 62443-2-4. Além disso, a evidência de conformidade fornece resposta a que nível de maturidade o requerente preencheu suas capacidades de segurança. A norma IEC 62443-2-4 é parte de uma série de documentos planejados sobre métodos de avaliação para partes relacionadas à IEC 62443; não especifica nenhum novo requisito, mas descreve como a conformidade com os requisitos IEC 62443-2-4 pode ser avaliada. A Figura 21 ilustra as responsabilidades resultantes implícitas nesta decisão de gerenciamento.

²⁶ Atualizações da norma podem ser encontradas em:
https://global.ihs.com/doc_detail.cfm?document_name=IEC%2062443%2D2%2D4&item_s_key=006549

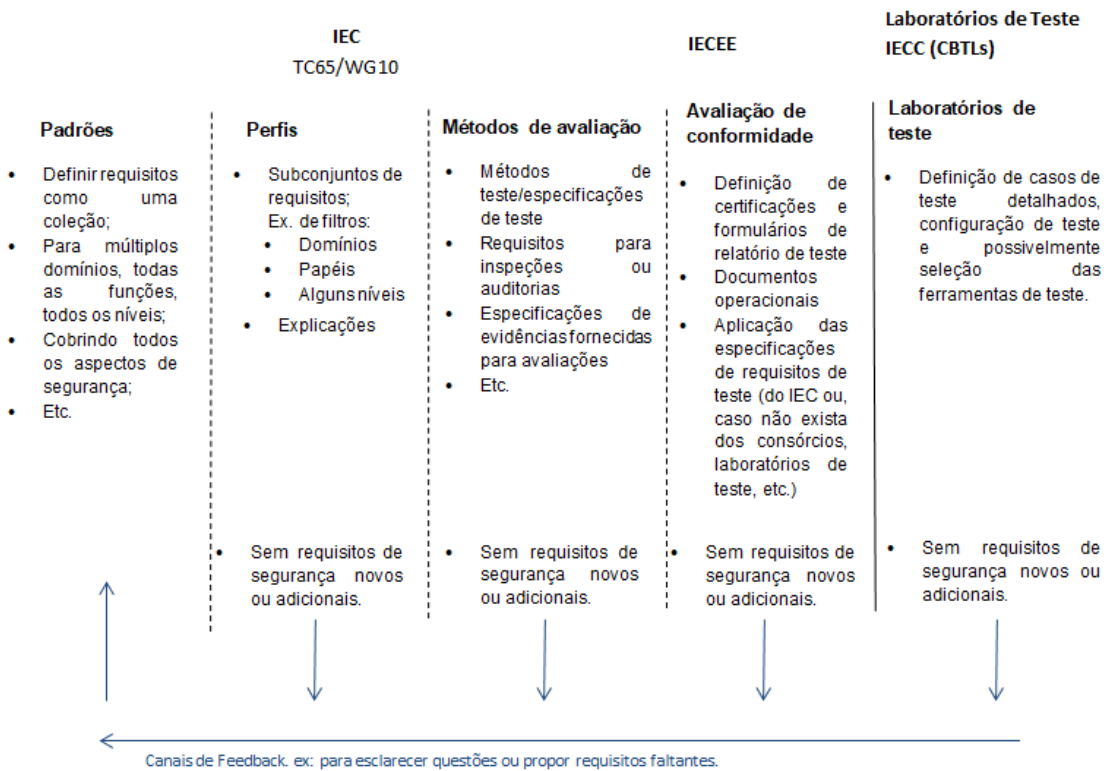


Figura 21 - Principais Responsáveis no Gerenciamento de Avaliação de Conformidade e suas respectivas atividades

Os requisitos da norma IEC 62443-2-4 são projetados usando o conceito de níveis de maturidade, conforme especificado em sua seção 4.2 da IEC 62443-2-4. O padrão divide os níveis de maturidade em quatro tipos:

ML-1- Inicial - os provedores de serviço normalmente realizaram pelo menos uma vez o serviço em um ad-hoc e muitas vezes de forma não documentada.

ML-2- Gerenciável - o provedor de serviços tem a capacidade de gerenciar a entrega e desempenho do serviço de acordo com políticas escritas.

ML-3- Definido - o provedor de serviços praticou um serviço para um proprietário de ativo pelo menos uma vez usando as políticas escritas conforme executado em ML-2, e o desempenho de um serviço de Nível 3 pode ser reproduzível em toda a organização do provedor de serviços.

ML-4- Melhorando - os prestadores de serviços controlam a eficácia e o desempenho de seu serviço e demonstrar melhoria contínua.

Assim, a Tabela 15 sumariza as normas que apresentam relevância para a classificação do processo de segurança IACS.

Tabela 15 - Normas referentes a tendências do grupo de Segurança para processo industrial

Norma	Escopo
IEC 62443-2-1 ED2	Requisitos do programa de segurança para proprietários de ativos IACS
IEC 62443-2-2 ED1	Classificações do programa de segurança IACS
IEC 62443-2-4	Diretriz para avaliações de conformidade

Por fim, a Figura 22 sumariza a evolução do grupo Segurança para medicação e controle dos processos industriais (IEC/TC65/WG10).

Segurança para processo industrial

ISO/TC 184/SC 4

Escopo

Segurança para medição e controle de processos Industriais - Segurança de rede e sistema



Figura 22 - Consolidação da análise do Grupo de Segurança para processo industrial

2.6.5 Relevância

Há perspectivas de aplicações dos conceitos e normas do grupo segurança para medição e controle dos processos industriais (IEC/TC65/WG10) na Indústria, Setor Público e Sociedade (IEC, 2016).

- Na Indústria e Gerenciamento de continuidade do negócio, o gerenciamento de continuidade do negócio (BCM) utiliza dados coletados pela empresa para garantir a continuidade dos processos. O objetivo é fornecer uma avaliação de riscos avançada para que medidas possam ser tomadas a fim de diminuir o impacto de incidentes adversos na organização. O BCM abrange recuperação de negócios, gerenciamento de crises e planejamento de contingências.
- No Setor público e cidades inteligentes, o conceito de Cidades Inteligentes, ou *Smart cities*, engloba uma série de plataformas de IoT que contém ampla variedade de sensores e bases de dados. Isso inclui sensores de temperatura, humidade, ruído, movimento, câmeras, celulares e muitos outros. Com essa enorme quantidade de dados coletados, é possível otimizar as operações nas cidades e, ao mesmo tempo, melhorar os serviços para os cidadãos. Entre as aplicações de uma plataforma *Smart City* estão a otimização da mobilidade urbana, economia de recursos como água e eletricidade e melhoria da segurança da população.
- Nos Usuários e transporte: O sistema ajuda passageiros, incluindo aqueles com necessidades especiais, a otimizarem suas rotas de transporte público baseados nas suas necessidades e preferências. É possível monitorar o movimento dos passageiros e oferecer rotas em tempo real, com previsões de tempo calculadas dinamicamente. Informações sobre passageiros também podem ser analisadas por operadores de transporte público e agências do governo e polícia para direcionar decisões de investimento futuros, criação de novas rotas e alocação de policiais. Esse sistema IoT também garante que existam ônibus e trens equipados para transportar pessoas com necessidades especiais em todas as rotas.

Um ecossistema completo de *Smart City* ainda não existe. Para que seja implementado com sucesso são necessários diversos avanços tecnológicos. Entre eles, estão: avanços em conectividade 5G para que a troca de informações em tempo real e de maneira rápida seja possível; um sistema ou interface padronizada usuários e outros *stakeholders*; algoritmos de *machine learning* capazes de suportar melhorias contínuas dos serviços conforme novos dados sobre usuários são gerados; soluções relacionadas à segurança e privacidade dos usuários e suas informações pessoais, que devem ser coletadas anonimamente.

2.6.5.1 Indústria e Gerenciamento de Continuidade de Negócio (BMC)

Todas as empresas, independentemente de onde estão localizadas e do setor em que atuam, devem estar preparadas para desastres. Os imprevistos podem ser causados por fenômenos naturais, como o furacão Katrina, Estados Unidos ou o terremoto em Fukushima, no Japão; fatores geopolíticos, como a saída da Inglaterra da União Europeia, conflitos entre Israel e Palestina, Rússia e Ucrânia ou Taiwan e China; e também fatores completamente imprevisíveis e aleatórios, como o navio encalhado no Canal de Suez ou a pandemia de Covid-19, que ocasionou, apenas no Brasil, o fechamento de 1 milhão de empresas no ano de 2020 (G1, 2021). Esses são apenas alguns exemplos recentes que chamaram atenção do mundo para a importância de ter um plano para contingenciar acidentes. Sendo assim, o Gerenciamento de Continuidade de Negócios (*Business Continuity Management, BCM*) abrange (NEC, 2017):

- Recuperação de desastres;
- Recuperação de negócios;
- Gerenciamento de crises;
- Gerenciamento de incidentes;
- Gerenciamento de emergência;
- Planejamento de contingência.

Ainda não são todas as empresas que possuem um BCM, mas o interesse é alto no mundo. Do ponto de vista internacional (PHENG; YING; KUMARASWAMY, 2010), um estudo sobre empresas do setor de construção no leste asiático evidenciou que 66,7% delas, entrevistadas na China, alegaram ter implementado práticas de BCM, enquanto 78,9% tinha interesse em implementar mais práticas. Quando perguntados sobre a principal dificuldade para implementar um plano de continuidade, a resposta mais frequente foi falta de pessoas com conhecimento no assunto (57,9%). Complementarmente, existem estudos que mostram a importância do BCM nas empresas, visto que pode gerar impacto financeiro nas empresas devido à falta de segurança. O Instituto Ponemon, em parceria com a IBM, elabora anualmente um relatório intitulado *The Cost of Data Breach* (IBM, 2021) (Custo de Vazamento de Dados, em Português). O relatório de 2020 entrevistou 3200 pessoas de 524 empresas em 17 países. O estudo mostrou que todas as organizações participantes tiveram uma violação de dados, que variaram entre 3.400 e 99.730 registros comprometidos. Além disso, os vazamentos de dados geram um prejuízo médio anual de US\$ 3,86 milhões por empresa, enquanto o tempo médio para identificar e conter uma ameaça é de 280 dias. É importante ressaltar que 52% desses vazamentos foram causados por ataques mal-intencionados, 25% por falhas no sistema e 23% por erro humano.

O mesmo estudo da IBM (mas de 2016) mostrou os benefícios dos Programas de Gerenciamento de Continuidade de Negócios em relação às empresas que não possuem esse planejamento (NEC, 2017): redução de 15% no custo total da violação de dados; redução de 52 dias no tempo médio para identificar uma violação de dados; redução de 36 dias no tempo médio para conter uma violação de dados; redução de 29% na probabilidade de uma violação de dados nos próximos dois anos. Assim, o BCM é utilizado para mitigar a violação de dados das empresas.

Um relatório global de BCM analisou em empresas de diferentes setores de 45 países como a pandemia de Covid-19 as afetou (BONGINI *et al.*, 2020). Antes da pandemia, somente 53% das empresas possuíam um BCM. Com base nos resultados do relatório, quando se analisa somente as empresas brasileiras, esse número sobe para 70%. O estudo também mostra que as empresas com BCM se adaptaram mais rápido às condições de trabalho impostas pela pandemia.

Além de existirem diversos frameworks e de consultorias que auxiliam na parte de gestão de continuidade e de riscos, no Brasil já existem cursos voltados à Gestão de Riscos e Gestão de Continuidade. Pode-se citar os cursos “Gestão de Crise e Continuidade de Negócios”, do Instituto de Desenvolvimento Empresarial (IDEMP) (IDEMP, 2020), que abordam temas como: gerenciamento de riscos e controles internos, gestão de continuidade dos negócios, planos de continuidade dos negócios, integração do plano de continuidade dos negócios. Entre esses, destaca-se o curso de especialização em “Segurança em Processos Industriais”, oferecido pela PUC-Minas (PUC/MG, 2021). Além disso, no Brasil, alguns Planos de Continuidade de Negócios (PCN) foram implementados em empresas com área de TI, visto que o mercado é bastante competitivo. Assim, com intuito de a empresa se manter competitiva no mercado de TI, PCN e outros planos ajudam a empresas a atender a expectativa dos clientes internos e externos com maior qualidade (SILVEIRA, 2009).

Por fim, a Figura 23 apresenta um resumo dos principais diferenciais de Indústria e BCM para o Grupo de Segurança para processo industrial.

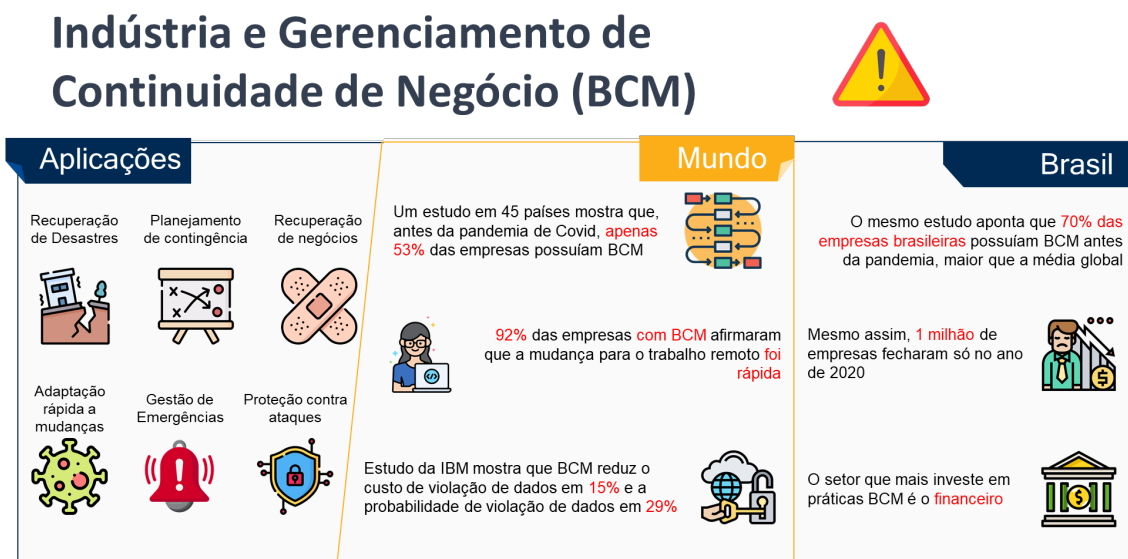


Figura 23 - Infográfico da Relevância da Indústria e BCM para o Grupo de Segurança para processo industrial

2.6.5.2 Setor público e cidades inteligentes

Os sistemas atuais falham em detectar ataques de controle de processo recentes que se manifestam como alterações não autorizadas na configuração dos controladores lógicos programáveis (PLC) de uma planta. No entanto, o impacto das falhas não é só em plantas, mas

sim em cidades, áreas urbanas e cidades inteligentes. Por isso, estudos estão sendo realizados para criar mecanismos de avaliação. Particularmente, uma das maneiras de aumentar a segurança em ambientes urbanos é com a criação de cidades inteligentes, as quais utilizam tecnologias e algoritmos que possibilitam que os dados sejam avaliados em tempo real. As cidades inteligentes podem usar soluções apropriadas (WORLD WIDE TECHNOLOGY, 2020), como o reconhecimento de placa de veículos; o gerenciamento e análise de tráfego; o monitoramento de segurança do parque da cidade; a solução de gerenciamento de resíduos (lata de lixo inteligente); o sensor de umidade do solo e otimização do sistema de sprinklers; a prevenção de despejo ilegal; os passeios virtuais; o monitoramento da qualidade do ar; monitoramento de câmera térmica de transformadores de superaquecimento; monitoramento de roubo de cobre; manejo da vegetação etc. Conseqüentemente, com a mensuração mais acurada, é possível que ações de segurança sejam mais rápidas e eficazes. Mundialmente, já existem vários *cases* de sucesso de cidades inteligentes. Alguns deles (IT2B, 2018) aparecem na Tabela 16.

Tabela 16 - Casos de cidades inteligentes

Cidades inteligentes	Destaques
Barcelona (Espanha)	Meio ambiente e estacionamento inteligente
Nova Iorque (Estados Unidos)	Iluminação de rua inteligente e gestão de tráfego inteligente
Inglaterra (Londres)	Alta tecnologia e dados abertos
Nice (França)	Meio ambiente e coesão
Cingapura (Ásia)	Gerenciamento inteligente de tráfego e uso criativo de tecnologias

Outra possível aplicação da tecnologia é no policiamento preditivo (INTEL; DELL TECHNOLOGIES, 2019). A cidade de Manchester, nos EUA, desenvolveu um sistema que integra imagens de satélite, estatísticas sobre crimes e até informações meteorológicas para indicar áreas onde há maior probabilidade de ocorrência de crimes. O sistema consegue prever, com 60% de precisão, uma área com raio de 150 metros onde crimes acontecerão. A iniciativa resultou em uma diminuição na criminalidade de 28%.

Além de cidades no mundo, o Brasil possui também algumas cidades inteligentes, conforme demonstrado na Tabela 17 (SUMMIT MOBILIDADE URBANA, 2021).

Tabela 17 - Casos de cidades inteligentes brasileiras

Cidades	Destaques
Campinas (São Paulo)	Economia e tecnologia e inovação, empreendedorismo, governança e mobilidade
São Paulo (São Paulo)	Mobilidade, acessibilidade e quilometragem de ciclovias
Curitiba (Paraná)	Atendimento urbano integral de água e esgoto

Além de tais cidades, no Rio de Janeiro, medidores de chuva e sirenes estão sendo usados na prevenção e combate de desastres naturais (RIOONWATCH, 2021). Ao todo, 117 áreas com risco de deslizamentos são monitoradas em tempo real. Por meio de dados meteorológicos,

imagens de satélite e sensores de chuva, é possível prever e alertar a população quando houver alta probabilidade de deslizamentos. Além disso, caso algum desastre de fato ocorra, as informações facilitam a identificação das áreas mais afetadas e que precisam de socorro com mais urgência. A cidade de São Paulo possui o programa “Wi-fi Livre SP” (WIFILIVRESP, 2021). Desde então, diversos pontos estratégicos da cidade, como atrações turísticas, praças, parques e museus, passaram a ter roteadores que fornecem acesso gratuito à internet ao usuário. Atualmente, cerca de 120 pontos na cidade contam com essa tecnologia, e a cidade tem a meta de aumentar esse número para 360 localidades.

O grupo Planet Smart City deseja construir dez cidades inteligentes no Brasil até 2022 (SUMMIT MOBILIDADE URBANA, 2021). Entre elas, destacam-se Aquiraz (CE), Laguna (CE), Natal (RN) e Viva!Smart (SP). A Smart City Laguna, que se encontra nas proximidades de Fortaleza (PLANET SMART CITY LAGUNA, 2021), apresenta soluções inteligentes (PLANET SMART CITY LAGUNA, s.d.) relacionadas ao meio ambiente (arborização urbana), infraestrutura (canteiro de Obras Racional e Sustentável), tecnologia (automação residencial, totem interativo, banco inteligente, entre outros) e pessoas (alimentação Smart).

Por fim, a Figura 24 resume as principais iniciativas do setor público e cidades inteligentes para o Grupo de Segurança em processos industriais.



Figura 24 - Infográfico da Relevância de Setor público e cidades inteligentes para o Grupo de Segurança para processos industriais

2.6.5.3 Usuários e transportes

A segurança na área de transportes também é muito forte. Mundialmente, estão sendo realizadas ações para garantir a confiabilidade e a segurança dos serviços prestados. Consequentemente, alguns casos na área de transporte foram consolidados na Tabela 18.

Tabela 18 - Casos de Transporte no mundo

Casos de Transporte no Mundo	Descrição
Optibus Startup, Tel Aviv, Israel (VB, 2018)	A empresa desenvolveu um programa que utiliza Inteligência Artificial para otimizar o itinerário dos motoristas e da frota, além de prever rotas e horários com maior probabilidade de congestionamento, de modo que contingências possam ser preparadas para garantir a pontualidade dos ônibus. O sistema reduziu custos de operação em até 15%.
Parceria entre Volvo e Nanyang Technological University (NTU), Cingapura (SUSTAINABLE BUS, 2019)	A Volvo Buses lançou o primeiro ônibus sem motorista de Cingapura. O ônibus, que é 100% elétrico, possui sensores e controles de navegação gerenciados por um complexo sistema de Inteligência Artificial que permitem com que ele se mova de maneira autônoma. Cingapura anunciou que os veículos devem entrar em circulação no país em 2022. O ônibus elétrico com tecnologia autônoma representa um passo importante em nossa visão de uma cidade mais limpa, segura e inteligente.
Melhora da programação do ônibus com algoritmos de IA em Londres (FACULTY, 2021)	Atualmente, o itinerário dos ônibus em Londres não é fixo. Ele é feito por 160 operadores que se comunicam com os motoristas para fazer ajustes nos horários de início e término das rotas ao longo do dia. Modelos criados com IA, que levam em consideração a hora, dia da semana e datas de feriados, tiveram resultados melhores que o benchmark utilizado pelos controladores. O melhor desses modelos entregou uma melhoria de 38% e será implementado em diversas rotas, gerando economia para a cidade e um serviço mais confiável para os londrinos.

Além de garantir mais segurança na área de transportes de passageiros, a área de logística também é afetada. No Brasil, para garantir maior segurança na entrega dos produtos, o Mercado Live criou o seu próprio sistema de entrega (MERCADO & CONSUMO, 2021). Em 2017, 95% das suas entregas eram feitas pelos Correios. Já em dezembro de 2020, a situação havia praticamente se invertido, com 90% das entregas feitas pelo próprio Mercado Livre.

Também estão cada vez mais populares os aplicativos de auxílio aos motoristas. No Brasil, alguns exemplos são (EXAME PELO BEM, 2019):

- **Waze**, possivelmente o mais conhecido, usa dados de GPS e informações de usuários para traçar as melhores rotas, levando em consideração os congestionamentos, acidentes e pedágios, garantindo segurança tanto para o motorista quanto passageiros. Consequentemente, é possível os motoristas evitem regiões perigosas com pouca movimentação (CARGO, 2018).

- **TruckPad** é uma plataforma que permite contratar serviços de fretes e pode ser utilizada por motoristas e empresas. As empresas podem selecionar motoristas autônomos de maneira segura e rápida, enquanto caminhoneiros podem acessar ofertas de cargas espalhadas pelo país. **Carteira Digital de Trânsito (CDT)** é uma evolução da CNH Digital. O novo aplicativo permite que o motorista consulte, pelo celular, sua Carteira de Habilitação e os documentos do seu veículo, facilitando a fiscalização e a segurança na via.

Complementarmente, já existem iniciativas que buscam modernizar a legislação brasileira referente a entregadores de aplicativos de *delivery* (NETSEG, 2020). De 18 a 25 de setembro de 2020, ocorreu em São Paulo a Semana Nacional do Trânsito, evento no qual a Associação Brasileira *Online to Offline* (ABO2O) e o Departamento Nacional de Trânsito (DETRAN) firmaram uma parceria visando a modernização da legislação para entregadores e fomento de iniciativas de segurança.

Por fim, a Figura 25 traz informações sobre usuários e transporte relacionados ou impactados pelas normas desenvolvidas em Segurança para medição e controle de processos industriais.



Figura 25 - Infográfico da Relevância dos usuários e transporte para o Grupo de Segurança de Processo Industrial

Concluindo, a Figura 26 resume as aplicações no mundo e no Brasil da segurança para medição de processos industriais.

Segurança para medição



Figura 26 - Infográfico da Relevância para o Grupo de Segurança de Processo Industrial

2.7 Conclusões da nota técnica sobre Segurança e Cibersegurança

A segurança é primordial na era digital, e as normas sobre o tema apoiam conceitos básicos, princípios gerais, fluxogramas, *frameworks*, *roadmaps* e casos de uso que podem ser usados por empresas que já possuem práticas avançadas de segurança ou por empresas que estão utilizando esse processo. O grupo de segurança de máquinas utiliza diversas outras tecnologias da Indústria 4.0 para atingir seu escopo, por exemplo, o uso de IA e *machine learning* para melhorar a performance da máquina. Além disso, o uso de AGV com a adoção de IA e como todo o processo pode gerar riscos de acidentes. Diante disso, as normas ajudam na análise de riscos de implementação das tecnologias de Indústria 4.0, com foco na segurança de máquinas. Como um dos enfoques da segurança na Indústria 4.0 é o trabalhador, as normas também abordam esse tema com intuito de mitigar os riscos a que os operadores digitais estão expostos, aumentando a segurança.

Ademais, o grupo prioritário que aborda segurança da informação, cibersegurança e proteção de privacidade de dados aborda elementos importantes de proteção e segurança cibernética, que inclui assinatura digital, modelo de autenticação, criptografia e sistemas biométricos. Os conceitos básicos também são destacados nas normas a fim de que todos possam compreender e aplicar as melhores práticas nas suas empresas. Complementarmente, as normas do grupo apresentem descrição da segurança cibernética e conceitos relevantes que podem apoiar empresas que estão iniciando o desenvolvimento desse tipo de segurança, mas também aquelas que já estão avançadas no uso. Ademais, as normas são capazes de fornecer orientação para organismos e entidades que avaliam e certificam o gerenciamento de segurança de informações. No entanto, mesmo que o público-alvo não sejam as empresas, elas devem as normas para entender como desenvolver uma segurança. Em relação a tecnologias da Indústria 4.0, por exemplo, as normas apresentam diretrizes sobre riscos, princípios e controles para segurança e privacidade de dispositivos IoT. Adicionalmente, elas

também abordam a segurança de *Big Data*, além de requisitos de competência dos colaboradores necessários para a gestão de segurança da informação. A relevância da cibersegurança está relacionada com marcos regulatórios, como o desenvolvimento da LGPD no Brasil.

O grupo prioritário de segurança de medição de processos industriais proporciona benefícios importantes para indústria, visto que a capacidade de segurança de sistemas é essencial para que as empresas consigam atingir a sua meta de segurança. Além disso, as normas do grupo abordam temas gerais, procedimentos, sistemas e componentes. Como consequência, as empresas conseguem entender desde conceitos e modelos de segurança até requisitos técnicos. Portanto, o grupo prioritário pode garantir a segurança da empresa, mitigando os riscos quando bem avaliados, visto que o design dos sistemas depende de uma avaliação de risco consolidada. Complementarmente, as empresas podem usar as normas como alicerce para se obter sucesso na segurança de medição de processos. Por exemplo, as empresas podem usar a norma para avaliar como está a proteção cibernética por meio de um esquema de proteção holística. Nesse sentido, muitas empresas criam planos de continuidade do negócio, apoiados também na pandemia. Por isso, a segurança também está relacionada ao mantimento do negócio em funcionamento.

2.8 Conclusões Gerais

Como conclusão, são apresentados alguns pontos de lições aprendidas ao longo do estudo completo dos dez grupos prioritários que compõem as três notas técnicas.

Complementariedade dos grupos: Mesmo que os grupos de trabalho desenvolvam normas específicas do tema, ambos se relacionam. Portanto, é imprescindível o entendimento do contexto em que as normas estão inseridas para facilitar o processo decisório das empresas. Nesse sentido, as empresas necessitam ter uma visão clara do que desejam com o uso das tecnologias, para que as normas possam auxiliar na potencialização dos resultados. Além disso, em muitas normas há casos de uso para que as empresas possam se identificar.

Desenvolvimento nacional com base no desenvolvimento internacional: o Brasil já possui diversas empresas que implementam as mais diferentes tecnologias com objetivos diversos. No entanto, quando não possui empresas que estão adotando as tecnologias, pode se espelhar em países mais avançados. Para isso, é essencial a realização do benchmarking internacional. Porém, são imprescindíveis avaliações claras e definições de diretrizes e objetivos tanto do país quanto das empresas que querem implementar tecnologias de Indústria 4.0.

Entendimento base das tecnologias, do vocabulário, dos casos de usos e do framework facilitam o uso da tecnologia e a integração dos dados nas empresas: muitas informações que constam nas normas podem ajudar as empresas a se desenvolverem e adotarem tecnologias da transformação digital, visto que os conhecimentos que as normas propiciam são amplos e precisos. Portanto, as empresas devem reestruturar seus processos digitais com base no conhecimento desenvolvido, de modo que o uso das normas pode facilitar esse complexo processo.

Visão integrativa do uso de tecnologias pode apoiar os resultados da empresa: as empresas devem desenvolver uma visão abrangente do uso das tecnologias e como elas podem ser usadas em conjunto para maximizar resultados. Muitas vezes, as tecnologias apresentam objetivos e funções únicas que, quando são utilizadas em conjunto, facilitam os processos das empresas. Com o uso das normas é possível integrar o uso de tecnologias.

Redes industriais e interoperabilidade

3 Redes industriais e interoperabilidade

3.1 Sumário executivo

3.1.1 Foco do estudo

Esta nota técnica também integra o grupo de três trabalhos similares desenvolvidos pelo CGEE a pedido da Câmara da Indústria 4.0, com o objetivo de analisar dez grupos considerados prioritários para a normalização no contexto da Indústria 4.0. A presente nota técnica analisa o contexto das **Redes Industriais e Interoperabilidade** na normalização internacional sobre a Indústria 4.0. O estudo tem como tema central a normalização em relação à transformação digital e à Indústria 4.0 e analisa a relevância das normas em relação a aplicações de segurança no seu contexto. Para tanto, são analisados cinco grupos prioritários: (i) Redes industriais (IEC/TC65/S65C); (ii) Fábrica Digital (IEC/TC65/WG16); (iii) Internet das coisas e gêmeo digital (ISO/IEC JTC1/SC41); (iv) Dados industriais (ISO/TC184/SC4); (v) Robótica (ISO/TC299).

3.1.2 Abordagem metodológica

O relatório utiliza uma abordagem mista, que combina a análise das normas/regulações, de relatórios, de empresas em relação aos grupos prioritários estudados, além de fazer uma análise sobre estudos anteriores do tema. Complementarmente, utilizou-se uma análise de conteúdo e figuras para facilitar a compreensão do tema.

3.1.3 Resultados

O relatório apresenta diversos resultados:

- No grupo Redes Industriais, diversas normas focam em dispositivos de comunicação sem fio, que são essenciais para automação industrial. Além disso, as normas trazem exemplos de como realizar a comunicação em um ambiente de automação industrial a fim de ajudar as empresas que se interessam no seu implemento. A série IEC 62657 de normas de Redes Industriais abrange os principais atores de diferentes que podem apoiar o desenvolvimento das tecnologias para as empresas adotarem a Indústria 4.0. Particularmente, algumas normas do grupo de Redes Industriais focam em redes de comunicação em tempo real que facilitam a transferência de dados e que minimizam os custos, favorecendo, assim, a adoção de tecnologias da Indústria 4.0, aumentando a eficiência operacional. Mundialmente, há uma projeção de crescimento no mercado de Redes Industriais, e as normas são um alicerce que pode apoiar tal crescimento. Além disso, no Brasil, existem diversos casos de empresas que tiveram resultados econômicos

no uso das diferentes tecnologias de redes associadas a outras tecnologias de Indústria 4.0 (por exemplo, robôs colaborativos, veículos autônomos, inteligência artificial).

- No grupo Fábrica Digital, busca-se desenvolver normas sobre representações digitais de sistemas de produção, apresentando um framework que define diversos modelos ativos de sistemas de produção e apresenta o fluxo de informações. As partes do framework relacionam-se ao ciclo de vida do sistema produtivo, destacando as principais atividades que a Fábrica Digital pode apoiar. No Brasil, as empresas que implementaram a Fábrica Digital obtiveram resultados positivos quanto ao aumento da eficiência e à redução de custos.
- No grupo IoT e Gêmeos Digitais, as normas oferecem uma arquitetura de infraestrutura IoT em que se mostra como a infraestrutura de entidades interconectadas com intuito de facilitar o processamento de informações entre mundo físico e virtual. Complementarmente, há normas que identificam cenários e casos de uso de IoT que podem ajudar as empresas e que também explicam requisitos de interoperabilidade de transporte de sistemas IoT e de troca de dados de IoT. O grupo prioritário foca em framework para dados em tempo real e monitoramento ecológico do ambiente. Além disso, IoT pode cobrir diversas áreas de Tecnologia da Informação: EPR, IoT Industrial, Virtualização de função de rede em IoT. Além de aplicações em TI, há a implementação de tecnologias IoT em veículos, na agricultura e na saúde. Mundialmente, IoT e Gêmeos Digitais pretendem aumentar as movimentações econômicas, diminuindo custos operacionais das empresas e aumentando a sua produtividade. Particularmente, no Brasil, o Plano Nacional de Internet das Coisas foi desenvolvido para facilitar a implementação de IoT no país.
- No grupo de Dados Industriais, as normas abordam a interoperabilidade, além de regras que abordam uma visão geral, definições e princípios básicos. Complementarmente, algumas delas abrangem a modelagem de dados de gerenciamento de manufatura, descrevendo fluxos de informações e indicadores-chave, gerenciamento de mudanças de manufatura. Além disso, há normas com foco na visualização 3D, com informações de fabricação de produtos utilizando o CAD. Elas criam estruturas para desenvolver Gêmeos Digitais na manufatura com diversas partes, apoiando a visualização de dados e favorecendo as análises. Em face disso, as normas estão focadas na qualidade de dados e da informação, e várias delas são desenvolvidas com esse foco. Os dados industriais são aplicados em diversas áreas: previsão de demanda, planos de manutenção preditiva, visão holística e monitoramento.

- No grupo de Robótica, as normas focam no desenvolvimento de um vocabulário específico sobre o tema. Além disso, elas ajudam no entendimento entre usuários e fabricantes de robôs na definição de características importantes e nos requisitos de segurança para integração de robôs industriais e sistemas de robôs. Complementarmente, realizam a categorização de robôs aplicados a áreas relevantes. Portanto, é possível analisar quais áreas e quais tecnologias podem estar associadas a robôs com descrições claras das categorias. Logo, os robôs podem ser aplicados em várias áreas da indústria, em funções colaborativas, de pintura, soldagem, remoção e transferência de peças. Mundialmente, o uso de robôs está crescendo e sendo aplicado em diversas indústrias, alimentos, têxtil e moveleira.

3.2 Introdução

O projeto tem o objetivo geral de desenvolver um estudo detalhado das discussões, propostas e tendências nos principais fóruns internacionais de normalização com foco na Indústria 4.0, facilitando a compreensão de empresas e entidades nacionais de sua relevância para o desenvolvimento da transformação digital da indústria brasileira. As três notas técnicas que compõem o estudo global analisam dez grupos prioritários, previamente definidos pelo Grupo de Trabalho “Regulação, Normalização Técnica e Infraestrutura para Normalização” da Câmara Brasileira da Indústria 4.0, com intuito de expor e explicar o estado atual do trabalho normativo, bem como propostas em discussão. Os temas abordados pelas três notas técnicas são:

Nota técnica A: **Inteligência artificial e 5G**

Nota técnica B: **Segurança e cibersegurança**

Nota técnica C: **Redes industriais e interoperabilidade**

3.2.1 Conteúdo deste relatório

O relatório contempla cinco grupos prioritários, seu escopo de atuação, *status quo* das normas publicadas, relacionamento com outros grupos prioritários, tendências de normalização para os próximos anos e relevância dos grupos para o Brasil. Os grupos prioritários abordados no relatório são:

1. Redes industriais (IEC/TC65/S65C)
2. Fábrica Digital (IEC/TC65/WG16)
3. Internet das coisas e gêmeo digital (ISO/IEC JTC1/SC41)
4. Dados industriais (ISO/TC184/SC4)
5. Robótica (ISO/TC299)

3.2.2 Grupos para o desenvolvimento de normas

Os grupos prioritários são comissões de estudo sobre temas específicos que têm como objetivo desenvolver normalizações acerca de temas relevantes para o desenvolvimento nacional em âmbito mundial. Portanto, os grupos prioritários são essenciais para as empresas que se baseiam no desenvolvimento de produtos e serviços. De forma geral, a participação nessas comissões é aberta a qualquer parte interessada. O Brasil, em alguns grupos, possui participação. É importante salientar que o país pode ser um membro P, que é mais atuante e participativo, e membro O, que é mais observador.

Complementando tais informações, é imprescindível entender a que institutos de normalização eles estão associados. Por exemplo, neste relatório, são a ISO, a IEC e a ITU. A ISO é a Organização Internacional de Normalização que desenvolve normas e relatórios técnicos quando há necessidade de mercado. Para isso, as normas são criadas por especialistas que podem ser profissionais da indústria, do governo, da universidade etc. 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.

Embora a ISO seja muito relevante, 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. Eles fazem publicações para a aplicação em fábricas e em diversos ambientes. É importante salientar que o desenvolvimento de normas é feito por meio do Comitê Nacional da IEC de cada país. Além da ISO e da IEC, a ITU aborda a padronização da área de Telecomunicações do ITU – União Internacional de Telecomunicações ("International Telecommunication Union"), focada também no desenvolvimento de normas. Com base nessas informações, a ITU é focada na parte de telecomunicações, enquanto a IEC aborda temas de eletroeletrônica. De forma geral, a ISO discute temas não abordados pelos comitês anteriores. Consequentemente, as três complementam as normas entre si, desenvolvendo novas normalizações para suportar as empresas. Em suma, elas podem ser consideradas “federações” que congregam os organismos de normalização nacionais de cada país (sendo permitida a participação de uma entidade por país, a qual pode ser membro de diversas entidades). A maior diferença entre eles é o fato de que a representação na ISO e IEC é feita por organismos de normalização, enquanto na ITU a participação é realizada pelos governos, uma vez que apresenta caráter mais estratégico.

No tocante às normas da ISO, é importante entender algumas discussões relacionadas ao desenvolvimento de normas e diferentes tipologias. Por exemplo, a escala de evolução do projeto até se tornar uma norma completa envolve diversas etapas. São elas:

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);
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 das etapas se encontra no Apêndice A. Quanto a tipologias de documentos, podem ser normas internacionais, mas também se abordam outros documentos, tais como Technical Specification (TS), Public Available Specification (PAS) e Technical Report (TR).

3.2.2.1 Coordenação

A participação na normalização internacional requer um bom nível de coordenação dos trabalhos. A atual nota busca mostrar as relações entre os grupos prioritários para facilitar e agilizar o processo de normalização com o enfoque na coordenação. Quando um certo grau de coordenação e gestão for alcançado entre os atores que participarão das diferentes discussões de normalização, maiores serão os ganhos para a indústria brasileira. Além disso, em busca de uma coordenação eficiente, ágil e eficaz, são abordados conceitos que facilitam o entendimento do vocabulário de Indústria 4.0.

3.2.2.2 Visão estratégica

É crítico desenvolver e implementar uma visão estratégica da participação na normalização internacional para a Indústria 4.0. Este relatório aborda uma visão estratégica ao adicionar observações importantes de diversos atores tanto na análise das normas quanto na relevância. Aborda, conseqüentemente, temas de governança de gestão, pois aponta aplicações práticas da implementação de tecnologias em diversos contextos, promovendo um entendimento estratégico sobre o assunto. Em alguns grupos prioritários, quando necessário, são destacadas as diferenças estratégicas dos países com objetivo de identificar sua relevância.

3.2.2.3 Recursos

Desenvolver normas e participar ativamente desse desenvolvimento exige recursos importantes. Este relatório aborda temas relativos aos recursos humanos competentes para desempenhar determinadas funções da Indústria 4.0. Ademais, abrange informações pertinentes a respeito das necessidades do desenvolvimento de capacidades dos usuários, dos desenvolvedores e dos colaboradores da Indústria 4.0. Assim, é possível entender como cada ator pode ajudar no desenvolvimento da transformação digital da indústria brasileira, destacando os principais conhecimentos que são necessários para tal.

3.2.2.4 Capacitação

A capacitação de recursos humanos para participação nas atividades de normalização internacional é um dos principais desafios. Este relatório traz embasamento das principais normas internacionais que podem ser utilizadas para desenvolver as capacidades e os conhecimentos dos colaboradores, capacitando atores do governo, das empresas e das universidades. Com base em uma visão holística, o relatório abrange discussões importantes que diferentes membros de uma instituição necessitam desenvolver para conseguirem alcançar os objetivos organizacionais de implementação das tecnologias da Indústria 4.0.

3.2.2.5 Priorização

É necessário priorizar temas, setores e atividades em que vale a pena se envolver ativamente, até com certa liderança, decidir aqueles que serão acompanhados e, também, aqueles a que não é prioritário se envolver. Respondendo a tal necessidade, este relatório prioriza, com base na análise completa das normas e da relevância dos grupos, os principais assuntos que devem ser considerados para a normalização, mostrando a relevância de cada grupo, tanto para o Brasil como para o mundo. Complementarmente, apresenta exemplos mundiais do uso das tecnologias para o desenvolvimento da Indústria 4.0, ampliando o número de países que foram citados nas notas técnicas anteriores e mostrando o quão relevante é a atuação de alguns e como as suas ações e melhores práticas apresentaram resultados positivos. Com base no *benchmarking* internacional, é possível entender como o Brasil está posicionado referente aos outros países no uso de tecnologias para a Indústria 4.0. Além do mais, o relatório apresenta como o Brasil e as empresas que operam no País são destaque internacional no uso de tecnologias, abordando as ações das empresas, as legislações desenvolvidas e os principais atores que interagem para o desenvolvimento de uma indústria brasileira mais avançada.

Ademais, o atual relatório agrega valor à diferença de desenvolvimento de alguns setores em relação aos outros e como o uso de algumas tecnologias está mais avançado, mostrando aplicações e seus resultados em diversas áreas. O relatório aborda também, quando possível, algumas previsões da literatura para o uso de tecnologias, os empregos que podem ser gerados e o desenvolvimento de ações nos próximos anos, expondo os benefícios esperados para o futuro.

Algumas definições da Indústria 4.0 e do uso de tecnologias necessitavam de um esclarecimento, visto que a literatura não convergia para uma definição comum, o que dificultava o entendimento de conceitos chave para a convergência e gestão de estratégias sobre o desenvolvimento da Indústria 4.0 no país. Considerando esse aspecto, foram destacadas, ao longo do relatório, algumas definições importantes para a adoção de tecnologias, propiciando o conhecimento necessário para o entendimento completo dos temas abordados com base na normalização. Favorecendo, dessa forma, a compreensão das principais definições, promovendo a disseminação do conhecimento sobre o tema e aprofundando, quando necessário, alguns elementos principais e definições que baseiam a adoção das tecnologias.

3.3 Metodologia

A partir da análise de conteúdo das normas dos grupos prioritários e de relatórios, artigos e sites oficiais, foram debatidos cinco principais tópicos para cada um dos grupos prioritários:

- (i) Escopo: aborda o escopo e algumas das principais definições do grupo prioritário;
- (ii) Status quo: apresenta as principais normas do grupo prioritário, mostrando o que foi realizado no passado até o que foi publicado em 2021;
- (iii) Mapa mental: facilita o posicionamento do grupo prioritário em relação a outros grupos e tópicos relacionados a ele;
- (iv) Tendências: aborda as tendências normativas a serem publicadas pelos grupos prioritários nos próximos anos, detalhando quais normas estão em desenvolvimento atualmente;
- (v) Relevância: aborda as principais aplicações dos temas relacionados ao grupo prioritários estudado, sua importância mundial e no Brasil.

Para facilitar a compreensão de como foi realizada cada etapa da análise dos grupos prioritários, consolidou-se o detalhamento das etapas na Tabela 19.

Tabela 19 - Detalhamento da metodologia para o conteúdo do Relatório

Etapas	Metodologia
(xi) Escopo	Realizou-se por meio da análise de conteúdo das normas.
(xii) Status quo	Realizou-se por meio da análise de conteúdo das <i>normas publicadas</i> selecionadas por meio de uma análise temporal e prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ²⁷
(xiii) Mapa mental	Realizou-se por meio da análise de conteúdo das normas, de entrevistas e de análise dos <i>Laisons</i> presentes nos sites dos grupos prioritários. ²⁸
(xiv) Tendências	Realizou-se por meio da análise de conteúdo das <i>normas em desenvolvimento</i> selecionadas por meio de uma análise temporal e prévia do escopo da norma em relação aos principais tópicos da Indústria 4.0. ²⁹
(xv) Relevância	Realizou-se por meio da análise de conteúdo de relatórios de consultorias, de artigos e de sites oficiais a fim de se destacar as primeiras aplicações, a importância mundial e importância no Brasil. ³⁰

²⁷ As normas foram analisadas em maio, junho e julho de 2021.

²⁸ As relações foram desenvolvidas nos meses de maio, junho e julho de 2021.

²⁹ As normas foram analisadas em maio, junho e julho de 2021. Algumas normas foram revisadas na semana de 16 a 20 de agosto de 2021.

Além das análises dos grupos prioritários, ao final do relatório apresenta-se uma avaliação das principais lições aprendidas com base nos temas desenvolvidos pelos grupos. A partir disso, foi possível a realização de uma série de abstrações dos temas tratados pelos grupos prioritários, obtendo percepções do desenvolvimento de diversas estruturas normativas internacionais e nacionais, e como elas, em conjunto, podem alavancar a Indústria 4.0 nas empresas brasileiras. Portanto, a reflexão das lições aprendidas oferece conclusões relevantes do uso de tecnologias da Indústria 4.0 para o desenvolvimento de uma indústria nacional mais tecnológica que acompanha as normatizações internacionais sobre o assunto.

3.4 Grupos de redes industriais (IEC/TC65/SC65C)

3.4.1 Escopo

O escopo do grupo prioritário sobre **rede industrial (IEC/TC65/SC65C)** abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.

3.4.2 Status quo

A **série IEC 61158** apresenta mais de 200 normas sobre as especificações Fieldbus. Fieldbus é um sistema de rede de comunicação industrial para controle em tempo real. É um termo genérico empregado para descrever tecnologias de comunicação industrial; o termo fieldbus abrange muitos protocolos para redes industriais (WIKIPÉDIA, 2020). Para compreender a IEC 61158 é importante entender alguns conceitos e estruturas. Entre eles, destacam-se as tarefas complexas, que são organizadas em camadas, com base na adaptação da **ISO/IEC 7498-1**, que é o modelo de referência ISO/OSI,³¹ com o propósito de modularizar a estrutura, decompor tarefas complexas, e facilitar interfaces e adaptações de tecnologias. Além disso, as camadas são descritas de dois modos complementares: por serviços e por protocolos que fornecem tais serviços. Diante disso, cada fieldbus é composto por uma ou mais camadas, a fim de que a comunicação aconteça e o sistema de automação funcione.

Primeiramente, a norma **IEC 61158-1: 2019** (Redes de comunicação industrial - Especificações do fieldbus - Parte 1: Visão geral e orientação para as **séries IEC 61158 e IEC 61784**) especifica o conceito genérico de fieldbuses. Ou seja, a norma IEC 61158-1:2019 apresenta uma visão geral e orientação para a série IEC 61158, explicando a estrutura e o conteúdo da série IEC 61158, relacionando a estrutura da série IEC 61158 com o Modelo de Referência OSI ISO/IEC 7498-1 e mostrando como usar partes da série IEC 61158 em combinação com a série IEC 61784. IEC 61158-1:2019 também fornece explicações de algumas especificidades da série IEC 61158 que são comuns às partes de tipo do IEC 61158-5, incluindo os conceitos de descrição de serviço da camada de aplicação e os tipos de dados fieldbus genéricos.

³¹ Em relação a rede, O **Modelo OSI (Open System Interconnection)** é um modelo de redes de computadores da ISO, que é dividido em várias camadas, facilitando a decomposição das tarefas.

Para complementar a IEC 61158, a finalidade da IEC 61784 é incluir todos os tipos de camadas de rede especificados na IEC 61158 de modos e configurações. Em geral, apenas algumas combinações das opções possíveis são compatíveis e podem ser interoperáveis. Assim, as recomendações para tais combinações são apresentadas na série IEC 61784. Logo, a série IEC 61784 define “Communication Profiles (CP)”. Um CP é estruturado como um conjunto de três camadas: PhL, DL e AL com suas devidas seleções e configurações. Como consequência, criam-se conjuntos “reais, interoperáveis e possíveis” das camadas de rede presentes na série IEC 61158 que resultam em redes fieldbus que concordam com as tecnologias disponíveis e estabelecidas no mercado internacional. Portanto, a IEC 61784 contém diversas “Communication Profile Families (CPF)” com um ou mais CP, de acordo com a tecnologia que os une.

Complementarmente, a IEC 61784-1: 2010 define um conjunto de perfis de comunicação específicos de protocolo com base principalmente na série IEC 61158, para ser usado no projeto de dispositivos envolvidos em comunicações na fabricação e controle de processos. Cada perfil seleciona especificações para a pilha de protocolo de comunicação em um dispositivo.

Além desses aspectos de comunicação, o grupo prioritário apresenta algumas normas que tratam de redes sem fio (Wireless). Entre elas, destacam-se:

- **IEC 62591: 2016**, que aborda uma rede de comunicação sem fio, especificando: (i) Definição de serviço da camada física e especificação de protocolo; (ii) Serviço e protocolo da camada de enlace de dados; (iii) Serviço e protocolo da camada de aplicativo; (iv) Gerenciamento de rede; (v) Segurança; (vi) Perfil de comunicação; (vii) Procedimentos wireless e gateway.
- **IEC 62061:2015** especifica a arquitetura do sistema e o protocolo de comunicação de redes sem fio para Automação Industrial - Automação de Processos (WIA-PA).
- **IEC 62657-1: 2017** (Redes de comunicação industrial - Redes de comunicação sem fio - Parte 1: Requisitos de comunicação sem fio e considerações de espectro) fornece os requisitos de comunicação sem fio ditados pelas aplicações de sistemas de comunicação sem fio em automação industrial e requisitos de contexto relacionado. É importante ressaltar que os requisitos são especificados de forma independente da tecnologia sem fio empregada. Logo, os requisitos são descritos em detalhes e de forma a serem entendidos por um grande público, incluindo leitores que não estão familiarizados com as aplicações da indústria.
- **IEC 62657-2: 2017** (Redes de comunicação industrial - Redes de comunicação sem fio - Parte 2: Gerenciamento de coexistência) tem sua abrangência bastante ampla. Entre elas, destacam-se os pressupostos, conceitos, parâmetros e procedimentos fundamentais para a coexistência de comunicação sem fio; especifica os parâmetros de coexistência e como eles são usados em uma aplicação que requer coexistência sem fio; fornece diretrizes,

requisitos e melhores práticas para a disponibilidade e desempenho da comunicação sem fio em uma planta de automação industrial; cobre o ciclo de vida da coexistência de comunicação sem fio; auxilia o trabalho de todas as pessoas envolvidas com as responsabilidades relevantes para lidar com temas críticos em cada fase do ciclo de vida da gestão da coexistência da comunicação sem fio em uma planta de automação industrial. Os constituintes do ciclo de vida incluem: planejamento, projeto, instalação, implementação, operação, manutenção, administração e treinamento; fornece um ponto de referência comum para a coexistência de comunicação sem fio para sites de automação industrial como uma diretriz homogênea para ajudar os usuários a avaliar e medir os esforços de suas instalações; trata de questões operacionais da coexistência de comunicação sem fio em relação à organização estática humana/ferramenta e à auto-organização dinâmica da rede.

- **IEC 62734: 2014 + A1: 2019** fornece especificações para uma operação sem fio confiável e segura para aplicações não críticas de monitoramento, alerta, controle de supervisão, controle de malha aberta e controle de malha fechada. Além disso, a norma define um conjunto de protocolos, incluindo gerenciamento de sistema, considerações de gateway e especificações de segurança, para conectividade sem fio de baixa taxa de dados com dispositivos fixos, portáteis e de movimento lento.
- **IEC 62948:2017** (Redes industriais - Rede de comunicação sem fio e perfis de comunicação - WIA-FA) especifica a arquitetura do sistema e protocolo de comunicação de WIA-FA (Redes sem fio para automação industrial - Automação de fábrica) com base na camada física IEEE STD 802.11-2012 (PHY). IEC 62948: 2017 se aplica a sistemas de rede sem fio para medição, monitoramento e controle de automação de fábrica. Uma nova versão retificada foi feita em março de 2021.

IEC 62541-1: 2020 apresenta os conceitos e visão geral da Arquitetura Unificada OPC (OPC UA). Além disso, a leitura do documento é útil para entender as partes restantes deste conjunto. Os documentos a seguir são mencionados no texto da IEC 62541-1: 2020:

- IEC TR 62541-2, arquitetura unificada OPC - Parte 2: Modelo de Segurança
- IEC 62541-3, arquitetura unificada OPC - Parte 3: Modelo de Espaço de Endereço
- IEC 62541-4, arquitetura unificada OPC - Parte 4: Serviços
- IEC 62541-5, arquitetura unificada OPC - Parte 5: Modelo de Informação
- IEC 62541-6, arquitetura unificada OPC - Parte 6: Mapeamentos
- IEC 62541-7, arquitetura unificada OPC - Parte 7: Perfis
- IEC 62541-8, arquitetura unificada OPC - Parte 8: Acesso a dados
- IEC 62541-9, arquitetura unificada OPC - Parte 9: Alarmes e condições
- IEC 62541-10, arquitetura unificada OPC - Parte 10: Programas
- IEC 62541-11, arquitetura unificada OPC - Parte 11: Acesso Histórico

- IEC 62541-12, arquitetura unificada OPC - Parte 12: Descoberta e serviços globais
- IEC 62541-13, Arquitetura Unificada OPC - Parte 13: Agregados
- IEC 62541-14, Arquitetura unificada OPC - Parte 14: PubSub

Assim, a Tabela 20 sintetiza as normas relevantes para a Indústria 4.0 dentro do grupo prioritário de Rede Industrial (IEC/TC65/SC65C).

Tabela 20 - Principais Normas do grupo de Rede Industrial

Norma	Escopo
IEC 61158-1: 2019	Redes de comunicação industrial - Especificações do fieldbus - apresenta uma visão geral e orientação para a série IEC 61158
IEC 61784	Abrange todos os tipos de camadas de rede especificados na IEC 61158 de modos e configurações
IEC 61784-1: 2010	Conjunto de perfis de comunicação específicos de protocolo
IE4C 62591:2016	Define uma rede de comunicação sem fio e suas especificações
IEC 62061:2015	Especifica a arquitetura para Automação Industrial
IEC 62657-1:2017	Fornecimento de requisitos de comunicação sem fio
IEC 62657-2:2017	Especifica os pressupostos, conceitos, parâmetros e procedimentos fundamentais para a coexistência de comunicação sem fio
IEC 62734: 2014 + A1: 2019	Fornece especificações para uma operação sem fio e confiável e segura
IEC 62948:2017	Especifica a arquitetura do sistema e protocolo de comunicação de WIA-FA
IEC 62451	Apresenta os conceitos e visão geral da Arquitetura Unificada OPC

3.4.3 Mapa mental de relação com outros grupos

A Figura 27 ilustra as conexões entre o grupo de Rede Industrial e os demais grupos prioritários, bem como outros grupos existentes. Em azul-claro à direita estão os grupos prioritários. Destaca-se o grupo “Segurança da informação, cibersegurança e proteção de privacidade”, que garante a integridade e confiabilidade dos dados e informações existentes nas redes industriais.

- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares.
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas

incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC e em cooperação com outros comitês técnicos da ISO e IEC.

- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais - Segurança de rede e sistema.
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. Tem como objetivo servir como proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, tem o objetivo de fornecer orientação a entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin.
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo a definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida, desde a concepção até o descarte.
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas para a proteção da informação e das tecnologias da informação e comunicação que inclui métodos genéricos, técnicas e diretrizes para abordar os requisitos de segurança e privacidade.
- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial é criar normas para subsidiar o desenvolvimento de programas de padronização, além de fornecer orientações aos comitês para o desenvolvimento de aplicações.
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas de *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.

Os grupos listados à esquerda, em amarelo, são aqueles não incluídos neste relatório, mas que possuem pontos em comum com o grupo Rede Industrial:

- **Aspectos do sistema:** Padrões relacionados a questões genéricas de sistemas usados em processos industriais de medições, controle e automação de manufatura: condições operacionais (incluindo EMC), metodologia para avaliação de sistemas, segurança funcional etc. SC65A também tem função piloto para preparar padrões acerca da segurança funcional de sistemas eletrônicos elétricos/eletrônicos/programáveis.
- **Telecomunicações e troca de informações entre sistemas:** Padronização no campo de telecomunicações referentes à troca de informações entre sistemas abertos, incluindo funções de sistemas, procedimentos, parâmetros e suas condições de uso. A padronização engloba protocolos e serviços de níveis mais baixos, incluindo físico, conexão de dados,

redes e transporte, assim como níveis mais altos, incluindo o Diretório e ASN.1: MFAN, NFC, PLC, Redes do Futuro e OID.

- **Gerenciamento de sistemas e troca de informações associadas:** Padrões para equipamento de controle de sistemas de poder, incluindo EMS (Sistemas de Gerenciamento de Energia), SCADA (Controle Supervisório e Aquisição de Dados), automação de distribuição, teleproteção, e troca associada para informação em tempo real ou não, usada em planejamento, operação e manutenção de sistemas de poder.
- **Interconexão de equipamentos de tecnologia da informação:** Padronização de sistemas microprocessados, interfaces, protocolos, arquiteturas e meios de interconexão associados a equipamentos e redes de tecnologia da informação para suportar ambientes de computação integrados e distribuídos, sistemas de armazenamento e outros componentes de entrada e saída.

Por fim, em vermelho estão os aspectos que fazem parte da transformação digital e que não deixam de estar conectados com os demais grupos.

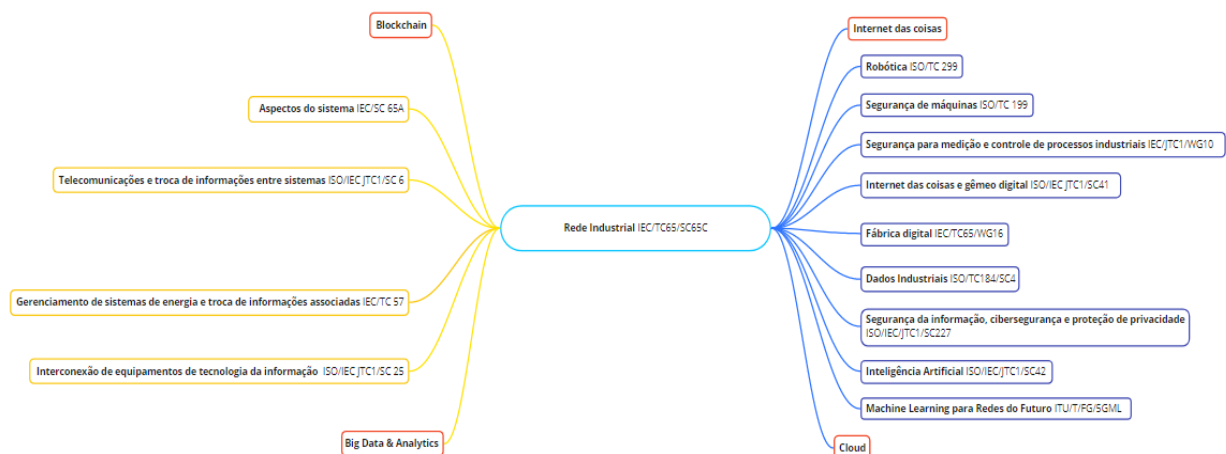


Figura 27- Mapa mental de relação do grupo de Rede Industrial com outros grupos

3.4.4 Tendências

3.4.4.1 Redes de comunicação industrial - Perfis - Parte 2-X: Perfis *fieldbus* adicionais para redes em tempo real (IEC 61784-2-X ED1)

IEC 61784-2-X ED1³² (Redes de comunicação industrial - Perfis - Parte 2-X: Perfis *fieldbus* adicionais para redes em tempo real com base em ISO/IEC /IEEE 8802-3 - publicada uma versão em 30-07-2021)³³ será dividido em várias subpartes para formar um **subsérie (IEC**

³² Atualizações da norma podem ser encontradas em: https://www.iec.ch/ords/f?p=103:30:506700163068045:::FSP_ORG_ID,FSP_LANG_ID:1376,25

³³ Essa norma foi analisada antes da publicação.

61784-2-x), compreendendo uma subparte para cada tipo de comunicação no documento original. Algumas das subpartes serão atualizadas para refletir mudanças nas tecnologias existentes, outras podem ser adicionadas para novas tecnologias. **IEC 61784-2** (e todas suas partes) define Perfis de comunicação (CP) adicionais para as existentes na IEC 61784-1 (inclusive todas as partes) e CPF adicionais. Esses CP adicionais são baseados na série IEC 61158, IEC 61784-1 e usa as disposições da ISO/IEC/IEEE 8802-3 (comumente conhecido como Ethernet) para as camadas inferiores de comunicação. Tais perfis de comunicação Real-Time Ethernet (RTE) fornecem soluções capazes de coexistir com aplicativos baseados em **ISO/IEC/IEEE 8802-3**.

As normas da Tabela 21 estão sendo trabalhadas em projeto de substituição de normas no futuro. No entanto, algumas delas estão em período inicial e serão publicadas somente em 2023.

Tabela 21 - Normas que estão sendo trabalhadas para substituir outras normas

Norma IEC	TÍTULO DA NORMA	Últimos documentos
IEC 61158-1	Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series.	65C/1016/RR em estágio ACDV, que significa a aprovação para que o projeto seja elaborado. O próximo estágio é a avaliação do CDV, que significa o projeto liberado para votação e comentários, previsto para estar pronto em 2023-05.
IEC 61784-1	Industrial communication networks - Profiles Part 1: Fieldbus profiles	O projeto IEC 61784-1-X ED1(65C/1035/CD) irá substituir a IEC 61784-1:2019 ED5.
IEC 61784-2	Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3	O projeto IEC 61784-2-X ED1 (65C/1036/CD) irá substituir a IEC 61784-2:2019

3.4.4.2 Modelo geral para gerenciamento de coexistência automatizada das redes sem fio (IEC 62657)

A **série IEC 62657** fornece histórico, fundamentos, processos e exemplos para alcançar a coexistência sem fio. Com um processo de gerenciamento de coexistência de acordo com a **IEC 62657-2**,³⁴ uma segurança previsível de coexistência pode ser alcançada para um determinado espectro, garantindo que os requisitos da aplicação continuem sendo atendidos. A Figura 28 sumariza os principais atores das partes e quais são os escopos. Com base na Figura 28, é possível visualizar a complementação.

³⁴ Atualizações das normas podem ser encontradas em: https://www.csagroup.org/store/product/iec_060939/

	Parte 1 Requisitos Wireless	Parte 2 Gerenciamento de Coexistência	Parte 3 Arquitetura e Uso	Parte 4 Coordenação Central
1. Regulador	✓			
2. Especialista em IA	✓			
3. Dono da planta		✓	✓	
4. Fabricante dos aparelhos		✓	✓	✓
5. Integrador de sistema	✓	✓	✓	✓

Figura 28 - Principais atores das diferentes partes da série IEC 62657

Já a **IEC 62657-3**³⁵ especifica uma abordagem de modelo geral para gerenciamento de coexistência automatizada e fornece orientação de aplicação de redes de comunicação. Este documento fornece o uso de parâmetros e interfaces para estabelecer e manter funções para gerenciamento automático de coexistência. Além disso, especifica uma descrição abstrata dos elementos do sistema, propriedades, interfaces e relacionamentos entre parâmetros e características de influência dos parâmetros especificados em IEC 62657-1 e IEC 62657-2.

Ademais, uma norma subsidia os sistemas de automação industrial. Com isso, é importante destacar alguns detalhes que dizem respeito à rede *wireless*. Os sistemas de automação industrial podem consistir em funções distribuídas espacialmente (por exemplo, detecção, medição, funções de controle), formando uma aplicação, conforme representado na Figura 29. As funções de comunicação sem fio de um sistema devem ser projetadas com vistas a garantir a cooperação das funções do aplicativo para uma operação ideal dos processos físicos.

A classe de automação industrial sem fio é denominada *Wireless Industrial Automation*. Um sistema de comunicação sem fio é usado para conectar os dispositivos que implementam as funções de automação local. Módulos sem fio que implementam as funções de comunicação são acoplados aos dispositivos do sistema de automação. Condições de propagação de rádio e interferências sem fio caracterizam o ambiente de rádio e o influenciam.

³⁵ Atualizações da norma podem ser encontradas em:
https://global.ihs.com/doc_detail.cfm?document_name=DSF%2FPREN%20IEC%2062657%2D3&item_s_key=00827901

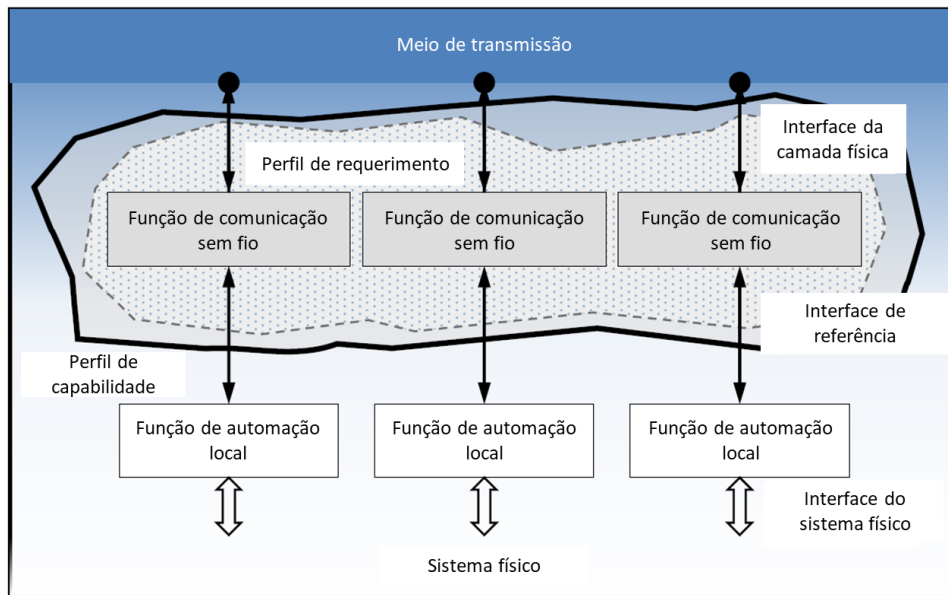


Figura 29 - Exemplo visual da comunicação sem fio em um ambiente de automação industrial

A norma **IEC 62657-4** especifica um conceito e métodos para coordenação central (CC) de aplicações de automação usando comunicações sem fio para estender o gerenciamento de coexistência, de acordo com IEC 62657-2. Ela estabelece os elementos do sistema, interfaces e relacionamentos para uma coordenação central. Além de fornecer subsídios a funções, dados e troca de dados para avaliar e manter o estado de coexistência são especificados. A parte 4 é aplicável para desenvolver, implementar ou modificar procedimentos ou soluções, fornecendo requisitos para sistemas automatizados de gestão de coexistência.

A Figura 30 exemplifica o modelo conceitual de coexistência, descrito na IEC 62657-2. No exemplo, três aplicativos de comunicação sem fio (A, B e C) são assumidos. De acordo com a definição de coexistência sem fio, todos os três aplicativos de comunicação devem cumprir seus requisitos de aplicativo. Uma parte compõe o sistema de comunicação sem fio (WCS). Ele usa o meio sem fio para comunicação, podendo interferir em outro WCS, por exemplo, WCS B. WCS B podem ser da mesma tecnologia *wireless* ou de outra. Cada WCS é caracterizado por certa robustez contra interferências. Assim, o gerenciamento de coexistência requer a investigação do estado de coexistência ao longo de todo o ciclo de vida do sistema. Isso requer que medidas sejam tomadas para determinar se todos os aplicativos de comunicação estão atendendo aos requisitos.

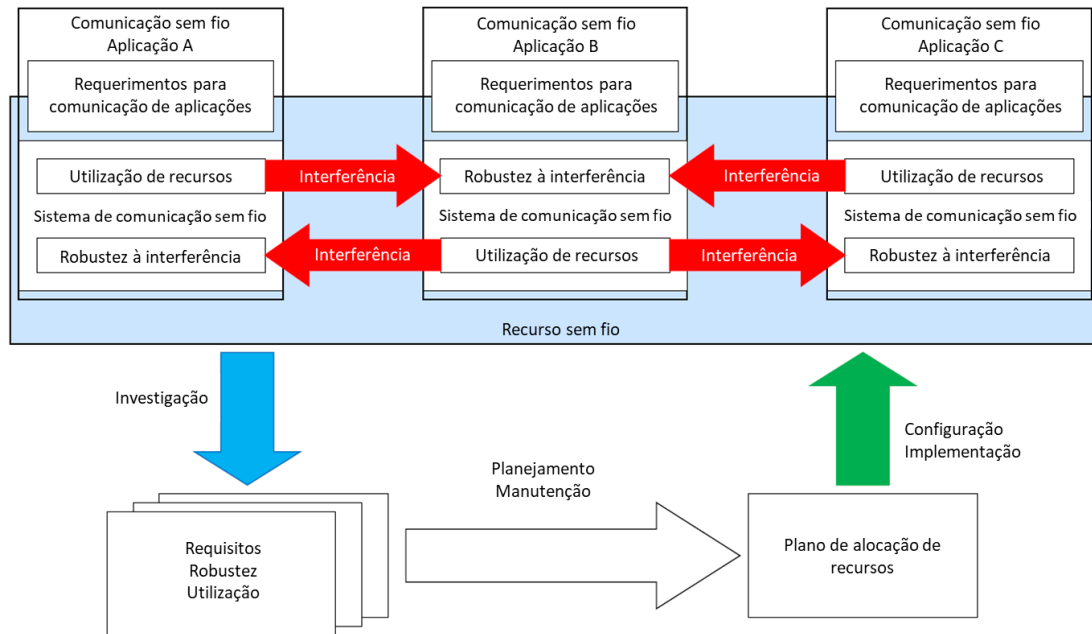


Figura 30 - Modelo conceitual de coexistência de comunicação sem fio em diversas aplicações

Assim, o escopo das normas do Grupo Rede Industrial (IEC/TC65/SC65C) relevantes para a Indústria 4.0 está consolidado na Tabela 22. Por sua vez, a Figura 31 sumariza a evolução das normas ao longo do tempo.

Tabela 22 - Normas referentes a tendências do grupo de Rede Industrial

Norma	Escopo
IEC 61784-2-X ED1	Perfis fieldbus adicionais para redes em tempo real.
IEC 61918:2018+A11:2019	Instalação de redes de comunicação em instalações industriais.
IEC CDV 62657-3	Descrição formal da gestão de coexistência automatizada e orientação de aplicação para redes <i>wireless</i> .

Redes industriais

IEC/TC65/SC65C

Escopo

Preparar padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste.

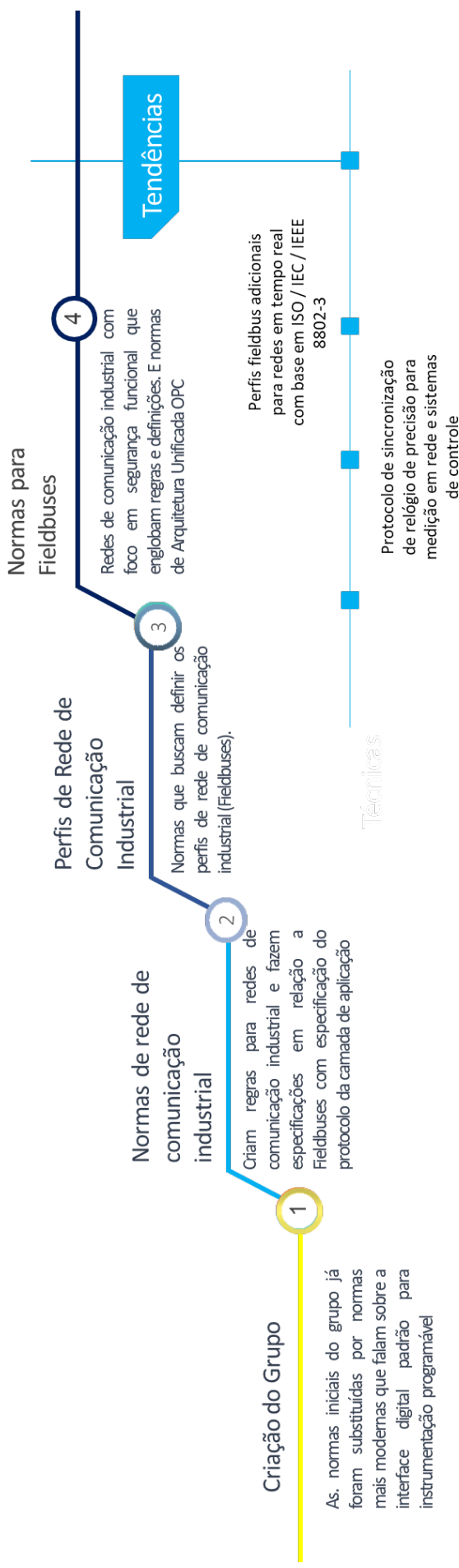


Figura 31 - Consolidação da análise do grupo de Rede Industrial

3.4.5 Relevância

As possibilidades de aplicação das redes industriais são imensas e estão presentes em diversos setores da indústria, uma vez que as redes são essenciais para a automação dos processos. Atualmente, há necessidade de aumentar a velocidade de processamento das informações, incluindo as mais complexas, considerando o grande número de controles de regulamentação existentes para viabilizar uma tomada de decisões mais ágil, com a finalidade de aumentar os níveis de produtividade e eficiência.

Portanto, o objetivo central da rede industrial é interligar os vários equipamentos de determinada aplicação, facilitando o intercâmbio de dados e visando a minimização de custos e aumento da eficiência operacional. Assim, a utilização das redes digitais de acordo com as normas internacionais proporcionará avanços significativos em áreas como: custos de instalação, operação e manutenção, medições multivariáveis, informação do controle e qualidade, procedimentos de manutenção com gerenciamentos ativos etc.

Ademais, o uso das redes permite uma conexão de sistemas de automação e sistemas de controle de processo com equipamentos de campo, como transmissores de temperatura e conversores. Além disso, admite a manutenção e a conexão/desconexão de equipamentos durante a operação sem interferir em outras áreas.

De acordo com um estudo publicado pelo Hardware Meets Software (HMS)³⁶ em 2020, a rede Ethernet Industrial representa 64% das novas redes instaladas em fábricas automatizadas, enquanto a Fieldbus representa 30%, e Wireless, 6%. Ainda segundo um estudo do Data Bridge Market Research de 2020, a comercialização das redes industriais deve apresentar uma taxa de crescimento anual de 20,37% entre 2020 e 2027.

Outra estimativa, apresentada em um estudo do instituto Marketsandmarkets (MARKETANDMARKETS, 2017), aponta que o tamanho do mercado de soluções de rede industrial global saltará de 9,18 bilhões de dólares em 2017 para 23,84 bilhões de dólares até 2022, a uma taxa composta de crescimento anual (CAGR) de 21,0% durante o período de previsão. Os principais fatores que devem impulsionar o crescimento do mercado incluem o crescimento da demanda por soluções de rede de longa distância definida por software (SDWAN) e o aumento da necessidade de manutenção preditiva. Além disso, a proliferação de tecnologias sem fio nas operações do setor e o advento da análise e processamento de dados são alguns dos fatores que devem impulsionar o crescimento do mercado.

O suporte aos usuários e empresas que adotam essa tecnologia também é um fator importante a ser considerado. Somente para auxiliar usuários que utilizam os serviços da rede PROFIBUS, existem 24 organizações regionais (RPAs) e 35 Centros de Competência em PROFIBUS (PCCs), que estão localizados estrategicamente em vários países. No Brasil, especificamente na Escola de Engenharia de São Carlos (SP) existe o único PCC da América Latina.

No que tange às indústrias brasileiras, segundo pesquisa da empresa Murrelektronik (MURRELEKTRONIK, 2017), 62% das entrevistadas afirmaram utilizar Ethernet Industrial. Também foi

³⁶ HARDWARE MEETS SOFTWARE, Annual Analysis of the industrial network market, 2020. Disponível em: <https://www.hms-networks.com/news-and-insights/2019/05/07/industrial-network-market-shares-2019-according-to-hms>

perguntado às empresas quais dispositivos elas utilizam, e 65% respondeu que faz uso dos Sensores Digitais, 50% que utiliza Inversores e 50% também que possui Sensores Analógicos. Outros dispositivos mencionados foram: Válvulas (49%) e Pressostatos (44%).

A Tabela 23 expõe algumas empresas que utilizam tecnologias que se relacionam com as redes industriais e os benefícios que essa adoção trouxe a elas no Brasil.

Tabela 23 - Empresas que utilizam tecnologias relacionadas às Redes Industriais no Brasil

Empresa	Área de atuação	Tecnologias utilizadas	Resultados
Deicmar	Armazenagem de cargas, operações portuárias e logística	Coletores de dados CN50 E CK70, interligados ao sistema ERP (Enterprise Resource Planning).	Melhora na disponibilidade e mobilidade em áreas inóspitas.
Dafiti	Vestuário	Equipamentos CK3 (computadores portáteis e robustos que suportam os processos necessários e as impressoras de código de barra modelo PD41) e Site Survey.	Aumento da taxa de transferência de dados e melhora na qualidade de impressão das impressoras, reduzindo de custos e melhorando a performance nos fechamentos de pedidos, classificação com código de barras e etiquetagem.
Natura	Cosméticos	Sensores, computação em nuvem, sistemas integrados e robôs colaborativos.	Diminuição significativa do número de acidentes, economia de energia elétrica, aumento da produtividade das linhas de produção e redução de custos em geral.
Vale	Mineração	Caminhões autônomos, drones, analytics, inteligência artificial e ambientes integrados.	Economia de US\$ 100 milhões em 2019. Aumento da vida útil dos pneus dos caminhões em 30%.

Com base nas informações, na Figura 32 apresenta-se um infográfico que resume as aplicações e os aspectos relevantes da Rede Industrial em nível mundial e no Brasil.

Redes Industriais

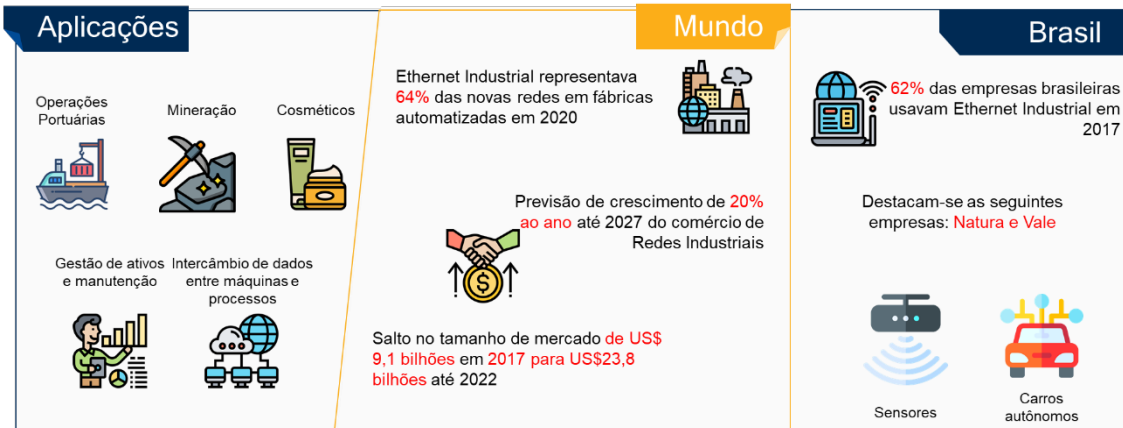


Figura 32 - Infográfico da Relevância da Rede Industrial

3.5 Grupo Fábrica Digital (IEC/TC65/WG16)

3.5.1 Escopo

O grupo denominado **Fábrica Digital (IEC/TC65/WG16)** tem como escopo a definição de um framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.

Para entender melhor o framework, é importante entender que um dicionário de dados consiste em classificações e atributos de dados compreensíveis por computador como seus elementos básicos e é conhecido como Dicionário de Dados Comum (CDD). É uma ontologia que fornece uma classificação de ativos e propriedades para descrever esses ativos de uma forma semanticamente inequívoca. Particularmente, os Dicionários de dados foram originalmente inventados para fornecer dados de produtos e para apoiar a aquisição de produtos.

O framework da fábrica digital define regras para estruturar dados usando dicionários de dados (não se limitando a CDD) que atendem a requisitos específicos para citar o conteúdo, mas não define os próprios dicionários de dados. Ademais, o framework visa construir uma representação digital de todo o sistema de produção, chamada de Fábrica Digital, e utilizar a informação amplamente em várias situações.

3.5.2 Status quo

Primeiramente, a **IEC TS 62832-1** (Medição, controle e automação de processos industriais - Estrutura de fábrica digital - Parte 1: Princípios gerais), que é uma Especificação Técnica, define

os princípios gerais da estrutura da Fábrica Digital (framework DF), que é um conjunto de elementos de modelo (modelo de referência DF) e regras para modelar sistemas de produção.

O framework DF define um modelo de ativos de sistema de produção; um modelo de relacionamento entre diferentes ativos do sistema de produção; o fluxo de informações sobre os ativos do sistema de produção. É importante ressaltar que se aplica aos três tipos de processos de produção (controle contínuo, controle de lote ou controle discreto) em qualquer setor industrial (por exemplo, indústrias aeronáuticas, automotivas, químicas, madeira). A Figura 33 resume a estrutura dos *frameworks* da fábrica digital, explicando quais as atividades que ela pode contribuir em quais partes do sistema do ciclo produtivo.

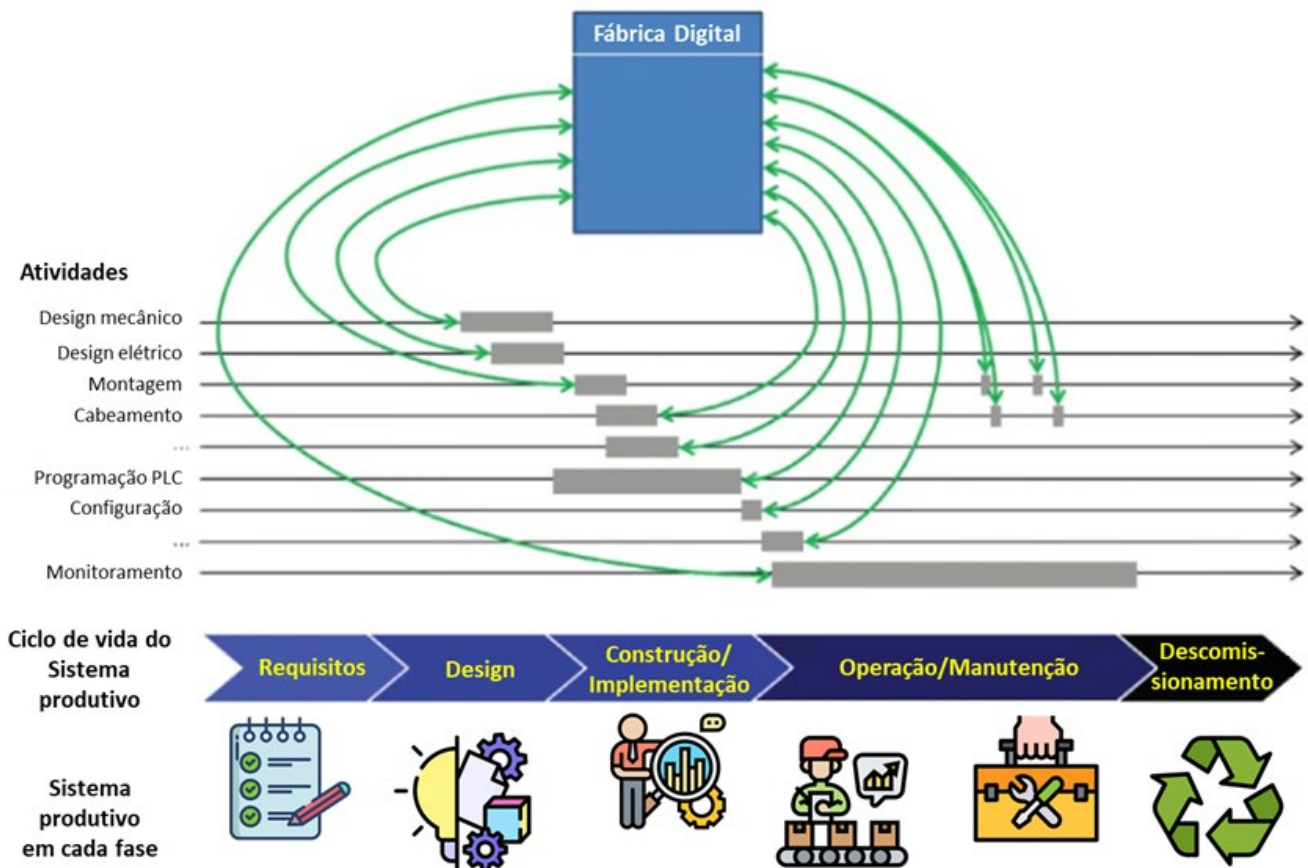


Figura 33 - Partes do framework da Fábrica Digital

Complementando a primeira parte, a norma **IEC 62832-2: 2020** especifica requisitos detalhados para elementos de modelo da estrutura de fábrica digital. É importante mencionar que o modelo define a natureza das informações fornecidas pelos elementos do modelo, mas não o formato dessas informações.

Além das partes anteriores da série, a norma **IEC 62832-3: 2020** (Medição de processo industrial, controle e automação - Estrutura de fábrica digital - Parte 3: Aplicação de Fábrica Digital para gerenciamento de ciclo de vida de sistemas de produção) especifica as regras da estrutura de Fábrica Digital para gerenciamento de informações de um sistema de produção em todo o seu ciclo de vida. Também define como as informações serão adicionadas, excluídas

ou alteradas na Fábrica Digital pelas diversas atividades durante o ciclo de vida do sistema de produção.

A Tabela 24 consolida as normas que compõe o Framework da Fábrica Digital.

Tabela 24 - Normas do grupo de Fábrica Digital

Norma	Escopo
IEC 628232-1	Princípios gerais da estrutura da fábrica digital e modelo de referência
IEC 628232-2	Especifica requisitos detalhados para elementos de modelo das estruturas da fábrica digital
IEC 628232-3	Aplicação de Fábrica Digital para gerenciamento de ciclo de vida de sistemas de produção

3.5.3 Mapa mental de relação com outros grupos

Como forma de explicitar as relações existentes entre o grupo “Fábrica Digital” e os demais grupos prioritários, tecnologias e outros grupos fora deste relatório, elaborou-se a Figura 34. Destacados em azul claro, à direita, estão os grupos prioritários que possuem relação com “Fábrica Digital”. Entre eles, o grupo “Inteligência Artificial”, que permite maior automatização e facilita a tomada de decisões sobre aspectos importantes das fábricas.

- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial (IA) é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA;
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC e em cooperação com outros comitês técnicos da ISO e IEC;
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas 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;
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, co-existência e avaliação de desempenho;
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo

prioritário tem intuito de fornecer orientação entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin;

- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais - Segurança de rede e sistema;
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados;
- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares;
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida desde a concepção até o descarte.

Os grupos que estão à esquerda, em amarelo, são os grupos não listados como prioritários, mas que possuem interconexões com o grupo em destaque:

- **Redes Industriais:** Padrões sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, coexistência e avaliação de desempenho.
- **Segurança de medição, controle e equipamentos de laboratório:** Padrões de segurança para equipamentos de teste e medição, equipamentos de controle de processos industriais e equipamentos de laboratório onde quer que sejam usados.
- **Sistemas de controle de lote:** Desenvolvimento de um glossário de termos e um modelo funcional para sistemas de controle de lote. Desenvolvimento de padrões para estrutura de dados e fornecimento de diretrizes para linguagens de sistemas de controle de lote.

Em vermelho, acima e abaixo dos demais, estão os grupos que possuem conexão direta com a transformação digital e também com o grupo “Fábrica Digital”.



Figura 34 - Mapa mental de relação do grupo de Fábrica Digital com outros grupos

3.5.4 Tendências

Atualmente, o grupo Fábrica Digital (IEC/TC65/WG16) não se encontra com normas em desenvolvimento. Por meio de contato dos autores deste estudo com a entidade que lidera o grupo, o Comitê Nacional Alemão, foi informado que o grupo está com reunião agendada para novembro de 2021, e que as normas deste grupo se manterão estáveis até 2024.

Por fim, a Figura 35 consolida todas as informações referentes ao grupo Fábrica Digital (IEC/TC65/WG16)

Fábrica Digital (DF)

IEC/TC65/WG16

Escopo

Definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção.

Para desenvolver uma rede sem fio industrial

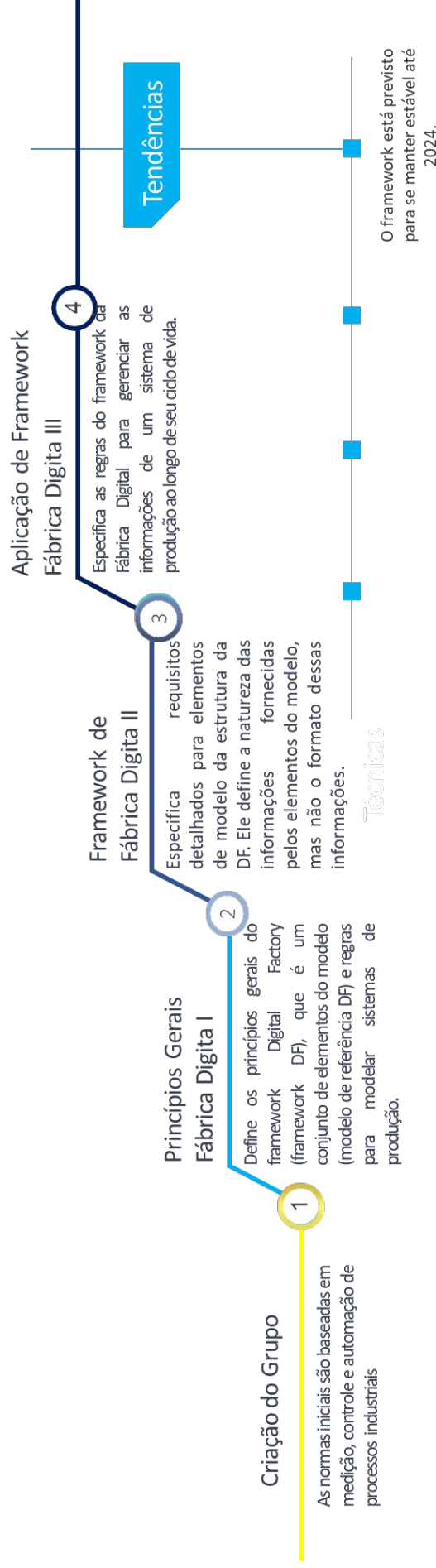


Figura 35 – Consolidação da análise do Grupo de Fábrica Digital

3.5.5 Relevância

A digitalização traz a otimização de processos tradicionais e propicia que as empresas invistam em novas oportunidades de negócios. No entanto, mesmo empresas que já tiveram contato com Indústria 4.0 ainda têm dificuldade para implementar a integração de processos. Cadeias de suprimentos lineares estão cada vez mais sendo substituídas por redes dinâmicas e integradas. Uma Fábrica Digital possui uma cadeia de suprimentos inteligente e interconectada e é o catalisador de geração de valor e novos modelos de negócio. A Figura 36 esquematiza os processos existentes em Fábricas Digitais.

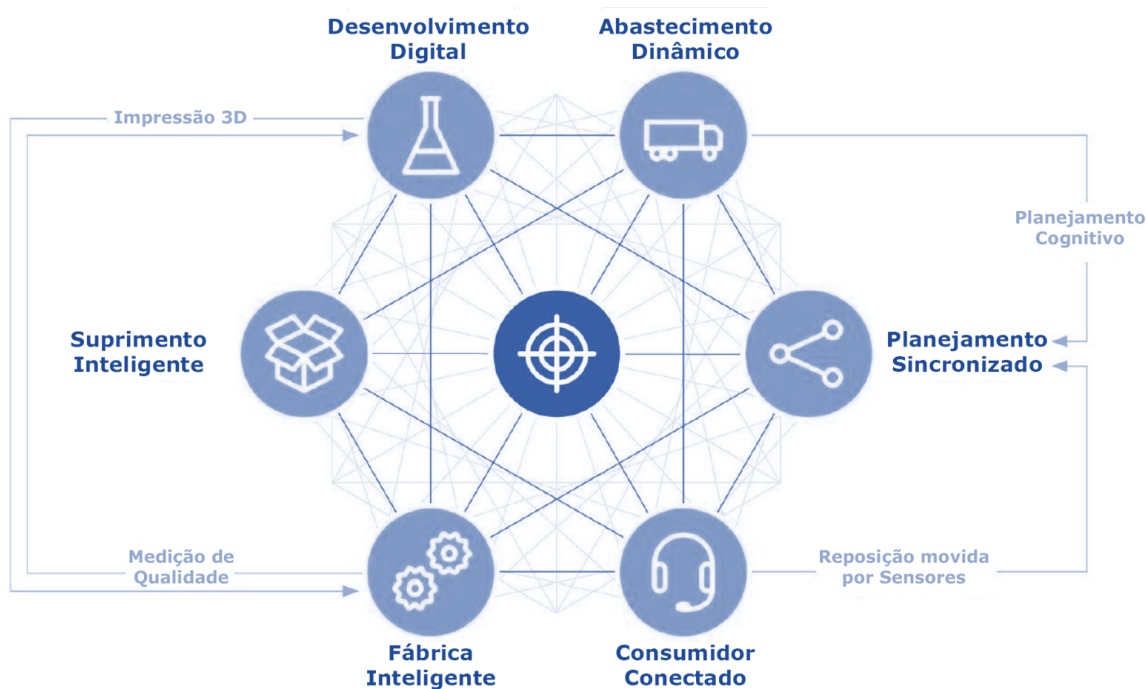


Figura 36 – Processos existentes em Fábricas Digitais

Uma Fábrica Digital permite que times e departamentos diferentes trabalhem juntos e em sintonia, com ferramentas que permitam análise rápida de dados e ajustes em tempo real para suprir demandas da melhor maneira possível. Entre os benefícios, destacam-se (MCKINSEY & COMPANY, 2020c):

- Redução de custos;
- Maior controle de qualidade dos produtos;
- Integração de Manufatura *Lean*;
- Conseguir lançar produtos ao mercado mais rapidamente;
- Ter maiores retornos com recursos já existentes;

Em média, investimentos em Fábricas Digitais retornam um aumento de produtividade de 10% (DELOITTE, 2019). No entanto, em alguns casos, os ganhos podem chegar até 40% (MENGES, 2005). Apesar dos grandes benefícios, um estudo da Deloitte (DELOITTE, 2019) aponta que, em

2019, 49% das indústrias dos Estados Unidos ainda não possuíam Fábricas Digitais. Também foram apontados os três principais fatores que estão impedindo a transformação digital dessas empresas:

- Falta de experiência (34%): O que é necessário para implementar e como priorizar as necessidades?
- Dificuldade de adaptação (32%): Como modificar os negócios e processos já existentes para acomodar essas mudanças?
- Falta de modelos de negócio convincentes (32%): Qual modelo de negócio escolher e como planejar ou implementar?

No Brasil, as iniciativas de Fábrica Digital já não são novidade. Por exemplo, a Embraer já investe em iniciativas de Fábrica Digital nas fases de concepção e fabricação de aeronaves. O objetivo dos investimentos é criar uma plataforma única com informações sobre os projetos e que possa ser facilmente integrada entre os projetistas e o chão de fábrica (PODER AÉREO, 2011). Com a migração para a Fábrica Digital, a Embraer também conseguiu eliminar completamente o uso de papel durante os projetos. Estima-se que para a concepção de cada aeronave, eram necessários entre 80 e 100 mil desenhos, que eram todos impressos e arquivados fisicamente (INFOMONEY, 2019).

A Figura 37 resume a relevância e as aplicações da Fábrica Digital, incluindo aspectos mundiais e brasileiros.



Figura 37 – Infográfico da Relevância para o Grupo de Fábrica Digital

3.6 Grupo Internet das coisas e gêmeos digitais} (ISO/IEC JTC 1/SC 41)

3.6.1 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.

Conforme a IEC (IEC, 2019), o grande volume de dados de IoT disponíveis de pessoas, coisas e máquinas, junto com a complexidade do processamento de eventos e tomada de decisão podem impulsionar a necessidade de uma infraestrutura IoT unificada. Tal infraestrutura pode servir de base para aplicações industriais que, por exemplo, permitem que as empresas acessem informações adicionais sobre as preferências do cliente e variações de mercado, produto e serviço. Facilitando, assim, com o uso de outras tecnologias da Indústria 4.0, como IA, a tomada de decisão dos gestores.

Considerando esses aspectos, Internet das Coisas (IoT) é definida na ISO/IEC 20924 como: “uma infraestrutura de entidades interconectadas, sistemas de pessoas e recursos de informação junto com serviços que processam e reagem às informações do físico e mundo virtual.” A IoT agrega valor como parte de um sistema ou sistema de sistemas. Os sistemas IoT têm como características principais: centralização na rede; distribuição e orientação por máquina a máquina (M2), com vários tipos de computação distribuída usando duas ou mais camadas; uso intensivo de dados.

3.6.2 Status quo

O grupo de Internet das Coisas e Gêmeos Digitais iniciou seu trabalho com foco em sensores. Após, iniciou o foco em IoT. Atualmente, está o início da normalização do Digital Twin. A norma **ISO/IEC TR 22417:2017** identifica cenários de IoT e casos de uso com base em aplicativos e requisitos do mundo real. É importante salientar que os casos de uso são uma ferramenta bem conhecida para expressar requisitos em um alto nível e demonstrar sua relevância na vida real. Complementarmente, os casos de uso fornecem um contexto prático para considerações sobre interoperabilidade e padrões com base na experiência do usuário. Eles também esclarecem onde os padrões existentes podem ser aplicados e destacam onde o trabalho de padronização é necessário. Consequentemente, a norma ISO/IEC TR 22417: 2017 tem como objetivo auxiliar na identificação de áreas potenciais para padronização no ambiente de IoT para garantir facilidade de operação e interoperabilidade.

Também em relação a Internet das coisas, a norma **ISO/IEC 30141: 2018** fornece uma arquitetura de referência de IoT padronizada usando um vocabulário comum, designs reutilizáveis e práticas recomendadas do setor. A norma usa uma abordagem de cima para baixo, começando com a coleta das características mais importantes da IoT, abstraindo-as em um Modelo Conceitual de IoT genérico. Na mesma temática das normas já citadas, a norma **ISO/IEC 21823-1: 2019** fornece uma visão geral da interoperabilidade conforme se aplica a sistemas IoT e um framework para interoperabilidade para sistemas IoT. Dessa maneira, a norma **ISO/IEC 21823-1: 2019** permite que os sistemas IoT sejam construídos de forma que as entidades do sistema IoT possam trocar informações e usar mutuamente as informações de

maneira eficiente. Com base nesse objetivo, a norma ISO/IEC 21823-1: 2019 foi desenvolvida com intuito de permitir a interoperabilidade ponto a ponto entre sistemas IoT separados, fornecendo um entendimento comum da interoperabilidade conforme ela se aplica aos sistemas IoT e às várias entidades dentro deles. A Figura 38 sumariza as principais facetas da interoperabilidade. Além disso, é importante entender como as diferentes facetas funcionam para aproveitar ao máximo o uso da tecnologia e seus respectivos resultados, conforme apresentado na Tabela 25.

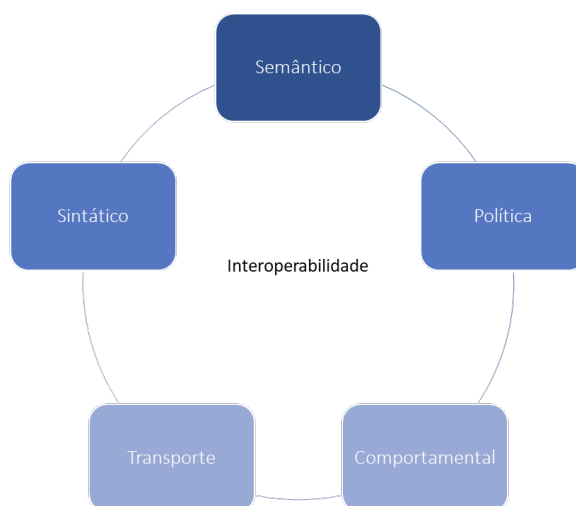


Figura 38 - Principais facetas da interoperabilidade

Tabela 25 - Compreendendo a interoperabilidade no IoT

Facetas	Objetivo	Objetos	Requerimentos	Exemplos
Transporte	Transferência de dados entre sistemas	Conexões físicas Sinais	Protocolos de transferência de dados	HTTP/S, MQTT
Sintático	Receber dados em um formato compreendido	Dados	Formatos de troca de dados padronizados	JSON, XML, ASN.1
Semântico	Receber dados usando um modelo de dados compreendido	Interface programáticos	Interpretação comum de modelo de informação de dados	Diretórios, chaves de dados, ontologia
Comportamental	Obter resultados esperados para interface de operações	Informação	Modelos comportamentais da entidade IoT	Modelos UML, pré e pós-condições, especificações de limitações
Política	Assegurar que sistemas interoperáveis seguem políticas regulatórias e	Contexto de interoperação de políticas regulatórias e organizacionais	Condições e controle para uso e acesso	Políticas de segurança dos <i>stakeholders</i> do sistema IoT, restrição de

	organizacionais aplicáveis			transferência de dados entre fronteiras, PIs controladores de de regulações
--	----------------------------	--	--	---

Complementando as outras normas, a norma **ISO/IEC 21823-2: 2020** especifica um framework 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 também entre entidades dentro de um sistema IoT. De forma geral, a norma ISO/IEC 21823-2: 2020 especifica: interfaces e requisitos de interoperabilidade de transporte entre sistemas IoT; e interfaces e requisitos de interoperabilidade de transporte dentro de um sistema IoT. Outrossim, é importante entender a rede, os serviços, as comunicações e os recursos da rede para conectar sistemas IoT, como exemplificado na Figura 39.

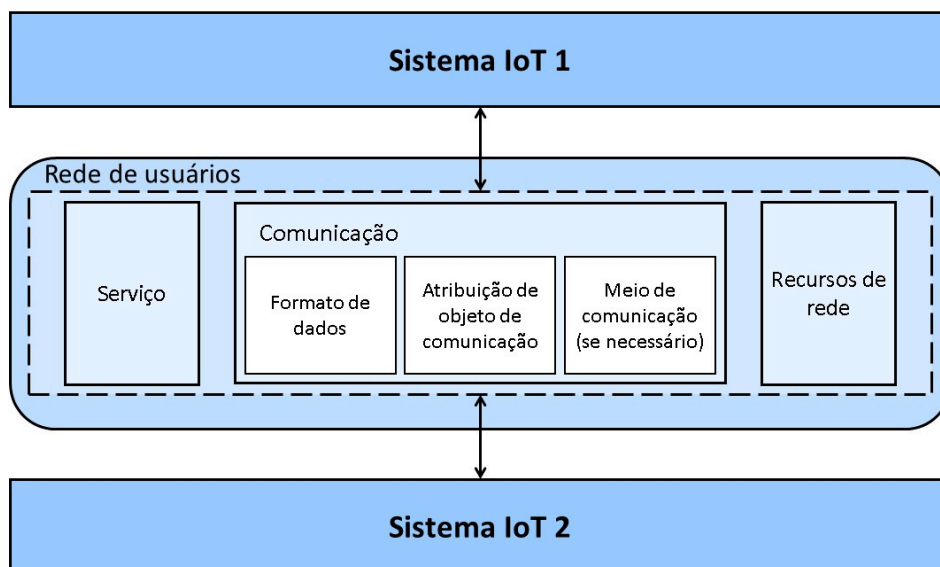


Figura 39 - Esquema de interoperabilidade de Sistemas IoT

Na terceira parte da série, a norma **ISO/IEC 21823-3** fornece detalhes sobre os conceitos básicos de interoperabilidade semântica para sistemas IoT, como descrito no modelo da ISO 21823 Parte 1. ISO/IEC 21823-3 também descreve tecnologias que podem suportar interoperabilidade semântica para IoT, incluindo:

- casos de uso e cenários de serviço que apresentam necessidades e requisitos de interoperabilidade semântica;
- requisitos das ontologias centrais para interoperabilidade semântica;

- ontologias IoT relevantes, juntamente com o estudo comparativo das características e abordagens em termos de modularidade, extensibilidade, reutilização, escalabilidade, interoperabilidade com ontologias superiores, entre outros;
- especificação de domínio cruzado e formalização de ontologias para fornecer a utilização harmonizada de ontologias existentes; e
- melhores práticas e orientação para usar ontologias e desenvolver aplicativos específicos.

Já a norma **ISO/IEC 30161-1: 2020** especifica requisitos para uma plataforma de troca de dados de Internet das Coisas (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 legado Serviços;
- o desempenho dos pontos finais nas redes de comunicação entre a IoT e os serviços legados;
- as funções e funcionalidades específicas de IoT que permitem a implantação eficiente de serviços de IoT;
- estrutura e infraestrutura das redes de comunicação de serviço de IoT; e
- a diretriz de implementação de serviço IoT para a plataforma de troca de dados IoT.

Complementarmente a essas normas, a **ISO/IEC TR 30164: 2020** descreve os conceitos comuns, terminologias, características, casos de uso e tecnologias de computação de ponta para aplicativos de sistemas IoT (incluindo gerenciamento de dados, coordenação, processamento, funcionalidade de rede, computação heterogênea, segurança, otimização de hardware / software). A norma também visa auxiliar na identificação de áreas potenciais para padronização em computação de ponta para IoT.

Para aplicação do IoT no ambiente industrial, a **ISO/IEC TR 30166: 2020** descreve: sistemas industriais IoT (IIoT) gerais que descrevem características, aspectos técnicos e funcionais, bem como elementos não funcionais da estrutura IIoT e uma lista de organizações de padronização, consórcios e comunidades de código aberto com trabalho em todos os aspectos da IIoT; considerações para a perspectiva de padronização futura da IIoT, incluindo análise de risco, novas tecnologias e colaboração identificada.

O uso de IoT e de redes de sensores é fundamental para as empresas. Por isso, a norma **ISO/IEC 30163: 2021** especifica os requisitos do sistema de uma plataforma baseada em tecnologia Internet das Coisas (IoT) / Rede de Sensores (SN) para monitoramento de bens móveis de apoio a serviços financeiros, incluindo: Infraestrutura do sistema que descreve os componentes funcionais; Requisitos de sistema e funcionais durante todo o processo de gestão de bens móveis, incluindo bens móveis em transição, entrada / saída de armazém, armazenamento, hipoteca etc.; Requisitos de desempenho e especificações de desempenho de cada componente funcional; Definição da interface do sistema integrado da plataforma.

Na Tabela 26, há a consolidação das normas do grupo prioritário de Internet das Coisas e Gêmeos Digitais (ISO/IEC JTC 1/SC 41).

Tabela 26- Tabela de Normas do grupo de Internet das Coisas e Gêmeo Digital

Normas	Escopo
ISO/IEC TR 22417: 2017	Cenários de IoT e casos de uso
ISO/IEC 30141: 2018	Arquitetura de referência para IoT
ISO/IEC 21823-1: 2019	Internet das coisas (IoT) - Interoperabilidade para sistemas de internet das coisas - Parte 1 - Framework
ISO/IEC 21823-2: 2020	Internet das coisas (IoT) - Interoperabilidade para sistemas IoT - Parte 2: interoperabilidade de transporte
ISO/IEC 21823-3	Internet das coisas (IoT) - Interoperabilidade para sistemas de Internet das coisas - Parte 3: interoperabilidade semântica
ISO/IEC 30161:2020	Requisitos da plataforma de troca de dados IoT para vários serviços IoT
ISO/IEC TR 30164: 2020	Internet of Things (IoT) – Edge computing
ISO/IEC TR 30166:2020	Internet of things (IoT) – Industrial IoT
ISO/IEC 30163:2021	Internet of Things (IoT) - Requisitos de sistema da plataforma integrada baseada em tecnologia IoT / SN para monitoramento de bens móveis e serviços financeiros

3.6.2.1 Mapa mental de relação com outros grupos

A Figura 40 foi elaborada como forma de exemplificar as relações existentes entre o grupo Internet das Coisas e Gêmeos Digitais e os demais grupos prioritários, tecnologias e grupos fora deste relatório. Os grupos prioritários estão listados em azul claro à direita:

- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares;
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC e em cooperação com outros comitês técnicos da ISO e IEC;
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como

para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, co-existência e avaliação de desempenho;

- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais - Segurança de rede e sistema;
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção;
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida desde a concepção até o descarte;
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas 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;
- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial (IA) é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA;
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.

Os grupos que estão à esquerda, em amarelo, são os grupos não listados como prioritários, mas que possuem interconexões com o grupo em destaque, são estes:

- **Automatização de sistemas e integração:** Padronização na área de sistemas de automação e sua integração para projeto, *sourcing*, fabricação, produção e entrega, suporte, manutenção e descarte de produtos e seus serviços associados. As áreas de padronização incluem sistemas de informação, sistemas de automação e controle e tecnologias de integração.
- **Processos, elementos de dados e documentos no comércio, indústria e administração:** Padronização e registro de negócios e processos administrativos e dados de suporte usados para o intercâmbio de informações entre e dentro de organizações individuais e suporte para atividades de padronização no campo de dados industriais.

- **Blockchain e tecnologias distribuídas de registro:** Padronização de tecnologias de *blockchain* e tecnologias de razão distribuída.
- **Telecomunicações e troca de informações entre sistemas:** Padronização no campo das telecomunicações, tratando da troca de informações entre sistemas abertos, incluindo funções do sistema, procedimentos, parâmetros, bem como as condições de seu uso. Essa padronização abrange protocolos e serviços de camadas inferiores, incluindo física, enlace de dados, rede e transporte, bem como aqueles de camadas superiores, incluindo, mas não se limitando a, Directory e ASN.1: MFAN, NFC, PLC, Future Networks e OID.
- **Engenharia de software e sistemas:** Padronização de processos, ferramentas de suporte e tecnologias de suporte à engenharia de produtos e sistemas de software.
- **Tecnologia da informação:** Padronização na área de tecnologia da informação.
- **Técnicas de identificação automática e captura de dados:** Padronização de formatos de dados, sintaxe de dados, estruturas de dados, codificação de dados e tecnologias para o processo de identificação automática e captura de dados e de dispositivos associados utilizados em aplicativos interindustriais e intercâmbios de negócios internacionais e para aplicativos móveis.

Finalmente, em vermelho estão aqueles conceitos conectados à transformação digital na Indústria 4.0, que também estão interconectados com o grupo em destaque.

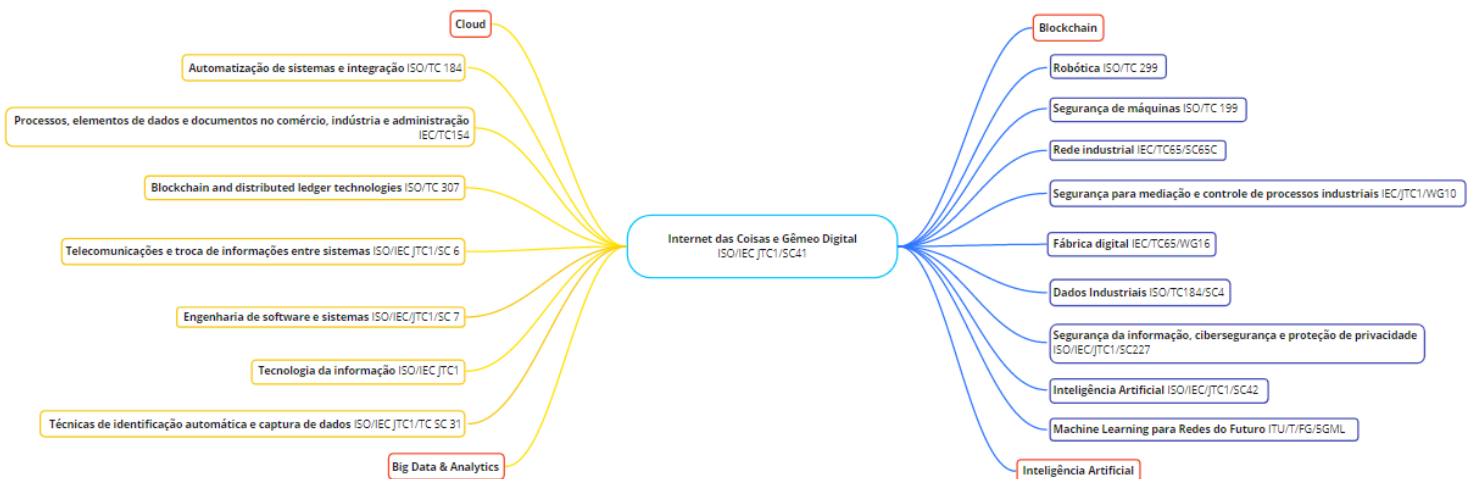


Figura 40 - Mapa mental de relação do grupo de Internet das Coisas e Gêmeo Digital com outros grupos

3.6.3 Tendências

3.6.3.1 Internet das coisas (IoT) - Interoperabilidade para sistemas de Internet das coisas - Parte 4: Interoperabilidade sintática

Dentro deste grupo, a **ISO/IEC 21823-4**³⁷ especifica a interoperabilidade IoT de um ponto de vista sintático. Já na **ISO/IEC 150 21823-1: Framework**, cinco facetas são descritas para interoperabilidade de IoT: transporte, semântica, sintática, comportamental e política. Neste documento, as seguintes especificações para a interoperabilidade de IoT de um ponto de vista sintático são abrangidas, descrevendo:

- Um princípio de como alcançar a interoperabilidade sintática entre os sistemas IoT que incluem dispositivos IoT;
- Requisitos de informações relacionadas a dispositivos IoT para interoperabilidade sintática;
- Uma estrutura para processos de desenvolvimento de regras de troca de informações relacionadas a dispositivos IoT do ponto de vista sintático.

3.6.3.2 Internet Das Coisas (IoT) - Sistema De IoT Socializada Da Dinâmica Da Interação Social Humana

O documento de **interação social-humana (JTC1-SC41/227/DTR - ISO/IEC TR 30174 ED1**³⁸) descreve:

- Principais recursos dos sistemas de IoT socializados, por exemplo, detecção do mundo físico externo, resolvendo as incertezas das metas, satisfazendo a demanda dos usuários e fornecendo qualidade de serviço;
- Atributos socializados, ou seja, rede socializada, colaboração socializada e serviços socializados, que são derivados dos principais recursos; e
- Diretrizes sobre como usar ou aplicar os atributos socializados no design e desenvolvimento de sistemas IoT.

Existem muitas semelhanças entre o sistema IoT abrangente e a dinâmica social humana, que podem ser ilustradas por três níveis hierárquicos:

- I. Vários tipos de sensores, por exemplo, sensores biomiméticos, sensores eletrônicos, sensores químicos, etc., agem como uma extensão de nossos órgãos sensoriais, como olhos, nariz, ouvidos, etc., para nos permitir explorar o mundo físico;

³⁷ Atualizações da norma podem ser encontradas em:

<https://standards.globalspec.com/std/14389676/dsf-iso-iec-21823-4-ed1>

³⁸ Atualizações e informações da norma podem ser encontradas em:

https://www.iec.ch/ords/f?p=103:30:506700163068045::::FSP_ORG_ID,FSP_LANG_ID:20486,25

- II. Após os sensores receberem as informações, os dados são transmitidos por meio de redes de sensores e / ou redes de comunicação de dados para unidade (s) de processamento dos dados para extrair e gerar informações ocultas, informações situacionais, informações preditivas, informações de auxílio à decisão , etc., por agregação, integração, fusão, mineração, análise, etc. e
- III. A fim de realizar uma percepção e compreensão abrangentes do mundo físico, a cooperação e colaboração das unidades de processamento de vários tipos de redes de sensores é necessária, que segue os indivíduos humanos em equipes que colaboram entre si e compartilham suas informações e conhecimento para tomar melhores decisões.

Os três níveis da dinâmica social humana para uso de IoT estão sumarizados na Figura 41.

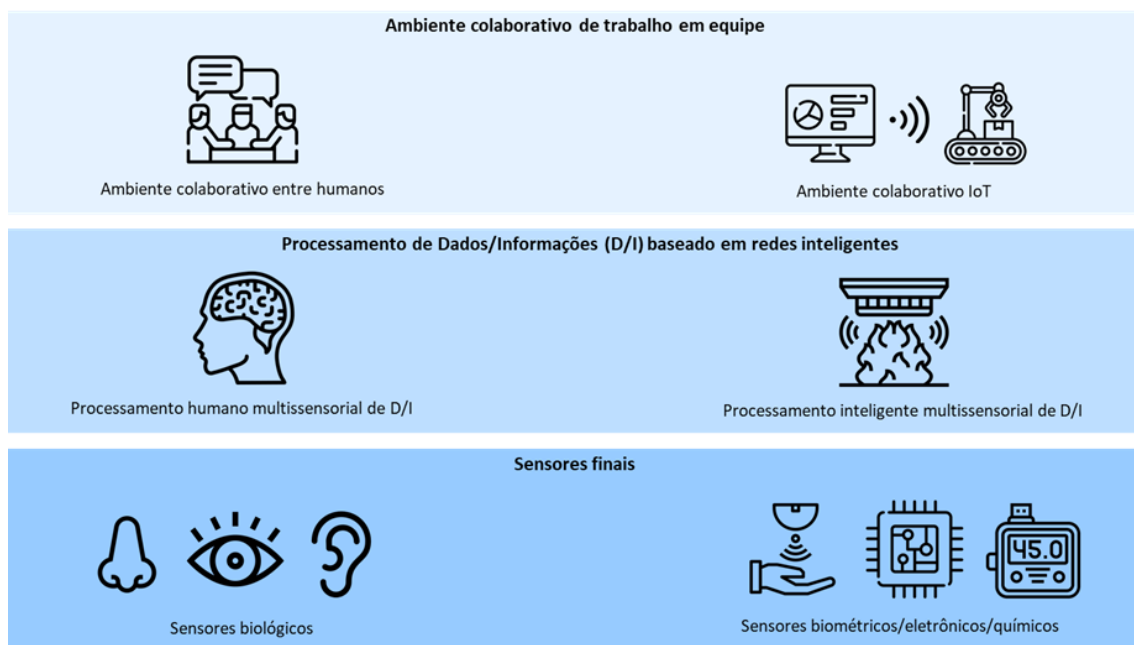


Figura 41 - Esquemática de três níveis da dinâmica social humana para o uso de IoT

3.6.3.3 Internet das coisas (IoT) - Requisitos de compatibilidade e modelo para dispositivos dentro de sistemas industriais IoT

Em relação à aplicação de IoT em ambientes industriais, a norma **ISO/IEC WD 30162** (que está no estágio 20,99³⁹) especifica modelos de rede para modelos de conectividade IIoT e compatibilidade geral dos requisitos para dispositivos e redes dentro de sistemas IIoT em termos de: • interação de protocolos de transmissão de dados; • interoperabilidade e

³⁹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/53282.html>

gerenciamento de dados distribuídos; • estrutura de conectividade; • conectividade de transporte; • conectividade de rede; • melhores práticas e orientação para uso na área de IIoT.

É importante ressaltar que a norma ISO/IEC WD 30162 mostra alguns exemplos de conexões que podem ser feitas com IoT. Entre elas, a conexão por meio de sistemas de controle industrial que descreve formas de conectar sistemas industriais de coleta e gerenciamento (C&M IS), que respondem pelo gerenciamento de um grupo de diferentes ferramentas industriais a serviços IIoT (Figura 42). Neste caso, as ferramentas industriais digitais são conectadas por um sistema industrial especial de coleta e gerenciamento. Este sistema está conectado a um serviço IIoT por um aplicativo cliente especial no C&M IS que se conecta ao gateway IIoT.



Figura 42 - Aplicação de um serviço de IIoT com os equipamentos industriais

3.6.3.4 Internet of Things (IoT) — Real-time IoT framework

Para aplicações de IoT em tempo real, a norma **ISO/IEC AWI 30165** (publicada em julho de 2021⁴⁰) especifica um framework do sistema de uma Internet das Coisas em tempo real (RT-IoT), incluindo:

- Modelo conceitual do sistema que descreve melhor cada domínio IoT;
- Quatro perspectivas: Visualização do tempo, Visualização da computação, Visualização da comunicação e Visualização do controle.

Cada visualização mostra, de um ângulo diferente, como o parâmetro de tempo afeta um sistema RT-IoT. ISO/IEC AWI 30165 é aplicável ao projeto e ao desenvolvimento do sistema RT-IoT.

⁴⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/53285.html>. A análise da norma foi feita antes da publicação.

3.6.3.5 Internet das Coisas - Integração de IoT e *Blockchain*: casos de uso

A norma **JTC1-SC41/220A/DTR - ISO/IEC TR 30176 ED1**⁴¹ identifica e coleta casos de uso para a integração do DLT / *Blockchain* dentro Sistemas, aplicativos e / ou serviços IoT. Na tabela 27, há a descrição dos principais casos de uso abordados pela norma.

Tabela 27 - Descrição dos principais casos de uso do *Blockchain* e IoT

Casos de Uso	Descrição
Rastreamento de produtos agrícolas	O rastreamento de produtos agrícolas fornece o recurso de gravações digitais para rastrear todo o processo ao qual bens agrícolas são expostos, desde a semeadura, cultivo, crescimento, colheita, armazenamento, transporte, etc. até os consumidores finais.
Serviços financeiros para piscicultura	Serviços financeiros, como seguros e empréstimos, são concedidos aos piscicultores por meio de uma parceria entre instituições financeiras e empresas de serviços operados com a Internet das Coisas. A modelo de colaborações empresariais é uma alternativa inovadora de serviços financeiros oferecidos aos piscicultores, viabilizada pelo uso da Internet das coisas e tecnologias de <i>blockchain</i> .
Serviços para hipoteca de bens móveis	Essa utilização exemplifica como integrar o sistema de IoT com dispositivos autorizados e plataformas integradas com <i>blockchain</i> para monitorar a hipoteca de depósitos, além de fornecer dados autorizados aos bancos para que eles possam avaliar o verdadeiro valor dos bens no depósito. Após a avaliação, o banco determina se prestará serviços financeiros (como empréstimos) às empresas.
Comercialização de energia distribuível	A infraestrutura de comercialização baseada em <i>blockchain</i> oferece uma plataforma descentralizada que permite uma comercialização de energia de pessoa para pessoa, entre consumidores e produtores de maneira segura. A privacidade de identidade e a segurança da transação são maiores em uma plataforma descentralizada quando comparada ao sistema tradicional no qual a transação é feita por meio de uma plataforma central, vulnerável às ameaças de segurança.
Serviço de pagamento de estacionamento automatizado	O pagamento automatizado de estacionamento é uma nova maneira para os usuários pagarem a taxa de estacionamento sem o fazerem manualmente, com dinheiro ou cartão de crédito. Esse caso exemplifica a ideia central sobre a automatização do pagamento do estacionamento sem detectar ou usar um dispositivo e como este serviço pode ser realizado.

Além disso, a norma apresenta alguns frameworks que sistematizam o uso de IoT. A Figura 43 apresenta uma sistematização do IoT na agricultura, mostrando a importância do uso do IoT e as relações entre usuários, aparelhos e redes e como o fluxo de informação ocorre para beneficiar o produto da agricultura.

⁴¹ Atualizações e informações da norma podem ser encontradas em:

https://www.iec.ch/ords/f?p=103:30:506700163068045:::FSP_ORG_ID,FSP_LANG_ID:20486,25

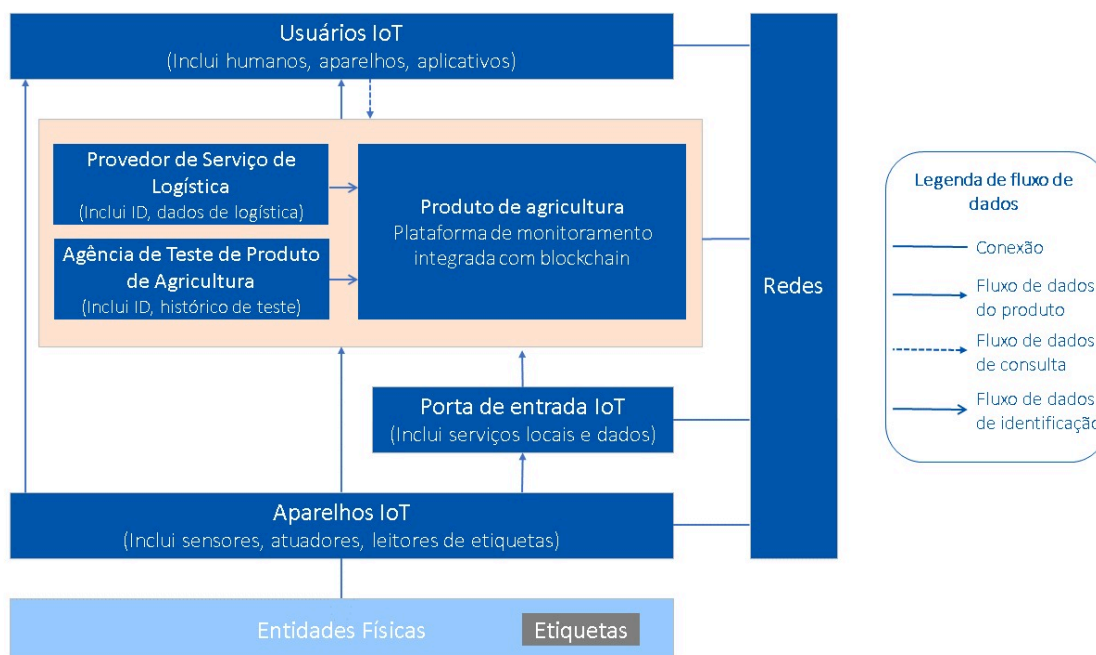


Figura 43 - Exemplificação do uso de IoT na área agrícola

3.6.3.6 Visão geral e requisitos gerais do sistema IoT para o monitoramento ecológico do ambiente (JTC1-SC41/215/NP)

A norma **TC1-SC41/215/NP - PNW JTC1-SC41-215 ED1**⁴² especifica o sistema da Internet das Coisas para monitoramento do ambiente ecológico em relação à:

- Infraestrutura do sistema e entidades do sistema do sistema IoT para ambiente ecológico monitoramento de entidades naturais, como ar, água, solo, criaturas vivas; e
- Os requisitos gerais do sistema IoT para monitoramento do ambiente ecológico.

O uso de tecnologias IoT para monitoramento de ambiente abordado na norma traz as seguintes vantagens no monitoramento e gerenciamento de ecossistemas:

- I. Transformação de uma estação de monitoramento de ponto único em um monitoramento de rede multiponto por meio de rede e compartilhamento de dados / informações;
- II. Garantir as observações e medições em tempo real e dinâmicas, adaptando-se efetivamente à complexidade e variabilidade dos objetos monitorados em comparação com as medições feitas manualmente e / ou por sistemas legados;
- III. Tomar ações proativas em relação a eventos ecológicos com antecedência, em vez de reagir depois que os eventos ocorreram;
- IV. Realizar uma gestão multinível e unificada das estações e sistemas de observação;

⁴² Atualizações e informações da norma podem ser encontradas em:

https://www.iec.ch/ords/f?p=103:30:506700163068045:::FSP_ORG_ID,FSP_LANG_ID:20486,25

- V. Observação de todo o ecossistema, em vez de áreas ou regiões geograficamente divididas (ou seja, usando uma observação de ponto único) em ambas as perspectivas macro e micro; e
- VI. Analisar as relações entre as entidades ecológicas para garantir o ecossistema sustentável e seu desenvolvimento.

A Tabela 28 resume as tendências do grupo de Internet das Coisas e Gêmeo Digital (ISO/IEC JTC 1/SC 41). A Figura 44 sumariza a evolução do grupo de Internet das Coisas e Gêmeo Digital (ISO/IEC JTC 1/SC 41).

Tabela 28 - Normas referentes a tendências do grupo de IoT e Gêmeo Digital

Norma	Escopo
ISO NP 21823-3:2017	Internet das coisas e afins tecnologias - Interoperabilidade para Sistemas de Internet das Coisas - Parte 3: interoperabilidade semântica
JTC 1-SC41/58/NP	Requisitos de compatibilidade e modelo para dispositivos em sistemas industriais de IoT
JTC1-SC41/67/NP	Internet das coisas (IoT) - estrutura de IoT em tempo real
JTC1-SC41/142/NP	Internet das coisas (IoT) - Interface de programação de aplicativos de confiança genérica para dispositivos IoT industriais
JTC1-SC41/148/NP	Internet das coisas (IoT) - aplicativos de IoT para sistema de etiqueta eletrônica (ELS)
JTC1-SC41/172/NP	Princípios de confiabilidade
JTC1-SC41/191/CD	Sistema IoT socializado que se assemelha à dinâmica de interação social humana
JTC1-SC41/196A/NP	Formato, valor e codificação de dados
JTC1-SC41/198/CD	Integração de IoT e DLT / <i>Blockchain</i> : casos de uso
JTC1-SC41/200/NP	Plataforma de troca de dados para serviços de IoT - Parte 2: Transporte
JTC1-SC41/213/NP	Princípios gerais do indicador de avaliação para sistemas IoT
JTC1-SC41/215/NP	Visão geral e requisitos gerais do sistema IoT para fins ecológicos de monitoramento do ambiente

IoT e Gêmeos Digitais (DT)

ISO/IEC JTC1/SC41

Escopo

Servir como foco e proponente do programa de padronização de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas.

Fornecer orientação para o desenvolvimento de aplicativos relacionados à Internet das Coisas e Digital Twin

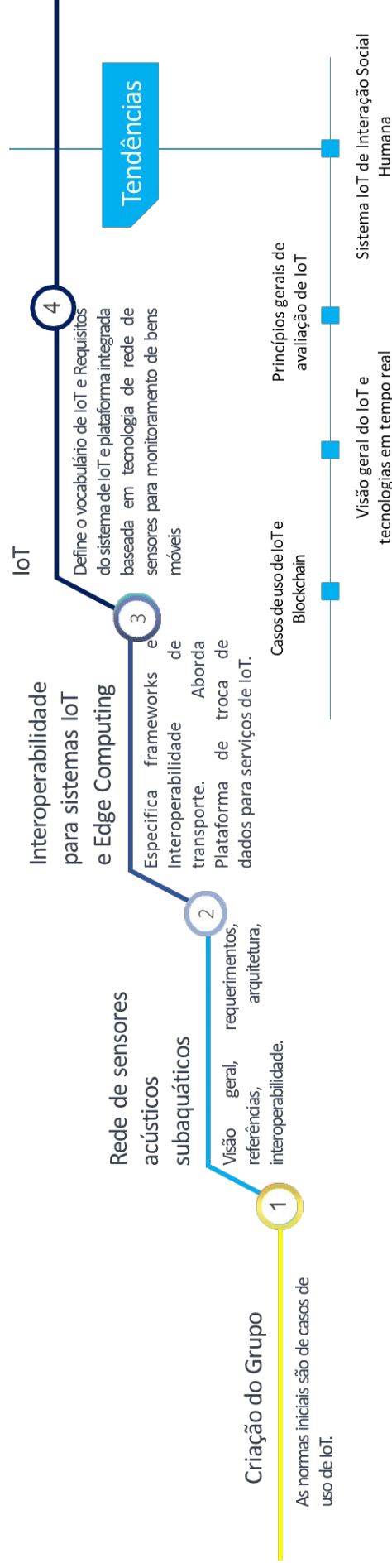


Figura 44 - Consolidação da análise do Grupo de Internet das Coisas e Gêmeo Digital

3.6.4 Relevância

3.6.4.1 IoT

De acordo com a IEC (IEC, 2014), *Internet of Things: Wireless Sensor Networks*, smart grid, casas inteligentes, redes de água inteligente, transporte inteligente são sistemas de infraestrutura que conectam o mundo. O elo mais comum de tais sistemas geralmente está associado a um único conceito, a internet das coisas (IoT), por meio do uso de sensores, toda a infraestrutura física é intimamente relacionada às tecnologias de informação e comunicação. Complementarmente, o monitoramento inteligente e o gerenciamento podem ser alcançados por meio do uso de dispositivos incorporados em rede. Em um sistema dinâmico tão sofisticado, os dispositivos são interconectados a fim de transmitir informações de medição úteis e instruções de controle por meio de redes de sensores distribuídas.

Conforme a Mind Commerce (MIND COMMERCE, 2021), as aplicações de IoT podem cobrir áreas específicas de integração de tecnologia de TIC, incluindo:

- **ERP em IoT:** Inclui soluções ERP habilitadas para IoT para conectar pessoas, processos, dados e coisas.
- **Geo IoT:** Inclui presença e localização junto com tecnologias IoT para aplicativos e serviços avançados
- **IoT industrial (IIoT):** inclui IoT na manufatura, Indústria 4.0, impressão 3D, robótica, teleoperação e muito mais
- **Chipsets de IoT:** Inclui avanços na indústria de semicondutores em apoio à IoT
- **IoT e computação contextual:** Inclui convergência de IoT com tecnologias de computação
- **IoT Operating Systems (OS):** Inclui sistemas operacionais em tempo real (RTOS) como um componente crítico para construir sistemas embarcados abrangentes para soluções de IoT
- **Virtualização de função de rede em IoT:** Inclui infraestrutura virtualizada em suporte de IoT.

Além disso, IoT pode ser aplicada em diferentes áreas (MIND COMMERCE, 2021). Entre elas, destacam-se Smart Buildings; Smart Workplace; Smart home; Smart Citie; e, IoT na Indústria, como exposto na Tabela 29.

Tabela 29 - Aplicações da Internet das Coisas

Smart Buildings	IoT em edifícios inteligentes, perspectivas e previsões do mercado Dados de IoT em tempo real em cidades inteligentes, edifícios e residências Edifícios inteligentes: IoT em cidades inteligentes, imóveis comerciais e residências. IoT em infraestrutura, cidades e edifícios inteligentes: análise de mercado e previsões. Mercado do Sistema de Gerenciamento do Local de Trabalho Integrado: Plataformas, software e soluções IWMS Perspectivas e previsões do mercado
Smart Workplace	Dispositivos, aplicativos e serviços inteligentes no local de trabalho Mercado de local de trabalho inteligente em verticais da indústria Mercado do Sistema de Gerenciamento do Local de Trabalho Integrado: Plataformas, software e soluções, perspectivas e previsões do mercado
Smart Home	Casa conectada e aparelhos inteligentes Dados de IoT em tempo real em cidades inteligentes, edifícios e residências Assistentes pessoais virtuais (VPA): o mercado de IA, consultores inteligentes e agentes inteligentes
Smart Cities	Cidades inteligentes: perspectivas e previsões globais Dados de IoT em tempo real em cidades inteligentes, edifícios e residências Edifícios inteligentes: IoT em cidades inteligentes, imóveis comerciais e residências IoT em infraestrutura, cidades e edifícios inteligentes: análise de mercado e previsões Motivadores, tecnologias, empresas e soluções de negócios da cidade inteligente: Perspectivas e previsões globais Urban ICT: Smart Cities, 5G, Industrial IoT e <i>Big Data</i> em análises e previsões do mercado de manufatura Multi-access Edge Computing (MEC) e dados em tempo real em cidades inteligentes, edifícios e residências
IoT in Industry	IoT em veículos conectados e transporte pessoal IoT na agricultura: perspectivas e previsões do mercado IoT em Saúde: Perspectivas de Mercado e Previsões Máquinas inteligentes em IoT empresarial e industrial: Perspectivas e previsões do mercado IoT industrial, análise de dados e inteligência artificial na manufatura conectada Smart Food Marketplace: IA, análise de dados e IoT na produção, distribuição e vendas de alimentos Mercado industrial de última geração: Teleoperação, manufatura conectada e soluções digitais duplas Internet das coisas industrial (IIoT) e manufatura conectada: análise das principais tecnologias da IIoT, aplicativos, soluções, perspectivas de mercado e previsões Internet das coisas (IoT) nas verticais do setor: IoT nos principais setores e perspectivas para serviços gerenciados e serviços de dados

As previsões do mercado de Internet das Coisas (IoT) mostram que a IoT já está causando um impacto global economia. De acordo com o white paper da IEC (IEC, 2020), intitulado “IoT 2020: Smart and secure IoT platform” que aborda as estimativas do impacto econômico durante os próximos cinco a dez anos variam ligeiramente, IDC estima US \$ 1,7 trilhão em 2020, Gartner vê um benefício de US \$ 2 trilhões nessa época, e a McKinsey prevê um crescimento de US \$ 4 trilhões para US \$ 11 trilhões até 2025. Considerando isso, há um consenso de que o impacto das tecnologias IoT é substancial e crescente.

Com base no BNDES, os países apresentam 4 perfis em relação ao IoT (BNDES, 2017a):

1. Liderança global em IoT: foco tanto no desenvolvimento quanto na implantação de IoT. Destacam-se países como Estados Unidos, Coréia do Sul e Reino Unido.

2. Liderança em verticais específicas: os países focam em determinadas verticais de IoT que estão alinhadas com suas políticas. Alemanha, Japão e China utilizam essa estratégia.
3. Aumento da competitividade: países que tem como objetivo o aumento da competitividade da indústria local, a geração de empregos e melhoria na qualidade de vida da população com base no desenvolvimento da IoT. União Europeia, Suécia e Rússia adotaram essa estratégia
4. Melhoria de qualidade de vida: países que adotaram o desenvolvimento de IoT para cidades inteligentes com intuito de melhorar a qualidade de vida da população. Por exemplo, pode-se citar Cingapura, Emirados Árabes e Índia.

Até 2025, IoT poderia adicionar de 4 a 11 trilhões à economia global e \$50-200 bilhões ao Brasil (BNDES, 2018, p.6). Entretanto, esse número pode ser mais expressivo se olharmos um horizonte de tempo de 10 anos. É possível que entre 2020 e 2030, a IoT deve movimentar cerca de US\$19 trilhões ao redor do mundo. Desse total, US\$860 bilhões impactarão especificamente as economias latino-americanas, sendo 40% (US\$352 bilhões) apenas no mercado brasileiro de Internet das Coisas (V2COM, 2020). Complementarmente, pesquisas indicam que o mercado brasileiro tem crescido a 20% anualmente, e o avanço pode ser mantido nos próximos anos (V2COM, 2020). Além disso, 35% das empresas brasileira fazem o uso de alguma tecnologia de IoT, e o Brasil possui 19% dos projetos de IoT da América Latina (V2COM, 2020). Em relação ao setor industrial, considerando uma base do Bytes de IoT, o Brasil já possui oferta de soluções de IoT: 116 atores com foco para indústria de base e 149, para fábricas (BNDES, 2017b) Além disso, a Finep lançou uma linha de financiamento chamada Finep IoT com novo no desenvolvimento tecnológico com base no conceito de IoT que os seguintes objetivos (FINEP, s.d.):

- Fomentar a transição tecnológica das empresas nacionais e da sociedade para ambientes produtivos e de prestação de serviços baseados em tecnologias digitais;
- Apoiar o desenvolvimento de plataformas de integração entre ambientes virtuais e físicos;
- Possibilitar a integração e adoção de tecnologias habilitadoras com intuito de conectar as diversas etapas da cadeia de valor.
- Proporcionar a otimização logística por meio do estabelecimento da integração entre fornecedores, empresas e clientes - integração horizontal da produção.
- Auxiliar a manutenção preditiva de máquinas e equipamentos e assegurar maior precisão nos procedimentos.
- Possibilitar ambientes produtivos caracterizados por comunicações instantâneas entre diferentes elos da cadeia produtiva e o desenvolvimento de sistemas de automação flexíveis que possibilitem a produção de diferentes bens em uma mesma linha de produção.

O Brasil desenvolveu o Plano Nacional de Internet das Coisas com intuito de implementar e desenvolver IoT no Brasil (BRASIL, 2019b). O Plano Nacional de internet das coisas abrange os seguintes objetivos (BRASIL, 2019c):

- I. melhorar a qualidade de vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT;
- II. promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital;
- III. incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor;
- IV. buscar parcerias com os setores público e privado para a implementação da IoT; e
- V. aumentar a integração do País no cenário internacional, por meio da participação em fóruns de padronização, da cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no País.

A Figura 45 resume as aplicações e os benefícios do uso de IoT no mundo e no Brasil

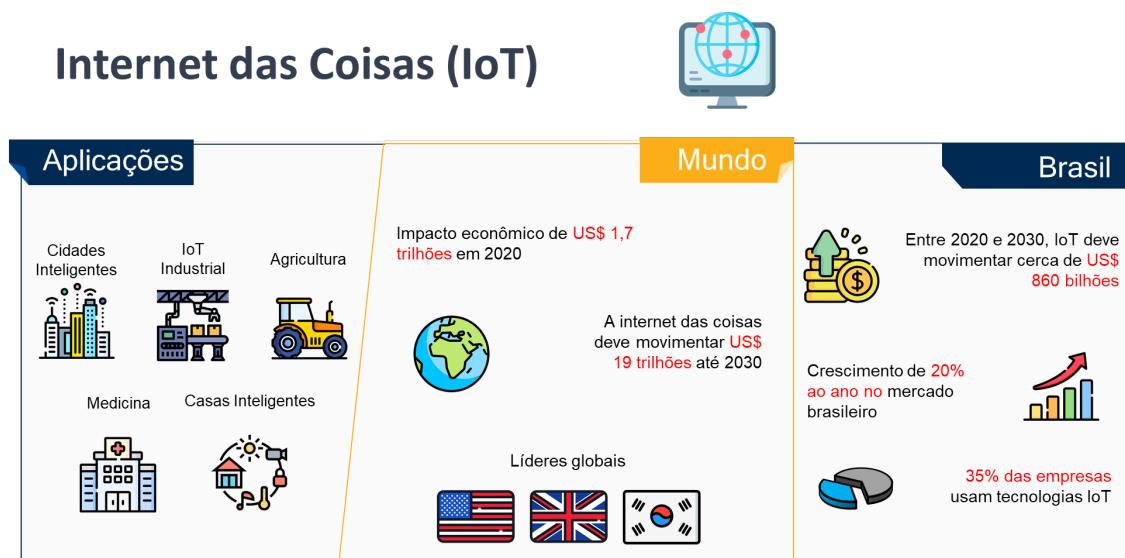


Figura 45 - Infográfico da Relevância da Internet das Coisas

3.6.4.2 Digital Twin

Digital Twin (DT) possuem aplicações desde projetos e simulações para produção até observação e controle em um ambiente operacional (MIND COMMERCE, 2021). Outrossim, DT contam com Inteligência Artificial (IA) para aprendizado baseado em máquina, análises e outros processos orientados a dados baseados em IA. Conseqüentemente, as soluções de DT são um bom exemplo do poder da Inteligência Artificial das Coisas (AIoT), pois alavancam a convergência de AI e IoT. O mercado de AIoT tem potencial para acelerar drasticamente os benefícios da transformação digital para os segmentos de mercado consumidor, empresarial, industrial e governamental. O uso do DT pode incluir:

- Internet of Things (IoT) Digital Twinning): Perspectiva de mercado para mapeamento e gerenciamento físico para virtual habilitado para IoT
- Mercado industrial de última geração: Teleoperação, manufatura conectada e soluções digitais duplas
- Convergência física e cibernética: IA, robótica em nuvem, IoT industrial e geminação virtual

Além disso, o DT possui aplicações nas mais diversas áreas (AI MULTIPLE, 2021):

- Manufatura: a fabricação conta com equipamentos de alto custo que geram grande volume de dados.
 - Desenvolvimento de produto: teste de viabilidade dos próximos produtos antes do lançamento.
 - Personalização de design: projetar várias permutações do produto para que se possa oferecer produtos e serviços personalizados aos seus clientes.
 - Melhoria de desempenho do chão de fábrica: monitorar e analisar produtos finais e verificar produtos defeituosos ou têm desempenho inferior ao pretendido.
 - Manutenção preditiva: prever tempos de inatividade potenciais das máquinas, de modo que as empresas minimizem as atividades de manutenção sem valor agregado e melhorem a eficiência geral das máquinas.
 - Aeroespacial: os engenheiros podem usar análises preditivas para prever qualquer problema futuro envolvendo a fuselagem, motor ou outros componentes para garantir a segurança das pessoas a bordo.
 - Automotivo: criação do modelo virtual de um veículo conectado com simulações e análises da fase de produção.
 - Desenvolvimento de carro autônomo: Os carros autônomos contêm vários sensores que coletam dados sobre o próprio veículo e o ambiente do carro. Devido às questões de responsabilidade que cercam os veículos autônomos, criar um gêmeo digital de um carro e testar todos os aspectos dos veículos está ajudando as empresas a garantir que danos e ferimentos inesperados sejam minimizados. Algumas aplicações dos gêmeos digitais na indústria automotiva são testes de estradas e manutenção de veículos.
- Assistência médica: ajudar os provedores de saúde a virtualizar a experiência de saúde para otimizar o atendimento ao paciente, o custo e o desempenho.

- Melhorar a eficiência operacional das operações de saúde: A criação de um DT de um hospital com modelos de atendimento que ajudam os profissionais de saúde a examinar o desempenho operacional da organização.
- Melhorando o atendimento personalizado: modelar o código do genoma, as características fisiológicas e o estilo de vida dos pacientes, para que as empresas de saúde possam fornecer cuidados personalizados, como medicamentos exclusivos para cada paciente.
- Supply chain
 - Previsão do desempenho dos materiais de embalagem: a embalagem do produto pode ser virtualizada e testada quanto a erros antes de ser embalada.
 - Melhorar a proteção da remessa: analisar como as diferentes condições de embalagem podem afetar a entrega do produto.
 - Otimizando o design do armazém e o desempenho operacional: teste dos layouts de depósito para que possam escolher o projeto de depósito mais eficiente para maximizar o desempenho operacional.
 - Criação de uma rede logística: projeção as rotas de distribuição e os locais de armazenamento de estoque.
- Construção: entender o desempenho de um edifício em tempo real, o que lhes permite ajustar o desempenho para otimizar a eficiência.
- Varejo e Modelagem e simulações de clientes: criação de personas do cliente para melhorar a experiência do cliente que eles oferecem.

O tamanho do mercado global de gêmeos digitais foi avaliado em US \$ 5,04 bilhões em 2020 (GRAND VIEW RESEARCH, 2021). Espera-se que se expanda a uma taxa de de 42,7% de 2021 a 2028 (GRAND VIEW RESEARCH, 2021). Infelizmente, o mercado experimentou uma queda em 2020 devido ao fechamento de locais de manufatura, por conta da pandemia de COVID-19. No entanto, devido às diversas aplicações de digital twin, o mercado está pronto para um crescimento exponencial, que deve ser acelerado pelas normas de distanciamento social, que auxilia na avaliação de desempenho de equipamentos, cria um ambiente sustentável e garante uma melhor experiência digital para clientes (GRAND VIEW RESEARCH, 2021). Além disso, associações e indústrias alemãs cria uma associação de DT (VDI BRASIL, 2021), Industrial Digital Twin Association, com o intuito de promover o uso e aplicação de um *roadmap* de DT da indústria de transformação (Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0 (INDUSTRIAL INTERNET CONSORTIUM, 2020).

No Brasil, já existem iniciativas de empresas que estão usando DT. A Petrobrás é um bom exemplo disso, visto que está desenvolvendo um projeto de DT em parceria com outras

empresas, Repsol Sinopec Brasil, AVEVA, Senai RJ e Senai Cimatec (BIP BRASIL, 2020). A Petrobras como um todo espera um grande benefício do DT: ganhos de US\$ 1,6 trilhão, redução de 40% nos investimentos (CAPEX) e 50% nas despesas (OPEX); além de ter ganhos em plataformas de US\$ 20 milhões/ano e ganhos de US\$ 3,82 milhões em 12 semanas (PETROBRAS, 2019). Além da Petrobras, outras empresas já estão utilizando DT no Brasil, e apresentando resultados positivos da sua implementação. Por exemplo, no ano de 2018, a Unilever fez testes com o DT no Brasil. Até o final de 2019, DT conseguiu economizar US\$ 2,8 milhões em custos operacionais e possibilitou um aumento de 3% na produtividade (BIP BRASIL, 2020). A Unilever pretende realizar implantação de DT em mais de 70 fábricas em parceria com a Microsoft (BIP BRASIL, 2020).

Além disso, no Brasil, alguns grupos estão trabalhando com um padrão chamado AAS: Asset Administration Shell (GOLDBACH, 2020) cujo objetivo é trocar dados relacionados a ativos entre ativos industriais e entre ativos e sistemas de orquestração de produção ou ferramentas de engenharia (ARC, 2019). Mas por que utilizar o ASSET Administration Shell? (PLATTFORM INDUSTRIE 4.0., 2019).

- Implementação do Digital Twin na Indústria 4.0;
- Estabelece cross-company interoperabilidade;
- Disponibilidade para produtos inteligentes e não inteligentes;
- Cobre o ciclo de vida completo dos produtos, dispositivos, máquinas e instalações;
- Permite o uso de cadeia de valor integrada;
- Base digital para sistemas autônomos e de IA.

A Figura 46 resume as aplicações e os benefícios do uso de DT no mundo e no Brasil.

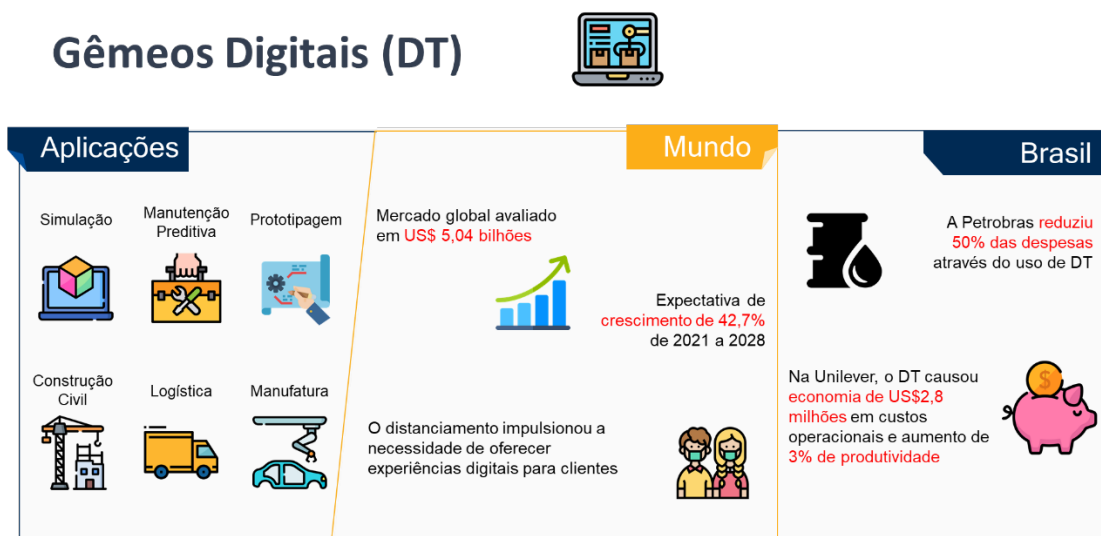


Figura 46 - Infográfico da Relevância para o Grupo de Internet das Coisas e Digital Twin – Parte 2 – Digital Twin

3.7 Grupo Dados industriais (ISO/TC184/SC4)

3.7.1 Escopo

O escopo do grupo prioritário de **Dados Industriais (ISO/TC184/SC4)** é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características, em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida desde a concepção até o descarte, juntamente com as interfaces necessárias para entregar e coletar as informações necessárias com intuito de dar suporte a qualquer processo comercial ou técnico ou serviço relacionado a esse produto de engenharia durante seu ciclo de vida.

A construção de padrões para dados industriais requer uma estrutura de alto nível para garantir a consistência e a interoperabilidade dos padrões. Os padrões desenvolvidos dentro da ISO/TC184/SC4 são baseados na premissa de que: existem semelhanças fundamentais entre as diferentes indústrias; os dados industriais podem ser considerados produtos de algum processo industrial e sujeitos a atividades generalizadas do ciclo de vida. Neste contexto, as definições mais importantes são:

- **Processo:** conjunto de atividades inter-relacionadas ou interagindo que usam entradas para entregar um resultado pretendido.
- **Requerimento:** necessidade ou expectativa declarada, geralmente implícita ou obrigatória.
- **Informação:** conhecimento sobre objetos, como fatos, eventos, coisas, processos, ou ideias, incluindo conceitos, que dentro de um determinado contexto tem um significado particular.
- **Dados:** representação re-interpretável de informações de uma maneira formalizada adequada para comunicação, interpretação ou processamento.
- **Qualidade de dados:** grau em que um conjunto de características inerentes de dados que cumprem os requisitos.
- **Gerenciamento de qualidade de dados:** atividades coordenadas para dirigir e controlar uma organização no que diz respeito à qualidade dos dados.

3.7.2 Status quo

O grupo **Dados industriais (ISO/TC184/SC4)** abrange os seguintes tópicos principais: interoperabilidade das definições de dados do produto (ISO 10303 e ISO 15926); fabricação (ISO 15531, ISO 18629, ISO 18828 e ISO 18876); visualização (ISO 14306 e ISO / PAS 17506).

Em relação à interoperabilidade das definições de dados, a norma **ISO 10303** fornece uma representação das informações do produto junto com os mecanismos e definições necessários

para permitir a troca de dados do produto. A troca é entre diferentes sistemas de computador e ambientes associados ao ciclo de vida completo do produto, incluindo projeto, fabricação, uso, manutenção e disposição final do produto. A ISO 10303-1, que foi revisada em 2021, define os princípios básicos da representação e troca de informações do produto usados na ISO 10303, especificando as características das várias séries de partes da ISO 10303 e as relações entre elas. Os tópicos que conformam a ISO 10303-1 são: declaração de escopo; visão geral; arquiteturas; estrutura; termos e definições usados; visão geral dos métodos de especificação de dados. Além disso, a série da ISO 10303 possui mais de 700 normas que podem ajudar as empresas. Por isso, é importante analisar detalhadamente a primeira norma (ISO 10303-1) que traz uma visão geral do contexto.

Também em relação à interoperabilidade das definições de dados, a norma **ISO 15926** especifica uma representação das informações associadas à engenharia, construção e operação de plantas de processo. Esta representação suporta os requisitos de informação das indústrias de processo em todas as fases do ciclo de vida de uma planta e o compartilhamento e a integração de informações entre todas as partes envolvidas no ciclo de vida da planta. Complementarmente, os itens a seguir estão dentro do escopo da ISO 15926:

- um modelo de dados conceitual genérico que suporta a representação de todos os aspectos do ciclo de vida de uma planta de processo;
- dados de referência que representam informações comuns a muitas plantas de processo e usuários;
- requisitos de escopo e informações para dados de referência adicionais;
- métodos de análise de requisitos e desenvolvimento de dados de referência;
- procedimentos para registro e manutenção de dados de referência;
- modelos para a troca de dados usados em um determinado contexto e seu mapeamento para o modelo de dados conceituais;
- métodos para o desenvolvimento de tais modelos e seu mapeamento para o modelo conceitual de dados;
- conformidade com os requisitos desta Norma.

Já, em relação à fabricação, a norma **ISO 15531-1: 2003** fornece uma visão geral de todo o padrão ISO 15531, especificando seu escopo e fornecendo uma série de definições básicas sobre as quais todo o padrão é construído de acordo com a "Teoria geral do sistema" e os conceitos definidos no dicionário APICS. Os anexos informativos fornecem uma descrição das relações entre o ISO 15531 e outras normas (especialmente as normas ISO / TC 184), bem como um esclarecimento dos conceitos de "capacidade e capacidade" conforme são usados no ISO 15531 e outras normas que se referem explicitamente ou implicitamente para a teoria do sistema. A norma **ISO 15531** aborda a modelagem de dados de gerenciamento de manufatura, como: dados de gerenciamento de recursos (modelo de recurso); recursos relacionados ao tempo (modelo de tempo); dados de gerenciamento de fluxo na manufatura (modelo de gerenciamento de fluxo). Outrossim, a norma ISO 15531 pode ser usada em qualquer aplicativo de software que trata das informações relacionadas ao gerenciamento de manufatura, como dados de gerenciamento de recursos, dados de gerenciamento de fluxo.

Consequentemente, o padrão visa facilitar a troca de informações entre aplicativos de software como ERP, software de gerenciamento de manufatura, software de gerenciamento de manutenção, software de cotação, etc.

Adicionalmente, o escopo **da ISO 18629-1** é o fornecimento de uma visão geral de toda a ISO 18629 e dos principais princípios básicos da Linguagem de Especificação de Processo (PSL). A ISO 18629-1 também especifica as características das várias séries de peças na ISO 18629 e as relações entre elas.

Os aspectos a seguir estão dentro do escopo da ISO 18629-1:

- visão geral da ISO 18629 e dos princípios básicos usados;
- estrutura da ISO 18629 e relações entre a série de partes das quais esta norma é composta;
- definições de termos usados em toda a ISO 18629;
- critérios de conformidade para aplicativos relacionados ao processo;
- critérios de conformidade para outras ontologias;
- critérios de conformidade para partes da ISO 18629.

O escopo desta parte da ISO 18629 inclui o fornecimento de explicações, abordando os seguintes aspectos:

- Antecedentes para o desenvolvimento da ISO 18629;
- Necessidade de semântica;
- Interoperabilidade;
- Arquitetura do PSL.

A norma **ISO/TR 18828-1:2018** descreve o framework da série ISO 18828 no planejamento de produção contínuo. A norma ISO/TR 18828-1:2018 inclui os seguintes aspectos:

- visão geral do framework da série ISO 18828
- descrição de cada parte
- aspectos inter-relacionais e aplicação do framework.

No entanto, é importante entender quais são as normas da ISO 18828, a Figura 47 consolida os principais tópicos da norma.

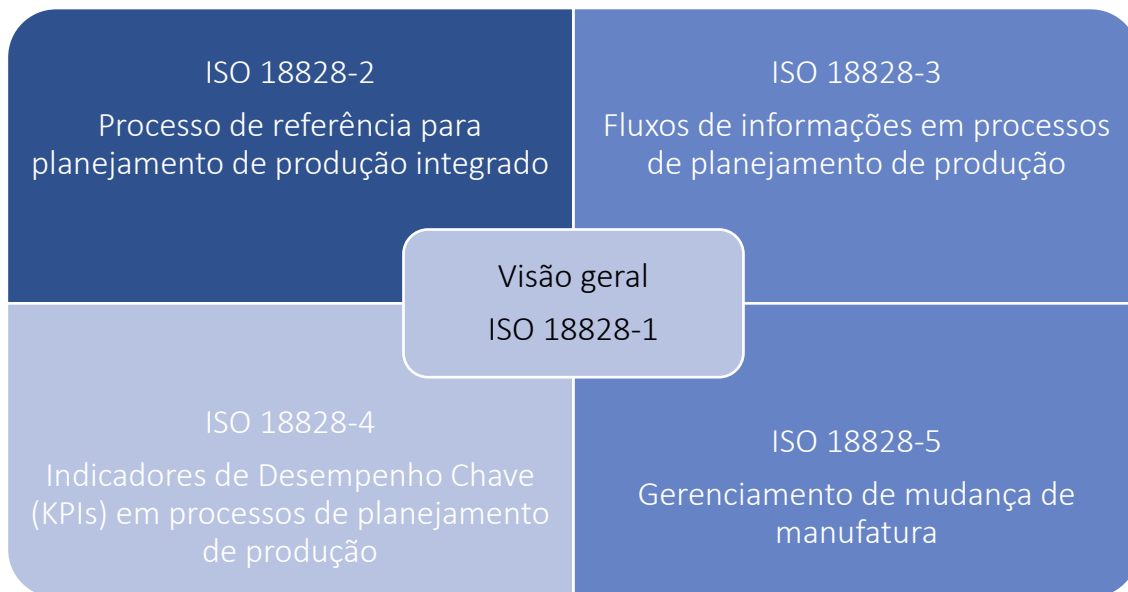


Figura 47 - Composição da Série 18228

Em relação à segunda parte da ISO 18828 (**ISO 18828-2: 2016**), a norma descreve um processo de planejamento de referência para o planejamento de produção contínuo. O escopo do processo de referência discutido concentra-se no planejamento de sistemas de produção, como produção para estoque ou montagem sob pedido. A análise das atividades do processo foi limitada àquelas dentro do planejamento da produção. Os seguintes aspectos estão dentro do escopo da ISO 18828-2: 2016:

- visão geral do processo de planejamento de referência;
- princípios básicos do modelo de processo;
- descrição de cada nível identificado dentro do processo de planejamento de referência para o planejamento da produção;
- estrutura de atividades e relações dentro de cada disciplina de planejamento;
- dependências de atividades interdisciplinares.

A terceira parte da série ISO 18828 (**ISO 18828-3: 2017**) descreve os fluxos de informações identificados para cada disciplina de planejamento dentro do planejamento da produção, de acordo com a ISO 18828-2. Os seguintes aspectos estão no escopo da ISO 18828-3: 2017:

- visão geral dos principais fluxos de informações dentro do processo de planejamento de referência;
- padrão básico para descrever os principais fluxos de informação;
- descrição detalhada de cada fluxo de informação principal;
- estrutura de notação dos principais objetos de fluxos de informação;
- descrições detalhadas para cada estado do objeto de informação;
- proposta de checklists para benchmarking de objetos de informação.

A quarta parte da ISO 18828 (**ISO 18828-4: 2018**) especifica um conjunto de indicadores-chave de desempenho no planejamento da produção, que permite a comparação e o monitoramento do processo de planejamento da produção em uma estrutura padronizada. Em uma primeira etapa, a utilização dos KPIs é elaborada de forma a organizar os indicadores em um sistema multinível levando em consideração diferentes faixas do processo de planejamento. Este desenvolvimento de um sistema multinível representa o núcleo da ISO 18828-4: 2018.

Na quinta parte, a norma **ISO 18828-5: 2019** especifica uma descrição formal dos processos de gerenciamento de mudanças de manufatura (MCM) para fornecer uma solução organizacional e técnica para o mapeamento abrangente e processamento de mudanças entre o planejamento de produção e as operações. O objetivo da ISO 18828-5: 2019 é capturar e rastrear uniformemente as medidas de mudança para prever e coordenar as capacidades necessárias para os processos de mudança nos departamentos de planejamento e produção. Complementarmente, a ISO 18828-5: 2019 apresenta uma visão orientada a dados para implementação de MCM. O aspecto mais importante da visão orientada a dados é que o elemento central de mudança está vinculado aos objetos da fábrica digital (ou seja, o processo, o produto e o recurso). A base para o MCM e as diferentes visões apresentadas neste documento são os processos de planejamento da produção. A ISO / TR 18828-1 oferece uma visão geral da série ISO 18828 e vincula o MCM às outras partes da ISO 18828, com foco nos processos de planejamento da produção, bem como fluxos de informações e indicadores-chave de desempenho. Os seguintes aspectos são cobertos na ISO 18828-5: 2019:

- processos de MCM;
- funções em MCM;
- visão orientada a dados do MCM;
- fluxo de trabalho de MCM.

Além disso, é muito importante entender as interrelações das diferentes partes da série ISO 18828 (Figura 48) e como o contexto do ciclo de vida e os domínios podem ajudar as empresas (Figura 49).

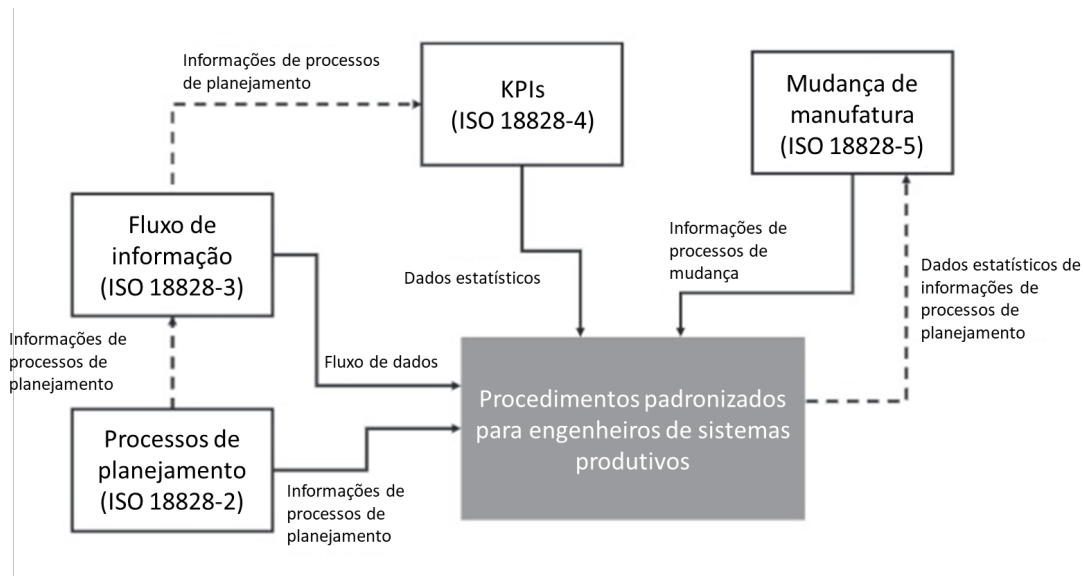


Figura 48 - Interrelação das diferentes partes da série ISO 18828

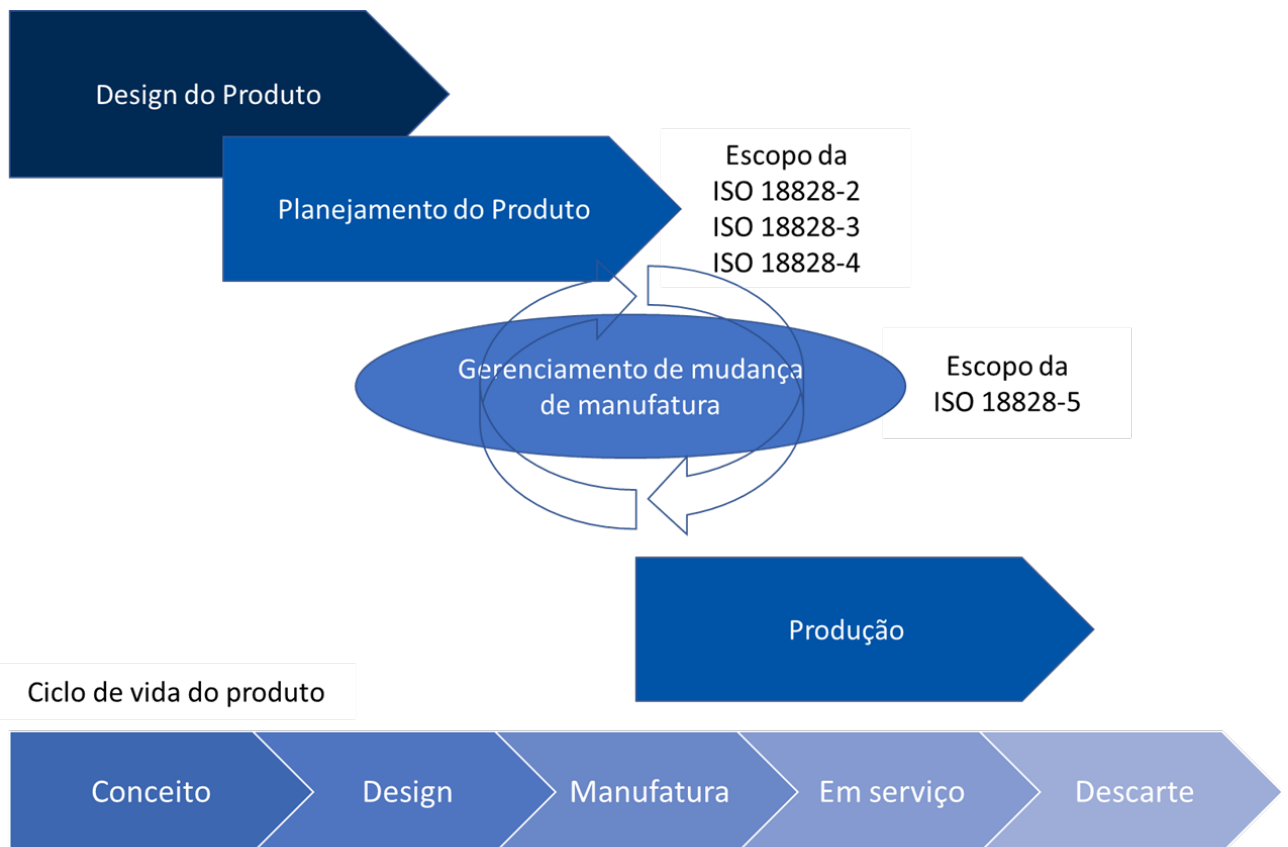


Figura 49 - Ciclo de vida das partes da série ISO 18828

Também em relação à fabricação, a norma **ISO/TS 18876-1: 2003** estabelece arquitetura e metodologia para integração de dados industriais para troca, acesso e compartilhamento. Mais especificamente, as seguintes atividades são suportadas pela ISO/TS 18876-1: 2003:

- integração de dados que podem ser de diferentes fontes ou contextos, descritos por diferentes modelos ou definidos em diferentes linguagens de modelagem;
- compartilhamento de dados entre aplicativos por meio de arquiteturas de integração de sistemas;
- resolução de conflitos entre modelos desenvolvidos com objetivos diferentes;
- tradução no dados entre codificações diferentes;
- modelos de tradução entre diferentes linguagens de modelagem.

Complementarmente, a norma **ISO/TS 18876-2: 2003** especifica métodos para: criar e estender modelos de integração; avaliar e selecionar um modelo de integração que pode integrar dois ou mais modelos de aplicativo; criar um modelo de aplicativo que é um subconjunto restrito de um modelo de integração para oferecer suporte requisitos específicos de domínio de aplicativo para troca, compartilhamento ou ambos; criar uma especificação de mapeamento entre um modelo de aplicativo e um modelo de integração. O escopo da norma ISO/TS 18876-2: 2003 abrange:

- métodos independentes de linguagem de modelagem para criar e estender um modelo de integração;
- métodos para integrar um modelo de aplicativo com um modelo de integração;
- métodos independentes de linguagem de mapeamento para mapear um modelo de aplicativo para um modelo de integração;
- critérios para a seleção de linguagens de modelagem e linguagens de mapeamento que podem ser usadas dentro dos métodos especificados para integração e mapeamento.

Em relação a aplicação de impressão 3D, a norma **ISO 14306: 2017** define a sintaxe e semântica de um formato de arquivo para a visualização 3D com informações de fabricação de produtos derivadas de sistemas CAD, usando ferramentas de software de visualização que não precisam da capacidade total de um sistema CAD. De forma geral, a norma ISO 14306: 2017 foi adotada como uma capacidade de visualização 3D além da série ISO 10303.

Também em relação à impressão 3D, a norma **ISO / PAS 17506: 2012** descreve o esquema COLLADA. COLLADA é uma atividade de design COLLABorativa que define um esquema baseado em XML para permitir que aplicativos de autoria 3D troquem ativos digitais livremente sem perda de informações. Além disso, é possível que vários pacotes de software sejam combinados em cadeias de ferramentas extremamente poderosas. O objetivo da ISO / PAS 17506: 2012 é fornecer uma especificação para o esquema COLLADA em detalhes suficientes para permitir que os desenvolvedores de software criem ferramentas para processar os recursos COLLADA. Em particular, é relevante para aqueles que importam ou exportam de aplicativos de criação de conteúdo digital (DCC), aplicativos interativos 3D e cadeias de ferramentas, ferramentas de prototipagem, aplicativos de visualização em tempo real, como aqueles usados nas indústrias de videogame e cinema, e Ferramentas CAD.

Na Tabela 30, estão sumarizadas as normas mais importantes do grupo Dados Industriais (ISO/TC184/SC4).

Tabela 30 - Normas do grupo de Dados Industriais

Normas	Escopo
ISO 10303	Representação das informações do produto junto com os mecanismos e definições necessários para permitir a troca de dados do produto
ISO 15926	Representação das informações associadas à engenharia, construção e operação de plantas de processo
ISO 15531-1: 2003	Visão geral de todo o padrão ISO 15531, especificando seu escopo e fornecendo uma série de definições básicas.
ISO 18629-1	Visão geral de toda a ISO 18629 e dos principais princípios básicos da Linguagem de Especificação de Processo (PSL).
ISO/TR 18828-1:2018 ISO 18828-2: 2016 ISO 18828-3: 2017 ISO 18828-4: 2018 ISO 18828-5: 2019	Parte 1 - Framework da série ISO 18828 no planejamento de produção contínuo. Parte 2 - Processo de planejamento de referência para o planejamento de produção contínuo. Parte 3 – Descreve os fluxos de informações identificados para cada disciplina de planejamento dentro do planejamento da produção Parte 4 - Especifica um conjunto de indicadores-chave de desempenho no planejamento da produção Parte 5 - Especifica uma descrição formal dos processos de gerenciamento de mudanças de manufatura
ISO/TS 18876-1: 2003 ISO/TS 18876-2: 2003	Estabelece uma arquitetura e metodologia para integração de dados industriais para troca, acesso e compartilhamento
ISO 14306: 2017	Define a sintaxe e semântica de um formato de arquivo para a visualização 3D
ISO / PAS 17506: 2012	Descreve o esquema COLLADA

3.7.3 Mapa mental de relação com outros grupos

Como forma de complementar a análise do grupo prioritário, a Figura 50 apresenta um mapa mental de relação do grupo de Dados Industriais com outros grupos. Os grupos que aparecem à direita na figura, em azul claro, são os grupos prioritários que possuem fatores em comum com o grupo “Dados Industriais”. Destaca-se o grupo *Machine learning* para Redes do Futuro, que permite a interpretação coerente dos dados industriais e possibilita a construção de conhecimento com base nesses dados.

- **Robótica** - O escopo do grupo prioritário de Robótica é a Padronização no campo de robótica, excluindo brinquedos e aplicações militares;
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC e em cooperação com outros comitês técnicos da ISO e IEC;
- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, co-existência e avaliação de desempenho;

- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais - Segurança de rede e sistema;
- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção;
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo prioritário tem intuito de fornecer orientação entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin;
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas 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;
- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial (IA) é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA;
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.

Os grupos que estão à esquerda, em amarelo, são os grupos não listados como prioritários, mas que possuem interconexões com o grupo em destaque, são estes:

- **Dispositivos e integração em sistemas empresariais:** Padrões especificando integração de dispositivos com sistemas de automação industrial. Os modelos desenvolvidos nessas normas tratam das propriedades, classificação, seleção, configuração, comissionamento, monitoramento e diagnósticos básicos do dispositivo. Integração de sistemas de automação industrial com sistemas corporativos.
- **Processos, elementos de dados e documentos no comércio, indústria e administração:** Padronização e registro de negócios e processos administrativos e dados de suporte usados para o intercâmbio de informações entre e dentro de organizações individuais e suporte para atividades de padronização no campo de dados industriais.

- **Blockchain e tecnologias distribuídas de registro:** Padronização de tecnologias de *blockchain* e tecnologias de razão distribuída.
- **Manufatura Inteligente:** Fornecer coordenação e aconselhamento no domínio da Manufatura Inteligente para harmonizar e avançar as atividades de Manufatura Inteligente na IEC, outros SDOs e Consórcios de acordo com a cláusula 2 em AC / 22/2017 substituída pela AC / 17/2018.
- **Medição, controle e automação de processos industriais:** Padrões para sistemas e elementos usados para medição, controle e automação de processos industriais. Padronização que afeta a integração de componentes e funções em tais sistemas, incluindo aspectos de proteção e segurança.
- **Engenharia de software e sistemas:** Padronização de processos, ferramentas de suporte e tecnologias de suporte à engenharia de produtos e sistemas de software.
- **Tecnologia da informação:** Padronização na área de tecnologia da informação.
- **Gerenciamento e intercâmbio de dados:** Padrões para gerenciamento de dados dentro e entre ambientes de sistemas de informação locais e distribuídos. SC 32 fornece tecnologias capacitadoras para promover a harmonização dos recursos de gerenciamento de dados em áreas específicas do setor.
- **Técnicas de identificação automática e captura de dados:** Padronização de formatos de dados, sintaxe de dados, estruturas de dados, codificação de dados e tecnologias para o processo de identificação automática e captura de dados e de dispositivos associados utilizados em aplicativos interindustriais e intercâmbios de negócios internacionais e para aplicativos móveis.

Já em vermelho, acima e abaixo dos grupos, se apresentam os principais conceitos conectados à transformação digital na Indústria, que também estão interconectados com os Dados Industriais.

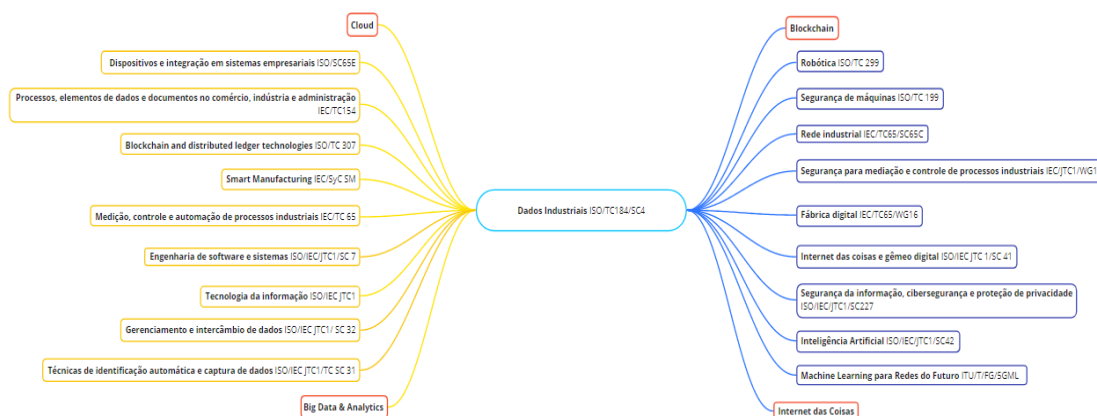


Figura 50 - Mapa mental de relação do grupo de Dados Industriais com outros grupos

3.7.4 Tendências

3.7.4.1 Framework de Digital Twin na manufatura (ISO 23247)

A **série ISO 23247** define uma estrutura para apoiar a criação de Digital Twins 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:

- I. **Parte 1: Visão geral e princípios gerais:** Princípios e requisitos gerais para o desenvolvimento de gêmeos digitais na manufatura (no estágio 50,20⁴³);
- II. **Parte 2: Arquitetura de referência:** Arquitetura de referência com vistas funcionais (no estágio 60,00 – em publicação⁴⁴);
- III. **Parte 3: Representação digital de elementos de manufatura:** Lista de atributos de informações básicas para os elementos de manufatura observáveis;⁴⁵
- IV. **Parte 4: Troca de informações:** Requisitos técnicos para troca de informações entre entidades dentro da arquitetura de referência⁴⁶.

A estrutura é direcionada a todos os tipos de manufatura, incluindo manufatura discreta e contínua de peças, conjuntos e materiais. O tipo real de manufatura suportado por uma implementação particular depende dos padrões e tecnologias disponíveis para modelar os elementos de manufatura observáveis. Em relação aos elementos de visualização de Digital

⁴³ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/75066.html>

⁴⁴ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78743.html>. A norma foi avaliada antes de agosto, houve alteração para publicação em 14 de agosto de 2021.

⁴⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78743.html>. A norma foi avaliada antes de agosto, houve alteração para publicação em 14 de agosto de 2021.

⁴⁶ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78743.html>. A norma foi avaliada antes de agosto, houve alteração para publicação em 14 de agosto de 2021.

Twins, a **ISO 24464**⁴⁷ complementa e articula os elementos de dados necessários para a visualização humana dos dados de design do produto do ponto de vista do gêmeo digital.

3.7.4.2 Qualidade de dados e da informação (ISO 8000)

Os dados digitais agregam valor ao aprimorar todos os aspectos do desempenho organizacional, incluindo:

- eficácia e eficiência operacional;
- segurança;
- reputação junto aos clientes e ao público em geral;
- conformidade com os regulamentos legais;
- custos do consumidor, receitas e preços das ações.

Portanto, é essencial investir na qualidade dos dados e da informação, a influência no desempenho origina-se do fato de os dados serem a representação formalizada da informação; essas informações permitem que as organizações tomem decisões confiáveis. Essa tomada de decisão pode ser realizada por seres humanos diretamente e também por processamento automatizado de dados, incluindo sistemas de inteligência artificial.

Assim, o seguinte está no escopo da **ISO/DIS 8000-64** (que está no estágio 40,20⁴⁸):

- indicadores de avaliação dos produtos de processamento de dados (conforme especificado pela ISO 8000-61) e, portanto, permitem a classificação do desempenho do processo, um atributo do processo especificado pela ISO/IEC 33020;
- o papel desempenhado por cada produto de trabalho nos processos de gestão de operações de manufatura;
- a conexão de cada produto de trabalho com os resultados dos processos de gestão de operações de manufatura.

Além do escopo claramente definido pela norma, ao implementar partes da **série ISO 8000**, uma organização obtém os seguintes benefícios:

- estabelece bases confiáveis para a transformação digital;
- reconhece como os dados em formato digital se tornaram uma classe de ativos fundamental em que as organizações contam para entregar valor;
- garante a confiabilidade dos dados e informações com base em evidências para todas as partes interessadas;
- cria dados portáteis que protejam contra a perda de propriedade intelectual e que sejam reutilizáveis em toda a organização e aplicativos;

⁴⁷ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78836.html>

⁴⁸ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/80752.html>

- alcança a rastreabilidade dos dados de volta às fontes originais;
- garante que todas as partes interessadas trabalhem com um entendimento comum dos requisitos de dados explícitos.

Ademais, a ISO 8000 está passando por um desenvolvimento ativo em várias partes, fortalecendo e refinando várias dimensões do padrão, incluindo as seguintes partes:

- **Parte 51: Governança de dados:** troca de declarações de política de dados (que está no estágio 30,20⁴⁹)
- **Parte 65: Gestão da qualidade dos dados:** questionário de medição do processo (publicada em 2020⁵⁰);
- **Parte 66: Gerenciamento de qualidade de dados:** indicadores de avaliação para processamento de dados em operações de manufatura (estágio 60,00⁵¹);
- **Parte 81: Avaliação da qualidade dos dados:** Criação de perfil (publicada em maio de 2021⁵²);
- **Parte 82: Avaliação da qualidade dos dados:** Criando regras de dados (estágio 30,99⁵³);
- **Parte 110: Dados principais:** Troca de dados característicos: sintaxe, codificação semântica e conformidade com a especificação de dados (publicado em 2009 e no estágio 50,20⁵⁴).

Além das partes mencionais das ISO 8000 que versam sobre o assunto, a **ISO 23952** - Estrutura de informações de qualidade (QIF) - abrange um modelo integrado de informações de qualidade de manufatura (publicada em 2020⁵⁵). Há uma Estrutura de Informação de Qualidade para a comunidade internacional por meio do processo. Além disso, o QIF fornece interoperabilidade de dados relacionados à qualidade para a identificação e enumeração do design do produto em um contexto de engenharia de qualidade.

A **ISO 15926** aborda a integração de dados de ciclo de vida para plantas de processo, incluindo instalações de produção de petróleo e gás. A ISO 15926 está focada em estruturas de dados e dados de referência com as seguintes atualizações:

- **Parte 14: modelo de dados adaptado para semântica** (estágio 30,99⁵⁶)

⁴⁹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78708.html>

⁵⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/73835.html>

⁵¹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/76390.html>.

⁵² Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77227.html>

⁵³ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78707.html>

⁵⁴ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/78501.html>

⁵⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77461.html>

⁵⁶ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/75949.html>

- **Parte 11: Metodologia para uso industrial simplificado de dados de referência** (estágio 90,92, visto que foi publicada em 2015 e será substituída por ISO/WD TS 15926-11⁵⁷)

A **ISO 17506** apresenta a especificação de esquema de ativo digital COLLADA para visualização 3D de dados industriais. A norma está sendo atualizada para o status de padrão internacional com aprimoramentos para se harmonizar com outros padrões de visualização (publicada em 2012, estágio 90,92 a ser revisada, será substituída por ISO/DIS 17506⁵⁸).

A **ISO 10303** trata sobre representação e troca de dados do produto e está passando por um desenvolvimento ativo para atualizar partes importantes do padrão e incorporar os requisitos da indústria ao protocolo de troca. As seguintes partes estão sendo desenvolvidas:

- Parte 1: Visão geral e princípios fundamentais (substituiu a versão de 1994 e está em revisão - 90,92⁵⁹)
- Parte 15: Métodos de descrição: SysML XMI para transformação XSD (publicada - estágio 60,60⁶⁰)
- Parte 16: Métodos de descrição: SysML XMI para transformação EXPRESS (publicada - estágio 60,60⁶¹)
- Parte 17: EXPRESS para transformação SysML XMI (estágio 30,99⁶²)
- Parte 59: Recurso genérico integrado: Qualidade dos dados da forma do produto (publicada em 2008 e em 2014 - estágio 90,92 – e está sendo desenvolvida a nova ISO 10303-59⁶³)
- Parte 113: Recurso de aplicativo integrado: recursos mecânicos (publicada em 2020⁶⁴)
- Parte 209: Protocolo de aplicação: análise e design multidisciplinar (publicada em 2001 e em 2014 - estágio 90,92 – em desenvolvimento a ISO/WD 10303-209⁶⁵)
- Parte 238: Protocolo de aplicação: manufatura integrada baseada em modelo (publicada em 2020⁶⁶)
- Parte 242: Protocolo de aplicativo: Engenharia 3D baseada em modelo gerenciado (publicada em 2020⁶⁷)

⁵⁷ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/57859.html>

⁵⁸ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/59902.html>

⁵⁹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/72237.html>

⁶⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77289.html>

⁶¹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77290.html>

⁶² Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/77291.html>

⁶³ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/60009.html>

⁶⁴ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/76135.html>

⁶⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/59780.html>

⁶⁶ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/72030.html>

⁶⁷ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/66654.html>

- Parte 243: Protocolo de aplicativo: Para modelagem e simulação de informações em um contexto de engenharia de sistemas colaborativos (MoSSEC) (estágio 40,99⁶⁸)

As normas mais relevantes para a qualidade de Dados Industriais estão sumarizadas na Tabela 31.

Tabela 31 - Normas referentes a tendências do grupo de Dados Industriais

Norma	Escopo
ISO 23247	Define uma estrutura para apoiar a criação de DT de elementos de manufatura
ISO 8000-61	Indicação de avaliação dos produtos de processamento de dados
ISO 8000 - Diversas partes	Diversas partes da norma estão passando por mudanças
ISO 23952	Estrutura de informações de qualidade
ISO 15926	Integração de dados de ciclo de vida
ISSO 17506	Esquema para visualização 3D de dados
ISSO 10303	Representação e troca de dados

Finalmente, a Figura 51 sumariza a evolução do Grupo Prioritário de Dados Industriais (ISO/TC184/SC4).

⁶⁸ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/72491.html>

Dados Industriais

ISO/TC 184/SC 4

Escopo

Padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características

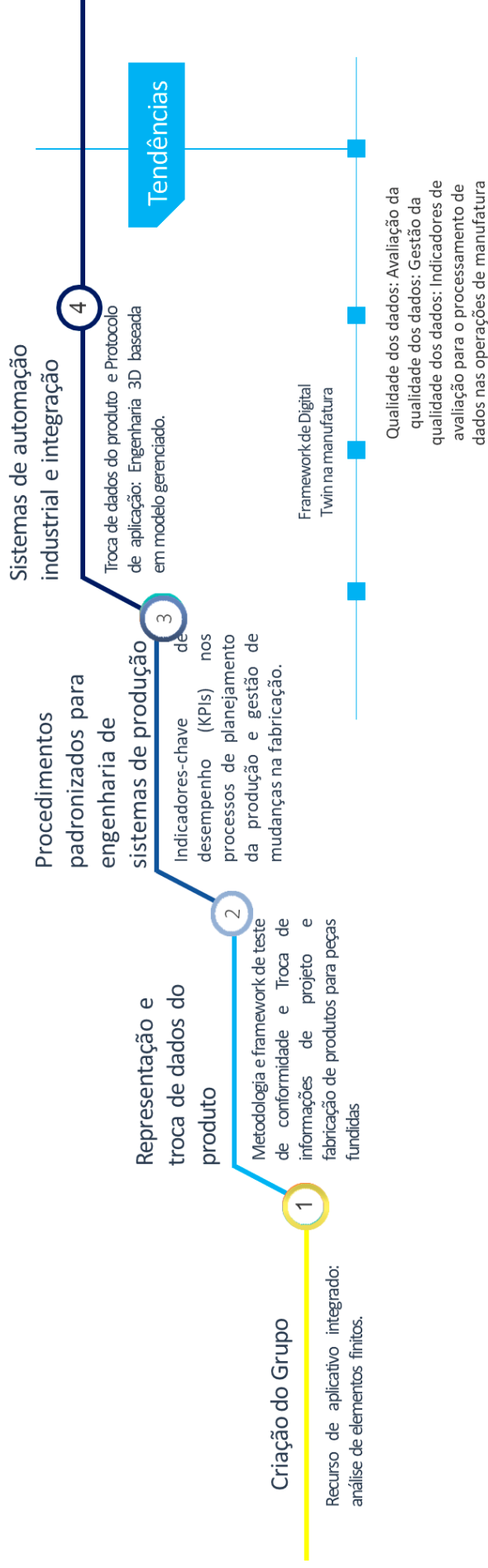


Figura 51 - Consolidação da análise do Grupo de Dados Industriais

3.7.5 Relevância

Dados industriais existem em todos os aspectos da sociedade. Desde as primeiras ideias de um produto até as fases conceituais, de manufatura e, por fim, reciclagem dos materiais usados. Dados industriais permitem que computadores criem uma representação digital dessas experiências. Eles se referem a todo conteúdo, estrutura, representação de informações usados para definir um produto de engenharia e suas características, em qualquer momento do seu ciclo de vida, desde conceito até descarte.⁶⁹

A importância de ter uma linguagem e ontologia padronizadas, como ISO15926, permite o uso de mecanismos de raciocínio e a capacidade de interconectar modelos e sistemas em todo o ciclo de vida do processo e do produto (LEE; CAMERON; HASSALL, 2019). É importante salientar que ISO15926 está em uso na maioria dos softwares CAD para o projeto e construção de plantas de processo. No entanto, as informações em uma ontologia ISO15926 raramente são transferidas das fases de projeto para a fase operacional de uma planta. Utilizar essas informações no formato ISO15926 oferece outras oportunidades como (LEE; CAMERON; HASSALL, 2019):

- A forma e a função dos componentes dentro do sistema são representadas, permitindo que os agentes de raciocínio sejam aplicados.
- A norma foi desenvolvida para representar o ativo físico ao longo do ciclo de vida do ativo.
- Fornece um protocolo de comunicação padrão para o ecossistema modelo.
- Pode ser mantido como o repositório central de todas as informações relacionadas ao ativo físico.

Informações e indicadores sobre o mercado, clientes e a própria empresa ajudam na tomada de decisões. As decisões baseadas em Dados Industriais são tomadas levando em consideração o histórico e o cenário atual da empresa. Desse modo, as decisões não são baseadas em palpites ou intuições, e sim dados reais e concretos, trazendo maior confiabilidade para as decisões e aumentando as chances de que os resultados esperados sejam atingidos.

Da mesma maneira, basear as decisões em dados concretos possibilita que os recursos disponíveis sejam alocados e utilizados da maneira mais eficiente possível, aumentando a produtividade, reduzindo desperdícios e riscos. No entanto, é importante saber que coletar Dados Industriais, organizá-los transformá-los em informações úteis requer o uso de ferramentas e tecnologia.

Os serviços de Dados Industriais podem ajudar a:

- Ganhar uma visão holística sobre todas as tarefas de uma empresa;
- Ter a capacidade de monitorar máquinas e operadores;
- Tomar decisões mais rápidas no evento de uma falha;
- Prever demandas futuras com maior exatidão;

⁶⁹ ISO. SC4 Industrial Data Framework. 2001. Disponível em: https://isotc.iso.org/livelink/livelink/fetch/-8837444/8838484/8838495/11568437/%28SC4N1167%29_SC4_Industrial_Data_Framework.pdf?nodeid=11567026&vernum=-2

- Desenvolver planos de manutenção preditiva;
- Ganhar competitividade.

Os Dados Industriais podem ser obtidos de diferentes fontes:

- Dados de sensores fornecem informações sobre temperatura, velocidade, utilização e outras informações referentes a máquinas nas linhas de produção. Essas informações são usadas para monitorar o desempenho dos equipamentos, facilitando a identificação de equipamentos com defeito e o planejamento de manutenções preditivas;
- Metadados de ativos fornecem informações sobre o maquinário, como modelo, ano de fabricação, números de serial, entre outros. Essas informações podem não parecer tão relevantes, mas são fundamentais na hora de fazer reparos, troca de equipamentos ou quando uma empresa planeja adquirir máquinas novas e deseja que elas trabalhem em conjunto com outras mais antigas;
- Sistemas de Controle Industrial (ICS) e Tecnologia Operacional (OT) fornecem a fábricas inteligentes: alertas sobre problemas, mudanças ou atualizações referentes a sistemas usados nas operações diárias. Os alertas podem ser referentes a problemas operacionais, tentativas de roubo de dados, performance dos equipamentos, entre outros. Esses sistemas ajudam a manter a empresa funcionando com alta performance e evitando falhas de segurança (DATUMIZE, 2020).

Além disso, cinco estratégias podem ser utilizadas para se aproveitar os dados industriais (LOGIQUE SISTEMAS, 2019):

1. As empresas devem saber realmente o que elas precisam medir, tendo como base os objetivos empresariais e não se restringe apenas ao chão de fábrica.
2. É essencial que os setores estejam integrados porque os dados podem ser utilizados em setores que não foram gerados para melhorar as atividades e os processos.
3. É crucial que as empresas escolham a metodologia de análise dos dados de forma adequada para que seja possível a informação para a tomada de decisão.
4. O uso de softwares que apoiem a coleta, armazenamento, tratamento e as análises é essencial para o uso de dados industriais.
5. As empresas devem investir em profissionais capacitados.

Além disso, existem outros sistemas utilizados globalmente com aplicações em diversos tipos de indústrias, como exemplificado na Tabela 32.

Tabela 32 - Aplicações dos Dados Industriais

Ferramenta	Descrição
Seeq	Um sistema analítico avançado que consegue detectar padrões e fazer previsões baseado nos dados de produção, que podem ser importados de sistemas SCADA. A Devon Energy utilizou o Seeq para agregar valor aos dados que a empresa já gerava. A empresa agora consegue prever eventos, melhorar prazos e agendamentos, acomodar pedidos novos com mais agilidade. Engenheiros e operadores também conseguem visualizar em <i>dashboards</i> dados atualizados em tempo real para tomar decisões e se adaptar a mudanças mais rapidamente (SEEQ, 2018).
ThingWorx Analytics	O produto da empresa PTC analisa Dados Industriais de diferentes bases de dados e máquinas em tempo real. Com ele, é possível utilizar aprendizado de máquina e automação para análises preditivas, detecção de anomalias e monitoramento remoto de grandes bases de dados. O sistema foi usado pela empresa Bell and Howell no planejamento de manutenção preditiva dos equipamentos. Os resultados foram redução de 60% no tempo médio de reparos redução de 30% na frequência das manutenções (PTC, 2020).
Microsoft Azure	Um pacote de programas que coletam, transformam e analisam dados em tempo real. A Pepsico utiliza o Azure Machine Learning para extrair <i>insights</i> das suas bases de dados já existentes. A partir disso, a Pepsico consegue prever a demanda de cada cliente por determinados tipos de produtos e, com isso, otimizar seu estoque e atender os pedidos da maneira mais eficiente possível. Em um teste inicial realizado em 700 lojas no Texas, o programa gerou um aumento de 40% na precisão da previsão de demandas (MICROSOFT, 2021).
Amazon Web Services (AWS)	Também funciona como um pacote de serviços equivalente ao Azure, que realizam diferentes tarefas como análise de dados em tempo real, aprendizado de máquina, previsões de demanda, otimização de processos e visualização de dados de diferentes fontes ao mesmo tempo. A AGCO migrou para a Amazon Web Services pois seu sistema próprio conseguia gerir a enorme quantidade de dados armazenada todos os dias na nuvem. Ao armazenar seus dados por meio da AWS, a AGCO: <ul style="list-style-type: none"> • Reduziu custos de armazenamento em 78%; • Dobrou a quantidade de registros que podem ser armazenados; • Diminuiu o tempo de extração de dados de até 30 segundos para 600 milissegundos (AMAZON, 2021);
SAP	SAP é conhecida pelo seu sistema ERP que auxilia as empresas a fazerem a gestão de produção, logística, estoque, remessas e contabilidade. Além disso, diversos setores utilizam o SAP como o Gás e Petróleo, hospitais, serviços, entre outros. O ERP da SAP é conhecido pela sua simplicidade, flexibilidade e constante atualização (IEBS, 2019). A empresa também tem soluções para o chão de fábrica que flexibilizam soluções e cenários. Essas soluções podem ser integradas com ERP com objetivo de enviar o planejamento de produção do sistema de ERP para o sistema MES e enviar os dados de performance da produção que estão no MES para o ERP. Consequentemente, facilitando o gerenciamento da produção, e essa integração pode ajudar também no gerenciamento de recursos, gerenciamento de qualidade, gerenciamento do estoque (TECHPLUS, s.d.a). A empresa também lançou a plataforma SAP Leonardo IoT com foco nas soluções da Indústria 4.0. A plataforma oferece interoperabilidade com a Microsoft Azure IoT Hub. Além disso, a plataforma fornece inovação e melhorias nos processos (ERP, 2019).

Sendo assim, há uma infinidade de ferramentas que podem ser usadas para análises de Dados Industriais e resultar em ganhos de produtividade para as empresas. Na Tabela 33, estão alguns exemplos de soluções desenvolvidas por empresas no Brasil.

Tabela 33 - Ferramentas utilizadas baseadas em Dados Industriais

Ferramenta / Empresa	Descrição
Fast Analytics / TOTVS	Uma solução que consolida informações disponíveis em indicadores. Com esses dados, é possível tomar decisões de maneira mais ágil e assertiva, o que trará mais competitividade para o negócio (A VOZ DA INDÚSTRIA, 2018).
BR-Plant Historian / Logique Sistemas	Coleta, armazenamento, processamento e distribuição de dados. O sistema já é utilizado em uma das plantas da Petrobras e, em 2 anos de operação, já armazenou mais de 4 bilhões de registros, mostrando que é capaz de ser utilizado em indústrias de grande porte (LOGIQUE SISTEMAS, 2018a).
BR-Collector / Logique Sistemas	Sistema que permite a padronização de informações e comunicação entre diversas fontes de Dados Industriais dentro de uma empresa. Ele coleta os dados gerados por sensores e equipamentos na linha de produção e os disponibiliza de maneira acessível. A solução já é utilizada em mais de 200 unidades industriais no Brasil (LOGIQUE SISTEMAS, 2018b).

Finalmente, a Figura 52 resume os aspectos relevantes do grupo de Dados Industriais (ISO/TC184/SC4), contendo as principais aplicações e como os dados industriais impactam as empresas no mundo e no Brasil.

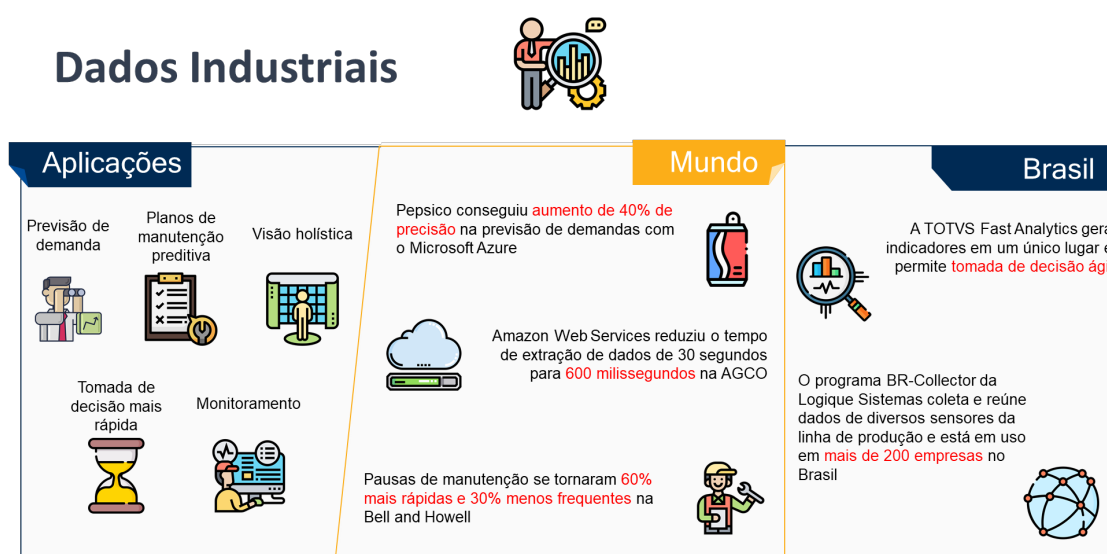


Figura 52 - Infográfico da Relevância para o Grupo de Dados Industriais

3.8 Grupo Robótica (ISO/TC299)

3.8.1 Escopo

O escopo do grupo de **Robótica (ISO/TC299)** é a padronização no campo de robótica, excluindo brinquedos e aplicações militares.

Para que a melhor compreensão das atividades e normas deste grupo de trabalho, alguns vocabulários da ISO/DIS 8373 são necessários:

- **Autonomia** - capacidade de realizar as tarefas pretendidas com base no estado atual e detecção, sem intervenção humana;
- **Sistema de controle** - conjunto de componentes de hardware e software que implementam lógica e controle de energia, e outras funções que permitem monitorar e controlar um comportamento do robô e sua interação e comunicação com outros objetos e humanos no ambiente;
- **Robô** - mecanismo atuado programado com um grau de autonomia para realizar locomoção, manipulação ou posicionamento. um robô inclui o sistema de controle e a interface do sistema de controle;
- **Robô industrial** - manipulador(es) multiuso reprogramáveis e controlados automaticamente, programáveis em três ou mais eixos, que podem ser fixos no local ou móveis para uso em aplicações de automação industrial.
- **Robô de serviço** - executa tarefas úteis para humanos ou equipamentos, excluindo aplicações de automação industrial (que pode ser fabricação, inspeção, embalagem e montagem).

Além disso, é importante diferenciar robôs industriais de robôs de serviço: enquanto robôs articulados usados em linhas de produção são robôs industriais, robôs articulados semelhantes usados para servir comida são robôs de serviço.

3.8.2 Status quo

Os esforços iniciais do grupo **Robótica (ISO/TC299)** focaram na manipulação dos robôs industriais, apresentando os resultados e as principais características. A norma **ISO 11593:1996** define termos relevantes para sistemas de troca automática de efetores finais usados para manipular robôs industriais. Além disso, a norma foi revisada em 2017. Além da norma ISO 11593:1996, a ISO 9283:1998 também faz parte de uma série de Normas Internacionais que tratam da manipulação de robôs industriais. A ISO 9283 visa facilitar o entendimento entre usuários e fabricantes de robôs e sistemas de robôs, definindo as características de desempenho importantes, descrevendo como as características devem ser especificadas e recomendando como devem ser testadas. É importante destacar que a norma ISO 9283:1998

foi revisada em 2021. Particularmente, a ISO 9283 descreve métodos de especificação e teste das seguintes características de desempenho de manipulação de robôs industriais:

- precisão de pose e repetibilidade de pose;
- variação multidirecional de precisão de pose;
- precisão de distância e repetibilidade de distância;
- tempo de estabilização da posição;
- ultrapassagem de posição;
- desvio das características da pose;
- permutabilidade;
- precisão do caminho e repetibilidade do caminho;
- precisão do caminho na reorientação
- desvios de curva;
- características de velocidade do caminho;
- tempo mínimo de colocação;
- conformidade estática;
- desvios de tecelagem.

Outra norma que faz parte do escopo de manipulação de robôs industriais é a **ISO 9946**, especificando como as características dos robôs devem ser apresentadas pelo fabricante. Dessa forma, o fabricante deve fornecer informações relacionadas às várias características e requisitos descritos como parte da documentação do robô. Por exemplo, o fabricante deve especificar o tipo principal da aplicação para que o robô se destina. Os exemplos de aplicações típicas são: manuseio; conjunto; soldagem por pontos; soldagem a arco; usinagem; pintura em spray; adesivo / vedação; inspeção.

A **ISO 10218-1: 2011** é outra norma do grupo prioritário e especifica requisitos e diretrizes para o design seguro inerente, medidas de proteção e informações para o uso de robôs industriais, descrevendo os riscos básicos associados aos robôs e fornecendo requisitos para eliminar ou reduzir adequadamente os riscos associados a esses perigos. É importante destacar que a ISO 10218-1: 2011 não se aplica a robôs não industriais, embora os princípios de segurança estabelecidos na ISO 10218 possam ser utilizados para esses outros robôs.

Já a parte 2 (**ISO 10218-2:2011**) especifica os requisitos de segurança para a integração de robôs industriais e sistemas de robôs industriais, conforme definido na ISO 10218-1, e célula (s) de robôs industriais. A integração inclui as seguintes etapas: projeto, fabricação, instalação, operação, manutenção do sistema ou célula de robô industrial; dispositivos componentes do sistema ou célula do robô industrial. Ademais, a ISO 10218-2: 2011 descreve os perigos básicos e as situações perigosas identificadas com esses sistemas e fornece requisitos para eliminar ou reduzir adequadamente os riscos associados a esses perigos. A ISO 10218-2: 2011 também especifica requisitos para o sistema de robô industrial como parte de um sistema de manufatura integrado.


A **ISO 8373: 2012** define os termos usados em relação a robôs e dispositivos robóticos que operam em ambientes industriais e não industriais, fornecendo definições e explicações dos termos mais comumente usados, que são agrupados em cláusulas por tópicos principais da robótica.

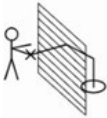

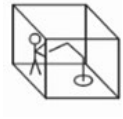
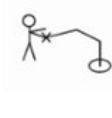
A norma **ISO 9787: 2013** (que foi revisada em 2020) define e especifica os sistemas de coordenadas do robô, fornecendo nomenclatura para os movimentos básicos do robô. Dessa maneira, a norma se destina a auxiliar no alinhamento, teste e programação do robô. Complementarmente, a ISO 9787:2013 se aplica a todos os robôs e dispositivos robóticos conforme definido na ISO 8373. A **ISO 9787: 2013 faz parte de uma série de Normas Internacionais que tratam de robôs e tópicos de cobertura robótica**, incluindo vocabulário, segurança, apresentação de características, critérios de desempenho e métodos de teste relacionados e interfaces mecânicas.

Além das normas já citadas, a norma **ISO 18646-1:2016** tem como objetivo facilitar a compreensão do desempenho de robôs com rodas entre usuários e fabricantes, definindo as características de desempenho importantes, descrevendo como são especificadas e recomendando como testá-las. A ISO 18646-1:2016 descreve métodos para especificar e avaliar o desempenho de locomoção de robôs com rodas em ambientes internos.

A **ISO/TS 15066: 2016** especifica os requisitos de segurança para sistemas de robôs industriais colaborativos e o ambiente de trabalho, complementando os requisitos e orientações sobre a operação colaborativa de robôs industriais em ISO 10218-1 e ISO 10218-2. A ISO/TS 15066: 2016 se aplica a sistemas de robôs industriais conforme descrito em ISO 10218-1 e ISO 10218-2. Assim como em outras normas, a ISO/TS 15066: 2016 não se aplica a robôs não industriais, embora os princípios de segurança apresentados possam ser úteis para outras áreas da robótica. Além disso, para complementar a análise, com base nas informações da norma ISO 15066, a Tabela 34 apresenta o tipo de aplicação, descrição, proteção e objetivos para sistemas de robôs industriais com intuito de facilitar o entendimento sobre o assunto.

Tabela 34 - Requisitos de segurança para sistemas de robôs industriais colaborativos

Tipo de aplicação	Descrição	Proteções	Objetivos
	<p>Janela de transferência</p>	<p>Operação automática autônoma dentro do espaço protegido</p> <p>O robô se movimenta na janela</p> <p>Nenhuma interrupção da operação automática durante o acesso</p>	<p>Protetores fixos ou sensíveis ao redor do espaço de trabalho</p> <p>Velocidade reduzida e espaço de trabalho reduzido próximo da janela</p> <p>Nenhum espaço de trabalho do robô fora da janela</p> <p>Quando a borda inferior da janela for menor que as proteções de 1000 mm, de acordo com 5.10.3</p> <p>Carregamento, descarregamento</p> <p>Testes, ensaio de bancada, limpeza</p> <p>Serviço</p>
		<p>Operação automática autônoma dentro</p>	<p>Protetores fixos ou sensíveis ao redor do espaço de trabalho</p> <p>Empilhamento/desempilhamento automático</p>

	<p>Janela de interface</p>	<p>do espaço protegido</p> <p>O robô para em uma janela de interface e, em seguida, pode ser movimentado manualmente para fora da interface</p>	<p>Velocidade reduzida e espaço de trabalho reduzido fora e próximo da janela</p> <p>Controle de ação contínua para movimento guiado</p>	<p>Montagem guiada Enchimento /esvaziamento guiado</p> <p>Testes, ensaios em bancadas, limpeza</p> <p>Serviço</p>
	<p>Espaço de trabalho colaborativo</p>	<p>Operação automática autônoma dentro de um espaço de trabalho comum (colaborativo)</p> <p>O robô reduz a velocidade e/ou para quando uma pessoa entra no espaço de trabalho comum (colaborativo)</p>	<p>Sistema de detecção de pessoas utilizando um ou mais sensores</p> <p>Velocidade reduzida de acordo com a distância (5.11.5.4)</p> <p>O robô para com segurança quando o espaço proibido é acessado e é possível nova partida automática após a desobstrução, se devidamente protegido</p>	<p>Montagem comum</p> <p>Manuseio comum</p> <p>Testes, ensaios em bancadas, limpeza</p> <p>Serviço</p>
	<p>Inspeção</p>	<p>Operação automática autônoma dentro do espaço protegido</p> <p>Uma pessoa entra no espaço de trabalho colaborativo enquanto o robô continua a operação com velocidade reduzida e curso reduzido</p>	<p>Protetores fixos ou sensíveis ao redor do espaço de trabalho</p> <p>Sistema de detecção de pessoas ou dispositivo de habilitação</p> <p>Velocidade reduzida e espaço de trabalho reduzido após a entrada na área de trabalho</p> <p>Medidas contra o uso indevido</p>	<p>Inspeção e ajuste de processos, por exemplo, aplicação de solda</p>
	<p>Robô guiado à mão</p>	<p>Espaço de trabalho específico na aplicação</p> <p>Movimento pela guia manual</p> <p>Movimentando a mão guiada ao longo da trajetória</p>	<p>Velocidade reduzida</p> <p>Controle de ação contínua</p> <p>Espaço de trabalho colaborativo, dependendo dos perigos da aplicação</p>	<p>Montagem guiada à mão, pintura, etc.</p>

A **ISO 19649: 2017** define termos relativos a robôs móveis que viajam em uma superfície sólida e que operam em aplicações de robôs industriais e robôs de serviço. A norma é usada para descrever mobilidade, locomoção e outros tópicos relacionados à navegação de robôs móveis.

A **série ISO/TR 20218** também é organizada pelo grupo prioritário. A norma **ISO/TR 20218-1:2018** fornece orientação sobre medidas de segurança para o projeto e integração de efetores finais usados para sistemas de robô. A norma ISO/TR 20218-1:2018 inclui os seguintes aspectos: fabricação, projeto e integração de efetores finais; informações necessárias para uso. De forma geral, a ISO/TR 20218-1:2018 fornece orientação para efetores finais em sistemas de robô, incluindo aplicativos colaborativos em que um sistema de robô e operadores compartilham o mesmo espaço de trabalho. Em tais aplicações colaborativas, o projeto do efector final é de grande importância, particularmente características como formas, superfícies e função de aplicação (por exemplo, forças de fixação, geração de material residual, temperatura).

Complementarmente, a norma **ISO/ TR 20218-2: 2017 (parte 2)** é aplicável a sistemas de robô para aplicações de carga / descarga manual nas quais uma zona de perigo é protegida ao impedir o acesso a ela. Para este tipo de aplicação, é importante considerar a necessidade de restrições de acesso às zonas de perigo e de locais de trabalho ergonomicamente adequados. De forma geral, a ISO / TR 20218-2: 2017 complementa a ISO 10218-2: 2011 e fornece informações e orientações adicionais sobre a redução do risco de intrusão nas zonas de perigo no projeto e proteção de instalações manuais de carga / descarga.

O grupo prioritário publicou algumas normas em 2021. A **ISO 18646-3:2021** descreve métodos de especificação e avaliação do desempenho de manipulação de robôs de serviço. Outrossim, existem outras características de apreensão e casos de uso para manipulação de robôs de serviço. A norma trata apenas do ambiente interno. No entanto, os testes descritos também podem ser aplicáveis a robôs operando em ambientes externos. Outra norma publicada em 2021 foi a ISO 22166. A norma **ISO 22166-1: 2021** apresenta requisitos e orientações sobre a especificação de estruturas modulares, sobre design modular aberto e sobre a integração de módulos para a realização de robôs de serviço em vários ambientes, incluindo setores pessoais e profissionais. A norma ISO 22166-1: 2021 é direcionada aos seguintes grupos de usuários: (i) desenvolvedores de estruturas modulares de robôs de serviço que especificam estruturas de desempenho; (ii) projetistas e / ou fabricantes de módulos que fornecem usuários finais ou integradores de robôs; (iii) integradores de robôs de serviço que escolhem os módulos aplicáveis para a construção de um sistema modular. Complementarmente, a norma ISO 22166-1: 2021 abrange diretrizes sobre como aplicar os padrões de proteção e segurança existentes aos módulos do robô de serviço. ISO 22166-1: 2021 se aplica especificamente a robôs de serviço, embora os princípios de modularidade apresentados neste documento possam ser utilizados por desenvolvedores de estruturas, fabricantes de módulos e integradores de módulos de outros campos não necessariamente restritos à robótica.

A **ISO / TR 23482-1: 2020** descreve métodos que podem ser usados para testar robôs de cuidados pessoais em termos de requisitos de segurança definidos na ISO 13482. Por exemplo, o fabricante deve determinar os testes necessários e os parâmetros de teste apropriados com base em uma avaliação de risco do design e uso do robô. É importante ressaltar que nem todos os métodos de teste são aplicáveis a todos os tipos de robôs. Por exemplo, os métodos de teste rotulados como "universais" são aplicáveis a todos os robôs de cuidados pessoais.

Para outros testes, o título indica para quais tipos de robô o teste pode ser aplicado (por exemplo, "para robô vestível" ou "para robô móvel").

Em relação a robôs de cuidados pessoais, a norma **ISO / TR 23482-2: 2019** fornece orientação sobre o uso da ISO 13482 e tem como objetivo facilitar o projeto de robôs de cuidados pessoais em conformidade com a ISO 13482. A norma ISO / TR 23482-2: 2019 fornece esclarecimento e orientação sobre os novos termos e requisitos de segurança introduzidos para permitir a interação próxima homem-robô e contato homem-robô em aplicações de robôs para cuidados pessoais, incluindo robôs servos móveis, robôs assistentes físicos e robôs transportadores de pessoas. A ISO / TR 23482-2: 2019 considera a aplicação da ISO 13482 a todos os robôs de serviço.

Além de todos esses aspectos, é importante a compreensão sobre a categorização dos robôs e a relação com outras áreas relevantes e com diferentes tipos de robôs. A Figura 53 esquematiza esses conceitos.

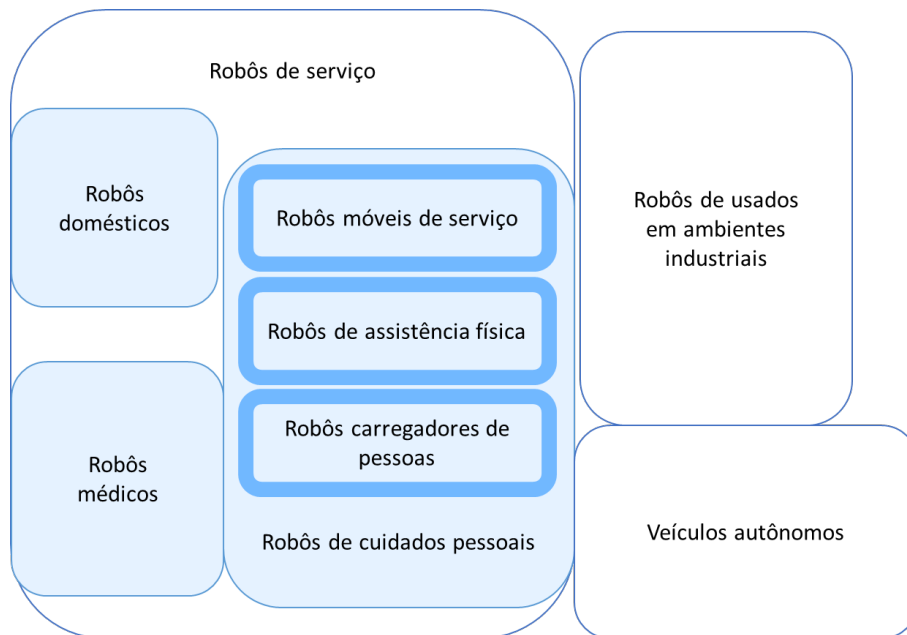






Figura 53 - Categorização dos robôs e a relação com outras áreas relevantes

Além do entendimento da categorização, A Tabela 35 apresenta qual é o propósito dos diferentes tipos de robôs, seus usuários e alguns exemplos para facilitar a correta aplicação das diferentes normas.

Tabela 35- Resumo das categorias de robôs

Categorias de robôs	Propósito	Usuários	Exemplos
<p>Robôs de cuidado pessoal</p> 	<p>Melhoria da qualidade de vida de humanos (em termos não-medicinais)</p>	<p>Leigos (não o paciente)</p>	<p>Robô móvel autônomo que pega objetos requisitados pelo usuário</p> <p>Exoesqueleto robótico para melhorar a capacidade física de uma pessoa saudável em um ambiente não industrial</p> <p>Robô pessoal de mobilidade que se auto equilibra</p>
<p>Robôs médicos</p> 	<p>Diagnóstico, tratamento ou monitoramento de um paciente; ou compensação ou alívio de doença, ferimento ou deficiência</p>	<p>Paciente</p> <p>Especialista médico</p>	<p>Exoesqueleto robótico para compensar deficiência de membros afetados</p> <p>Robôs cirúrgicos</p> <p>Robô capaz de transferir o paciente da cama para cadeira de rodas</p>
<p>Robôs domésticos</p> 	<p>Implementação de tarefas domésticas para humanos</p>	<p>Leigos (não o paciente)</p>	<p>Aspirador de pó autônomo</p> <p>Robô cortador de grama</p>
<p>Robôs usados em ambientes industriais</p> 	<p>Implementação de tarefas em automação industrial</p>	<p>Trabalhador</p>	<p>Robô móvel de armazém</p> <p>Robô soldador</p>

Por fim, as normas que foram abordadas como mais relevantes no grupo Robótica (ISO/TC299) estão consolidadas na Tabela 36.

Tabela 36 - Normas do grupo de Robótica

Normas	Escopo
ISO 11593:1996	Manipulação de robôs industriais – Principais características
ISO 9283:1998	Manipulando robôs industriais - Critérios de desempenho e métodos de teste relacionados
ISO 9946:1999	Manipulando robôs industriais - Apresentação de características
ISO 10218-1:2011	Robôs e dispositivos robóticos - Requisitos de segurança para robôs industriais - Parte 1: Robôs
ISO 10218-2:2011	Robôs e dispositivos robóticos - Requisitos de segurança para robôs industriais - Parte 2: Sistemas e integração de robôs
ISO 8373: 2012	Robôs e dispositivos robóticos - Vocabulário
ISO 9787: 2013	Robôs e dispositivos robóticos - Sistemas de coordenadas e nomenclaturas de movimento
ISO 18646-1:2016	Robótica - Critérios de desempenho e métodos de teste relacionados para robôs de serviço - Parte 1: Locomoção para robôs com rodas
ISO/TS 15066:2016	Robôs e dispositivos robóticos - robôs colaborativos
ISO 19649:2017	Robôs móveis – vocabulário
ISO/TR 20218-1:2018	Robótica - Projeto de segurança para sistemas de robôs industriais - Parte 1: Efetores finais
ISO/TR 20218-2:2017	Robótica - Projeto de segurança para sistemas de robôs industriais - Parte 2: Estações manuais de carga / descarga
ISO 18646-3:2021	Robótica - Critérios de desempenho e métodos de teste relacionados para robôs de serviço - Parte 3: Manipulação
ISO 22166-1: 2021	Robótica - Modularidade para robôs de serviço - Parte 1: Requisitos gerais
ISO / TR 23482-1: 2020	Robótica - Aplicação da ISO 13482 - Parte 1: Métodos de teste relacionados à segurança
ISO / TR 23482-2: 2019	Robótica - Aplicação da ISO 13482 - Parte 2: Diretrizes de aplicação

3.8.3 Mapa mental de relação da Robótica com outros grupos

Na Figura 54, apresenta-se uma análise do grupo prioritário de Robótica em relação a outros grupos e tecnologias da Indústria 4.0. Em azul e a direita do elemento central estão os grupos que conectados ao da robótica:

- **Fábrica Digital** – O grupo prioritário denominado Fábrica Digital tem como escopo da definição de framework da Fábrica Digital, que especifica os elementos do modelo e regras para a criação e gerenciamento de representações digitais de sistemas de produção;

- **Rede Industrial** – O escopo do grupo prioritário sobre rede industrial abrange a preparação de padrões internacionais sobre redes industriais com fio, ópticas e sem fio para medição de processos industriais, controle e automação de fabricação, bem como para sistemas de instrumentação usados para fins de pesquisa, desenvolvimento e teste. O escopo inclui cabeamento, interoperabilidade, co-existência e avaliação de desempenho;
- **Segurança para medição e controle de processos industriais** – Segurança para medição e controle de processos industriais - Segurança de rede e sistema;
- **Internet das Coisas e Gêmeo Digital** – O grupo prioritário de internet das coisas e gêmeos digitais foca na padronização na área de Internet das Coisas e Digital Twin, incluindo suas tecnologias relacionadas. O grupo prioritário tem como objetivo servir como o proponente do programa de padronização na Internet das Coisas e Digital Twin. Além disso, o grupo prioritário tem intuito de fornecer orientação entidades que desenvolvem aplicativos relacionados à Internet das Coisas e Digital Twin;
- **Segurança de máquinas** – O grupo prioritário de Segurança de máquinas tem como objetivo padronizar os conceitos básicos e princípios gerais para segurança de máquinas incorporando terminologia, metodologia, proteções e dispositivos de segurança dentro da estrutura do ISO / IEC e em cooperação com outros comitês técnicos da ISO e IEC;
- **Dados Industriais** – O escopo do grupo prioritário de dados industriais é a padronização do conteúdo, significado, estrutura, representação e gestão da qualidade das informações necessárias para definir um produto de engenharia e suas características em qualquer nível de detalhe exigido em qualquer parte de seu ciclo de vida desde a concepção até o descarte;
- **Segurança da informação, cibersegurança e proteção de privacidade** – O desenvolvimento de normas 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;
- **Inteligência Artificial** – A proposta do grupo de Inteligência Artificial (IA) é criar normas para subsidiar o desenvolvimento de programas de padronização da IA, além de fornecer orientações aos comitês para o desenvolvimento de aplicações em IA;
- **Machine Learning para redes do futuro** – O grupo prioritário elaborou especificações técnicas para *machine learning* para redes futuras, incluindo interfaces, arquiteturas de rede, protocolos, algoritmos e formatos de dados.

Os grupos que estão à esquerda, em amarelo, são os grupos não listados como prioritários, mas que possuem interconexões com o grupo em destaque. São eles:

- **Produtos auxiliares:** Padronização no campo de produtos de assistência e serviços relacionados para ajudar uma pessoa a compensar por habilidades reduzidas.
- **Automatização de sistemas e integração:** Padronização na área de sistemas de automação e sua integração para projeto, sourcing, fabricação, produção e entrega, suporte, manutenção e descarte de produtos e seus serviços associados. As áreas de padronização incluem sistemas de informação, sistemas de automação e controle e tecnologias de integração.
- **Interface do usuário:** Padronização no campo das interfaces usuário-sistema em ambientes de tecnologia da informação e comunicação (TIC) e suporte para que essas interfaces atendam a todos os usuários, incluindo pessoas com acessibilidade ou outras necessidades específicas, com prioridade de atendimento aos requisitos JTC 1 para aspectos culturais e linguísticos adaptabilidade.
- **Comunicação de dados:** Padronização na área de comunicação de dados para aplicações em veículos.

Por fim, em vermelho estão os principais conceitos que fazem parte da transformação digital e que estão conectados aos diferentes grupos.

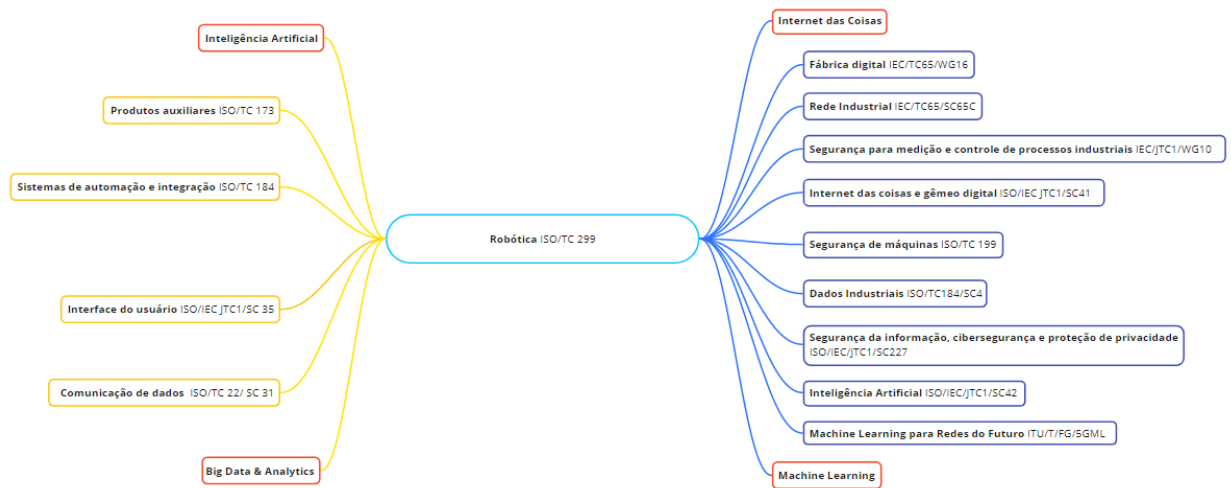


Figura 54 - Mapa mental de relação do grupo de Robótica com outros grupos

3.8.4 Tendências

3.8.4.1 Critérios de desempenho e métodos de teste relacionados para robôs de serviço (Série 18646)

A norma **ISO 18646-3** (publicada em junho de 2021⁷⁰) define características para o desempenho de manipulação de robôs de serviço e descreve como especificá-los e testá-los. Com o uso da norma, pretende-se que seja possível selecionar as características de desempenho de testes relacionados para robôs de serviço. Complementarmente, a norma define critérios de desempenho e métodos para a realização de testes para locomoção de robôs móveis, como medição da velocidade nominal e características de parada que são fornecidos na ISO 18646-1 (publicada em 2016, mas está em revisão, estágio 90,20⁷¹). Além disso, os testes de precisão de pose e repetibilidade de pose para robôs móveis também são fornecidos na ISO 18646-2.

Já a norma **ISO/FDIS 18646-4** tem como objetivo facilitar a compreensão do desempenho de robôs de apoio para a região lombar, definindo as características de desempenho importantes e descreve como especificá-las e testá-las. As características apresentadas na norma afetam significativamente o desempenho do robô.

3.8.4.2 Serviços prestados por robôs de serviço (ISO/CD 31101:2021 e ISO/NP 22166-201)

A **ISO/CD 31101:2021** (estágio 30,60⁷²) tem como objetivo fornecer os requisitos do sistema de gerenciamento de segurança de robô de serviços como uma estrutura de operação segura de serviços de robô. O gerenciamento baseia-se no conceito de Plan-Do-Check-Act (PDCA). O modelo PDCA fornece um modelo iterativo para alcançar a melhoria contínua. Por exemplo, uma empresa que deseja demonstrar conformidade com a norma pode realizar as seguintes ações: - fazendo uma autodeterminação e autodeclaração; buscando a confirmação de sua conformidade por partes com interesse na organização, tais como clientes; buscando a confirmação de sua autodeclaração por uma parte externa à organização, ou buscando a certificação / registro por uma organização externa.

A **ISO/NP 22166-201** (proposta realizada em 2021⁷³) apresenta requisitos e diretrizes para modelos de informações comuns (CIM) para módulos de robôs de serviço. Algumas orientações que a ISO/NP 22166-201 fornece tem como objetivo: (i) facilitar a integração de módulos; (ii) entender funções mínimas para módulos de robô de serviço; (iii) permitir que designers de módulo e fabricantes definam e usem funções de módulo para alcançar as características do módulo do robô de serviço; (iv) permitir que os usuários do módulo recebam módulos de robô de serviço apropriados.

⁷⁰ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/73591.html>

⁷¹ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/63127.html>

⁷² Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/80886.html>

⁷³ Atualizações da norma podem ser encontradas em:

<https://standardsdevelopment.bsigroup.com/projects/9021-05009#/section>

3.8.4.3 Requisitos para a integração de sistemas de robôs industriais (ISO/DIS 10218-2)

A norma **ISO/DIS 10218-2** (criada em 2011 e revisada em 2021, estágio 40,99⁷⁴) especifica os requisitos para a integração de sistemas de robôs industriais, aplicações de robôs industriais e células de robôs industriais. Os seguintes temas são abordados: projeto, integração, comissionamento, operação, manutenção, descomissionamento e descarte do sistema; integração de máquinas e componentes ao sistema, aplicativo ou célula do robô industrial; informações para uso para o projeto, integração, comissionamento, operação, manutenção, descomissionamento e descarte do sistema, aplicativo ou célula do robô industrial.

3.8.4.4 Vocabulários de Robótica (ISO/DIS 8373)

A norma **ISO/DIS 8373** (que está no estágio 50,20⁷⁵) aborda o vocabulário usado em relação aos robôs. Não é um dicionário, mas uma lista de termos mais comumente usados em padrões desenvolvidos pela ISO TC 299.

Por fim, a Tabela 37 resume as normas que estão em desenvolvimento pelo grupo Robótica (ISO/TC 299).

Tabela 37 - Normas referentes a tendências do grupo de Robótica

Normas	Escopo
ISO/FDIS 18646-3	Desempenho de manipulação de robôs de serviço
ISO/FDIS 18646-4	Desempenho de robôs de apoio para a região lombar
ISO/CD 31101:2021	Requisitos do sistema de gerenciamento de segurança de robô de serviço
ISO/NP 22166-201	Requisitos e diretrizes para modelos de informações comuns (CIM) para módulos de robôs de serviço
ISO/DIS 10218-2	Requisitos de segurança para sistemas de robô em um ambiente industrial - Sistemas de robôs, aplicativos de robôs e células de robôs integração
ISO/DIS 8373	Vocabulários da Robótica

Concluindo, a Figura 55 sumariza a evolução das atividades e normas do grupo Robótica (ISO/TC 299).

⁷⁴ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/73934.html>

⁷⁵ Atualizações da norma podem ser encontradas em: <https://www.iso.org/standard/75539.html>

Robótica

ISO/ITC 299

Escopo

Padronização no campo de robótica, excluindo brinquedos e aplicações militares

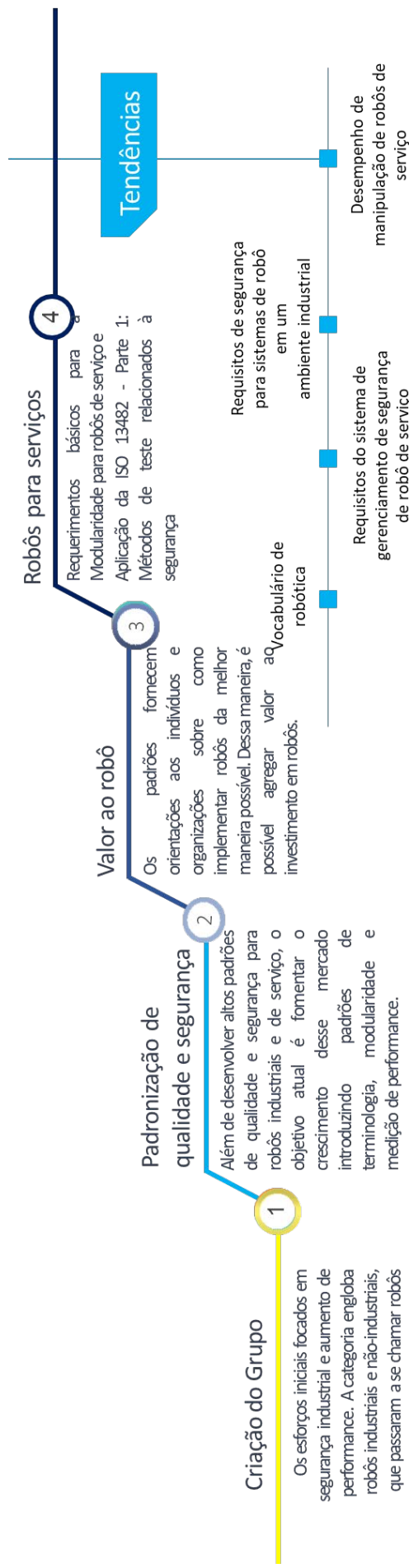


Figura 55 - Consolidação da análise do Grupo de Robótica

3.8.5 Relevância

Robótica se refere ao *design*, construção e aplicação de máquinas (robôs) para realizar tarefas tradicionalmente feitas por humanos. Robôs são usados nos mais diversos tipos de indústrias. Algumas das principais aplicações que se destacam na indústria são (GENESIS-SYSTEMS, 2020):

- I. Robôs Colaborativos Industriais (INTERNATIONAL FEDERATION OF ROBOTICS - IFR, 2020a): são projetados para realizar tarefas em colaboração com os trabalhadores da indústria setores. Os robôs colaborativos fornecem um ponto de entrada economicamente viável para a automação robótica. Eles podem ser usados para automatizar peças de uma linha de produção com mudanças mínimas para o resto da linha, fornecendo empresas que ainda não automatizaram os processos de produção - como pequenas e médias fabricantes - uma entrada para as melhorias de produtividade e qualidade oferecidas pelos robôs.
- II. Pintura Robótica: é perfeito para robôs, porque a pintura precisa ser altamente consistente em uma grande área de pintura, e reduzir a quantidade de material desperdiçado pode representar uma grande economia;
- III. Soldagem Robótica: cada carro precisa de um grande número de soldas antes de ser concluído. Dado o alto valor do produto acabado, a produtividade da automação é enorme.
- IV. Conjunto robótico: os robôs estão montando componentes menores, como instalação de para-brisas e montagem de rodas para aumentar o rendimento.
- V. Remoção de material: alta consistência e repetibilidade tornam os robôs perfeitos para processos de remoção de material, como aparar e cortar.
- VI. Transferência de peças e manuseio da máquina: verter metal fundido, transferir carimbos de metal e carregar e descarregar máquinas CNC são mais bem executados por um robô, pois são perigosos.

Além dessas aplicações, os robôs podem ser utilizados para segurança; entretenimento; agricultura; preparação de comida; serviços de saúde (GEEKSFORGEES, 2020), conforme apresentado anteriormente. Particularmente, também são muito úteis em ambientes de trabalho perigosos ou nocivos aos humanos, como na exploração subterrânea, oceânica ou espacial. Além disso, robôs são essenciais em operações que requerem grande precisão, como cirurgias complexas ou na fabricação de semicondutores e componentes eletrônicos. Ademais, A robótica está diretamente relacionada à Inteligência Artificial, visto que os robôs mais modernos têm sensores que permitem com que eles consigam enxergar, fazer medições e até mesmo tomar decisões. Por exemplo, a Udacity oferece um curso gratuito de Inteligência Artificial para Robôs que ensina como programar todos os principais sistemas de um carro

robótico do líder das equipes de direção autônomas do Google e de Stanford (UDACITY, 2021). A inteligência artificial em robôs oferece às empresas novas oportunidades para aumentar a produtividade, tornar o trabalho mais seguro e poupar. Além disso, pesquisas focam no uso de IA para expandir a funcionalidade do robô. As aplicações disponíveis comercialmente incluem o uso de IA para (IFR, 2018a):

- Permitir que os robôs detectem e respondam ao seu ambiente;
- Otimizar o desempenho do robô e do processo, economizando dinheiro para as empresas;
- Permitir que robôs funcionem como sistemas de informação móveis e interativos em vários
- configurações de espaços públicos a hospitais e lojas de varejo, economizando tempo dos indivíduos.

Adicionalmente, o uso da robótica avança rapidamente em todo mundo. Entre 2010 e 2019, a instalação anual de robôs industriais aumentou mais de 3 vezes, alcançando mais de 380 mil unidades espalhadas pelo mundo (IFR, 2021). Entre umas das principais tendências para o futuro da robótica, destacam-se Autonomous Mobile Robots (AMRs) que são robôs capazes de navegar de maneira autônoma pelo interior das fábricas e podem ser usados para o transporte de materiais e abastecimento de linhas de produção.

A robótica também está aumentando sua participação em setores que foram historicamente dominados pelo trabalho manual, como as indústrias de alimentos, têxtil, moveleira e produtos sob medida em geral. É crucial destacar que já existem robôs capazes de se adaptar e realizar diferentes tarefas (IFR, 2020b), diferentemente de robôs mais antigos, que só conseguiam realizar um tipo de movimento repetitivo. De 2020 a 2022, espera-se que quase 2 milhões de novas unidades de robôs industriais sejam instaladas em fábricas em todo o mundo (IFR, 2020b).

Complementarmente, o aumento da precisão dos robôs também permite que menos produtos sejam descartados por falta de qualidade, diminuindo o desperdício de matéria-prima. Por exemplo, em comparação com os humanos, os robôs são magnitude em mais precisos e possuem alta repetibilidade (SOUTHIE AUTONOMY, 2020). Estudos focados especificamente em robôs mostram uma contribuição para o crescimento da produtividade, impulsionada por robôs respondendo por 10% do crescimento total do PIB em 14 anos e previsões de crescimento contínuo da produtividade impulsionado pela automação de até 1,4% anualmente nos próximos 50 anos (IFR, 2018b). Conforme IFR (IFR, 2021), o impacto positivo que o aumento da produtividade dos robôs tem sobre o emprego já pode ser visto nas nações industrializadas mais avançadas. A indústria automotiva dos EUA, por exemplo, instalou mais de 60.000 robôs industriais entre 2010 e 2015. Durante o mesmo período, o número de funcionários no setor automotivo dos EUA aumentou em 230.000. De acordo com o McKinsey Global Institute, mais de 90 por cento dos trabalhos não serão totalmente automatizados no futuro. Em vez disso, robôs e humanos trabalharão juntos.

De acordo com o relatório da McKinsey de 2019 *“Industrial robotics: Insights into the sector’s future growth dynamics”* (MCKINSEY & COMPANY, 2019) entrevistas foram feitas com

multinacionais do setor automotivo, farmacêutico e eletrônico, o principal fator listado – citado por 82% dos respondentes - que impulsiona o investimento em robótica é diminuir custos de produção. Em segundo lugar, citado por 55% dos entrevistados, está o aumento de qualidade. Por outro lado, 69% citam que o maior obstáculo que atrapalha a implementação dos robôs é o seu custo de aquisição. Em segundo lugar, com 41%, está a falta de um sistema ou plataforma que consiga integrar robôs de diferentes tipos e fabricantes.

O Brasil é um país que apresenta grandes oportunidades para o desenvolvimento da robótica. Segundo dados da International Federation of Robotics (IFR), o país ocupa a 39ª posição, com apenas 10 robôs para cada 10 mil funcionários (FORBES, 2018).

Em 2018, o governo federal zerou o imposto de importação sobre robôs industriais, incluindo os *collaborative robots* (cobots). Os cobots já são amplamente utilizados na América do Norte e Europa, podendo aumentar a eficiência de produção em até 85% (DATASEBRAE, 2018). Esse tipo de robô trabalha lado a lado com os seres humanos e é fundamental para fortalecer o processo de industrialização brasileiro e aumentar a competitividade internacional. É importante ressaltar que, atualmente, nenhum cobot é produzido no Brasil.

Pelo relatório de 2018 da Confederação Nacional das Indústrias (CNI) (SIEMBRA AUTOMAÇÃO, 2018), entre 2016 e 2018, houve um aumento de 15% das grandes empresas que utilizam pelo menos uma tecnologia digital, passando de 63% para 73% das grandes indústrias. Além disso, quase metade (48%) afirma que irá investir em novas tecnologias nos próximos anos. Porém, mesmo com todas as medidas, em 2020, o Brasil ocupava a 62ª posição no Índice Global de Inovação (WIPO, 2020). Na América Latina, o Brasil está apenas atrás do Chile e México (54ª e 55ª posição, respectivamente).

Concluindo, a Figura 56 sumariza os principais aspectos que demonstram a relevância do grupo Robótica (ISO/TC299).

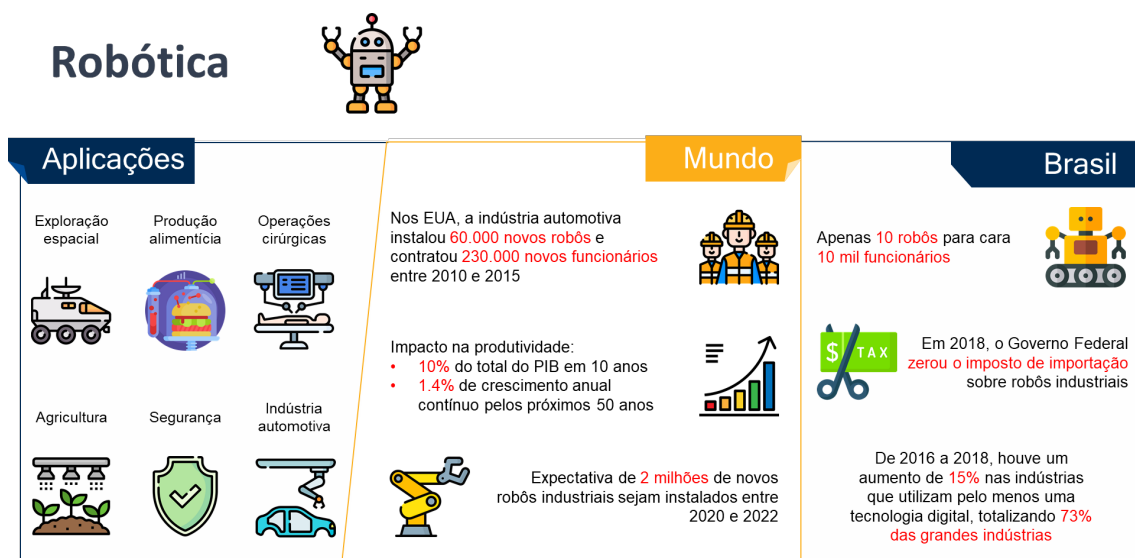


Figura 56 - Infográfico da Relevância para o Grupo de Robótica

3.9 Conclusões do grupo redes industriais e Interoperabilidade

As normas do grupo de Redes Industriais são essenciais para a implementação da Indústria 4.0 nas fábricas, visto que interligar equipamentos facilita o intercâmbio e o uso de dados para otimizar a tomada de decisão. Sendo assim, as normas destacadas no relatório podem ajudar as empresas a aprimorarem as suas redes industriais a fim de implementar as tecnologias da Indústria 4.0. Além disso, a nota técnica sumariza exemplos de empresas de diversas áreas que obtiveram resultados positivos no uso de redes industriais e tecnologias da Indústria 4.0, resumindo os benefícios de seu uso em conjunto e demonstrando como essa estratégia pode melhorar os resultados empresariais.

O grupo de Fábricas Digitais traz normas com inúmeros benefícios à indústria, uma vez que existem diversos processos que estão interligados para otimizar os resultados empresariais. As Fábricas Digitais possuem diversos processos (Desenvolvimento digital, suprimento inteligente, planejamento sincronizado são apenas alguns exemplos) que precisam ser monitorados, e o uso de tecnologias da Indústria 4.0 podem auxiliar. Para que a Fábrica Digital seja alcançada, frameworks internacionais foram desenvolvidos para facilitar o processo, ajudando na redução de custos, na melhoria da qualidade dos produtos e no lançamento de novos produtos. As oportunidades no Brasil são inúmeras, logo é importante desenvolver um sistema de normas estruturados para promover o desenvolvimento de Fábricas Digitais no país.

As normas de IoT e Gêmeos Digitais podem ser aplicadas em diversos setores da economia, promovendo o desenvolvimento sustentável do país. Entre eles, destacam-se a construção, saúde, agricultura e cidades inteligentes. Em nível nacional, é importante destacar que existem quatro perfis de países: liderança global em IoT; liderança em verticais específicas; aumento da competitividade; melhoria na qualidade de vida. O Brasil já realizou medidas a fim de financiar o desenvolvimento de IoT no Brasil com intuito de possibilitar a integração e adoção de tecnologias para diversas etapas da cadeia de valor. Além dessa iniciativa de financiamento, o Brasil lançou um Plano Nacional de Internet das Coisas para melhorar a qualidade de vida das pessoas, fomentar a competitividade e aumentar a integração do país internacionalmente. Complementarmente, os Gêmeos Digitais também podem ser utilizados nos mais diversos tipos de indústria, e a sua adoção já reduziu despesas em grandes empresas no país

As normas de Dados Industriais trazem um vocabulário para o melhor entendimento de conceitos chave. Além disso, há diversas normas focadas em qualidade de dados a fim de que os dados estejam com um grau de características inerentes. As normas sobre o tema abordam aspectos importantes: processos, fluxos de informações, indicadores e gerenciamento da mudança que ajudam as empresas a usarem o framework como base para maximizar o uso de dados industriais. Como o fluxo de dados e informações que podem ser de diversas fontes (sensores, sistemas de controle industrial) é essencial na Indústria 4.0, e o uso das tecnologias (*Impressão 3D e machine learning*) pode auxiliar a melhorar o seu desempenho. As empresas vêm utilizando diferentes estratégias para o melhor aproveitamento dos dados industriais, e muitos fornecedores estão criando sistemas para viabilizar esse processo.

As normas de Robótica abordam conceitos e definições indispensáveis para as empresas, auxiliando no entendimento básico dos diversos tipos de robôs e as suas funções. As normas também fornecem diretrizes para fornecedores a fim de que requisitos básicos sejam atendidos. Como existem diversos tipos de robôs (robôs domésticos, robôs médicos, veículos

autônomos), as normas trazem explicações claras de seu objetivo e exemplos de uso. Dessa forma, as empresas podem utilizar os robôs da melhor forma possível. Mundialmente, o crescimento do uso de robôs é visível, e os resultados impactam na produtividade e no PIB de alguns países. Além disso, existem oportunidades no Brasil, mesmo com o aumento no número de robôs, o país criou diversos incentivos para que as empresas pudessem comprar robôs.

3.10 Conclusões Gerais do estudo dos grupos prioritários

Como conclusões são apresentados alguns pontos de lições aprendidas ao longo do estudo que compreende os dez grupos prioritários de normalização.

Complementariedade dos grupos: Mesmo que os grupos de trabalho, desenvolvam normas específicas do tema, as normas e os grupos prioritários se relacionam. Portanto, é imprescindível o entendimento do contexto que as normas estão inseridas para facilitar o processo decisório das empresas. Portanto, as empresas necessitam ter uma visão clara do que desejam com o uso das tecnologias para que as normas possam auxiliar na potencialização dos resultados. Além disso, em muitas normas, há casos de uso para que as empresas possam se identificar ou não.

Desenvolvimento nacional com base no desenvolvimento internacional: o Brasil já possui diversas empresas que implementam as mais diferentes tecnologias com objetivos diversos. No entanto, quando o Brasil não possui empresas que estão adotando as tecnologias, pode se espelhar em países mais avançados. Para isso, é essencial a realização do benchmarking internacional. Porém, são imprescindíveis avaliações claras e a definições de diretrizes e objetivos tanto do país quanto das empresas que querem implementar tecnologias de Indústria 4.0.

Entendimento base das tecnologias, do vocabulário, dos casos de usos e do framework facilitam o uso da tecnologia e a integração dos dados nas empresas: muitas informações que constam nas normas podem ajudar as empresas a se desenvolverem e adotarem tecnologias da transformação digital, visto que os conhecimentos que as normas propiciam são amplos e precisos. Portanto, as empresas devem reestruturar os seus processos digitais com base no conhecimento desenvolvido, e o uso das normas pode facilitar esse processo complexo.

Visão integrativa do uso de tecnologias pode apoiar os resultados da empresa: as empresas devem desenvolver uma visão abrangente do uso das tecnologias e como elas podem ser usadas em conjunto para maximizar os resultados das empresas. Muitas vezes, as tecnologias apresentam objetivos e funções únicas e, quando são utilizadas em conjunto, facilitam os processos das empresas. Com o uso das normas, é possível integrar o uso de tecnologias.

Siglas encontradas nesta publicação

AGV – *Automated Guided Vehicle*
AIoT – Inteligência Artificial das Coisas
AJB – Água Jurisdicional Brasileira
AMRs – *Autonomous Mobile Robots*
AR – Realidade aumentada
AWS – *Amazon Web Services*
BCM – Gerenciamento de continuidade do negócio
BDRA – Arquitetura de Referência de *big data*
BOK – Corpo de Conhecimento
C&M IS – Sistemas Industriais de Coleta e Gerenciamento
CAT – Comunicação de Acidentes de Trabalho
CC – Coordenação Central
CDD – Dicionário de Dados Comum
CIO – *Chief Information Officer*
CNI – Confederação Nacional das Indústrias
COLLADA – *COLLABorative Design Activity*
COSO – *Committee of Sponsoring Organizations of the Treadway Commission*
CP – Communication Profiles
CPF – *Communication Profiles Families*
CRs – Componentes do Sistema de Controle Técnico
CTO – *Chief Technology Officer*
DC – Confidencialidade dos Dados
DCC – Criação de Conteúdo Digital
DT – *Digital Twin*
EBIT – Lucros antes de juros e imposto de renda
ELS – Sistema de Etiqueta Eletrônica
FRs – Sete Requisitos Básicos
GPIN – Grupo de Pesquisa em Inteligência de Negócio
IA – Inteligência Artificial
IAC – Controle de Identificação e Autenticação
IACS – Automação Industrial e Sistemas de Controle
ICCS – Sistemas de Controle Industrial
IDEMP – Instituto de Desenvolvimento Empresarial
IDMZ – Zona Desmilitarizada Industrial
IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos⁷⁶
IFR – Índice de Força Relativa
IFR – *International Federation of Robotics*
IIoT – Internet das coisas industrial
IMS – Sistema de Manufatura Integrados
IoT – Internet das coisas
KDC – Centro de Distribuição de Chaves

⁷⁶ Entidade profissional setorial de alcance mundial

KTC – Centro de Tradução de Chaves
MCM – Gerenciamento de Mudanças de Manufatura
MEC – *Multi-access Edge Computing*
ML – *Machine Learning*
ML – *Maturity Level*
MoSSEC – Modelagem e simulação de informações em um contexto de engenharia de sistemas colaborativos
OS – *Operating Systems*
OT – Tecnologia Operacional
PCN – Plano de Continuidade de Negócios
PDCA – *Plan-Do-Check-Act*
PIB – Produto Interno Bruto
PII – Informações de Identificação Pessoal
PIMS – Sistema de Gerenciamento de Informações de Privacidade
PLC – Controlador Lógico Programável
PLCs – controladores lógicos programáveis
PSL – Linguagem de Especificação de Processo
PUC-Minas – Pontifícia Universidade Católica de Minas Gerais
QIF – Estrutura de Informações de Qualidade
RA – Disponibilidade de Recursos
RDF – Fluxo de Dados Restrito
RTOS – Sistemas Operacionais em Tempo Real
SDL – Ciclo de vida de Desenvolvimento Seguro
SGSI – Sistema de Gestão de Segurança da Informação
SI – Integridade do Sistema
SISO – Sistema Integrado de Segurança Operacional
SMS – Sistema de gerenciamento de segurança
SN – Rede de Sensores
SP – Programa de Segurança
SP – São Paulo
SPR – Classificação do programa de segurança
SRP/CS – Segurança de sistemas de controle
ST – Alvos de Segurança
TIC – Tecnologia da Informação e Comunicação
TOE – *Target Of Evaluation*
TRE – Resposta Oportuna a Eventos
TTP – *Trusted Third Party*
UC – Controle de Uso
VR – Realidade Virtual
WCA – Aplicativo de Comunicação sem Fio
WCS – Sistema de Comunicação sem Fio
WEF – Fórum Econômico Mundial
WIA-FA – Redes sem fio para automação industrial - Automação de fábrica
WIA-PA – Automação Industrial - Automação de Processos

Lista de Figuras

Figura 1 - Mapa mental da relação do grupo de Inteligência Artificial com outros grupos.....	20
Figura 2 - Consolidação da análise do grupo de Inteligência Artificial.....	25
Figura 3 - Infográfico da Relevância para o Grupo de Inteligência Artificial.....	27
Figura 4 - Mapa mental de relação do grupo de machine learning para Redes do Futuro com outros grupos.....	32
Figura 5- Consolidação da análise do Grupo de ML para Redes do Futuro....	34
Figura 6 - Infográfico da Relevância para o Grupo de ML para redes do futuro (5G).....	38
Figura 7 - Mapa mental de relação do grupo de Segurança de Máquinas com outros.....	53
Figura 8 - Consolidação da análise do grupo de Segurança de Máquinas.....	56
Figura 9 - Categorias tecnológicas da Indústria 4.0 e aspectos de OHS.....	58
Figura 10 - Infográfico da Relevância para o Grupo de Segurança de Máquinas.....	60
Figura 11 - Mapa mental de relação do grupo de Segurança da informação, cibersegurança e proteção de privacidade com outros grupos	68
Figura 12 - Ciclo de vida de um serviço IoT para compreensão de pontos de risco	71
Figura 13 - Consolidação da análise do grupo de Segurança da Informação	74
Figura 14 - Aspectos preventivos da cibersegurança na Indústria 4.0.....	75
Figura 15 - Principais aspectos de IA em todo o programa de segurança crítico.....	77
<i>Figura 16 - Infográfico da Relevância do Grupo de Segurança da Informação</i>	<i>79</i>
Figura 17 - Mapa mental de relação do grupo de Segurança para medição de processos industriais com outros grupos.....	83
Figura 18 - Consolidação das diferentes partes da IEC 62443.....	84
Figura 19 - Esquematização dos recursos de segurança usados na Automação Industrial.....	86
Figura 20- Exemplo de Matrizes para Determinação do valor de SPR	88

Figura 21 - Principais Responsáveis no Gerenciamento de Avaliação de Conformidade e suas respectivas atividades.....	90
Figura 22 - Consolidação da análise do Grupo de Segurança para processo industrial.....	92
Figura 23 - Infográfico da Relevância da Indústria e BCM para o Grupo de Segurança para processo industrial.....	95
Figura 24 - Infográfico da Relevância de Setor público e cidades inteligentes para o Grupo de Segurança para processos industriais.....	97
Figura 25 - Infográfico da Relevância dos usuários e transporte para o Grupo de Segurança de Processo Industrial.....	99
Figura 26 - Infográfico da Relevância para o Grupo de Segurança de Processo Industrial.....	100
Figura 27- Mapa mental de relação do grupo de Rede Industrial com outros grupos.....	117
Figura 28 - Principais atores das diferentes partes da série IEC 62657.....	119
Figura 29 - Exemplo visual da comunicação sem fio em um ambiente de automação industrial.....	120
<i>Figura 30 - Modelo conceitual de coexistência de comunicação sem fio em diversas aplicações.....</i>	<i>121</i>
Figura 31 - Consolidação da análise do grupo de Rede Industrial.....	122
Figura 32 - Infográfico da Relevância da Rede Industrial.....	125
Figura 33 - Partes do framework da Fábrica Digital.....	126
Figura 34 - Mapa mental de relação do grupo de Fábrica Digital com outros grupos.....	129
Figura 35 – Consolidação da análise do Grupo de Fábrica Digital.....	130
Figura 36 – Processos existentes em Fábricas Digitais.....	131
<i>Figura 37 – Infográfico da Relevância para o Grupo de Fábrica Digital.....</i>	<i>132</i>
Figura 38 - Principais facetas da interoperabilidade.....	134
Figura 39 - Esquema de interoperabilidade de Sistemas IoT.....	135
Figura 40 - Mapa mental de relação do grupo de Internet das Coisas e Gêmeo Digital com outros grupos.....	139
Figura 41 - Esquematização de três níveis da dinâmica social humana para o uso de IoT.....	141

Figura 42 - Aplicação de um serviço de IIoT com os equipamentos industriais.....	142
Figura 43 - Exemplificação do uso de IoT na área agrícola.....	144
Figura 44 - Consolidação da análise do Grupo de Internet das Coisas e Gêmeo Digital	146
Figura 45 - Infográfico da Relevância da Internet das Coisas.....	150
Figura 46 - Infográfico da Relevância para o Grupo de Internet das Coisas e Digital Twin – Parte 2 – Digital Twin.....	153
Figura 47 - Composição da Série 18228	157
Figura 48 - Interrelação das diferentes partes da série ISO 18828.....	159
Figura 49 - Ciclo de vida das partes da série ISO 18828	159
Figura 50 - Mapa mental de relação do grupo de Dados Industriais com outros grupos.....	164
Figura 51 - Consolidação da análise do Grupo de Dados Industriais.....	169
Figura 52 - Infográfico da Relevância para o Grupo de Dados Industriais..	173
Figura 53 - Categorização dos robôs e a relação com outras áreas relevantes.....	179
Figura 54 - Mapa mental de relação do grupo de Robótica com outros grupos.....	183
Figura 55 - Consolidação da análise do Grupo de Robótica.....	186
Figura 56 - Infográfico da Relevância para o Grupo de Robótica.....	189

Lista de Tabelas

Tabela 1 - Detalhamento da metodologia para o conteúdo do Relatório.....	16
Tabela 2 - Normas do grupo de Inteligência Artificial.....	18
Tabela 3 - Normas em relação a tendências do grupo de Inteligência Artificial	24
Tabela 4 - Casos de uso de machine learning em redes futuras.....	29
Tabela 5 - Normas do grupo de Machine Learning para Redes do futuro.....	30
Tabela 6 - Detalhamento da metodologia para o conteúdo do Relatório.....	48
Tabela 7- Normas do grupo de Segurança de Máquinas	51
Tabela 8 - Normas referentes a tendências do grupo de Segurança de Máquinas.....	55
Tabela 9 - Normas Regulamentadoras, de Segurança de Máquinas objetivos e exemplos de aplicações na Indústria 4.0	59
Tabela 10 - Normas do grupo de Segurança da informação, cibersegurança e proteção da privacidade.....	64
Tabela 11 - Normas referentes a tendências do grupo de Segurança da informação	72
Tabela 12 - Ciclo de vida de produção inteligente e risco cibernético (DELOITTE., 2020).....	76
Tabela 13 - Desafios e soluções de segurança na digitalização industrial.....	79
Tabela 14 - Normas do grupo de Segurança de processos industriais	81
Tabela 15 - Normas referentes a tendências do grupo de Segurança para processo industrial	91
Tabela 16 - Casos de cidades inteligentes	96
Tabela 17 - Casos de cidades inteligentes brasileiras.....	96
Tabela 18 - Casos de Transporte no mundo.....	98
Tabela 19 - Detalhamento da metodologia para o conteúdo do Relatório ..	111
Tabela 20 - Principais Normas do grupo de Rede Industrial	115
Tabela 21 - Normas que estão sendo trabalhadas para substituir outras normas.....	118
Tabela 22 - Normas referentes a tendências do grupo de Rede Industrial.	121
Tabela 23 - Empresas que utilizam tecnologias relacionadas às Redes Industriais no Brasil.....	124
Tabela 24 - Normas do grupo de Fábrica Digital	127

Tabela 25 - Compreendendo a interoperabilidade no IoT.....	134
Tabela 26- Tabela de Normas do grupo de Internet das Coisas e Gêmeo Digital.....	137
Tabela 27 - Descrição dos principais casos de uso do Blockchain e IoT	143
Tabela 28 - Normas referentes a tendências do grupo de IoT e Gêmeo Digital.....	145
Tabela 29 - Aplicações da Internet das Coisas.....	148
Tabela 30 - Normas do grupo de Dados Industriais.....	161
Tabela 31 - Normas referentes a tendências do grupo de Dados Industriais	168
Tabela 32 - Aplicações dos Dados Industriais.....	172
Tabela 33 - Ferramentas utilizadas baseadas em Dados Industriais.....	173
Tabela 34 - Requisitos de segurança para sistemas de robôs industriais colaborativos	176
Tabela 35- Resumo das categorias de robôs.....	180
Tabela 36 - Normas do grupo de Robótica.....	181
Tabela 37 - Normas referentes a tendências do grupo de Robótica	185

Referências

AI MULTIPLE. **15 Digital Twin Applications**. 2021. Disponível em: <https://research.aimultiple.com/digital-twin-applications/>

AMAZON. **AGCO Lowers costs, boosts speed, and increases retention using Amazon Kinesis Services**. 2021. Disponível em: https://aws.amazon.com/solutions/case-studies/agco-case-study/?did=cr_card&trk=cr_card

ARC. **Concepts and applications of the i4.0 asset administration shell**. 2019. Disponível em: <https://www.arcweb.com/blog/concepts-applications-i40-asset-administration-shell>

ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA DE MÁQUINAS E EQUIPAMENTOS – ABIMAQ; UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL - UFRGS, NÚCLEO DE ENGENHARIA ORGANIZACIONAL - NEO. **Indústria 4.0**. Transformação digital e inovação de modelos de negócio na indústria de máquinas e equipamentos. pesquisa industrial. 2021. 33 p. Disponível em: <https://camara40.com.br/wp-content/uploads/2021/06/Relatorio-Geral-ABIMAQ-Final-R05.pdf>

AUTOMAÇÃO INDUSTRIAL. **A LGPD na Indústria 4.0**. 2021. Disponível em: <https://www.automacaoindustrial.info/a-lgpd-na-industria-4-0/>

A VOZ DA INDÚSTRIA. **Análise de dados industriais: decisões rápidas e seguras**. 2018. Disponível em: <https://avozdaindustria.com.br/industria-40-totvs/anlise-de-dados-industriais-decises-rpidas-e-seguras>

BADRI, Adel; BOUDREAU-TRUDEL, Bryan; SOUISSI, Ahmed Saâdeddine. Occupational health and safety in the industry 4.0 era: A cause for major concern?. **Safety science**, v. 109, p. 403-411, 2018. Disponível em: <https://iranarze.ir/wp-content/uploads/2018/09/E9588-IranArze.pdf>

BANCO NACIONAL DO DESENVOLVIMENTO - BNDES. **Internet das Coisas: Um plano de ação para o Brasil**. 2018. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/445c4dd8-069b-47c1-b191-767caee4a5ae/produto-9B-relatorio-final-sintese-do-estudo-de-lot-atualizado.pdf?MOD=AJPERES&CVID=m87qOtl>

BANCO NACIONAL DO DESENVOLVIMENTO - BNDES. **Produto 3, análise de oferta e demanda**. Relatório parcial – Aspiração do Brasil em Internet das Coisas. 2017. 20 p. Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/d1348f10-c93d-408e-8c2d-a2c2a6e4efb1/170614_Produto_Parcial_Frente+3_Aspiracao_IoT_Final.pdf?MOD=AJPERES&CVID=IOOirj1

BANCO NACIONAL DO DESENVOLVIMENTO - BNDES. **Produto 7D: Aprofundamento de verticais – Indústrias**. 2017. Disponível em: <https://www.bndes.gov.br/wps/wcm/connect/site/cfbd69ff-56d7-43f4-82df-f05b40459ec7/relatorio-aprofundamento-das-verticais-industria-produto-7D.pdf?MOD=AJPERES&CVID=m3xwf3m>

BENETTI, Estela. **Anatel autoriza testes de 5G na indústria. WEG faz o projeto experimental.** 2020. Disponível em: <https://www.nsctotal.com.br/colunistas/estela-benetti/anatel-autoriza-testes-de-5g-na-industria-weg-faz-o-projeto-experimental>

BENETTI, Estela. **WEG conclui testes de conectividade de redes 5G em fábrica de Jaraguá do Sul.** 2021. Disponível em: <https://www.nsctotal.com.br/colunistas/estela-benetti/weg-conclui-testes-de-conectividade-de-redes-5g-em-fabrica-de-jaragua-do>

BIP BRASIL. **Digital twins:** o produto digital da indústria de capital intensivo. 2020. Disponível em: <https://bipbrasil.com.br/digital-twins-o-produto-digital-da-industria-de-capital-intensivo/>

BONGINI, Paola *et al.* **Global report on business continuity planning and management (BCP/BCM).** Survey results. nov. 2, 2020, 2020. Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3764401_code2141546.pdf?abstractid=3764401&mirid=1

BRASIL. Ministério da Economia. **Análise de impacto regulatório.** Norma Regulamentadora n. 05; Comissão interna de prevenção de acidentes. 2021b. 126 p. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/air/relatorios-de-air/seprt/strab/sit/relatorio-air-nr-05.pdf>

BRASIL. Ministério da Economia. **Análise de impacto regulatório.** Norma Regulamentadora n. 17; Ergonomia. 2021c. 152 p. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/air/relatorios-de-air/seprt/strab/sit/relatorio-air-nr-17.pdf>

BRASIL. Ministério da Ciência, Tecnologia e Inovações - MCTI. **Publicada estratégia brasileira de inteligência artificial.** 12 abr. 2021a. Disponível em: <https://www.gov.br/pt-br/noticias/educacao-e-pesquisa/2021/04/publicada-estrategia-brasileira-de-inteligencia-artificial>

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Plano nacional de internet das coisas.** 2019b. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas>

BRASIL. Presidência da República. **Decreto nº 9.854, de 25 de junho de 2019.** Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. 2019c. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/ArquivosInternetDasCoisas/d9854.pdf>

BRASIL. Presidência da República. **Lei Geral de Proteção de Dados (LGPD);** Lei nº 13.853 de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

CARGO. **Segurança em transporte de cargas:** um guia para evitar prejuízos. 2018. Disponível em: <https://cargox.com.br/blog/seguranca-de-transporte-das-cargas-um-guia-para-evitar-prejuizos>

CB INSIGHTS. **AI 100:** the artificial intelligence startups redefining industries. 7 apr. 2021. Disponível em: <https://www.cbinsights.com/research/report/artificial-intelligence-top-startups/>

CIO FROM DIG. **Para CIOs e CTOs, machine learning, IA, 5G e IoT serão as tecnologias mais importantes em 2021.** 2020. Disponível em: <https://cio.com.br/tendencias/para-cios-e-ctos-machine-learning-ia-5g-e-iot-serao-as-tecnologias-mais-importantes-em-2021/>

CISCO; ROCKWELL AUTOMATION. Travessia segura de dados IACS pela zona desmilitarizada industrial. 2015. 6 p. Disponível em: https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp038_-pt-p.pdf

COOPERAÇÃO ALEMÃ PARA O DESENVOLVIMENTO SUSTENTÁVEL POR MEIO DA DEUTSCHE GESELLSCHAFT FÜR INTERNATIONALE ZUSAMMENARBEIT - GIZ; SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL - SENAI; NÚCLEO DE ENGENHARIA ORGANIZACIONAL, DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO E TRANSPORTES UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL - NEO-UFRGS. **Profissões emergentes na era digital:** Oportunidades e desafios na qualificação profissional para uma recuperação verde. 2021. 79 p. 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

DATASEBRAE. **Cobots.** 2018. Disponível em: <https://datasebrae.com.br/cobots/>

DATUMIZE. **Types of Industrial Data services you need to know about in 2020.** 2020. Disponível em: <https://blog.datumize.com/types-of-industrial-data-services-you-need-to-know-about-in-2020>

DEEPSIG. **How artificial intelligence improves 5G wireless capabilities.** 2021. Disponível em: <https://www.deepsig.ai/how-artificial-intelligence-improves-5g-wireless-capabilities>

DELOITTE. **2019 Deloitte and MAPI smart factory study.** Capturing value through the digital journey. 2019. Disponível em: https://www2.deloitte.com/content/dam/insights/us/articles/6276_2019-Deloitte-and-MAPI-Smart-Factory-Study/DI_2019-Deloitte-and-MAPI-Smart-Factory-Study.pdf

DELOITTE. Industry 4.0 and cybersecurity. **Managing risk in an age of connected production** 2020. 24 p. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/cip/deloitte-cn-cip-industry4-0-cybersecurity-en-180119.pdf>

ERP. **SAP anuncia solução com foco na indústria 4.0.** 2019. Disponível em: <https://portalerp.com/sap-anuncia-solucao-com-foco-na-industria-40>

EXAME PELO BEM. **6 aplicativos para facilitar a vida do caminhoneiro.** 2019. Disponível em: <http://www.tommasianalitica.com.br/examepelobem.com.br/pt-br/post/aplicativos-para-caminhoneiros/>

FACULTY. **Improving bus scheduling with AI algorithms.** 2021. Disponível em: <https://faculty.ai/ourwork/improving-bus-scheduling-with-ai-algorithms/>

FINEP. **Finep IoT.** s.d. Disponível em: <http://www.finep.gov.br/apoio-e-financiamento-externa/programas-e-linhas/finep-iot>

FORBES. **15 países com mais mão de obra robotizada**. 2018. Disponível em <https://www.forbes.com.br/principal/2018/05/15-paises-com-mais-mao-de-obra-robotizada/>

G1. Economia. **Em meio à pandemia, Brasil abriu 2,3 milhões de empresas a mais do que fechou em 2020, diz ministério**. 2021. Disponível em: <https://g1.globo.com/economia/noticia/2021/02/02/brasil-registra-saldo-positivo-de-23-milhoes-empresas-abertas-em-2020-diz-ministerio-da-economia.ghtml>

GARTNER. **5 Questions that CISOs must answer before adopting artificial intelligence**. 2020. 25 p. Disponível em: <https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/466678-5-questions-that-cisos-must-answer-before-adopting-artificial-intelligence.pdf>

GEEKSFORGEES. **Top 10 applications of robotics in 2020**. 2020. Disponível em: <https://www.geeksforgeeks.org/top-10-applications-of-robotics-in-2020/>

GENESIS-SYSTEMS. **Robots in automotive manufacturing: top 6 applications**. 2020. Disponível em: <https://www.genesis-systems.com/blog/robots-automotive-manufacturing-top-6-applications>

GOLDBACH. **Conheça o coração do Gêmeo Digital: AAS**. 2020. Disponível em: <https://www.linkedin.com/pulse/conhe%25C3%25A7a-o-cora%25C3%25A7%25C3%25A3o-do-g%25C3%25AAmeo-digital-aas-claudio-henrique-goldbach/?trackingId=LADdUvtxQbuap792204mzg%3D%3D>

GRAND VIEW RESEARCH. **Digital twin market size, share & trends analysis report by end-use**. 2021. Disponível em: <https://www.grandviewresearch.com/industry-analysis/digital-twin-market>

IACO. **Indústria 4.0 e segurança no trabalho**. 2019. Disponível em: <https://iaco.com.br/industria-4-0/>

IBM. **Cost of a Data Breach Report 2021**. 2021. Disponível em: <https://www.ibm.com/security/data-breach>

IDEMP. **Gestão de crise e continuidade de negócios**. 2020. Disponível em: <http://idemp-edu.com.br/cursos/308>

IEBS. **O que é SAP e para que serve?** 2019. Disponível em: <https://www.iebschool.com/pt-br/blog/software-de-gestao/o-que-e-sap-e-para-que-serve/>

IND 4.0. **LGPD: O que você precisa saber**. 2020. Disponível em: <https://www.industria40.ind.br/artigo/20330-igpd-o-que-voce-precisa-saber>

INDUSTRIAL 4.0. **As normas regulamentadoras na indústria 4.0**. 2019. Disponível em: <https://industrial4-0.com.br/as-normas-regulamentadoras-na-industria-4-0/>

INDUSTRIAL INTERNAET CONSORTIUM. **Digital twin and asset administration shell concepts and application in the industrial internet and industrie 4.0**. 2020. Disponível em: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Digital-Twin-and-Asset-Administration-Shell-Concepts.pdf?__blob=publicationFile&v=9

INFOMONEY. **Indústria 4.0: a Embraer e a nova revolução industrial.** 2019. Disponível em: <https://www.infomoney.com.br/negocios/industria-4-0-a-embraer-e-a-nova-revolucao-industrial/>

INFORCHANNEL. **Uso combinado de 5G, IoT, Big Data e IA traz novas possibilidades para os negócios.** 2020. Disponível em: <https://inforchannel.com.br/2020/11/03/uso-combinado-de-5g-iot-big-data-e-ia-traz-novas-possibilidades-para-os-negocios/>

INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS - IEEE. **Artificial intelligence and machine learning, 5G, and IoT will be the most important technologies in 2021, according to new IEEE study.** 2020. Disponível em: <https://www.ieee.org/about/news/2020/survey-chief-information-officers-and-chief-technology-officers.html>

INTEL; DELL TECHNOLOGIES. **Smarter, safer cities; improving public safety in the age of AI and IoT.** 2019. 35 p. Disponível em: <https://www.delltechnologies.com/asset/en-hr/products/gateways-and-embedded-computing/briefs-summaries/intel-dell-improving-public-safety-in-the-digital-age-ebook.pdf>

INTERNATIONAL ELECTROTECHNICAL COMMISSION - IEC. **Factory of the future.** White paper. 2019. 49 p. Disponível em: https://storage-iecwebsite-prd-iec-ch.s3.eu-west-1.amazonaws.com/2019-09/content/media/files/iec_wp_factory_of_the_future_en_lr.pdf

INTERNATIONAL ELECTROTECHNICAL COMMISSION - IEC. **Internet of Things: Wireless Sensor Networks.** White Paper. 2014. 78 p. Disponível em: <http://pubweb2.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf>

INTERNATIONAL ELECTROTECHNICAL COMMISSION - IEC. **IoT 2020: Smart and secure IoT platform.** White paper. 2020. 181 p. Disponível em: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/englisch/iecWP-IoT2020-LR.pdf

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **Artificial intelligence in robotics.** 2018a. Enviado por email pela IFD

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **Demystifying collaborative industrial robots.** 2020. Enviado por email pela IFR.

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **Robots create jobs!** 2021. Disponível em: <https://ifr.org/robots-create-jobs>

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **The impact of robots on productivity, employment and jobs.** 2018b. Enviado por email pela IFR.

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **Top 5 robot trends 2021.** 2021. Disponível em: <https://ifr.org/ifr-press-releases/news/top-5-robot-trends-2021>

INTERNATIONAL FEDERATION OF ROBOTICS - IFR. **Top trends robotics.** 2020a. Disponível em: <https://ifr.org/news/top-trends-robotics-2020>

IT2B. **Conheça 5 smart cities do mundo e se inspire nesses cases de sucesso.** 2018. Disponível em: <https://www.it2b.com.br/2018/05/10/conheca-5-smart-cities-do-mundo-e-se-inspire-nesses-cases-de-sucesso/>

ITU. **Global cybersecurity index**. 2018. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

ITU. **ITU AI/ML in 5G Challenge**. 2020. Disponível em: <https://www.itu.int/en/ITU-T/AI/challenge/2020/Pages/default.aspx>

JORDAN, M.I.; MITCHELL, T.M. Machine learning: Trends, perspectives, and prospects. **Science**, v. 349, n. 6245, p. 255-260. 2015. Disponível em: <https://www.cs.cmu.edu/~tom/pubs/Science-ML-2015.pdf>

KLUMPP, M.; HESENIUS, M.; MEYER, O.; RUINER, C.; GRUHN, V. Production logistics and human-computer interaction—state-of-the-art, challenges and requirements for ^{the} future. **International Journal of Advanced Manufacturing Technology**, v. 105, n. 9, p. 3691–3709. 2019. Disponível em: <https://link.springer.com/content/pdf/10.1007/s00170-019-03785-0.pdf>

LEE, John; CAMERON, Ian; HASSALL, Maureen. improving process safety: What roles for digitalization and industry 4.0?. **Process safety and environmental protection**, v. 132, p. 325-339, 2019. Disponível em: <https://www.semanticscholar.org/paper/Improving-process-safety%3A-What-roles-for-and-4.0-Lee-Cameron/1b5c917c9ca41c886d17e5f175eefe7df39a0402>

LOGIQUE SISTEMAS. **5 estratégias essenciais para melhor aproveitar os dados gerados pela sua indústria**. 2019. Disponível em: <https://www.logiquesistemas.com.br/blog/como-aproveitar-dados-industriais/>

LOGIQUE SISTEMAS. **BR-Collector** – Estudo de caso: Sistema integrado de coleta de dados. 2018b. Disponível em: <https://www.logiquesistemas.com.br/blog/sistema-de-coleta-de-dados-br-collector/>

LOGIQUE SISTEMAS. **Sistema historiador de dados [Case: BR-PlantHistorian]**. 2018a. Disponível em: <https://www.logiquesistemas.com.br/blog/historiador-de-dados-br-planthistorian/>

MARKETANDMARKETS. **Industrial networking solutions market by technology (SDWAN, WLAN, & IIoT), service (network planning & optimization, & integration), application (predictive maintenance, & emergency & incident management), vertical, and region - Global Forecast to 2022**, 2017. Disponível em: <https://www.marketsandmarkets.com/Market-Reports/industrial-networking-solutions-market-263573485.html>

MCKINSEY & COMPANY. **Brazil digital report 2019**. 2020b. Disponível em: https://www.mckinsey.com/br/~/_media/McKinsey/Locations/South%20America/Brazil/Our%20Insights/Brazil%20Digital%20Report/Brazil-Digital-Report-1st-Edition_Portuguese-vAjustado.pdf

MCKINSEY & COMPANY. **Growth dynamics in industrial robotics**. 2019. Disponível em: <https://www.mckinsey.com/industries/advanced-electronics/our-insights/growth-dynamics-in-industrial-robotics>

MCKINSEY & COMPANY. **The state of AI in 2020**. Survey: 17 nov. 2020a. Disponível em: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020>

MCKINSEY & COMPANY. **Welcome to the Digital Factory**: The answer to how to scale your digital transformation. 2020c. Disponível em: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/welcome-to-the-digital-factory-the-answer-to-how-to-scale-your-digital-transformation>

MENGES, R. Frühzeitige produktbeeinflussung und prozessabsicherung. zeitschrift für wirtschaftlichen fabrikbetrieb. München: **Carl Hanser Verlag**. 2005. p. 25-31

MERCADO & CONSUMO. **Mercado Livre**: Entrega no mesmo dia reforça aposta em logística para fidelizar cliente. 2021. Disponível em: <https://mercadoeconsumo.com.br/2021/06/21/mercado-livre-entrega-no-mesmo-dia-reforca-aposta-em-logistica-para-fidelizar-cliente/>

MICROSOFT. **PepsiCo uses Azure Machine Learning to identify consumer shopping trends and produce store-level actionable insights**. 2021. Disponível em: <https://customers.microsoft.com/en-us/story/754571-pepsico-consumer-goods-azure-machine-learning>

MIND COMMERCE. **Internet of Things (IoT) Information and Reports**. 2021. Disponível em: <https://mindcommerce.com/report-category/internet-of-things/>

MURR ELEKTRONIK. **Mercado brasileiro de automação industrial**: Análise da pesquisa, 2017. Disponível em: <http://blog.murrelektronik.com.br/mercado-brasileiro-de-automacao-industrial-analise-pesquisa/>

NEC. **BCM para conter violação de dados**. 2017. Disponível em: <https://blog.nec.com.br/bcm-para-conter-a-violacao-de-dados>

NETSEG. **ABO20 e Detran.SP firmam parceria para segurança no trânsito com aplicativos**. 2020. Disponível em: <https://netseg.com.br/not.php?id=7946>

PETROBRAS. **O que são digital twins e como podem aumentar a eficiência operacional**. 2019. Disponível em: <https://nossaenergia.petrobras.com.br/pt/energia/o-que-sao-digital-twins-e-como-podem-aumentar-a-eficiencia-operacional/>

PHENG, Low Sui; YING, Liu Jun; KUMARASWAMY, Mohan. Institutional compliance framework and business continuity management in Mainland China, Hong Kong SAR and Singapore. **Disaster Prevention and Management: An International Journal**, v.19, n.5, 2010. Disponível em: <https://ur.booksc.eu/dl/52762891/1b220e>

PLANET SMART CITY LAGUNA. **Smart City Laguna**. 2021. Disponível em: <https://www.planetsmartcity.com/projects/smart-city-laguna/>

PLANET SMART CITY LAGUNA. **Soluções smart**. s.d. Disponível em: <https://www.planetsmartcity.com.br/smart-solutions/laguna>

PLATTFORM INDUSTRIE 4.0. **Details of the asset administration shell from idea to implementation**. 2019. 60 slides. Disponível em: <https://www.plattform->

i40.de/PI40/Redaktion/EN/Downloads/Publikation/vws-in-detail-presentation.pdf?__blob=publicationFile&v=12

PODER AÉREO. **Embraer implantará “fábrica digital”**. 2011. Disponível em: <https://www.aereo.jor.br/2011/04/28/embraer-implantara-fabrica-digital/>

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS - PUC/MG. Instituto de Educação Continuada. **Segurança em processos industriais**. 2021. Disponível em: https://www.pucminas.br/Pos-Graduacao/IEC/Cursos/Paginas/Seguranca%20em%20Processos%20Industriais_BH%20-%20Campus%20Coracao%20Eucaristico_Especializacao%20e%20Master.aspx

PTC. **Bell and Howell drives innovation with IoT process automation**. 2020. Disponível em <https://www.ptc.com/en/case-studies/bell-and-howell>

REDE RS INDÚSTRIA 4.0. **Como startups e suas provas de conceito (PoCs) podem auxiliar a sua empresa na jornada 4.0?** 2021. Disponível em: <https://redeindustria40.com.br/como-startups-e-suas-provas-de-conceito-pocs-podem-auxiliar-a-sua-empresa-na-jornada-4-0/>

REGIS *et al.* Aspectos relevantes sobre Cibersegurança na Indústria 4.0. *In*: CONGRESSO BRASILEIRO DE ENGENHARIA DE PRODUÇÃO, 9., Ponta Grossa, PR 04-06 dez. 2019. **Anais...** Ponta Grossa, PR, 2019. 11 p. Disponível em: http://aprepro.org.br/conbrepro/2019/anais/arquivos/09302019_230913_5d92b3e18708f.pdf

RIOONWATCH. **Rio de Janeiro’s landslide mitigation tactics**. Part 1: A technical history and overview. 2021. Disponível em: <https://rioonwatch.org/?p=54009>

ROLDÁN, J.J.; CRESPO, E.; MARTÍN-BARRIO, A.; PEÑA-TAPIA, E.; BARRIENTOS, A. A training system for Industry 4.0 operators in complex assemblies based on virtual reality and process mining. **Robotics and Computer-Integrated Manufacturing**, v. 59, p. 305-316. 2019. Disponível em: https://oa.upm.es/67144/1/INVE_MEM_2019_334893.pdf

SAS. **Machine learning**. What it is and why it matters. 2021. Disponível em: https://www.sas.com/en_us/insights/analytics/machine-learning.html

SEEQ. **Case study**: Devon Energy uses real-time data and advanced analytics to make better decisions. 2018. Disponível em: <https://info.seeq.com/devon-energy-uses-real-time-data-and-advanced-analytics-to-make-better-decisions>

SENIOR. **A relação da cibersegurança com a indústria 4.0**. 2020. Disponível em: <https://www.senior.com.br/blog/a-relacao-da-ciberseguranca-com-a-industria-4-0>

SERCON. **Profissional de SST (na indústria) 4.0**. 2019. Disponível em: <https://serconmed.com.br/profissional-sst-industria-40/>

SIEMBRA AUTOMAÇÃO. **Entenda o cenário da automação industrial no Brasil**. 2018. Disponível em: <https://www.siembra.com.br/noticias/entenda-o-cenario-da-automacao-industrial-no-brasil/>

SILVEIRA, P.M. da. Plano de continuidade de negócios para a empresa ALFA: uma proposta com base na NBR 15999, no ITIL e no COBIT. **Revista da Graduação**, v. 2, n. 2. 2009. Disponível

em: <https://revistaseletronicas.pucrs.br/ojs/index.php/graduacao/article/view/6065> e <https://revistaseletronicas.pucrs.br/ojs/index.php/graduacao/article/view/6065/4366>

SIMPLE. 5G e inteligência artificial: o que esperar dessa relação? 2020. Disponível em: <https://simple.nama.ai/post/5g-e-inteligencia-artificial-o-que-esperar-dessa-relacao>

SOUTHIE AUTONOMY. Robotics myth 1: repeatability and accuracy. 2020. Disponível em: <https://www.southieautonomyworks.com/blog/2020/5/18/robotics-myth-1-repeatability-and-accuracy>

STEFANINI GROUP. As 7 principais aplicações da inteligência artificial nas empresas. Disponível em: <https://stefanini.com/pt-br/trends/artigos/as-7-principais-aplicacoes-de-inteligencia-artificial-nas-empres>

SUMMIT MOBILIDADE URBANA. Quais são as 3 cidades mais inteligentes do Brasil? 2021. Disponível em: <https://summitmobilidade.estadao.com.br/ir-e-vir-no-mundo/quais-sao-as-3-cidades-mais-inteligentes-do-brasil/>

SUSTAINABLE BUS. Artificial Intelligence under the bonnet. Volvo Buses unveiled the first driverless bus in Singapore. 2019. Disponível: <https://www.sustainable-bus.com/news/artificial-intelligence-under-the-bonnet-volvo-buses-unveiled-the-first-driverless-bus-in-singapore/>

TECHPLUS. 5 formas que a tecnologia da Indústria 4.0 pode contribuir com a segurança. s.d. Disponível em: <https://www.techplus.com.br/5-formas-tecnologia-industria-4-0-contribuir-seguranca/>

TECHPLUS. Integração do SAP com chã-de-fábrica através de B2MMI. s.d. Disponível em: <https://www.techplus.com.br/sap/>

UDACITY. Artificial intelligence for robotics. 2021. Disponível em: <https://www.udacity.com/course/artificial-intelligence-for-robotics--cs373>

UPPERTOOLS. Cibersegurança na Indústria 4.0: qual a importância e como garanti-la? 2020. Disponível em: <https://www.uppertools.com.br/blog/ciberseguranca-na-industria-4-0-qual-a-importancia-e-como-garanti-la/>

V2COM. Brasil tem 19% dos projetos de IoT em produção na América Latina. 2020. Disponível em: <https://v2com.com/2020/06/30/mercado-brasileiro-internet-das-coisas-20/>

VDI BRASIL. Instituições alemãs criam Associação de Digital Twin. 2021. Disponível em: <https://www.vdibrasil.com/instituicoes-alemas-criam-associacao-de-digital-twin/>

VENTURE BEAT - VB. Brazil is emerging as a world-class Ai innovation hub. 12 jan.2020. Disponível em: <https://venturebeat.com/2020/01/12/brazil-is-emerging-as-a-world-class-ai-innovation-hub/>

VENTURE BEAT - VB. Optibus raises \$40 million for AI that optimizes bus routes. 2018. Disponível em: <https://venturebeat.com/2018/12/12/optibus-raises-40-million-for-ai-that-optimizes-bus-routes/>

VOITTO. Cibersegurança: a chave para a proteção de dados! 2020. Disponível em: <https://www.voitto.com.br/blog/artigo/ciberseguranca>

WIFILIVRESP. **O que é o programa WifilivreSP**. 2021. Disponível em:
<https://wifilivre.sp.gov.br/programa.html>

WIKIPÉDIA. **Fieldbus**. 2020. Disponível em: <https://pt.wikipedia.org/wiki/Fieldbus>. Acesso em:
15 ago. 2021.

WIPO. **Índice global de inovação 2020**. 2020. Disponível em:
https://www.wipo.int/edocs/pubdocs/pt/wipo_pub_gii_2020.pdf

WORLD ECONOMIC FORUM - WEF. **Future of jobs report**. oct. 2020. 163 p. Disponível em:
http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

WORLDFIRST. **Cybersecurity threats to Industry 4.0 – and the key to resilience**. 2020.
Disponível em: <https://www.worldfirst.com/uk/blog/economic-updates/industry-4-0-cyber-security-threats/>

WORLD WIDE TECHNOLOGY. **11 Smart city use cases**. 2020. Disponível em:
<https://www.wwt.com/article/11-smart-city-use-cases>



Centro de Gestão e Estudos Estratégicos
Ciência, Tecnologia e Inovação

CÂMARA DE
INOVAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA E
INOVAÇÕES



PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL