

5G NA INDÚSTRIA

A QUESTÃO DA SEGURANÇA CIBERNÉTICA

DATA: 26/08/21 HORÁRIO: 10:00h-12:00h



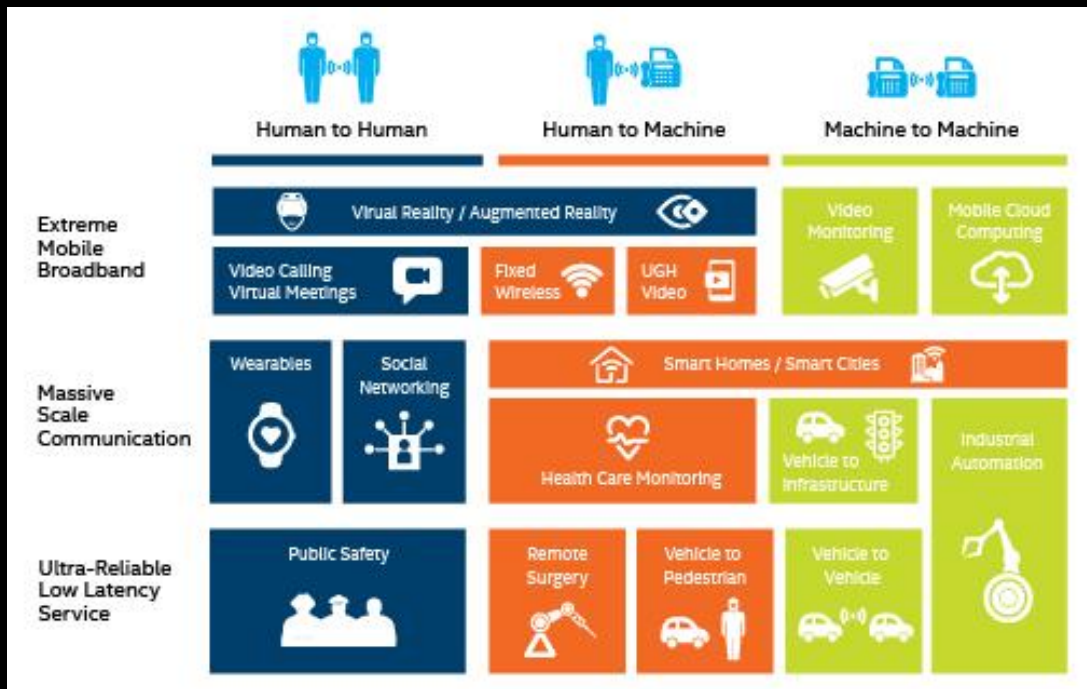
Tecnologia 5G, o que é?



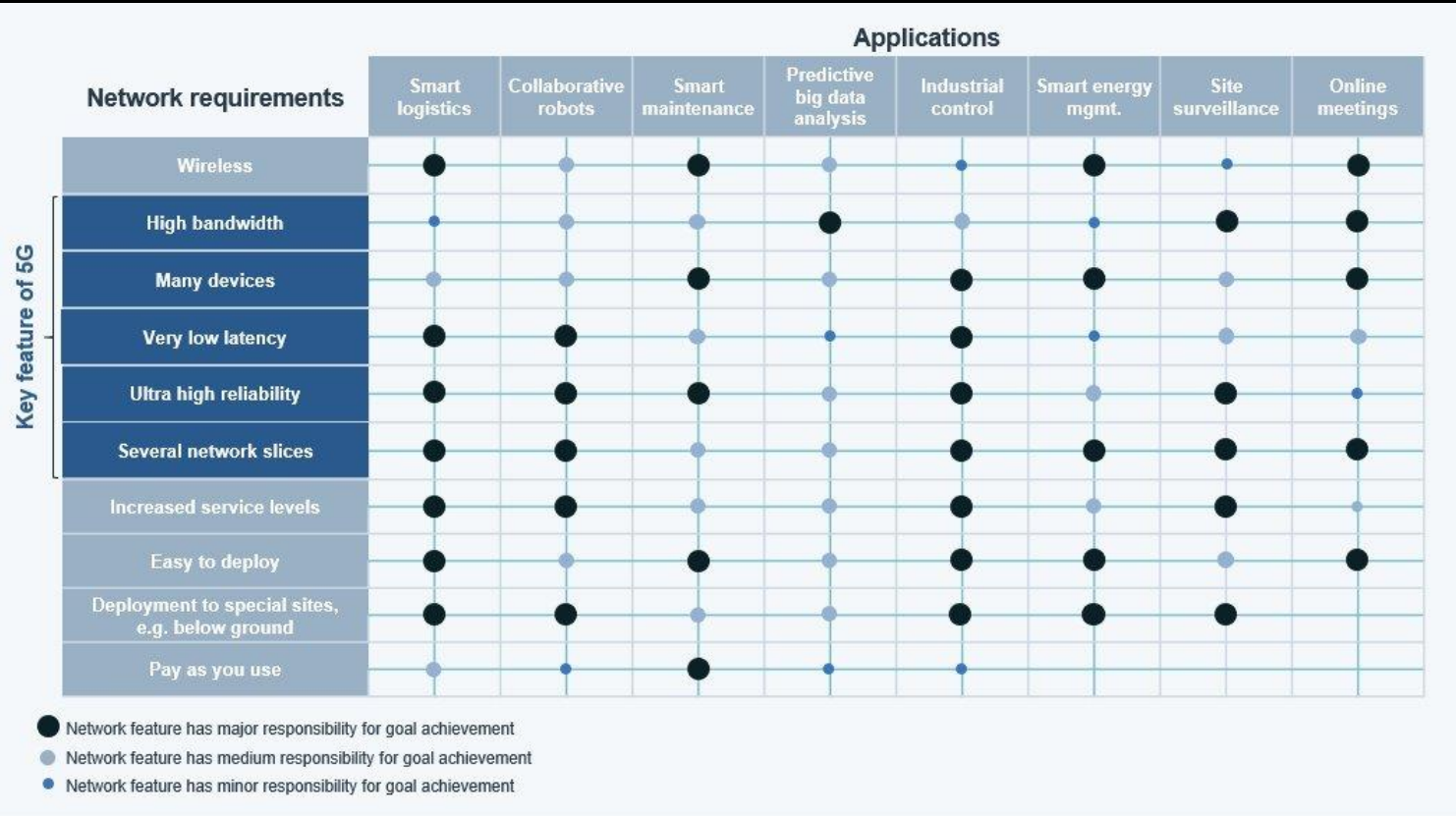
**Visão IMT-2020
(Rec. ITU-R M.2083-0)**

5G

**Infraestrutura Wireless
para Conectar
o Mundo**



Por que o 5G na Indústria?



Por que o 5G na Indústria?

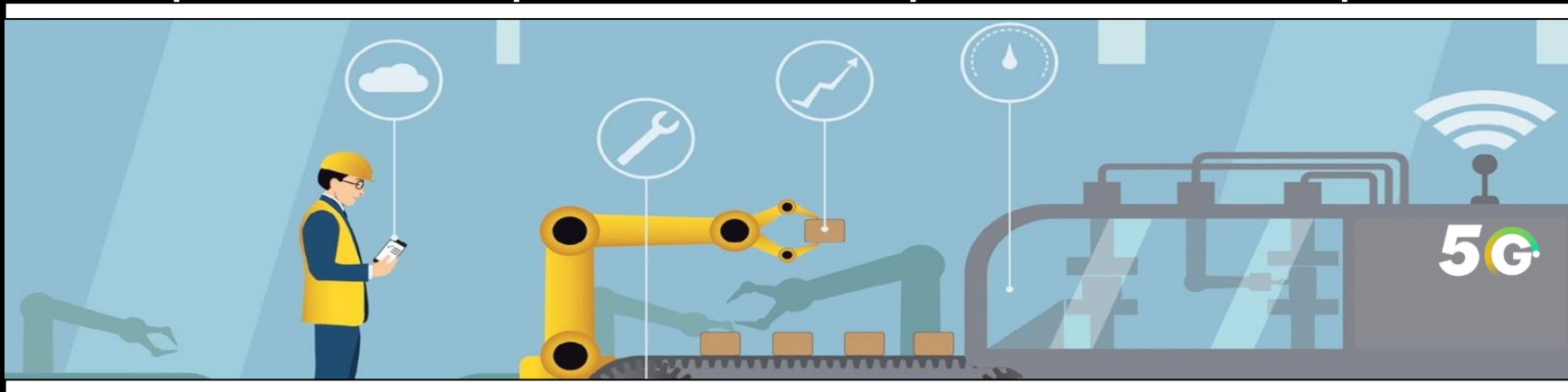


Equipamentos conectados
e auto sensíveis

Análise, inspeção e
predição por visão
computacional

Digital Twin: Predição de
falhas e prescrição de
ações de resposta

Dados em Realidade
Aumentada: desempenho,
histórico, instruções, ...



Rastreabilidade da
cadeia produtiva com
blockchain

Soluções de
Sensoriamento para
ambientes perigosos

Automação por comando
de voz e interfaces
conversacionais

Embarque de Inteligência
Artificial em produtos e
equipamentos

Por que o 5G na Indústria?

A questão-chave é o quanto deste Mercado poderemos capturar no Brasil ?

Criação Valor nas cadeias estratégicas



Benefícios acumulados com aplicações 5G em setores estratégicos do BR em 2030

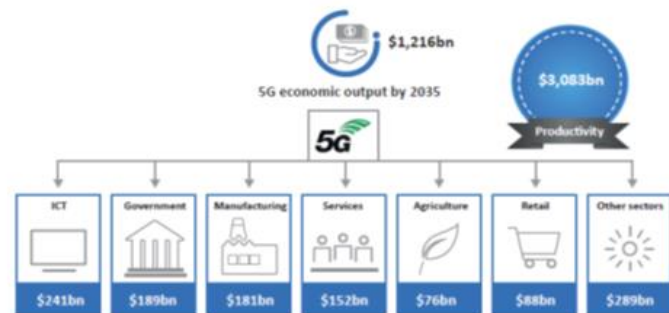


- **R\$ 323 Bi** de geração de benefícios em 10 anos em todos os setores da economia brasileira
- Impacto anualizado em **0,54% do PIB**
- Aplicações vs. Mercados mais promissores:
 - Drones
 - Veículos autônomos
 - Automação industrial
 - Portos
 - Indústria petrolífera

Fonte: Análise Deloitte
(em elaboração)

Por que o 5G na Indústria?

Figure 5.16: Brazil, 5G economic and social value impact



Source: Omdia, based on Omdia and Bell Lab economic models

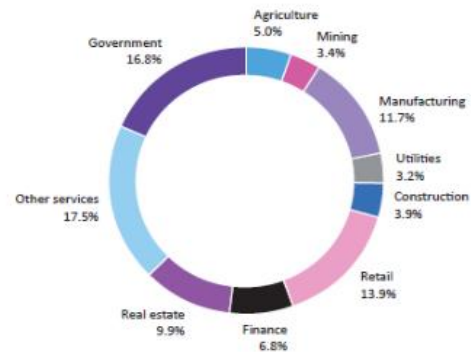


Table 5.1: 5G economic and social impact by Latin American country, 2020–35

	Argentina	Brazil	Chile	Colombia	Mexico	Peru	Total
Agriculture	33.6	76.8	10.5	15.1	33.7	11.0	180.7
Mining	16.4	48.6	23.8	11.4	43.6	21.6	165.4
Manufacturing	57.9	181.2	29.3	29.5	134.3	22.7	454.8
Utilities	10.2	36.2	6.2	5.4	77.0	2.5	77.0
Construction	14.5	47.9	14.1	13.3	149.1	8.1	149.1
Retail	23.5	88.2	10.4	17.6	75.3	8.1	223.1
ICT	54.8	240.8	40.8	13.9	136.9	–	487.2
Finance	12.7	88.6	11.7	9.7	41.9	0.0	164.7
Real estate	19.8	68.1	10.2	9.8	51.9	0.0	159.8
Other services	34.3	151.2	39.5	9.7	112.8	51.4	399.0
Government	21.2	189.0	9.5	26.3	29.0	0.0	275.0
Entertainment	3.1	0.0	0.0	3.9	2.9	0.0	9.9
Total 5G Economic Impact	301.9	1,216.4	206.4	165.4	730.1	125.4	2,745.6
Productivity	778.4	3,083.6	517.2	574.1	2,121.1	401.3	7,475.9

Source: Omdia, based on Omdia and Bell Lab economic models



Ameaças cibernéticas à uma rede 5G



<https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/>



<https://www.ncsc.gov.uk/information/5g-round-up>



Ameaças cibernéticas à uma rede 5G



	Ciber criminosos	Insiders	Outras nações	Guerreiros cibernéticos	Hacktivistas	Corporações	Terroristas cibernéticos	Curiosos
Atividade ilegal/ Abuso	✓	✓	✓	✓	✓	✓	✓	✓
Espionagem/ interceptação	✓	✓	✓	✓	✓	✓	✓	✓
Desastres			✓	✓			✓	
Danos não intencionais	✓	✓	✓	✓				✓
Queda da rede	✓	✓	✓	✓	✓		✓	
Falha na rede	✓	✓	✓	✓	✓	✓	✓	✓
Legais	✓	✓	✓	✓	✓	✓	✓	
Ataques físicos	✓	✓	✓	✓	✓	✓	✓	



Cibercrime um negócio extremamente rentável





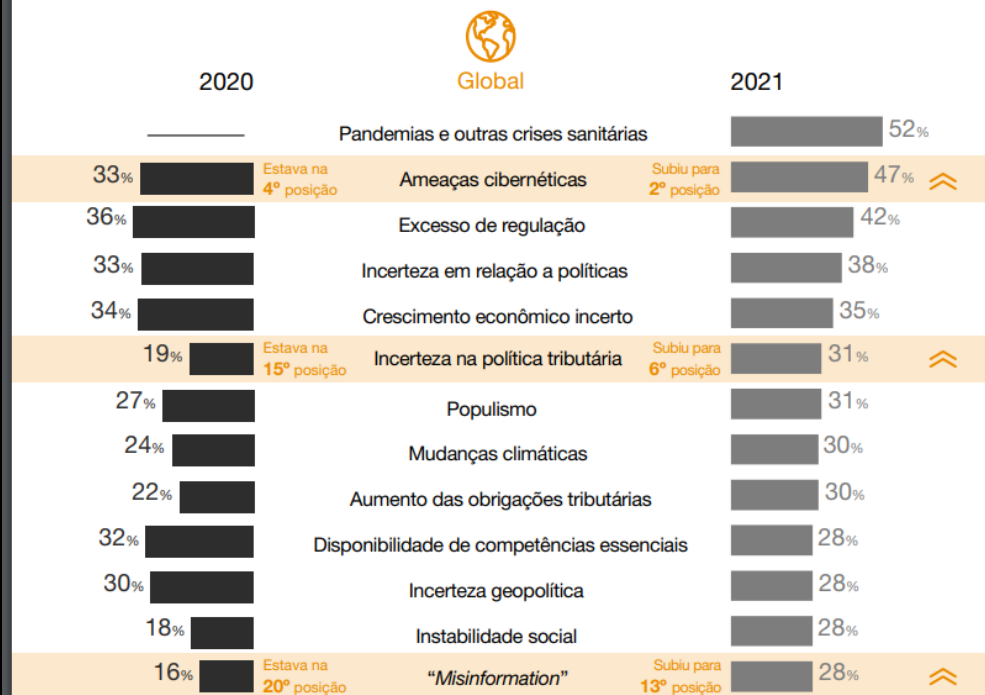
Importância do assunto



PwC | 24ª CEO Survey

| 6

Nível de preocupação com ameaças comerciais, econômicas, políticas, sociais e ambientais para o crescimento da empresa*





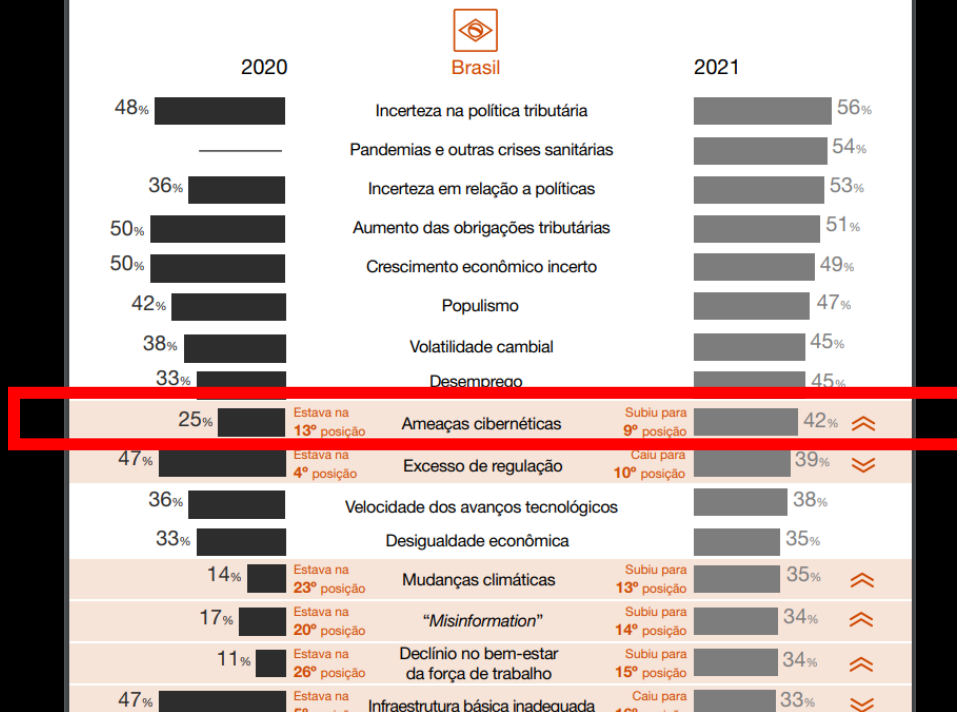
Importância do assunto



PwC | 24ª CEO Survey

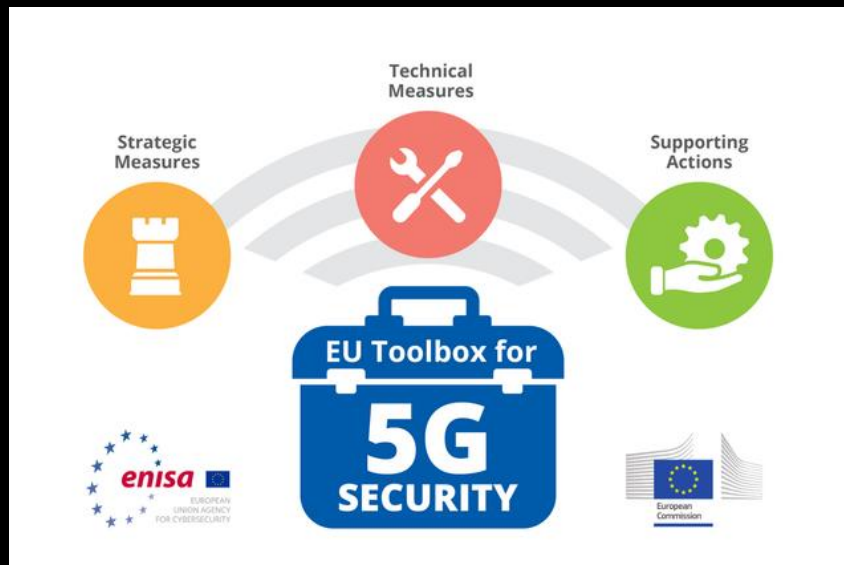
| 8

Nível de preocupação com ameaças comerciais, econômicas, políticas, sociais e ambientais para o crescimento da empresa*





Melhores práticas para implantação de redes 5G



Implementation maturity →	Very Low	Low	Low-Medium	Medium	Medium-High	High	Very High
Toolbox measure ↓							
SM01: Strengthening the role of national authorities				•			
SM02: Performing audits on operators and requiring information				•			
SM03: Assessing the risk profile of suppliers and applying restrictions* for suppliers considered to be high risk				•			
SM04: Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support				•			
SM05: Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies		•					
SM06: Strengthening the resilience at national level		•					
SM07: Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU			•				
TM01: Ensuring the application of baseline security requirements (secure network design and architecture)				•			
TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards			•				
TM03: Ensuring strict access controls				•			
TM04: Increasing the security of virtualised network functions			•				
TM05: Ensuring secure 5G network management, operation and monitoring				•			
TM06: Reinforcing physical security				•			
TM07: Reinforcing software integrity, update and patch management				•			
TM08: Raising the security standards in suppliers' processes through robust procurement conditions			•				
TM11: Reinforcing resilience and continuity plans				•			

Table 1: Overview of the level of maturity in the implementation of the Toolbox measures

<https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>



Melhores práticas para implantação de redes 5G

[Sign up for newsletter](#)

[About the Center](#) ▾ [Projects](#) ▾ [Partners](#) [News](#) ▾ [Events](#) [Library](#)

5G Cybersecurity

Building Blocks

[5G Security](#)[Adversarial Machine Learning](#)[Applied Cryptography](#)[Data Security](#)[Derived PIV Credentials](#)[Internet of Things](#)[Mobile Device Security](#)[Patching the Enterprise](#)[Supply Chain Assurance](#)

Download the Practice Guide

The NCCoE has released the preliminary draft version of NIST Cybersecurity Practice Guide SP 1800-33A, 5G Cybersecurity. Use the button below to view this publication in its entirety. Work continues on Volumes B and C of this practice guide.

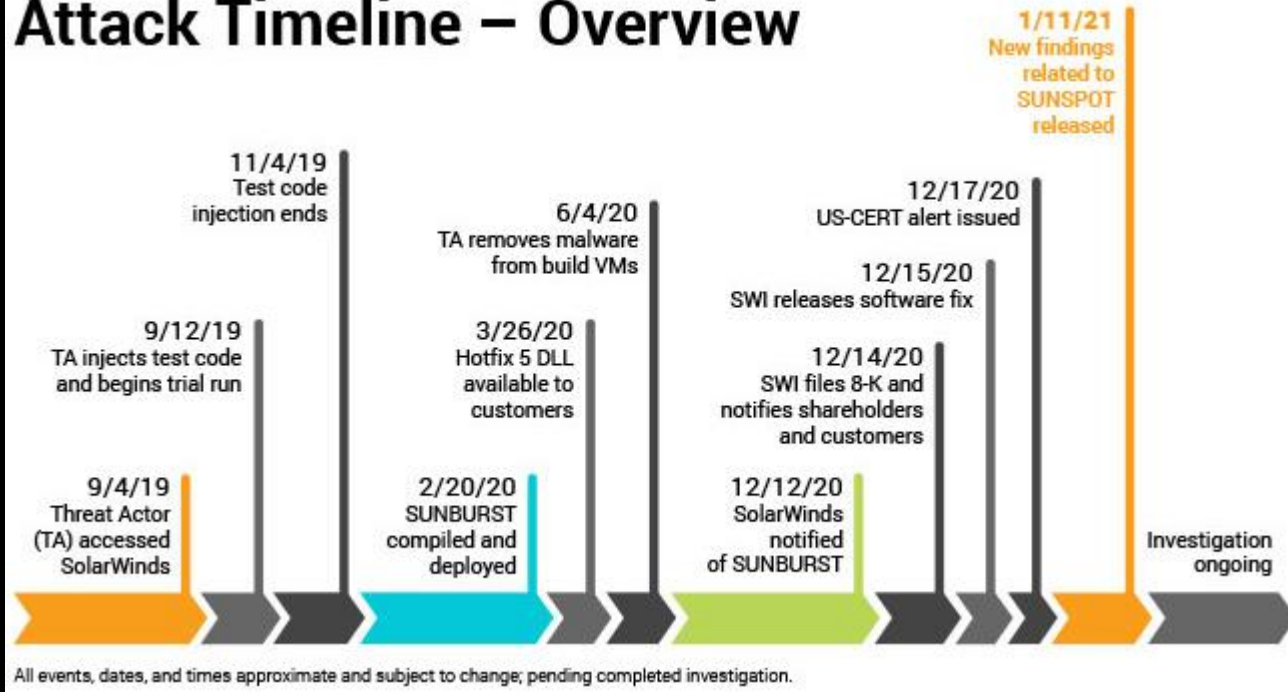
[Download PDF »](#)



Alertas : Capacidade e Oportunidade (Ataque à Solarwinds)



Attack Timeline – Overview



Vítimas nos EUA:

- 9 agências federais (Departamento do Tesouro, Comércio, Energia, Estado e Segurança Nacional, etc.)

- Mais de 100 empresas (Intel, Nvidia, Cisco, Microsoft, VMWare, Deloitte, etc)

<https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/>

<https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies>



Cibersegurança: Fator Humano



The Recent Water Treatment Facility Hack Was A Result Of Poor Password Security

🕒 1 month ago Ninad Mishra

Poor Password Results In Water Treatment Plant Hack

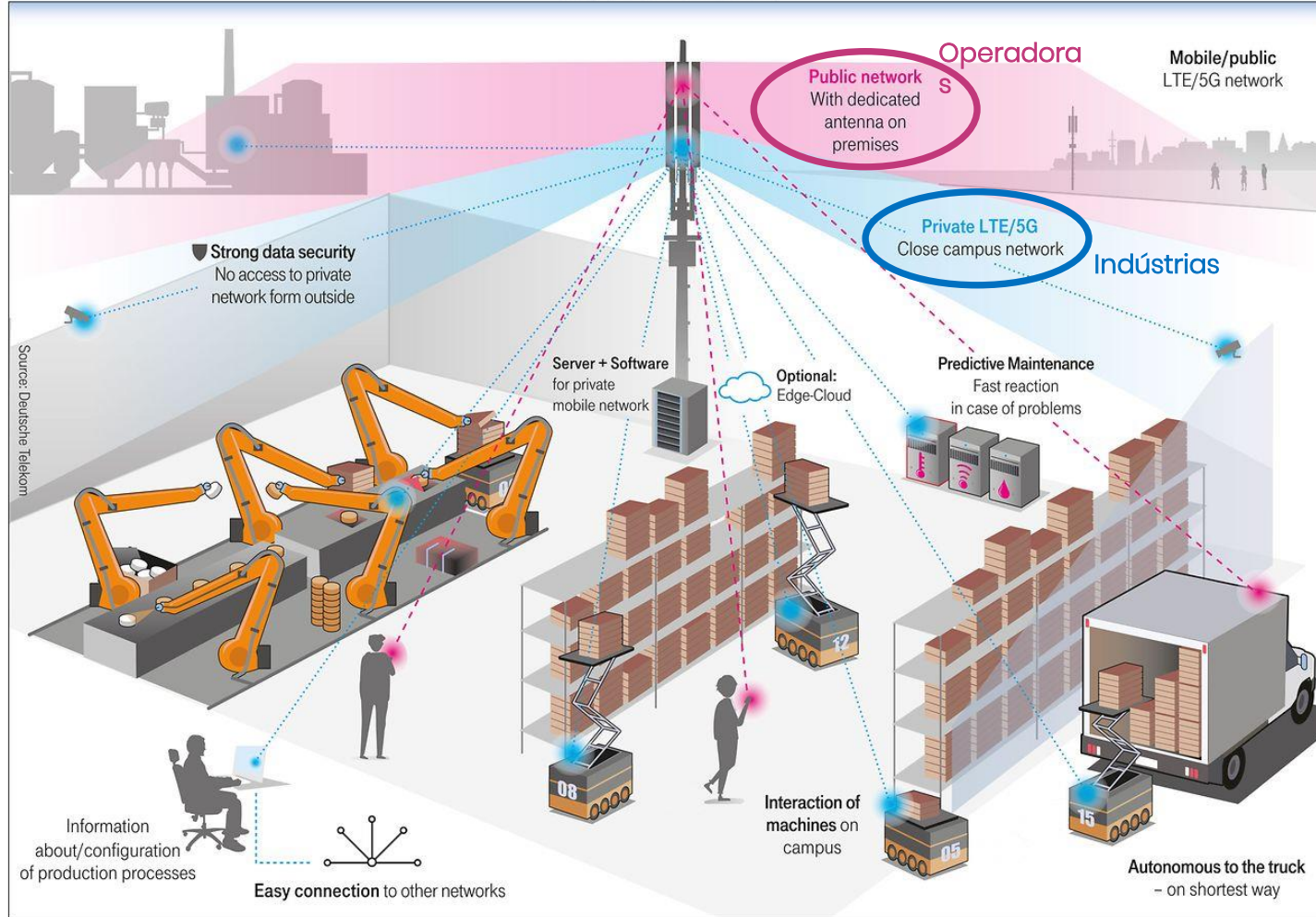




Indústria
4.0

CAMPUS-SOLUTION

Reliable, high-performance network solutions for industry 4.0



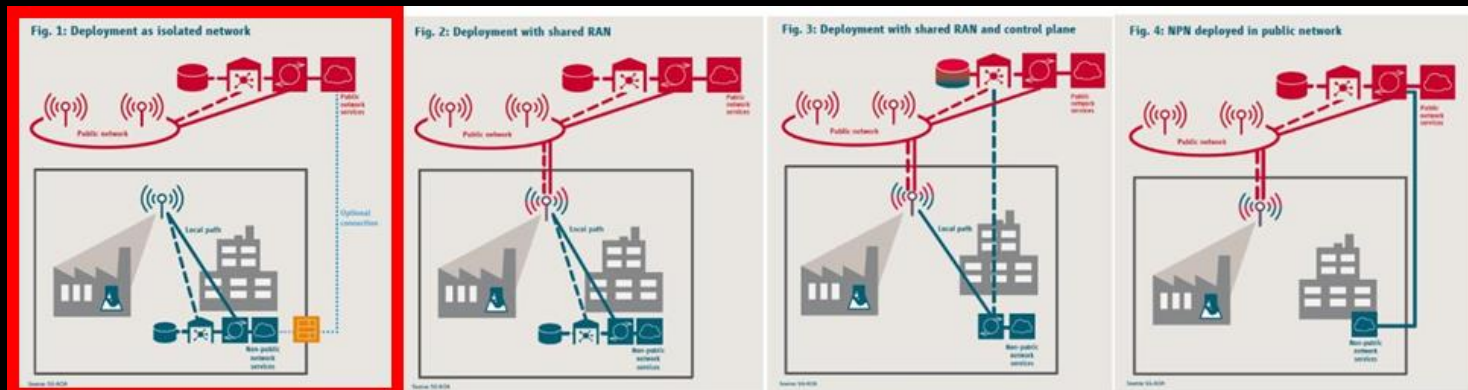


**Indústria
4.0**





Redes Privadas 5G como medida de mitigação de riscos



1

2

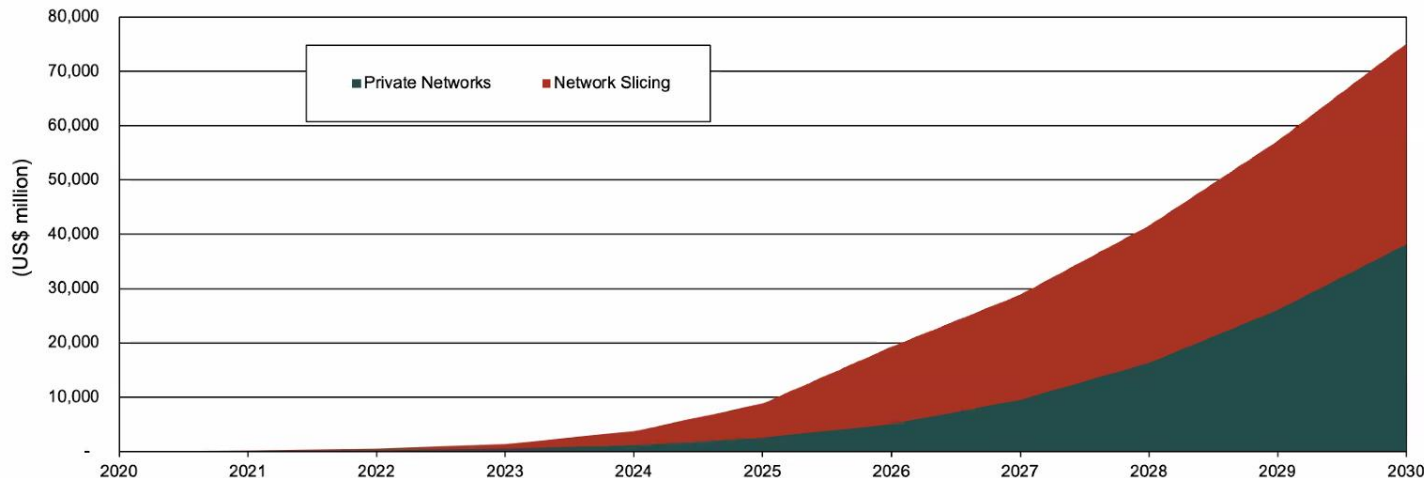
3

4

	Standalone Private Network	Hybrid Private Network		Virtual Private Network
Applications	Customer	Customer	Customer	Customer
Management	Customer	Customer / SP	SP	SP
Services	Customer	Customer / SP	Customer / SP	SP
Infrastructure	Customer	Customer / SP	Customer / SP	SP
Spectrum	Customer / SP	SP (Customer - optional)	SP (Customer - optional)	SP
Devices	Customer	Customer	Customer	Customer
SIMs	Customer	Customer	SP	SP



Redes Privadas 5G como medida de mitigação de riscos



- The total addressable market for 5G in the enterprise verticals domain will amount to more than **US\$ 75 billion** by 2030, with private network deployments accounting for **51%** and network slicing accounting for **49%** of 2030 revenues.
- Completely isolated private network deployments target **large enterprises** while hybrid network & network slicing offerings will be appealing to **SMEs**.
- Key verticals driving the demand for enterprise connectivity: Industrial manufacturing, Logistics and Oil & Gas and mining.

Main Drivers behind Enterprise 5G Adoption

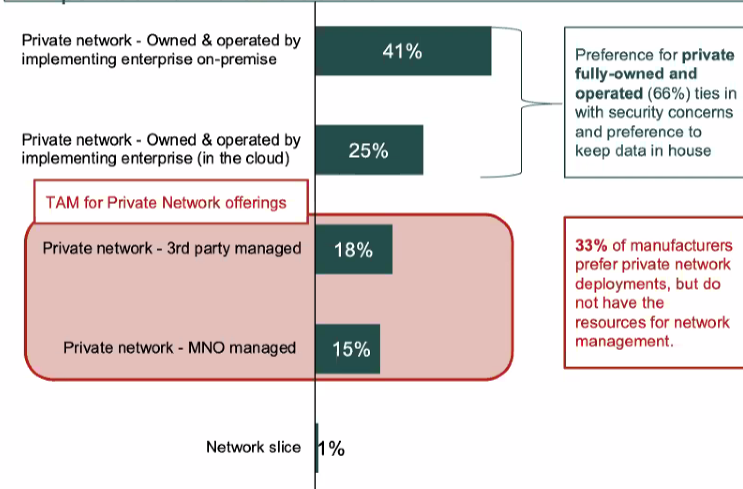
Customizability, Quality of Service & network integrity

Most important considerations for private network deployments

1. Customizability:
 - Orchestration of network slices to separate mission-critical from non-mission-critical applications
 - Customization of KPIs for different network slices
2. QoS and SLA control:
 - Full ownership of all network components (RAN, edge, and core) makes it easier to guarantee constant QoS
3. Network integrity:
 - Intrinsic motivation:
 - Data on number and condition of production assets needs to be protected against unauthorized access
 - Extrinsic motivation:
 - Regulatory decisions on privacy and data protection for handling sensitive healthcare patient data

Voice of the Enterprise:

- Private cellular connectivity is seen as a key enabler for enterprise digitization
- *Private network* does not automatically exclude third parties from the value chain



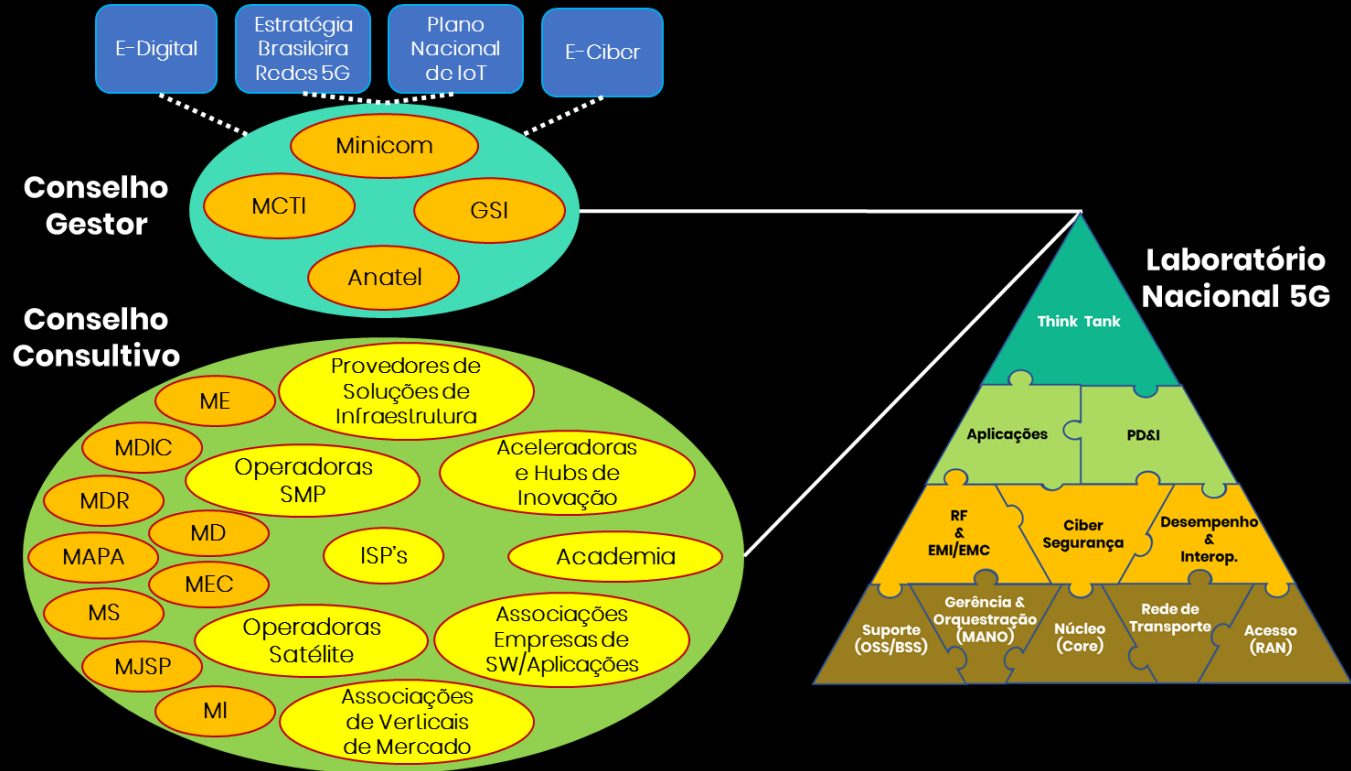
Source: ABI Research & Nokia Digital Transformation Survey among Industrial manufacturers.
Q: "If deploying wireless technology *4G/5G) is part of your digital transformation plan, how do you envision to deploy the network?"

N= 528

Proposta CPQD

Consulta Pública no 09

Anatel - Edital 5G



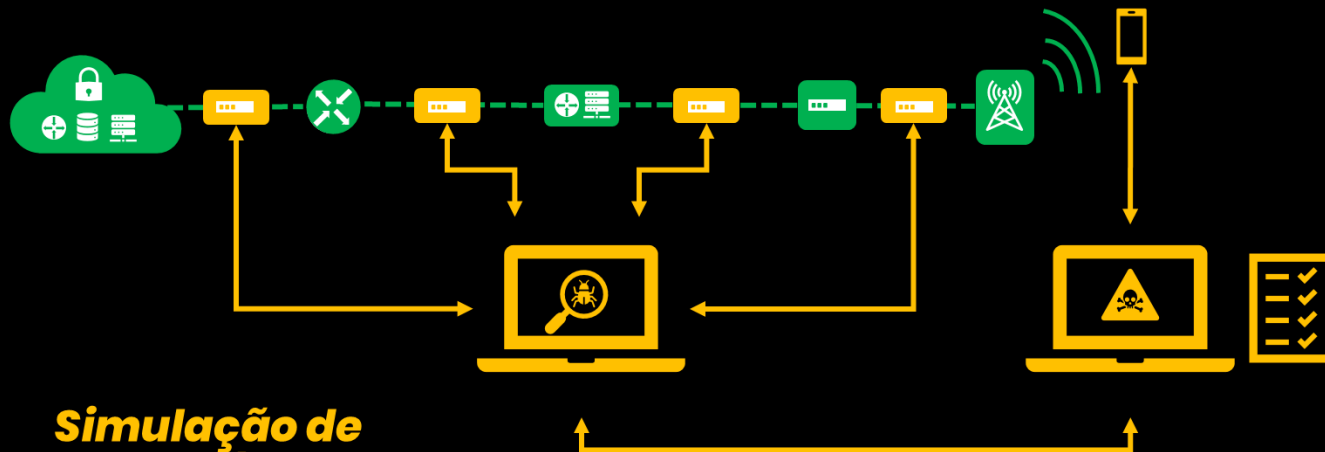
Proposta CPQD

Consulta Pública no 09

Anatel - Edital 5G



Conformidade em Segurança Cibernética



**Simulação de
ataques/falhas
conhecido(a)s**



Consultoria em Telecomunicações

Engenharia de Redes e Inteligência Regulatória



Suporte à decisão

Análises tecnológicas e regulatórias visando subsidiar a estratégia de clientes e parceiros em decisões de curto, médio e longo prazo (Plano Diretor).



Inteligência regulatória

Desenvolvimento de metodologias de análise e caracterização, perícia e laudos técnicos, revisão de obrigações e apoio em questões litigiosas.



Radiofrequência e interferência

Estudos técnicos e de campo para estimativa de cobertura e análise de interferência entre serviços.



Projetos de rede sob medida

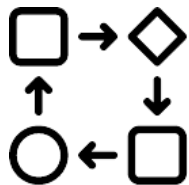
Projetos de redes de comunicação customizados para a necessidade do cliente, seja na perspectiva de uma infraestrutura própria ou de terceiros.

Soluções Analíticas Especializadas

IA habilitando aplicações de Inteligência de Dados

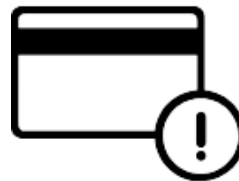


São aplicações que visam à resolução de problemas reais de negócios, com inúmeros casos de sucesso em diferentes perfis de clientes e mercados.



Automação de Decisão Operacional

Automação baseada em tratamento de eventos, regras, perfis históricos, modelagem preditiva, automação de workflow e gestão de casos e alertas, com o objetivo de reduzir a perda de eficiência e produtividade



Detecção de Fraude e Prevenção de Perdas

Detecção em tempo real de fraudes e desvios operacionais, baseada em tratamento de eventos, regras, perfis históricos e comportamentos de clientes e usuários.



Predição e Prescrição em Produtos e Processos

Tratamento de dados coletados de ativos físicos (sensores e dispositivos de IoT), visando à detecção de anomalias e ao reconhecimento de padrões para predição de falhas e prescrição de medidas e ações.

Ensaio e certificação de produtos e sistemas



Atendimento às exigências regulatórias e demanda de clientes

O CPQD possui uma das maiores infraestruturas laboratoriais da América Latina e dispõe de equipes altamente qualificadas para prestar serviços especializados e desenvolver soluções sob medida



Certificação de Produtos e Sistemas

Certificações voluntárias e compulsórias de uma ampla variedade de produtos e sistemas com o objetivo de garantir o atendimento aos requisitos aplicáveis.



Ensaio Laboratoriais

Para fins de desenvolvimento, validação e certificação de produtos e sistemas, incluindo a elaboração de cadernos de ensaios para a homologação de componentes e ambientes críticos e avaliações para benchmarking.



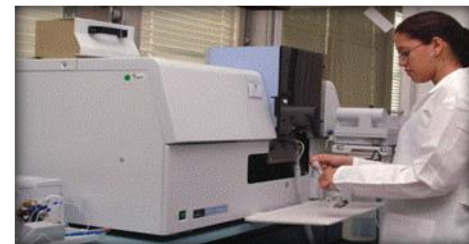
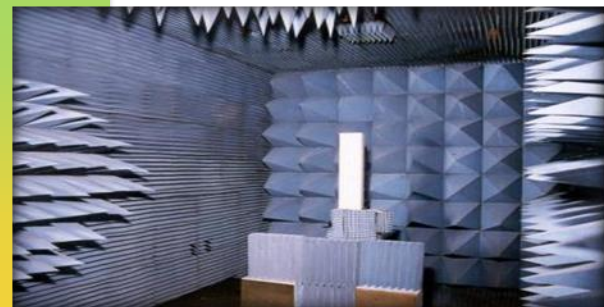
Ensaio e Testes em Campo

Para avaliação de desempenho e qualidade de redes de telecomunicações (RNI e interferências de RF).



Ensaio e certificação de produtos e sistemas

Infraestrutura Laboratorial



Soluções Inovadoras com apoio de fomento



**Um mecanismo moderno e ágil
de fomento à inovação
industrial**

**Inovação
em
produto**

**Inovação
em
processo**



NÃO HÁ CHAMADA PÚBLICA OU
NECESSIDADE DE SUBMETER O
PROJETO



OS RECURSOS JÁ ESTÃO DISPONÍVEIS
NA UNIDADE EMBRAPÍ CPQD



NEGOCIAÇÃO DIRETA ENTRE
INDÚSTRIA E A UNIDADE EMBRAPÍ
CPQD



NÃO REEMBOLSÁVEIS NA ORDEM DE
1/3 DO VALORO DO PROJETO
REALIZADO PELO ICT



Início > Apoio e Financiamento > Programas e Produtos > **Finep Conecta**

Apoio e Financiamento

- O que apoiamos
- Como obter financiamento
- Condições Operacionais
- Programas e Produtos**
- Apoio Direto à Inovação
- Centelha
- Finep 2030
- Finep 2030 Empresarial
- Finep Ações Emergenciais
- Crédito

Finep Conecta

Tem como objetivo estimular a cooperação entre empresas e Instituições Científicas, Tecnológicas e de Inovação (ICTs), de forma a levar conhecimento gerado nas ICTs para as empresas brasileiras, promover maior alinhamento dos objetivos da Ciência Nacional às demandas empresariais, elevar os dispêndios em P&D e incentivar projetos de maior risco tecnológico.

Público-alvo

O público alvo são empresas brasileiras e outras pessoas jurídicas com fins lucrativos com receita operacional bruta anual ou anualizada igual ou superior a R\$ 90 milhões que realizem Planos Estratégicos de Inovação em parceria com ICTs.

Quando a empresa for controlada por outra ou pertencer a um grupo econômico, a classificação de porte considerará a receita consolidada do grupo econômico.

Empresas e outras pessoas jurídicas do direito privado com receita operacional bruta anual ou anualizada inferior

Obrigado!

Gustavo Correa Lima

**CPQD – Diretoria de Soluções Tecnológicas
e Consultoria**

Cel.: +55 19 9 9838-2282

gcorrea@cpqd.com.br

