Observatório Nacional da Indústria

Segurança Cibernética

A PROTEÇÃO CONTRA AMEAÇAS ÀS ORGANIZAÇÕES

CNI Confederação Nacional da Indústria

SESI Serviço Social da Indústria

SENAI Serviço Nacional de Aprendizagem Industrial

IEL Instituto Euvaldo Lodi

Folha de Fato

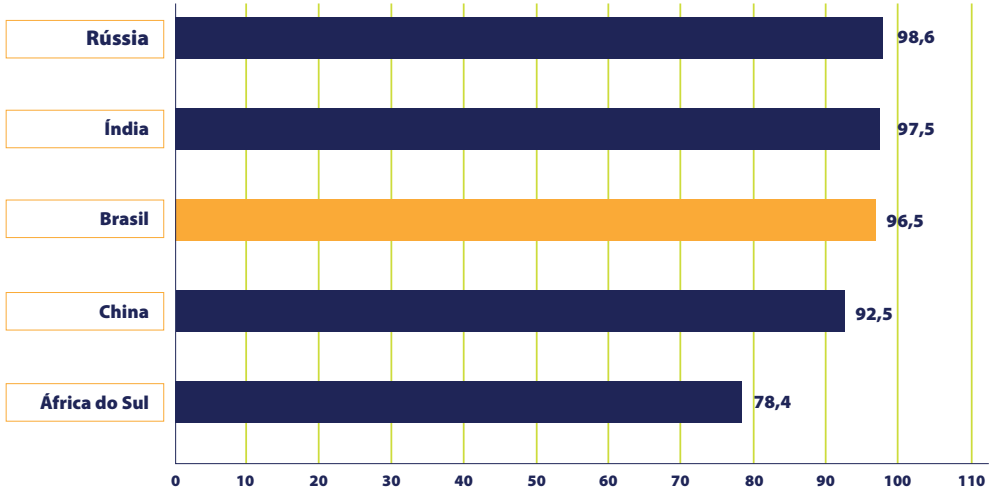
A segurança cibernética é um mecanismo de proteção para sistemas de computação, redes e dados, defendendo-os contra acessos, usos ou danos não autorizados. Ela é crucial para proteger a sociedade e a economia de ameaças online que podem afetar a confidencialidade, a integridade e a disponibilidade em diversos setores, como empresas, governo, forças armadas, saúde, educação e energia.

As soluções de segurança cibernética são fundamentais para a proteção de dados e detecção de ameaças, autenticando dispositivos IoT, criptografando dados e detectando ameaças avançadas. Tecnologias como *big data*, inteligência artificial, *machine learning*, biometria comportamental, *blockchain* e computação quântica permitem prever ataques em tempo real por meio da análise de indicadores e padrões.

As ameaças cibernéticas podem causar impactos variados, incluindo perdas financeiras, interrupções operacionais, danos à reputação, responsabilidades legais, danos físicos e riscos à segurança nacional.

Índice Global de Segurança Cibernética em 2020

Fonte: International Telecommunication Union (ITU, 2020); fDi Benchmark (2023).

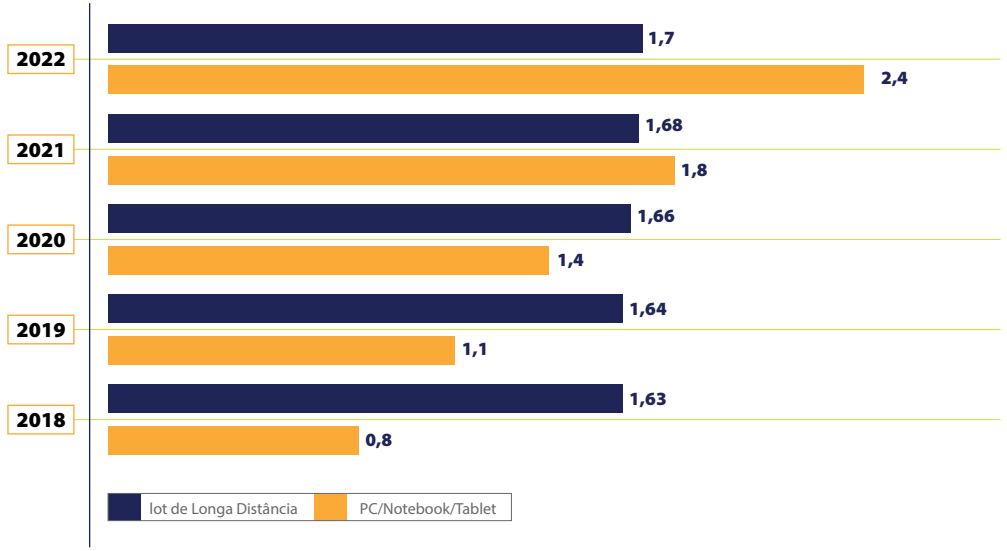


O Índice Global de Segurança Cibernética é uma referência confiável que mede o compromisso dos países com a cibersegurança em nível global. Dentre os cinco países dos BRICS, o Brasil ocupa a 3ª posição.

A diminuição dos custos dos dispositivos e o surgimento de novos modelos de negócios têm impulsionado a penetração de mercado da Internet das Coisas (IoT), aumentando assim o número de dispositivos conectados, incluindo carros, máquinas, medidores, dispositivos vestíveis e eletrônicos de consumo.

Dispositivos conectados por um IoT [Mundo]

Fonte: Mordor Intelligence (2022) - Elaboração: Observatório Nacional da Indústria - Período: 2018 a 2022



Os cinco primeiros depositantes nessa área são: China, Estados Unidos, Coréia do Sul, Japão e depósitos via EP (escritório europeu). O Brasil ocupa a 16ª posição, com 508 depósitos.

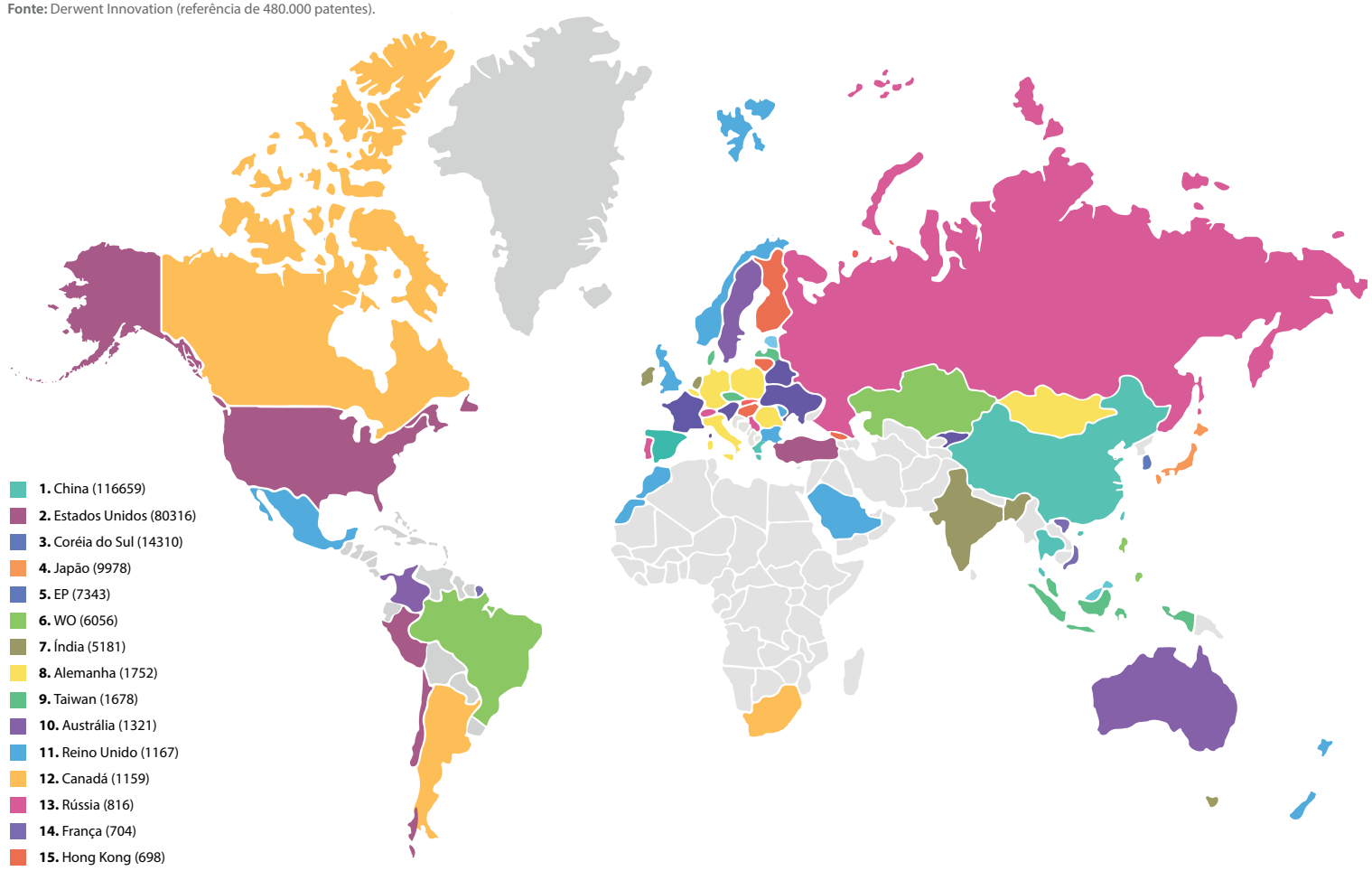
Os principais players são: Microsoft, Alphabet Inc (Google), IBM, Cisco, Siemens, Honeywell International e Accenture.

No nicho de soluções, a proteção de infraestrutura é o maior em termos de receita, com USD 27,07 bi em 2022 e previsão de alcançar USD 51,73 bi, em 2027, uma CAGR de 12,65%.

WO é a sigla para Organização Mundial da Propriedade Intelectual e é usada para identificar patentes depositadas internacionalmente através do Tratado de Cooperação em Matéria de Patentes (PCT). Portanto, "WO" em depósitos de patentes indica uma patente depositada internacionalmente.

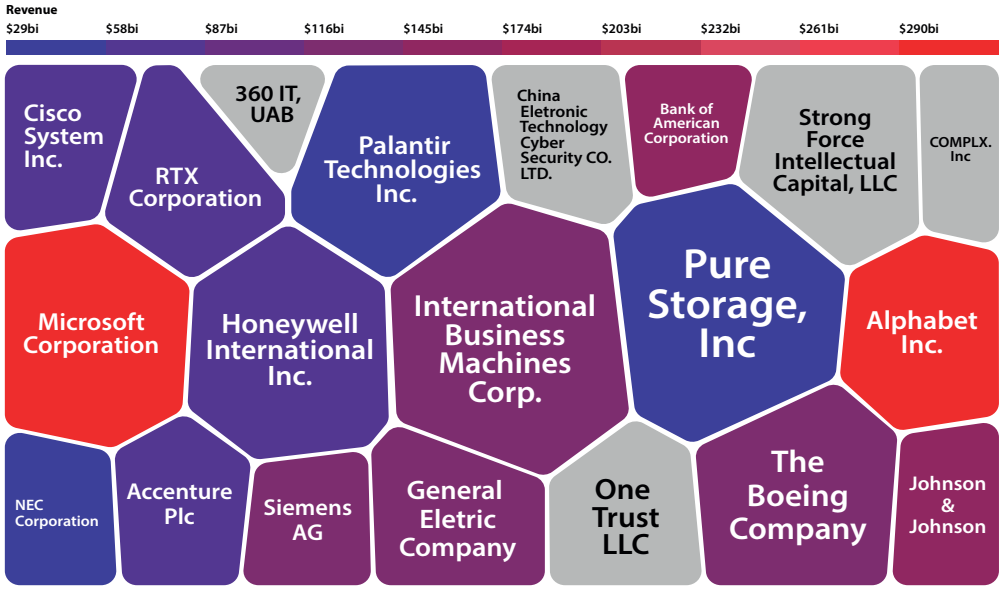
Principais países depositantes de patentes na área de segurança cibernética

Fonte: Derwent Innovation (referência de 480.000 patentes).



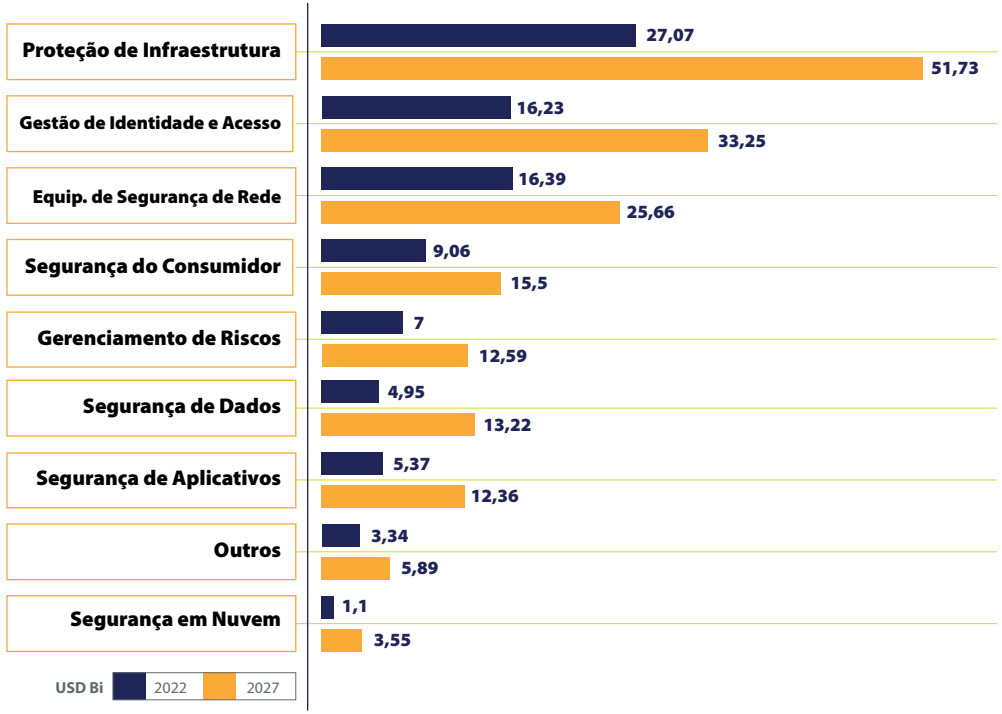
Principais depositantes de patentes na área de Segurança Cibernética x receita

Fonte: Innography (Clarivate)



Mercado e projeção para soluções de cibersegurança [mundo]

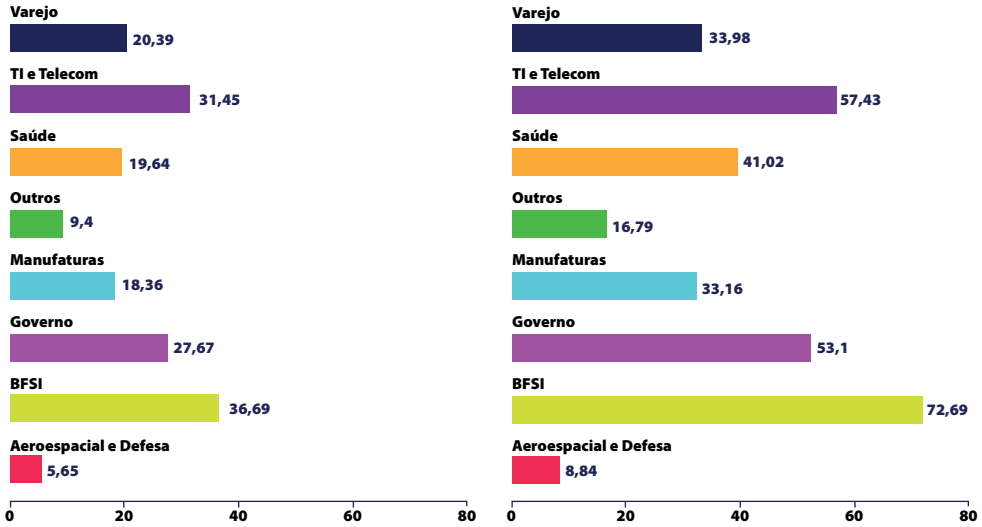
Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022)
- Elaboração: Observatório Nacional da Indústria



Os usuários finais dividem-se em BFSI (Bancos, serviços financeiros e seguros), Saúde, Aeroespacial e Defesa, TI e Telecom, Governo, Varejo, Manufatura e outros.

Mercado e projeção por usuário final [mundo]

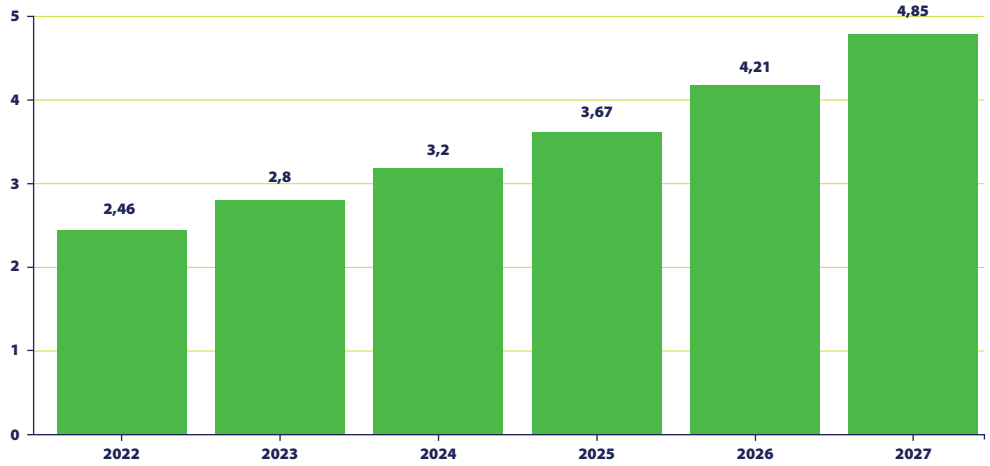
Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração Observatório Nacional da Indústria.



O mercado de segurança cibernética no Brasil é o maior da América Latina em termos de receita (USD 2,46 bi em 2022), representando um *market share* de 39,68%. A projeção é de alcançar USD 4,85 bi, em 2027 e uma CAGR de 10,18%.

Mercado e projeção de receita em cibersegurança (USD bi) [Brasil]

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022)
- Elaboração: Observatório Nacional da Indústria.



A preocupação com a segurança cibernética é constante entre líderes empresariais, governamentais e de entidades em geral.

As ameaças cibernéticas buscam acessar informações das organizações para fins nefastos, podendo resultar em danos financeiros e de reputação. É crucial investir em tecnologia, inovação e recursos humanos para combater essas ameaças cibernéticas.

SUMÁRIO

Lista de Figuras


Tag
Clouds
Observatório
Nacional da
Indústria
Segurança Cibernética

1. Caracterização da Tecnologia

A expansão acelerada da internet nas últimas décadas, conhecida como "cibercivilização", revolucionou a sociedade, a economia e as infraestruturas críticas, alterando a forma como comunicamos, fazemos negócios e acessamos informações.

1.1. Introdução

A internet tornou-se essencial para a troca de informações e é fundamental na vida moderna, sendo utilizada por indivíduos e organizações em áreas críticas, como bancos, saúde, governos, educação, gestão de recursos humanos, cidades inteligentes e sistemas de rede.

A segurança cibernética, que protege indivíduos, sociedades, organizações, sistemas e tecnologias contra atividades anormais, é aplicável em diversas áreas e enfrenta desafios de várias fontes, incluindo *hackers*, cibercriminosos, atores estatais, terroristas e profissionais internos. Ela mantém a confidencialidade, a integridade e a disponibilidadedos recursos informáticos e fornece um mecanismo de defesa contra ameaças online que podem comprometer vários setores.

O atual cenário de segurança cibernética é marcado pelo surgimento constante de ameaças cibernéticas sofisticadas e diversificadas, afetando tanto indivíduos quanto organizações. As ameaças mais comuns em 2022 incluem *malware*, *phishing*, *ransomware*, engenharia social, entre outras. As soluções de internet em nuvem são cruciais em vários contextos, incluindo segurança nacional, economia e proteção de dados. As soluções de segurança cibernética são fundamentais para autenticar dispositivos IoT, criptografar dados e detectar ameaças avançadas. O uso de big data, inteligência artificial e aprendizado de máquina permite prever ataques em tempo real.

As ameaças cibernéticas podem causar perdas financeiras, interrupções operacionais, danos à reputação, responsabilidades legais, danos físicos e riscos à segurança nacional. Para melhorar a segurança cibernética, empresas e indústrias utilizam tecnologias e técnicas de segurança, como sistemas de detecção e prevenção de intrusões, *firewalls*, software antivírus e criptografia. Além disso, as empresas estão implementando melhores práticas, incluindo atualizações frequentes de software, diretrizes rigorosas de senha e treinamento em segurança cibernética dos funcionários. A segurança cibernética é uma grande preocupação no ambiente de TI e é um dos aspectos mais importantes da implementação de qualquer infraestrutura de TI.

1.2. Função da tecnologia

O conceito de valor pode variar dependendo do contexto, mas, em termos empresariais, é definido como o conjunto de benefícios e utilidades proporcionados por um produto ou serviço menos o seu custo de aquisição. O valor pode ser percebido de quatro formas: custo, uso, estima e troca.

No contexto da segurança cibernética, o valor está ligado à tecnologia que oferece *benefícios* como a proteção de dados, programas, processos e arquivos em computadores, nuvens e outros dispositivos. A segurança cibernética fornece um mecanismo de defesa contra acesso não autorizado, uso indevido ou danos, protegendo diversos setores contra ameaças online.

As soluções de segurança cibernética podem ser aplicadas em várias áreas, como segurança em nuvem e IoT, e-commerce e pagamentos, segurança nacional e inteligência de ameaças. A segurança cibernética é relevante em quase todos os setores da economia, incluindo governos, sistema bancário, defesa, economia, sistema de saúde e empresas em geral.

1.3. Requisitos para funcionamento da tecnologia

Existe um desafio recorrente relacionado à discrepância entre a velocidade do desenvolvimento de soluções tecnológicas e a velocidade da nuvem. Muitas organizações de TI descobriram que os modelos de segurança existentes não acompanham a "velocidade da nuvem" e não oferecem suporte suficiente aos desenvolvedores em áreas como análises.

Esse desalinhamento entre as equipes de desenvolvimento e segurança cibernética pode resultar em perda de oportunidades de negócios, pois as novas soluções demoram para chegar ao mercado. Em alguns casos, a pressão para preencher essa lacuna aumentou a vulnerabilidade, pois as equipes de desenvolvimento alteram as regras para contornar políticas e padrões de segurança. As atividades do ciclo de desenvolvimento incluem arquitetura e design, implementação, revisão de código, testes e implantação.

Fig. **01**

As ações necessárias para a segurança cibernética incluem o projeto de uma arquitetura segura, a revisão segura de código e a configuração de ambientes em nuvem para atender aos padrões de segurança. A agilidade na resposta a incidentes cibernéticos é crucial, pois uma resposta rápida pode minimizar o impacto na reputação e proporcionar a vantagem competitiva de uma organização. A detecção rápida é essencial para uma resposta eficaz a ataques cibernéticos e violações de dados.

As organizações devem focar na construção de controles preventivos para lidar com ameaças cibernéticas conhecidas e no desenvolvimento de uma capacidade de resposta sofisticada para lidar com ameaças complexas, desconhecidas e novas.

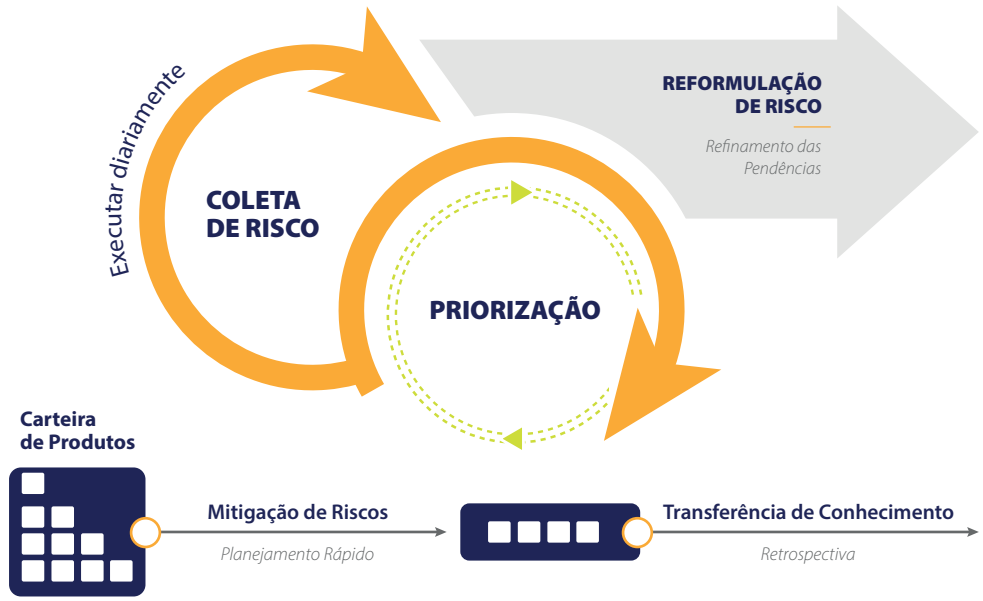
A **Figura 2** apresenta um *framework* dividido em cinco etapas, cada uma abordando um dos cinco principais desafios de gestão de riscos de segurança cibernética para desenvolvedores de software, enquanto apoia o processo de desenvolvimento ágil. Dada a importância da agilidade no contexto da prevenção, as empresas devem se esforçar para fornecer condições que permitam aos profissionais de TI agir de forma preventiva na gestão de riscos de ameaças cibernéticas.

Manter-se atualizado sobre as mais recentes tecnologias de segurança cibernética é essencial para combater efetivamente ameaças e proteger dados sensíveis. As tecnologias emergentes incluem Inteligência Artificial (IA), *Machine Learning* (ML), Biometria Comportamental, Arquitetura Zero Trust, *Blockchain*, Computação Quântica, Segurança em Nuvem e Segurança de IoT.

Fig. **02**

Framework de risco da gestão da agilidade

Fonte: Salin e Lundgren (2022) – Adaptação



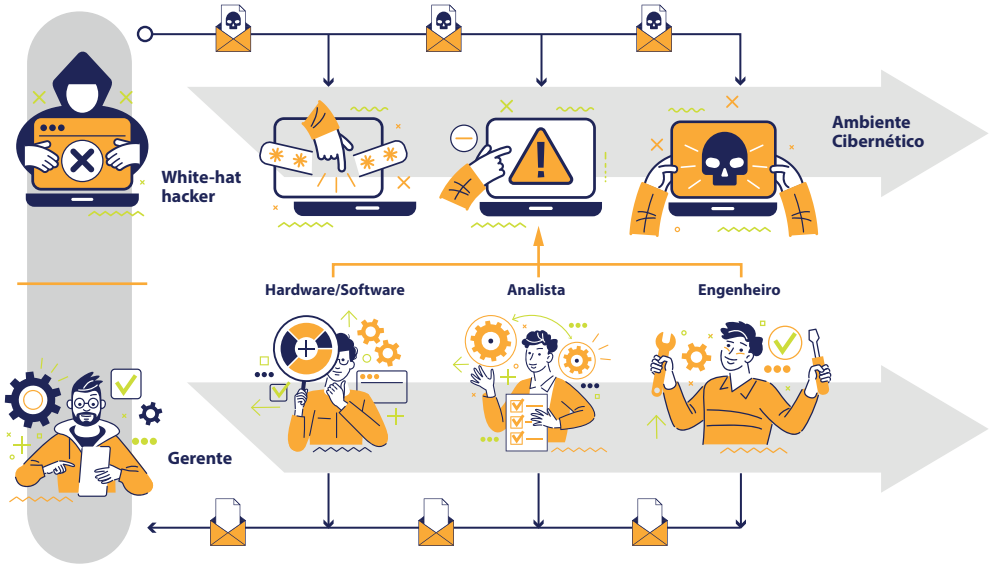
Desse modo, é crucial manter-se atualizado sobre as mais recentes tecnologias e tendências em segurança cibernética. À medida que o cenário de ameaças evolui, novas tecnologias e estratégias emergem para ajudar empresas e organizações a protegerem seus dados e redes. Incorporar essas tecnologias emergentes em sua estratégia de segurança cibernética pode melhorar a proteção de suas informações confidenciais.

No contexto de fornecedores de soluções tecnológicas para prevenção de ameaças cibernéticas, os insumos não são físicos, mas uma infraestrutura tecnológica e um ambiente cibernético, incluindo hardware, software de desenvolvimento e simulação, redes de comunicação, armazenamento em nuvem e profissionais de TI (**Figura 3**).

Fig. **03**

Ambiente cibernético

Fonte: Adaptado de Beuran et al. (2017)



No ambiente cibernético, é crucial considerar os parceiros, sejam desenvolvedores ou fornecedores de serviços, como possíveis vetores de ameaças se não estiverem devidamente protegidos. Os gestores devem exigir que seus parceiros também estejam preparados para combater potenciais ameaças cibernéticas. Mesmo as empresas bem estruturadas têm pontos críticos que precisam ser monitorados. No contexto cibernético, é necessário ter procedimentos para identificar essas vulnerabilidades. A **Figura 4**, por sua vez, apresenta uma proposta de *framework* de fatores críticos de sucesso em segurança cibernética que abrange dimensões internas (organizacionais, de infraestrutura, estratégicas, de processo) e externas para as empresas.

Fig. **04**

Fatores críticos de sucesso em segurança cibernética organizacional

Fonte: Adaptado de Yeoh et al. (2022)

1.4. Diferenciais da tecnologia

O mercado de segurança cibernética é caracterizado por várias soluções que protegem dispositivos ou servidores contra violações de dados. Essas soluções não têm um substituto direto, pois trabalham juntas para garantir a segurança cibernética.

Com o advento da Inteligência Artificial (IA), muitos ataques triviais podem ser antecipados com bastante antecedência, reduzindo a intervenção humana a longo *prazo*. Tecnologias de IA, como *Machine Learning* e Processamento de Linguagem Natural, coletam informações e auxiliam na identificação de ameaças. No entanto, a combinação de técnicas de cibercriminosos com IA pode tornar a detecção de ameaças cada vez mais difícil. Nesse contexto, os aspectos como privacidade de dados, equidade, rastreabilidade, robustez, confiabilidade, causalidade, transparência e governança de dados são cruciais para o desenvolvimento de sistemas de segurança cibernética que utilizam IA.

Segundo a IBM, as melhores práticas em segurança cibernética incluem treinamento de conscientização em segurança, gestão de identidade e acesso, gestão da superfície de ataque, detecção, prevenção e resposta a ameaças, e recuperação de desastres.

1.5. Gartner Hype cycle

O Hype Cycle é uma apresentação gráfica (**Figura 6**) desenvolvida pela consultoria Gartner para representar os ciclos de aparecimento, adoção, maturidade e aplicação de tecnologias no mercado.

Gráfico das etapas do ciclo de inovação Hype-Gartner

Fonte: Gartner.

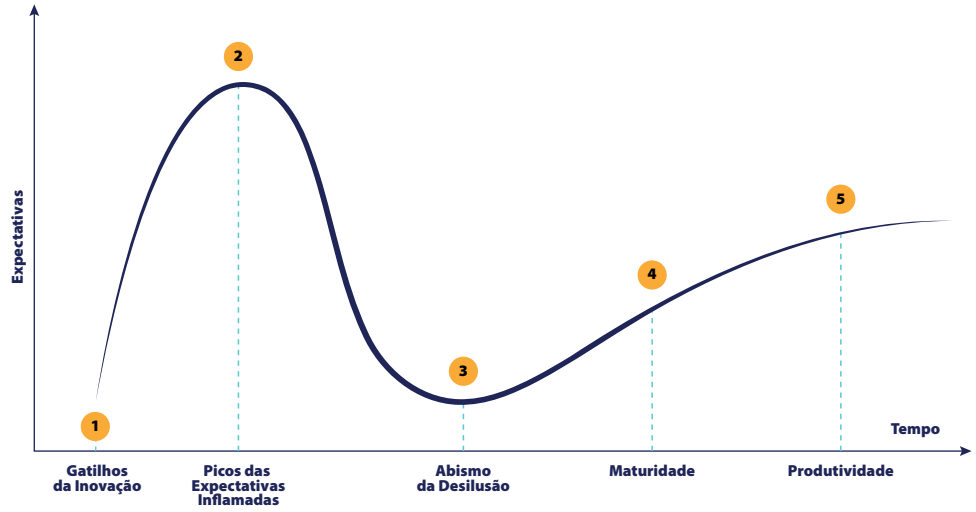
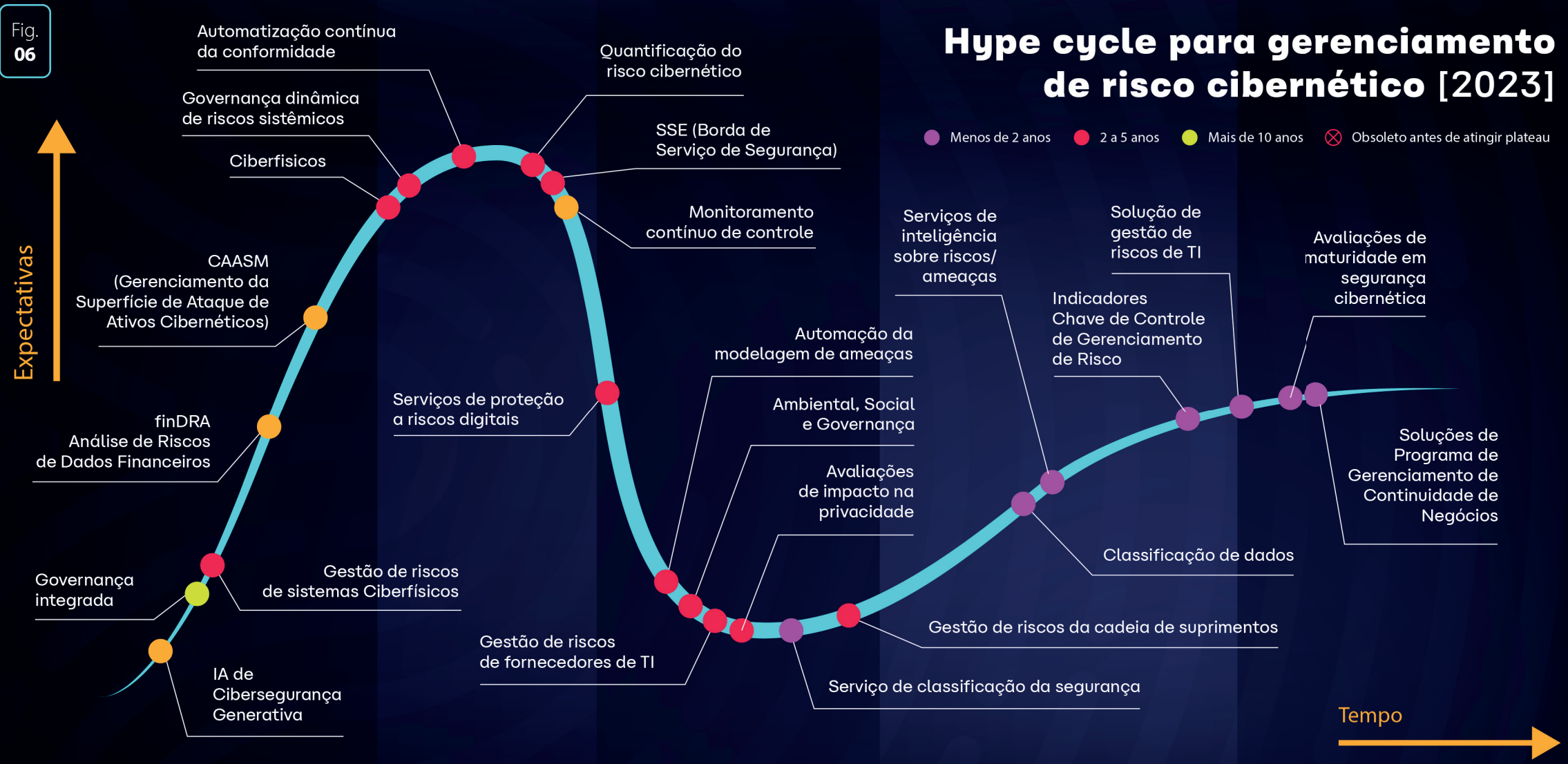


Fig. **05**

Fig. **06**

Hype cycle para gerenciamento de risco cibernético [2023]



O gráfico analisa as tendências e investimentos em novas tecnologias. Após a inovação e adoção pelo mercado, é crucial monitorar os casos de sucesso e fracasso de uma tecnologia quando se torna um produto, especialmente durante o Pico de Expectativas Inflacionadas e sua subsequente queda.

A fase seguinte é caracterizada por uma queda devido à desconfiança do mercado, que deve ser cuidadosamente analisada até atingir o Vale da Desilusão. Depois, começa a fase de maturidade do produto e do mercado, marcada por um aumento gradual de maturidade. Finalmente, o produto atinge o Platô de Produtividade, em que se estabiliza no mercado e não retorna ao estágio anterior, a menos que se torne obsoleto.

A **Figura 6** apresenta o ciclo Hype de Gartner para a gestão do risco cibernético, que avalia as expectativas ao longo do tempo. Esse ciclo orienta os líderes de segurança e gestão de risco a utilizar essa pesquisa para avaliar o impacto de soluções novas e emergentes, a fim de tomar decisões de adoção adequadas. A pesquisa destaca que a adoção de tecnologias de gerenciamento de risco cibernético, como o monitoramento contínuo de controles, é útil para entender o impacto do risco cibernético e apoiar os objetivos de negócios e conformidade.

1.6. Indicadores

O Índice Global de Segurança Cibernética (IGSC), desenvolvido pela União Internacional de Telecomunicações (UIT), uma agência especializada da Organização das Nações Unidas (ONU), foi criado para aumentar a conscientização mundial sobre a importância da segurança cibernética. A UIT desenvolveu um questionário avaliativo enviado a 194 países para avaliar a situação de cada um em termos de segurança cibernética. O IGSC é uma referência confiável que mede o compromisso dos países com a segurança cibernética em nível global. O nível de desenvolvimento ou engajamento de cada país é avaliado em cinco pilares: medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidade e cooperação. Essas avaliações são então agregadas em uma pontuação geral (**Figura 7**).

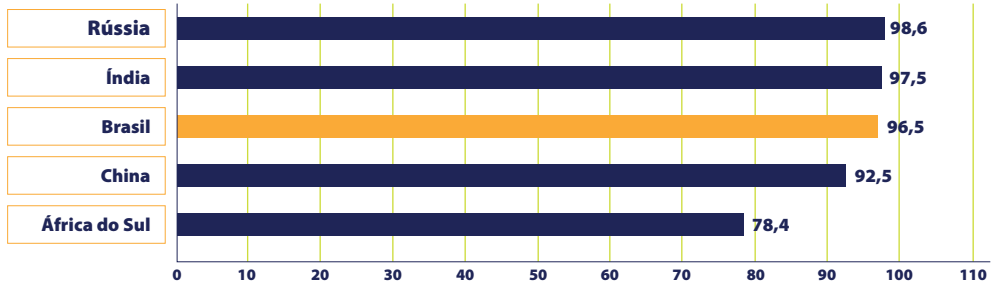
Fig. **07**

Na avaliação de 2020 do Índice Global de Segurança Cibernética, o Brasil ocupou a 18ª posição com uma pontuação de 96,6. Os três países com as pontuações mais altas foram os Estados Unidos, com 100, o Reino Unido e a Arábia Saudita, com 99,54, e a Estônia, com 99,48. Dentre os cinco países dos BRICS, o Brasil ocupa a 3ª posição (**Figura 8**).

Fig. **08**

Índice Global de Segurança Cibernética em 2020

Fonte: International Telecommunication Union (ITU, 2020); fDi Benchmark (2023).



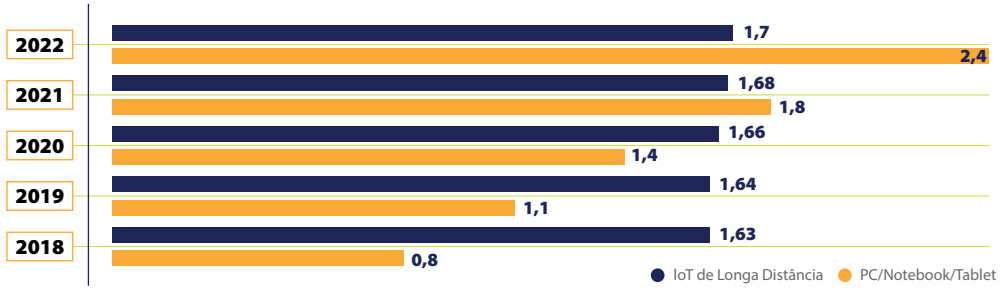
Segundo a Mordor Intelligence (2022), existem ainda dois indicadores globais relevantes relacionados ao uso de dispositivos de Internet das Coisas (IoT) e conexões máquina a máquina (M2M) associados ao contexto de segurança cibernética.

A redução significativa nos custos dos dispositivos, juntamente com a emergência de novos modelos de negócios, tem sido fundamental para aumentar as taxas de penetração de mercado da IoT. Isso, por sua vez, aumentou o número de dispositivos conectados, incluindo carros, máquinas, medidores, dispositivos vestíveis e eletrônicos de consumo (**Figuras 9 e 10**).

Dispositivos conectados por um IoT [Mundo]

Fonte: Mordor Intelligence (2022) - Elaboração: Observatório Nacional da Indústria - Período: 2018 a 2022

Fig. **09**



Conexões M2M (Máquina a Máquina) [Mundo]

Fonte: Mordor Intelligence (2022) - Elaboração: Observatório Nacional da Indústria

Fig. **10**

Os ataques a dispositivos de Internet das Coisas (IoT) são frequentes e a possibilidade de interrupção em indústrias, como a manufatura, aumenta a importância da segurança cibernética no mercado atual.

A emergência da tecnologia 5G deve acelerar o uso de dispositivos conectados nas indústrias, impulsionando a Revolução Industrial 4.0, que promove a conectividade por meio do crescimento da IoT e conexões M2M. Com o aumento de dispositivos conectados à internet, prevê-seum aumento na ocorrência de novas ameaças e ataques cibernéticos.

2. Análise de Patentes

Uma pesquisa de patentes usando as palavras-chave "CYBERSECURITY" ou "CYBER SECURITY" foi conduzida na plataforma Derwent Innovation da Clarivate Analytics. O objetivo era obter uma visão geral dos documentos de patentes, utilizando a opção "Smart Search" para abranger todos os resultados possíveis. Um filtro foi aplicado para incluir apenas patentes "vivas" e "indeterminadas", excluindo as "mortas". Isso resultou em aproximadamente 480.000 patentes.

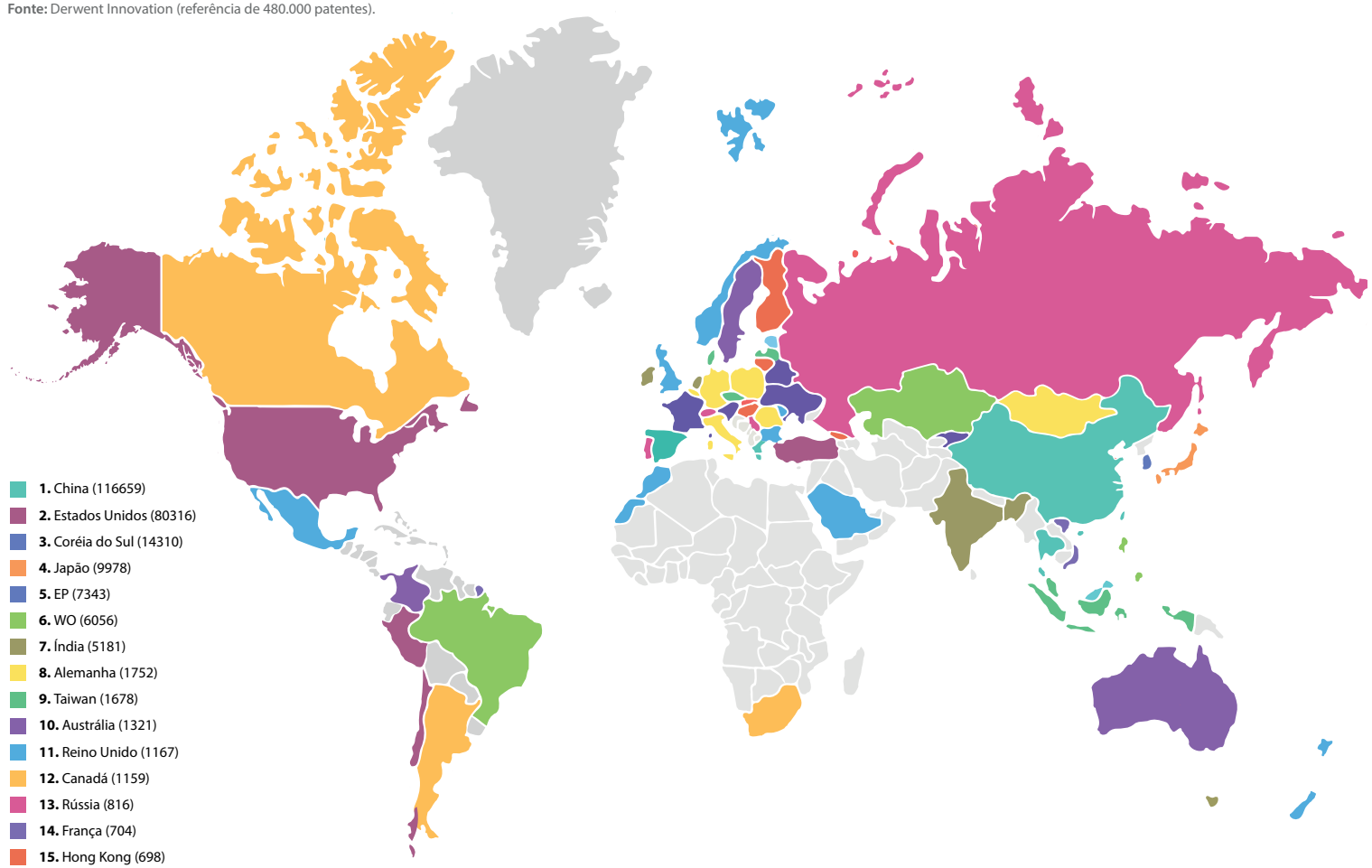
2.1. Os principais países que depositaram patentes relacionadas à Segurança Cibernética

Os cinco primeiros depositantes nessa área são : China, Estados Unidos, Coreia do Sul, Japão e depósitos via EP (escritório europeu). O Brasil ocupa a 16ª posição, com 508 depósitos. WO é a sigla para Organização Mundial da Propriedade Intelectual e é usada para identificar patentes depositadas internacionalmente através do Tratado de Cooperação em Matéria de Patentes (PCT). Portanto, "WO" em depósitos de patentes indica uma patente depositada internacionalmente.

Principais países depositantes de patentes na área de segurança cibernética

Fonte: Derwent Innovation (referência de 480.000 patentes).

Fig. **11**



A **Figura 12** mostra as principais áreas de desenvolvimento nas patentes encontradas relacionadas com processamento de dados digitais elétricos, transmissão de informações digitais e tecnologia da informação e comunicação (TIC) adaptada para fins administrativos, comerciais ou financeiros, que compõem mais de 83% dos resultados.

Fig. **12**

Tendências tecnológicas dos depósitos de patentes

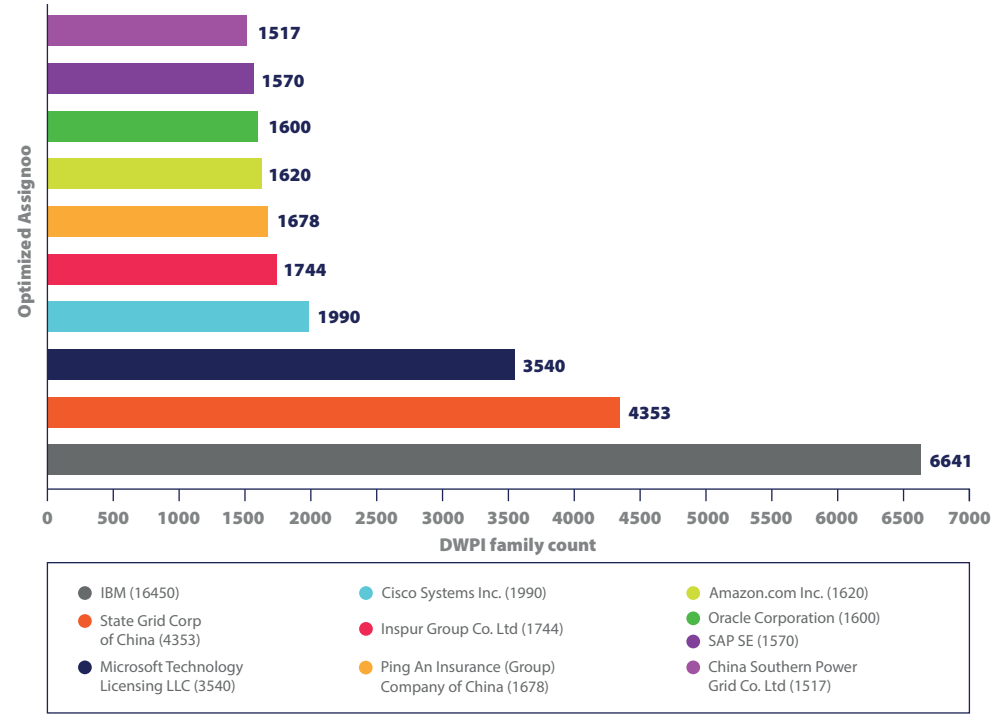
Fonte: Derwent Innovation (referência de 480.000 patentes).

A **Figura 13** mostra as dez principais empresas que depositaram patentes na área de segurança cibernética, todas multinacionais, incluindo IBM, Microsoft, Samsung, Cisco, Oracle e Amazon.

Principais depositantes de patentes na área de segurança cibernética

Fonte: Derwent Innovation (referência de 480.000 patentes).

Fig. **13**

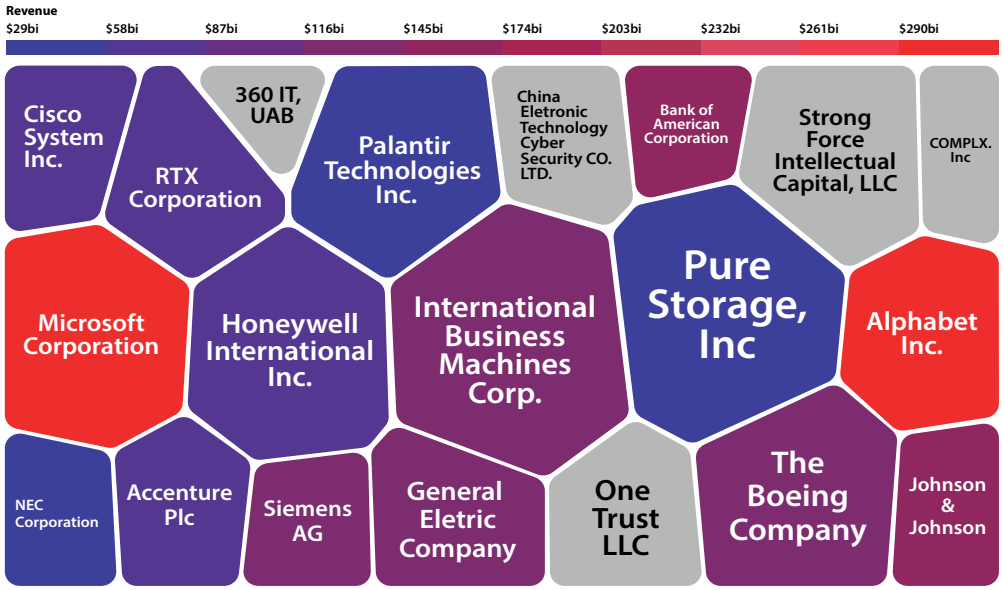


Outro aspecto interessante é sobre os depositantes de patente de segurança cibernética e sua respectiva receita. A **Figura 14** mostra esse aspecto, e os principais players são: Microsoft, Alphabet Inc (Google), IBM, Cisco, Siemens, Honeywell International e Accenture.

Fig. **14**

Principais depositantes de patentes na área de Segurança Cibernética x receita

Fonte: Innography (Clarivate)

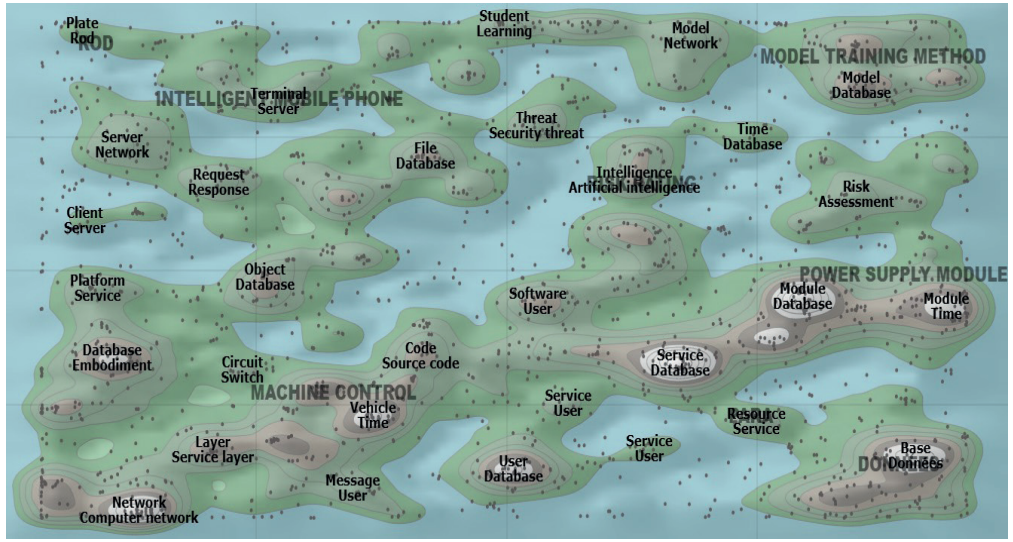


A **Figura 15** mostra o ThemeScape Map de segurança cibernética, uma representação gráfica de um conjunto de patentes agrupadas por similaridade temática, usando critérios de proximidade tecnológica. Esse gráfico foi gerado com a capacidade máxima da ferramenta, analisando 60.000 patentes consideradas relevantes. O ThemeScape Map facilita a criação rápida de panoramas tecnológicos, formando grupos-chave para identificar tendências em mercados internacionais de tecnologia.

Fig. **15**

ThemeScape Map de Segurança Cibernética

Fonte: Derwent Innovation (referência de 60.000 patentes).



O ThemeScape Map identifica nove temas principais, que são picos associados à concentração de depósitos de patentes, mostrando uma relação entre os registros. As temáticas com maior concentração de registros de patentes são: Network Computer Network, Vehicle Time, Database Embodiment, User Data Base, Service Database, Module Database, Module Time e Base Donnees.

A **Figura 16** apresenta os principais países que desenvolvem tecnologias/produtos com a utilização de segurança cibernética. Nessa lista, os quatro primeiros países são: Estados Unidos, China, Coreia do Sul e Japão.

Fig. 16

Principais países que desenvolvem tecnologias/produtos com segurança cibernética

Fonte: Derwent Innovation (referência de 480.000 patentes).

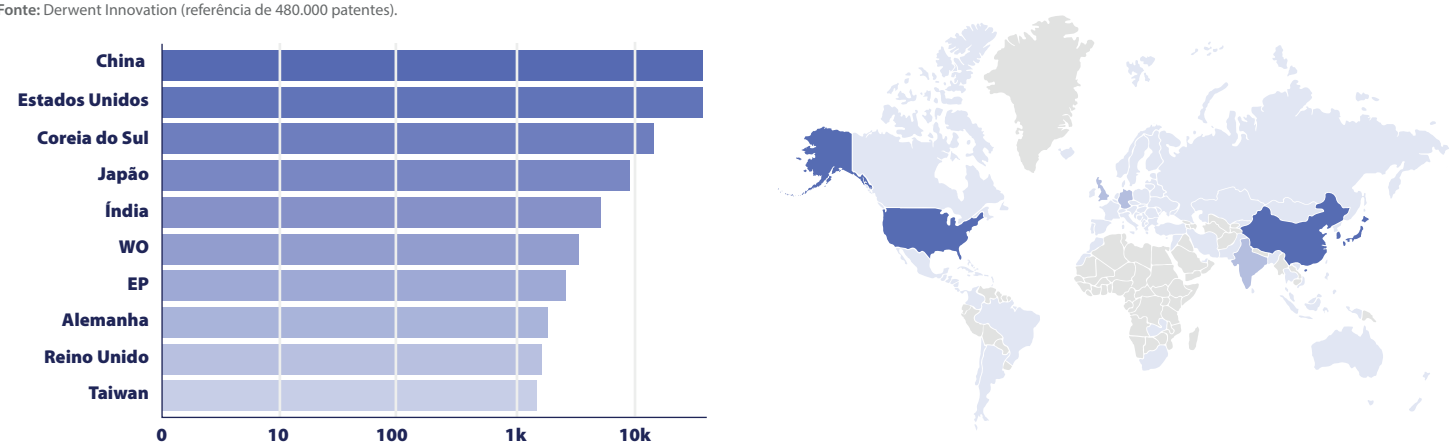
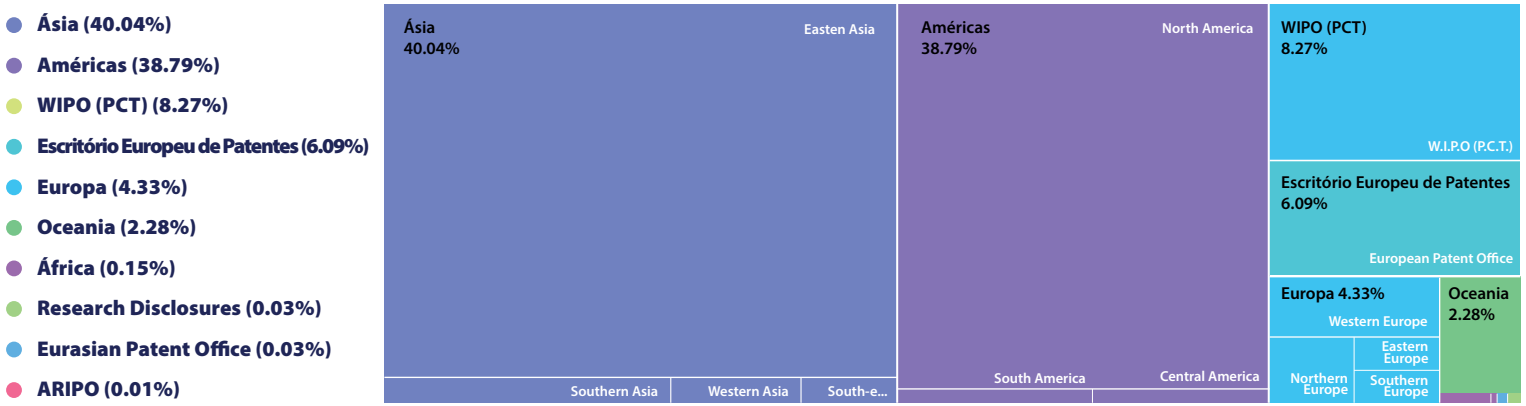


Fig. 17

Principais mercados para as invenções à base de segurança cibernética

Fonte: Derwent Innovation (referência de 480.000 patentes)



A **Figura 17** apresenta os principais mercados para as invenções relacionadas com a aplicação de segurança cibernética no mundo. Esses mercados de tecnologias/produtos são concentrados na Ásia (40,04%) e nas Américas (38,79%).

Segundo a plataforma Derwent Innovation, 51% dos registros mundiais nestes resultados são concedidos, o que indica proteção para patentes ativas (vivas) nos mercados relevantes. 49% desse conjunto de resultados são aplicações pendentes. Altas porcentagens de aplicações podem sugerir um mercado emergente ou em expansão, enquanto baixas taxas podem indicar mercados estabelecidos ou de crescimento lento. Apenas 2% das empresas têm registros em mais de quatro países, o que pode indicar um potencial de mercado crescente se adotada uma estratégia de registro global.

3. Estudo de Mercado

2024

O mercado de segurança cibernética é segmentado por tipos de produto, tipo de implementação, indústria de uso final e região.

3.1. Setores nos quais a tecnologia se insere

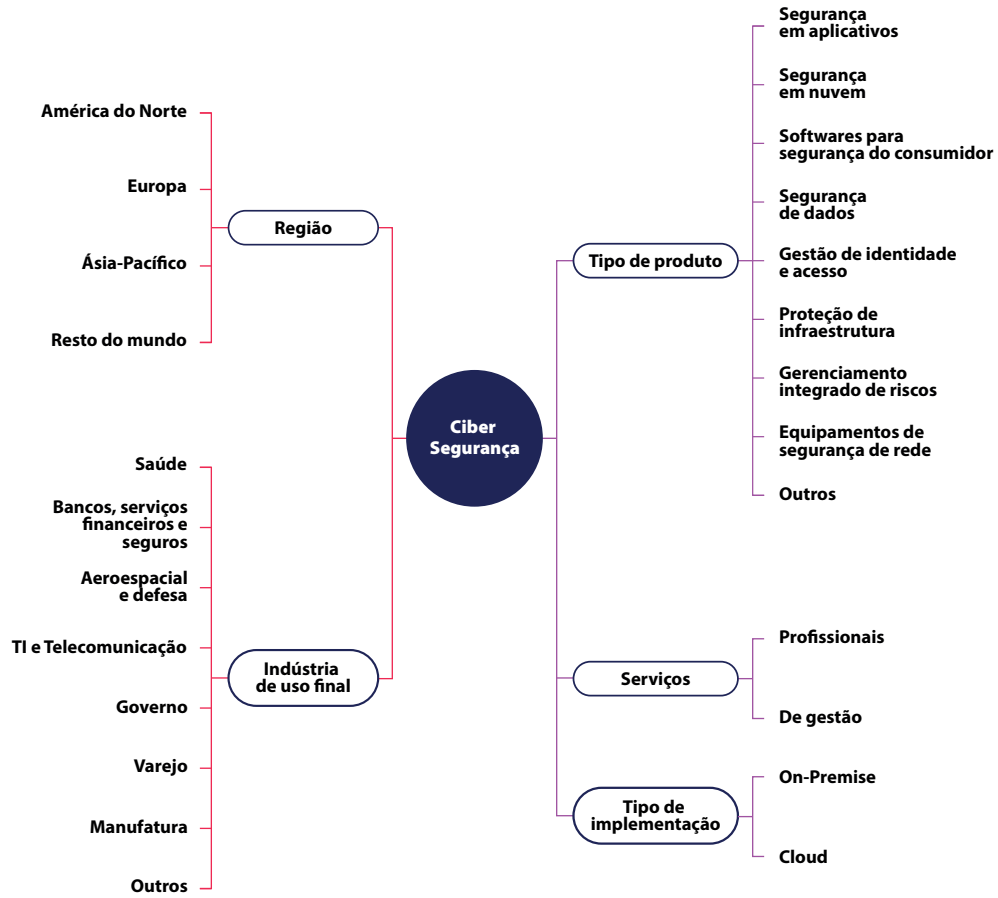
O segmento "tipo de produto" é dividido em soluções e serviços. As soluções incluem segurança de aplicativos, segurança em nuvem, programas para segurança do consumidor, segurança de dados, gestão de identidade e acesso, gerenciamento integrado de riscos, equipamentos de segurança de rede, entre outros. As atividades envolvem serviços profissionais, como consultorias, integrações, treinamento e suporte estratégico, e serviços de gestão, voltados para o planejamento, a construção e a execução de projetos de segurança cibernética. O segmento "tipo de implementação" é dividido em *on-premise*, que se refere à implantação de soluções de segurança diretamente nas instalações das empresas, e *cloud*, que se refere à implantação de soluções de segurança baseadas em nuvem. Os outros dois segmentos referem-se aos usuários finais, que abrangem vários setores, e regiões.

Como mostra a **Figura 18**, o mercado de segurança cibernética é segmentado por tipos de produto, tipo de implementação, indústria de uso final e por região.

Fig. **18**

Segmentação do mercado de segurança cibernética

Fonte: Adaptado de Mordor Intelligence (2022)



3.2. Análise de Mercado

O mercado de segurança cibernética está passando por um crescimento significativo, impulsionado pela crescente conscientização sobre os riscos cibernéticos e a necessidade de proteger sistemas e dados.

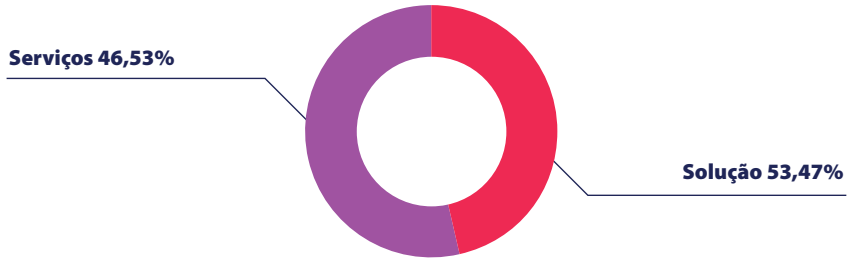
Esse crescimento resultou no surgimento de muitas *startups* de segurança cibernética e um aumento nas fusões e aquisições no setor. As características que impulsionam o mercado de segurança cibernética incluem o aumento das ciberameaças, o investimento substancial no setor, as regulamentações rigorosas sobre proteção de dados e privacidade, a crescente conscientização sobre riscos cibernéticos e a expansão da adoção de dispositivos IoT.

O mercado de soluções lidera com 53,47% da fatia de mercado (USD 90,50 bi) em 2022 (**Figura 19**). A previsão é que alcance 54,81% (USD 173,76 bi) em 2027, uma CAGR de 9,77%.

Fig. **19**

Market share (%) em receita por tipo de produto - 2022 [Mundo]

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional da Indústria



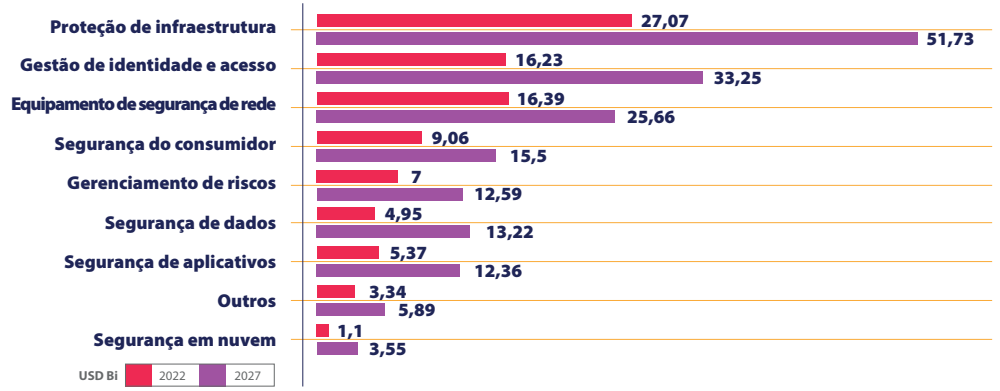
Dentro do nicho de soluções de segurança cibernética, a proteção de infraestrutura é a maior em termos de receita, gerando USD 27,07 bilhões em 2022, com previsão de alcançar USD 51,73 bilhões em 2027, um crescimento anual composto (CAGR) de 12,65%.

Esse crescimento está relacionado ao aumento dos esforços de governos e empresas em iniciativas de transformação digital para modernizar e conectar infraestruturas, como água, utilidades, transmissão e distribuição de energia, o que aumentou a vulnerabilidade a ataques cibernéticos (**Figura 20**).

Fig. **20**

Mercado e projeção de crescimento global de soluções em segurança cibernética, em USD bi

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional de Indústria

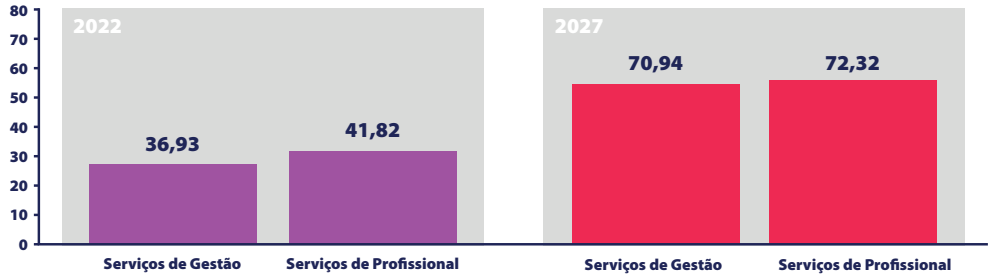


No nicho de serviços de segurança cibernética, os serviços profissionais registraram USD 41,82 bilhões em 2022, correspondendo a 53,1% da participação de mercado global (**Figura 21**). A previsão é que alcance USD 72,32 bilhões em 2027, com um crescimento anual composto (CAGR) de 8,14%. Espera-se que esses serviços cresçam significativamente, pois as empresas estão optando por consultoria antes de selecionar as soluções de segurança cibernética adequadas às suas necessidades devido às constantes ameaças cibernéticas, destacando a necessidade desse nicho.

Fig. **21**

Mercado e projeção de crescimento global de serviços em segurança cibernética em USD bi

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional de Indústria

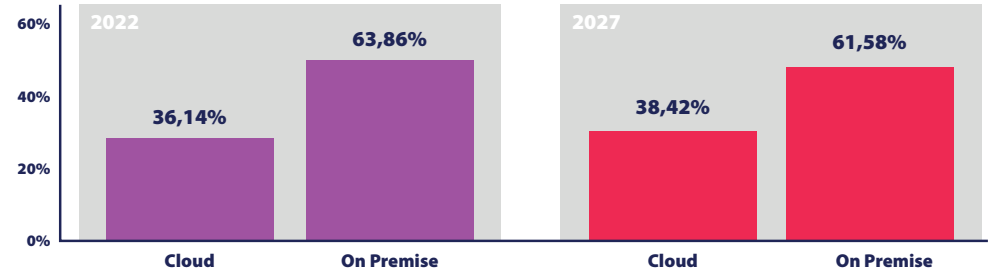


A segmentação do mercado de segurança cibernética também pode ser feita por tipo de implementação, que pode ser *on-premise* ou em nuvem. Em 2022, as implementações *on-premise* representavam quase 64% do *market share* de receita global, com USD 108,08 bilhões (**Figura 22**).

Fig. **22**

Mercado e projeção de market share de tipos de implementação de segurança cibernética

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional de Indústria



A previsão é que alcance USD 195,23 bilhões em 2027, com um crescimento anual composto (CAGR) de 8,14%. Por outro lado, estima-se que as implementações em nuvem aumentem sua participação de mercado de 36,14% para 38,42% até 2027, alcançando USD 195,23 bilhões, com um CAGR de 10,34%.

De acordo com a Mordor Intelligence (2022), as soluções de segurança *on-premise* geralmente oferecem melhor proteção contra ameaças em comparação com as implementações em nuvem. No entanto, com o avanço das inovações tecnológicas, espera-se que a plataforma em nuvem se torne mais segura, permitindo que as empresas respondam mais rapidamente às ameaças, se concentrem na mitigação de riscos e economizem em investimentos em infraestrutura local.

Os usuários finais se dividem em vários setores, incluindo bancos, serviços financeiros e seguros (BFSI), saúde, aeroespacial e defesa, TI e telecomunicações, governo, varejo, manufatura, entre outros. O setor BFSI é o que gera a maior receita no mercado global, com um *market share* de 21,68% em 2022 (USD 36,69 bilhões), prevendo-se que alcance 22,92% em 2027 (USD 72,69 bilhões), com um crescimento anual composto (CAGR) de 10,26% (**Figura 23**).

Na segmentação por região, a América do Norte lidera com 48,04% do *market share* em 2022 (USD 81,3 bilhões), com previsão de alcançar USD 129,82 bilhões em 2027, um crescimento anual composto (CAGR) de 6,91%. Em seguida, na **Figura 24,** vêm a Europa e a Ásia-Pacífico, com 28,64% e 18,20% da participação de mercado global, respectivamente. Estima-se que a participação da Ásia-Pacífico aumente de 18,20% para 26,70% até 2027.

Fig. 23

Mercado e projeção global por uso final em USD bi

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração Observatório Nacional da Indústria.

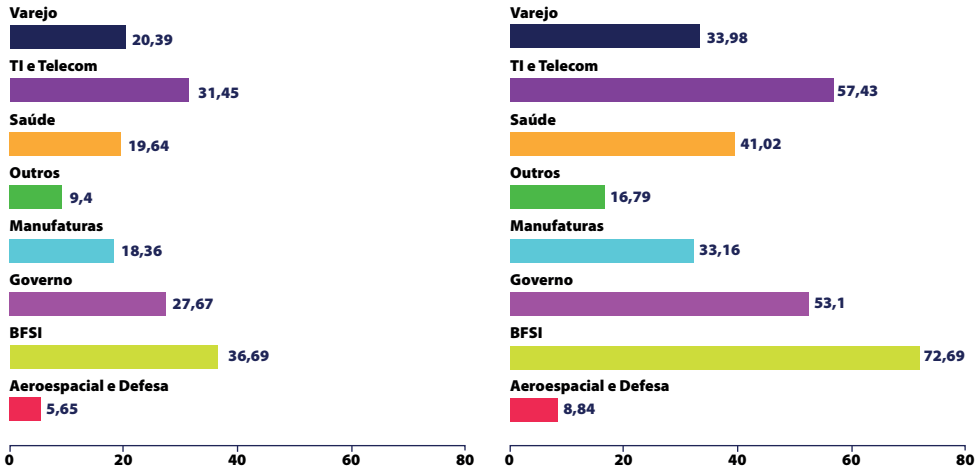
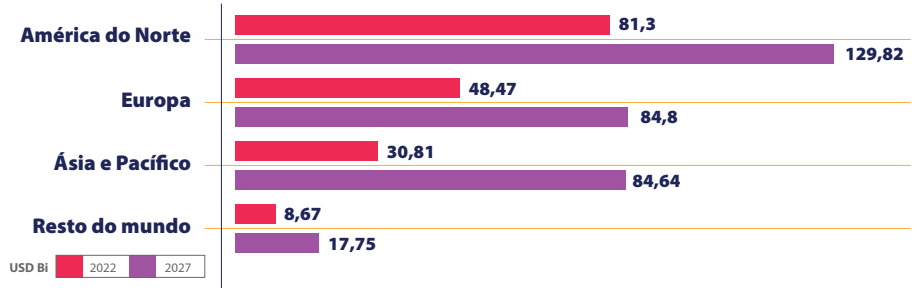


Fig. 24

Mercado e projeção global por região em USD bi

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional de Indústria



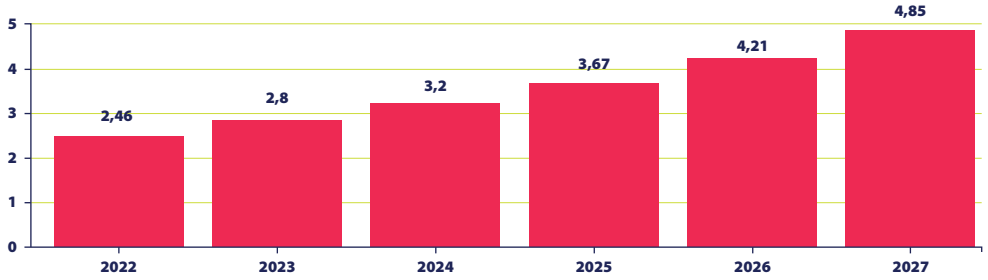
O mercado de segurança cibernética no Brasil é o maior da América Latina em termos de receita, gerando USD 2,46 bilhões, em 2022, e representando 39,68% do *market share*.

A previsão é que alcance USD 4,85 bilhões em 2027, com um crescimento anual composto (CAGR) de 10,18%. Isso se deve ao alto índice de cibercrimes no Brasil, incluindo ataques de *ransomware* e *malware*, levando as empresas brasileiras a sofrerem perdas substanciais e destacando a necessidade de investimentos em segurança cibernética. A inteligência artificial e a segurança cibernética são prioridades para o setor bancário e outras indústrias no Brasil, refletindo o desejo de adotar tecnologias avançadas para proteger sistemas e dados contra ameaças cibernéticas. O mercado de inteligência artificial no Brasil registrou USD 492 milhões em 2022, com previsão de alcançar USD 1.495,7 bilhões em 2029, um CAGR de 17,21%. No que diz respeito aos estados, São Paulo lidera com USD 107,26 milhões em 2022, com projeção para USD 326,06 milhões em 2029, um CAGR de 17,21% (**Figura 25**).

Fig. 25

Mercado e projeção de crescimento de segurança cibernética no Brasil em receita (USD bi)

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022) - Elaboração: Observatório Nacional da Indústria.



3.3. Análise de Pestel

A **Figura 26**, de acordo com a Agência de Segurança Cibernética da União Europeia (ENISA), ilustra os fatores envolvidos na segurança cibernética para cada dimensão, levando em consideração critérios de impacto e probabilidade.

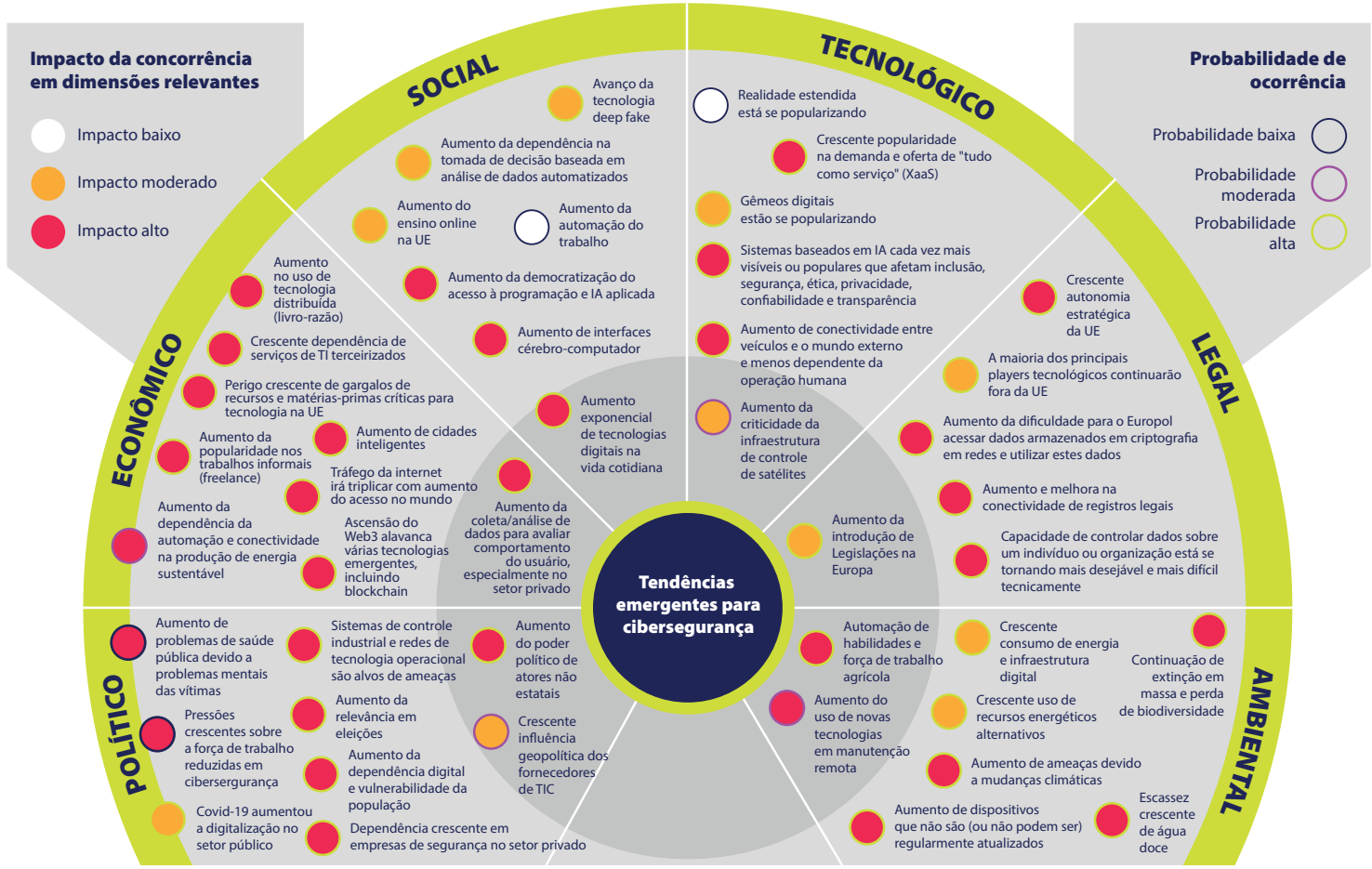
O mercado de segurança cibernética é influenciado por uma variedade de fatores econômicos, sociais, tecnológicos, ambientais, políticos e legais:

- Economicamente, a crescente dependência de tecnologias digitais, a popularização de serviços de *freelancer* e a coleta e análise de dados para entender o comportamento do usuário

Fig. **26**

Análise PESTEL das tendências emergentes em segurança cibernética

Fonte: Adaptado de ENISA (2023)



evidenciam a mudança no cenário de trabalho, impulsionada pela digitalização e flexibilidade nas atividades laborais.

- Socialmente, o aumento exponencial das tecnologias digitais no cotidiano das pessoas traz consigo diversos riscos e ameaças. A democratização do uso de IA pode levar a problemas de segurança se os sistemas forem desenvolvidos por pessoas sem treinamento adequado.
- Tecnologicamente, a dependência das organizações de serviços XaaS pode implicar uma crescente externalização de soluções de TI e, consequentemente, o surgimento de novos desafios e riscos.
- Ambientalmente, a ameaça de eventos climáticos extremos destaca a necessidade de proteger a infraestrutura crítica, incluindo a tecnológica, diante desses desafios.
- Politicamente, o aumento de problemas de saúde mental pelas vítimas de ataques cibernéticos, aumento de ameaças em redes industriais e em eleições, aumento de poder político de atores não governamentais, bem como dependência do governo de empresas do setor privado são fatores relevantes.
- Legalmente, a necessidade de conformidade com regulamentos de proteção de dados e privacidade é crucial, particularmente diante do crescente monitoramento e coleta de dados pessoais.

3.4. Legislação/Regulamentação

A regulamentação em segurança cibernética ainda é bastante limitada entre as grandes indústrias. Nos Estados Unidos, a North American Electric Reliability Corporation (NERC), uma agência da indústria elétrica, recebeu autorização para estabelecer padrões de proteção de infraestrutura crítica (CIP). Esses padrões regulam controles técnicos e procedimentais. No entanto, muitas grandes empresas industriais estão enfrentando dificuldades para desenvolver seus próprios padrões de segurança para Tecnologia da Informação (TI) e Tecnologia Operacional (TO), combinando-os a partir de várias normas da indústria.

A **Figura 27** indica algumas normas internacionais relativas à segurança cibernética.

Fig. **27**

Normas de segurança cibernética internacionais

Fonte: Observatório Nacional da Indústria (2023).

Documento	Descrição
DFARS	Conjunto de regulamentos que se aplica a todos os contratos e subcontratos do Departamento de Defesa dos EUA.
ISO 22301	Descreve como as organizações podem garantir a continuidade dos negócios e se proteger de desastres.
ISO/IEC 27001	Norma internacional para segurança da informação que fornece uma estrutura para gerenciar informações confidenciais da empresa.
ISO/IEC 27002	Código de prática para a gestão da segurança da informação. Fornece orientação e recomendações sobre como implementar controles de segurança dentro de uma organização. Suporte à ISO 27001.

Continua >>

Documento	Descrição
ISO/IEC 27031	Fornece orientações sobre como as organizações podem usar as TIC* para proteger suas operações de negócios e garantir a continuidade em caso de incidente ou desastre.
ISO/IEC 27032	Diretrizes para organizações se protegerem contra ataques cibernéticos e gerenciarem os riscos associados ao uso da tecnologia.
ETSI EN 303 645	Fornece um conjunto de requisitos básicos para segurança em dispositivos de Internet das Coisas (IoT) do consumidor.
ISO/SAE 21434	Propõe medidas de cibersegurança para o ciclo de vida de desenvolvimento de veículos rodoviários.
ISO/IEC 27701	Especifica os requisitos para um PIMS (sistema de gerenciamento de informações de privacidade) com base nos requisitos da ISO 27001.

*TIC = Tecnologia da Informação e Comunicação

No contexto da Indústria 4.0 (I4.0), a **Figura 28** mostra normas e diretrizes relacionados à segurança cibernética:

Fig. **28**

Normas e diretrizes para segurança cibernética na I4.0

Fonte: Corallo, Lazoi e Lezzi, (2020)

Documento	Descrição
ISA/IEC 62443	Sistemas de Automação e Controle Industrial (IACS)
Estrutura de Certificação em Cibersegurança do IACS (ICCF)	Sistemas de Automação e Controle Industrial (IACS)
ANSSI Cibersegurança para Sistemas de Controle Industrial (ICS)	Sistemas de Controle Industrial (ICS)
API Standard 1164	Sistema de Controle e Aquisição de Dados (SCADA)
Compendium de Segurança para Sistemas de Controle Industrial (ICS)	Sistemas de Controle Industrial (ICS)
Catálogo de Segurança de Sistemas de Controle	Sistemas de Controle de Infraestruturas Críticas e Recursos-chave
Avaliações ICS-CERT	Sistemas de Controle Industrial (ICS)
NIST 800-82	Sistemas de Controle Industrial (ICS)

A institucionalização da segurança cibernética no Brasil foi catalisada pela aprovação do Marco Civil da Internet em 2013 e pelos esforços relacionados aos megaeventos realizados no país entre 2012 e 2016. Esses esforços incluíram a criação do Centro de Defesa Cibernética (CDCiber), iniciativas de capacitação em segurança cibernética, aumento da colaboração entre o governo e o setor privado, e o estabelecimento de políticas e diretrizes de segurança cibernética.

A coleta e o processamento de dados pessoais no Brasil são regulamentados pela Lei Geral de Proteção de Dados (LGPD), que se aplica a todas as pessoas naturais ou jurídicas que coletam dados pessoais de cidadãos brasileiros. A lei não se aplica ao processamento de dados realizado por pessoa natural exclusivamente para fins privados e não econômicos, ou para fins jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional e investigação e repressão de crimes.

O Brasil enfrenta desafios significativos em relação à segurança cibernética, incluindo a falta de coordenação e estratégia coesa em iniciativas de segurança cibernética, a falta de recursos de aplicação da lei, a prevalência de crimes violentos, a produção local de *malware* e desafios de infraestrutura e regulamentações insuficientes para

proteger novas tecnologias. Para garantir a segurança cibernética, o país precisa de uma estratégia abrangente e de um esforço coordenado em todas as esferas governamentais e entre os setores público e privado.

3.5. Detalhamento do setor principal

O setor de bancos, serviços financeiros e seguros (BFSI) tem a maior receita no mercado global de segurança cibernética, com um *market share* de 21,68% em 2022 (USD 36,69 bilhões) e previsão de alcançar 22,92% em 2027 (USD 72,69 bilhões), com um crescimento anual composto (CAGR) de 10,26%. Esse setor, que tem se transformado agressivamente por meio da digitalização, enfrenta um aumento de ciberataques, incluindo ataques de *phishing*, ataques de negação de serviço (DoS), *spear-phishing*, *ransomware*, ataques de *malware*, entre outros, que visam roubar dinheiro e sabotar a reputação da marca.

Para combater essas ameaças, o setor BFSI está adotando medidas proativas para proteger os processos de TI, dados críticos dos clientes e cumprir regulamentações governamentais, o que envolve a implementação de tecnologias de segurança de ponta. Além disso, a colaboração entre o setor bancário e as autoridades governamentais para fortalecer a resiliência cibernética e combater o cibercrime é um ponto a destacar.

Os fatores que impactam o setor incluem a rápida adoção de tecnologias como IA, *Machine Learning* e *Blockchain*, a crescente dependência de serviços de TI terceirizados, a popularização de serviços de freelancer, a coleta e análise de dados para entender o comportamento do usuário, a crescente dependência de dispositivos IoT e a tendência BYOD (*Bring Your Own Device*), e a necessidade de conformidade com regulamentos de proteção de dados e privacidade.

3.6. Modelo para captura do potencial de valor da tecnologia

O valor na segurança cibernética está intrinsecamente ligado à tecnologia, que proporciona benefícios significativos. As ameaças cibernéticas são potenciais fatores que podem causar a perda de valor do negócio. Segundo a Mordor Intelligence (2022), uma hipótese é que a demanda por segurança cibernética está crescendo devido ao aumento das conexões M2M/IoT nas empresas. A redução significativa nos custos dos dispositivos e os novos modelos de negócios emergentes têm sido fatores cruciais para a crescente penetração da IoT no mercado global. No entanto, o desafio é identificar o modelo de captura de valor das tecnologias no ambiente cibernético.

As organizações estão enfrentando várias megatendências, como sustentabilidade, ameaças à segurança cibernética, digitalização, automação, inflação, ativismo dos acionistas, polarização de pontos de vista e constituintes, igualdade e diversidade social, equidade e inclusão. Segundo a Gartner, essas tendências estão mudando fundamentalmente a estratégia e os modelos operacionais e criam novas expectativas por parte de uma série de partes interessadas.

Nesse ambiente complexo, os modelos tradicionais de valor empresarial não são suficientes para tomar decisões que gerem valor sustentado. A Gartner (2022) desenvolveu uma nova equação de valor empresarial que reflete melhor esse constante "dar e receber" de valor que as empresas devem equilibrar entre as partes interessadas e as ações atuais (**Figura 29**).

A equação de valor empresarial proposta pela Gartner destaca a existência de dois domínios: o dos stakeholders e o da empresa. No centro de tudo está a criação de valor ("dar") e a realização do valor ("receber"). A lógica do valor é evidenciada pelo fluxo que percorre tanto a criação de valor, considerando as prioridades e preocupações das partes

Fig. **29**

Equação de valor empresarial do Gartner

Fonte: Gartner (2022) - Adaptação

interessadas e a alavancagem do valor, quanto à realização do valor, considerando os impactos nas múltiplas partes interessadas e a realização do retorno à organização.

Por exemplo, abordar novas ameaças, como a cibersegurança, e oportunidades, como a sustentabilidade, amplia os resultados empresariais para além da conformidade regulatória a uma série de partes interessadas. Os benefícios ou impactos em jogo incluem segurança, inovação, privacidade, ecossistema e alinhamento com valores. O impacto pode aumentar o valor da marca, a reputação e a lealdade da organização, ultrapassando em troca os custos associados.

3.7. Atores do ecossistema associados à tecnologia

A indústria internacional de segurança cibernética opera em três principais conjuntos distintos: a Baía de São Francisco, a região metropolitana de Washington D.C. e Israel. Essas regiões possuem duas características essenciais: uma cultura de inovação de *startups* e alta tecnologia, que impulsiona o crescimento de todos os três ecossistemas. A Baía de São Francisco e Israel possuem ecossistemas prósperos de *startups*, com um fluxo substancial de capital de risco e um foco intensivo em produtos. Em contraste, Washington tem uma proporção maior de empresas baseadas em serviços.

Outro ponto importante é a ligação entre o capital humano e a segurança nacional. A qualidade e a disponibilidade de especialistas em segurança cibernética nessas áreas são de importância crítica para a segurança nacional, considerando a crescente interdependência entre as esferas pública e privada em relação à segurança cibernética.

Segundo a Mordor Intelligence (2022), o ecossistema de segurança cibernética é dividido em três tipos de empresas: "Pure Play Cybersecurity Firms", que são empresas especializadas exclusivamente em soluções e serviços de segurança cibernética, como Checkpoint e Symantec (agora Broadcom); "Non-Pure Play Cybersecurity Firms", que são empresas que oferecem produtos ou serviços relacionados à segurança cibernética como parte de suas ofertas mais amplas, como Microsoft, Cisco e IBM; e "Non-Cyber Security *Firms*", que são empresas que não estão diretamente envolvidas em fornecer soluções de segurança cibernética, como hospitais, companhias aéreas, escolas, entre outros.

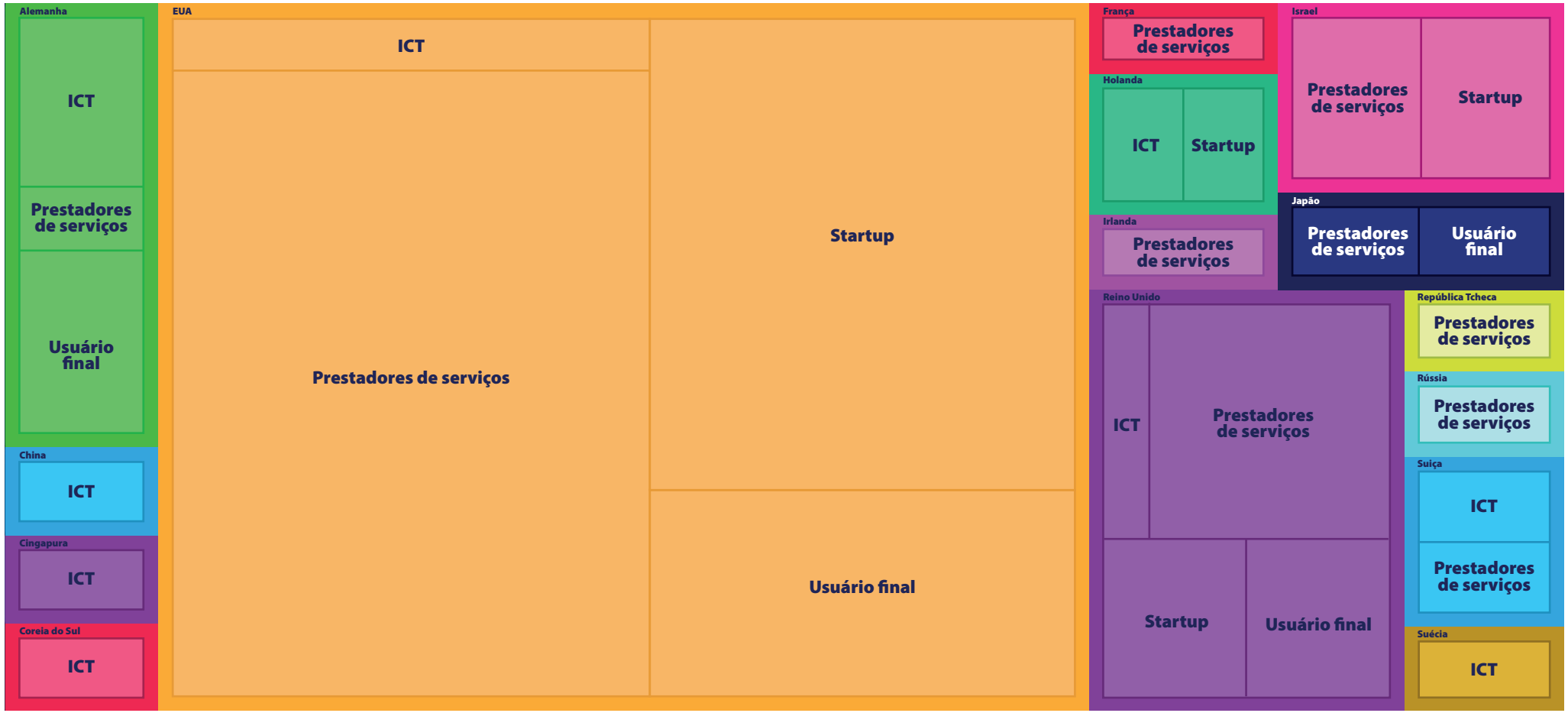
A **Figura 30** apresenta alguns dos atores internacionais envolvidos na segurança cibernética. Esses atores oferecem uma variedade de serviços, incluindo consultoria em segurança cibernética, gestão de riscos, testes de segurança e auditoria, monitoramento de segurança e resposta a incidentes, proteção de rede e infraestrutura, e treinamentos. Eles atendem a uma ampla gama de usuários finais, abrangendo praticamente todos os setores, como bancos, indústrias manufatureiras, *e-commerce*, entre outros, e também incluem institutos de ciência e tecnologia.

É importante destacar que muitas dessas empresas que fornecem serviços de segurança cibernética possuem em seu portfólio consultorias, treinamentos, softwares, entre outros.

Fig. 30

Atores do ecossistema internacional

Fonte: Global Cybersecurity Market Report (Mordor Intelligence, 2022); Cybersecurity Worldwide (Statista, 2023) Elaboração: Observatório Nacional da Indústria

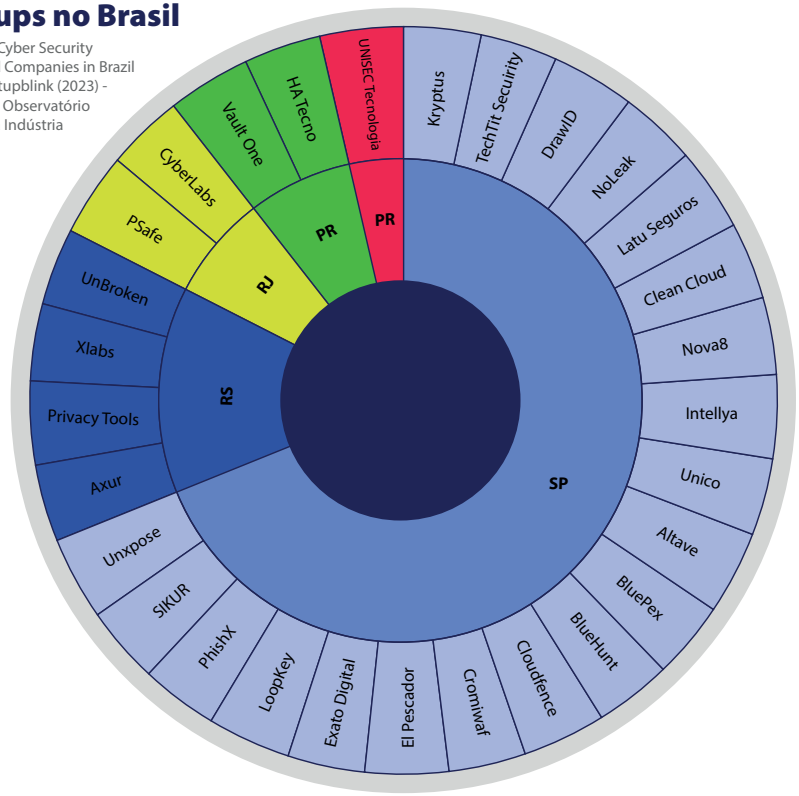


A **Figura 31** ilustra algumas startups no Brasil, que envolvem proteção para empresas em caso de violações de dados e ameaças cibernéticas, proteção de operações e transações virtuais, documentos e dispositivos, segurança de identidade e acesso baseado em Zero Trust, sistemas para LGPD, segurança em *cloud*, entre outros.

Fig. **31**

Startups no Brasil

Fonte: Top Cyber Security Startup and Companies in Brazil (2023); Startupblink (2023) - Elaboração: Observatório Nacional da Indústria

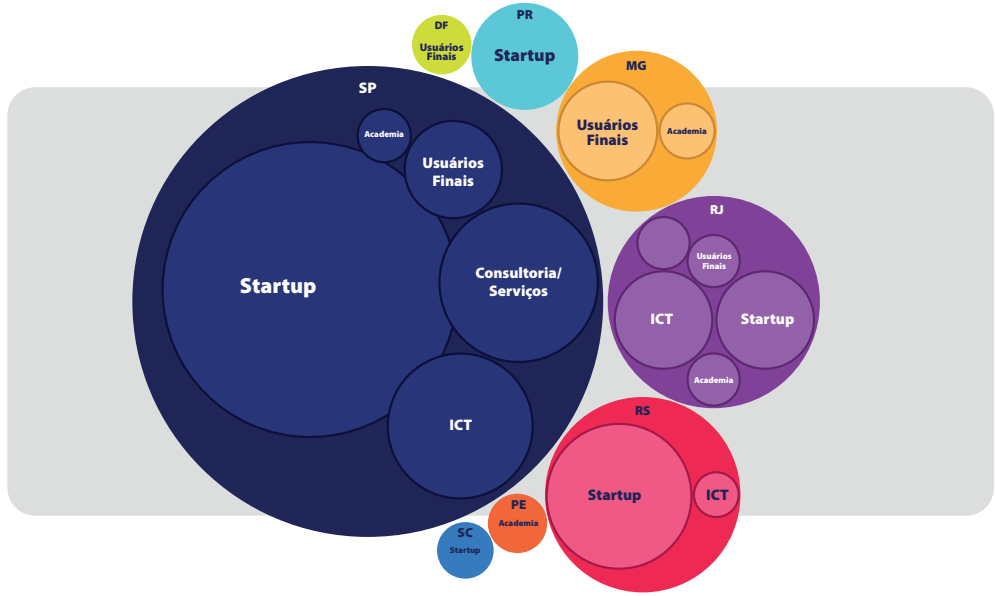


Além das *startups*, o ecossistema de segurança cibernética no Brasil inclui uma variedade de usuários finais, semelhante ao ecossistema internacional. Esses usuários finais incluem instituições financeiras, grandes indústrias que compõem a economia nacional, como petroquímicas, automotivas, papel e celulose, entre outras, institutos de pesquisa, prestadores de serviços, incluindo consultoria, treinamentos, softwares, etc., universidades e faculdades, e também o governo federal. A **Figura 33** apresenta alguns desses atores relevantes.

Fig. **32**

Atores do ecossistema nacional em segurança cibernética

Fonte: Top Cyber Security Startup and Companies in Brazil (2023); Startupblink (2023) - Elaboração: Observatório Nacional da Indústria



Vários atores realizam testes de segurança cibernética, incluindo o Instituto Nacional de Telecomunicações (Inatel), que possui mais de 40 centros de pesquisa e um foco específico em segurança cibernética. A Clavis oferece serviços e soluções para segurança e privacidade de dados para todas as organizações, enquanto a Hackersec realiza testes de segurança black, white e grey-box. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) presta serviços para redes que utilizam recursos do NIC.br. O Centro de Computação da Unicamp oferece serviços relacionados a certificados digitais e segurança da informação. O CPQD é um dos maiores centros de pesquisa e desenvolvimento da América Latina, com foco em tecnologias da informação e comunicação, incluindo prevenção inteligente contra fraudes e perdas usando *Machine Learning*.

Internacionalmente, programas como o Programa de Auxílio à Segurança Cibernética Estadual e Local dos EUA, o financiamento em segurança cibernética da UE e o Fundo Global para segurança cibernética do Banco Mundial, ajudam a lidar com riscos e ameaças de segurança cibernética e apoiam a pesquisa e inovação na área. No Brasil, a EMBRAPII cofinancia projetos de segurança cibernética e outras áreas tecnológicas. O Plano Inova Telecom do BNDES coordena ações de fomento à inovação no setor de telecomunicações, incluindo a segurança cibernética. O BNDES Finem-Segurança Pública investe na expansão e modernização de infraestruturas de segurança. A FINEP disponibiliza recursos para a transformação digital de empresas industriais, incluindo a segurança cibernética.

Anteriormente, as autoridades de segurança nacional consideravam as redes digitais como inofensivas e os ciberataques como ameaças improváveis à segurança de um país. No entanto, com o avanço dos sistemas ciberfísicos e da internet das coisas, além da sofisticação dos atores mal-intencionados, os ciberataques tornaram-se uma questão de segurança humana.

Diante disso, empresas de tecnologia começaram a formar alianças de segurança cibernética. Grandes empresas, como Airbus, Cisco, HP, Microsoft, Siemens e Telefônica, formaram grupos para lidar com questões relacionadas ao futuro da internet e das redes digitais. Essas alianças buscam a paz digital, apoio governamental a empresas sob ataque e cooperação para limitar o uso de sistemas e redes privadas contra cidadãos. Elas defendem valores como confiança e responsabilidade em segurança cibernética e incentivam a ação coletiva pela paz e não agressão. Parcerias em segurança cibernética facilitam a troca de informações sobre ameaças, fortalecendo coletivamente os mecanismos de defesa das empresas.

PUC-Rio e a UFMG também oferecem cursos de educação continuada e técnicos, respectivamente. O Mackenzie oferece graduação, MBA em segurança de dados e pós-graduação lato sensu na área de computação.

ESTUDO DE MERCADO 2024

4. Análise de demandas por treinamentos e qualificação

A falta de profissionais qualificados é uma das principais causas de ciberataques, especialmente em regiões como Europa, Ásia-Pacífico, América Latina e Oriente Médio.

A demanda por especialistas em segurança cibernética nestas regiões (Europa, Ásia-Pacífico, América Latina e Oriente Médio) supera a oferta, especialmente nos setores financeiro, governamental e privado/industrial. Muitos profissionais nessas regiões não possuem a experiência necessária para lidar com as crescentes ameaças cibernéticas.

No Oriente Médio, por exemplo, apenas 30% dos profissionais têm mais de dez anos de experiência, enquanto especialistas sugerem que pelo menos 56% da força de trabalho deveria ter essa experiência.

No Brasil, segundo país com mais profissionais de segurança cibernética (só perde para os Estados Unidos), existem diversos cursos na área, desde técnicos até graduações em universidades federais, estaduais e privadas, abordando temas como Ciência da Computação, Engenharia da Computação, Sistemas de Informação, Segurança da Informação, entre outros.

Instituições como Senai, Centro Paula Souza, Senac, Unicamp, USP, UFPE, PUC-Rio, UFMG, Mackenzie e Uniasselvi oferecem cursos voltados para a segurança cibernética. O Senai possui academias de segurança cibernética em vários estados e o Centro Paula Souza e Senac oferecem cursos técnicos na área. A Unicamp, USP, UFPE, PUC-Rio e UFMG oferecem graduação e pós-graduação em áreas relacionadas à computação, com linhas de pesquisa em segurança de redes e computadores. A Uniasselvi oferece um curso EAD de Tecnologia em Cibersegurança. Além disso, a PUC-Rio e a UFMG também oferecem cursos de educação continuada e técnicos, respectivamente.

O Mackenzie oferece graduação, MBA em segurança de dados e pós-graduação *lato sensu* na área de computação.

Um aspecto importante a ser considerado é o perfil do profissional requerido no ambiente cibernético. As **Figuras 33, 34 e 35** mostram esse tipo de perfil atuante em empresas industriais de segurança cibernética.

Fig. **33**

Perfil do engenheiro de segurança cibernética

Fonte: Observatório Nacional da Indústria

Profissional	Funções/Atividades
Engenheiro de segurança cibernética	Experiência em testes de penetração e outras ferramentas de cibersegurança;
	Uso das ferramentas para manter a empresa segura contra ameaças internas e externas;
	Formação em ciência da computação;
	Especialização em segurança;
	Experiência prática na área.

Fig. 34

Perfil do Técnico em Internet das Coisas (IoT)

Fonte: Observatório Nacional da Indústria

Profissional	Funções/Atividades
Técnico em internet das coisas (IoT)	Programar dispositivos utilizados em aplicações IoT;
	Integrar protocolos de comunicação para interoperabilidade entre sistemas, equipamentos e dispositivos utilizados em aplicações industriais;
	Integrar redes físicas para comunicação entre sensores, sistemas, equipamentos e dispositivos;
	Identificar os requisitos de segurança da informação necessários em aplicações com tecnologia IoT;
	Aplicar métodos, técnicas e ferramentas para garantir a segurança da informação na conexão entre os sensores e demais dispositivos;
	Determinar as tecnologias de sensores aplicáveis para cada solução, considerando as condições operacionais e de rastreabilidade.

Fig. 35

Perfil do técnico em sistemas de informação de processos produtivos

Fonte: Observatório Nacional da Indústria

Profissional	Funções/Atividades
Técnico em sistemas de informação de processos produtivos (informação e automação)	Implementar filtros de modelagem para conversão de dados em informação relevante para a análise dos processos industriais;
	Implantar as tecnologias para garantia da segurança das informações dos processos produtivos;
	Assegurar que o desempenho dos sistemas de segurança da informação dos processos produtivos esteja alinhado com as políticas de segurança cibernética;
	Implementar sistemas de comunicação de dispositivos dos processos produtivos em redes com e sem fio.

A popularização da tecnologia tem levado ao acúmulo de experiência na área de segurança cibernética, com profissionais experientes ministrando cursos de extensão e especialização. Embora os cursos de graduação e pós-graduação sejam fundamentais, eles têm um longo tempo de formação e a mudança de currículos é um processo demorado.

Muitas empresas, especialmente multinacionais, possuem seus próprios centros de qualificação e treinamento, conhecidos como Universidades Corporativas, que oferecem cursos específicos para seus profissionais. Exemplos de sucesso incluem a Universidade Petrobras, Académie Accor, Universidade Corporativa do Banco do Brasil, Academia Santander, Universidade Ambev, Universidade do Hambúrguer, Leroy Merlin, Universidade Corporativa da Caixa Econômica Federal, Googleplex, Celepar, Intelbras, Intel e Universidade Corporativa da E&Y. Essas instituições oferecem treinamento e capacitação em diversas áreas, incluindo segurança cibernética.

Observatório Nacional da Indústria

CNI Confederação Nacional da Indústria

SESI Serviço Social da Indústria

SENAI Serviço Nacional de Aprendizagem Industrial

IEL Instituto Euvaldo Lodi