ipea Instituto de Pesquisa Econômica Aplicada

Título do capítulo	CAPÍTULO 9 **O PAPEL DA SEGURANÇA CIBERNÉTICA NO UNIVERSO DIGITAL: A IMPORTÂNCIA DO FATOR HUMANO**
Autor(es)	Emilio Tissato Nakamura
DOI	DOI: http://dx.doi.org/10.38116/9786556350660cap9

Título do livro	**Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil**
Organizadores(as)	Luis Claudio Kubota
Volume	1
Série	-
Cidade	Rio de Janeiro
Editora	Instituto de Pesquisa Econômica Aplicada (Ipea)
Ano	2024
Edição	1a
ISBN	9786556350660
DOI	DOI: http://dx.doi.org/10.38116/9786556350660

LC/BRS/TS.2024/1

Este estudo foi elaborado no âmbito do Programa Executivo de Cooperação entre a CEPAL e o Ipea.

CAPÍTULO 9

O PAPEL DA SEGURANÇA CIBERNÉTICA NO UNIVERSO DIGITAL: A IMPORTÂNCIA DO FATOR HUMANO

Emilio Tissato Nakamura[1]

1 INTRODUÇÃO

A transformação digital se reflete na evolução social e econômica, afetando a rotina de pessoas, organizações, empresas e países. As integrações, interdependências e os avanços tecnológicos característicos do universo digital têm tornado o cotidiano mais dinâmico, ao mesmo tempo em que há o aumento da complexidade no desenvolvimento de produtos e serviços. Todos possuem responsabilidades para que o universo digital seja um ambiente saudável, possibilitando a evolução da sociedade e os avanços das nações, de uma forma integrada e sinérgica. A confiança é fundamental, e um de seus pilares é a percepção de segurança, com os riscos cibernéticos exercendo uma pressão que exige adequação no comportamento dos envolvidos.

Como indivíduos, há a necessidade de atenção e diligência quanto ao compartilhamento de informações, exigindo que governos e empresas realizem o tratamento dos dados pessoais com a devida proteção. Adicionalmente, há a responsabilidade cada vez maior para que a transformação digital não seja um elo nos ataques cibernéticos que comprometem cada vez mais intensamente empresas, organizações e países. Uma empresa, um governo ou uma organização de qualquer natureza ou tamanho deve, imprescindivelmente, adotar uma postura de segurança cibernética adequada para construir, utilizar e prover sistemas, serviços ou plataformas seguras, operando com segurança adequada e estando preparado para os incidentes cibernéticos, criando uma proposta de valor. E, no caso do país, é fundamental estabelecer a segurança cibernética em um ambiente em que a interdependência entre infraestruturas críticas nacionais aumente a complexidade, de modo que não haja um aumento sem controle da superfície de ataques cibernéticos, que pode levar a impactos em cadeia.

Desse modo, no universo digital, a segurança cibernética é imprescindível e depende cada vez mais do fator humano, exigindo uma evolução educacional

1. Diretor-adjunto de cibersegurança da Rede Nacional de Ensino e Pesquisa (RNP).

para o desenvolvimento tecnológico e a construção de serviços e plataformas confiáveis para a sociedade. Com o fortalecimento de uma cultura de segurança e privacidade, há condições para que todos estejam preparados para os ataques cibernéticos e possam exercer seus direitos e deveres em uma sociedade mais digital.

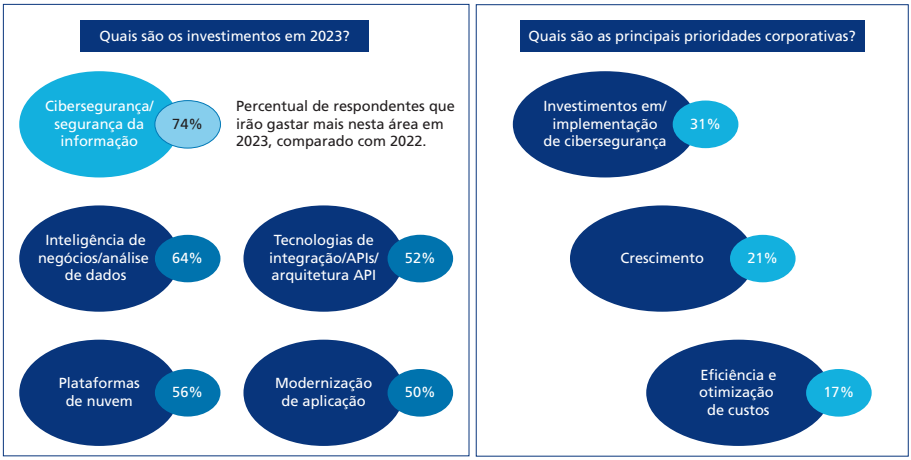
Este capítulo discute o papel da segurança cibernética no universo digital, com ênfase na importância do fator humano, iniciando com os riscos cibernéticos e incidentes de segurança da informação no Brasil e no mundo, que avançam rapidamente. A complexidade da segurança cibernética é decorrente das dimensões que devem ser tratadas, bem como do dinamismo universal que leva à evolução da própria cibersegurança. O fator humano na segurança cibernética é discutido logo a seguir, incluindo as vulnerabilidades humanas que estão sendo exploradas em ataques cibernéticos e a necessidade de conscientização, de treinamento e de fortalecimento de uma cultura de segurança da informação. Um panorama do Brasil também é apresentado, com a educação em segurança cibernética sendo discutida em conjunto com as principais tendências e com a apresentação de uma proposta de estratégia para que o fator humano na cibersegurança seja trabalhado em conjunto com a iniciativa pública e privada.

2 RISCOS CIBERNÉTICOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NO BRASIL E NO MUNDO

As necessidades de segurança cibernética se tornam ainda mais evidentes com o aumento do número de incidentes nessa área que acontecem no Brasil e no mundo. Os investimentos necessários devem levar em consideração a visão de riscos, que são específicos de cada um, e são de diferentes naturezas, incluindo os riscos cibernéticos. Para as empresas brasileiras, a figura 1 indica que a prioridade para 2023 é a cibersegurança. Além de 74% das empresas indicarem que irão aumentar os investimentos em cibersegurança em 2023, para 31% delas a segurança cibernética é a prioridade corporativa, mais do que a busca do crescimento (para 21% das empresas) e do que a busca da eficiência e otimização de custos (17%).

Os investimentos mostram que os riscos cibernéticos já não são uma questão técnica ou tecnológica, e sim uma questão de negócio e organizacional. Isso é reforçado pela maior convergência entre as visões de líderes das organizações e de líderes de cibersegurança ao longo dos anos, como mostra a tabela 1 (FEM, 2023a). Para a maioria dos líderes de negócios, a cibersegurança é um habilitador-chave de negócio, enquanto para a maior parte dos líderes de cibersegurança, ela é um custo necessário para se realizar um negócio. Em outras respostas, os líderes descreveram a segurança cibernética como um diferencial competitivo ou uma decorrência da conformidade regulatória.

FIGURA 1
Prioridades de investimentos no Brasil em 2023



Fonte: Gartner, 2022. Disponível em: https://www.gartner.com/document/4021757.
Elaboração do autor.

TABELA 1
A visão dos líderes de negócios e de cibersegurança está convergindo
(Em %)

	Diferenciação de produto e serviço	Cibersegurança é um custo necessário para realizar um negócio	Cibersegurança é um habilitador-chave de negócio	Conformidade direcionada nossos controles de segurança
Líderes de negócios	10	37	51	2
Líderes de cibersegurança	14	39	32	14

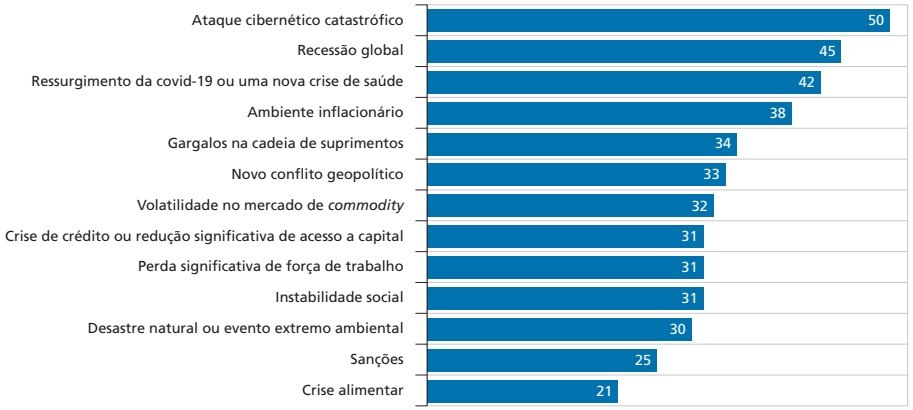
Fonte: WEF (2023a).
Elaboração do autor.

2.1 Dos riscos cibernéticos aos incidentes de segurança

Em um mundo em transformação digital, os riscos globais envolvem, de uma forma cada vez mais forte, os riscos cibernéticos. O Fórum Econômico Mundial (FEM) indica os crimes cibernéticos e a insegurança cibernética como um dos principais riscos globais, ao lado de riscos econômicos, ambientais, geopolíticos e sociais (FEM, 2023b).

Já em uma pesquisa realizada globalmente em 2023, os planos de continuidade de negócios consideram como pior risco o de ataques cibernéticos, sendo mais citado do que uma recessão global ou o ressurgimento da covid-19, como pode ser visto no gráfico 1.

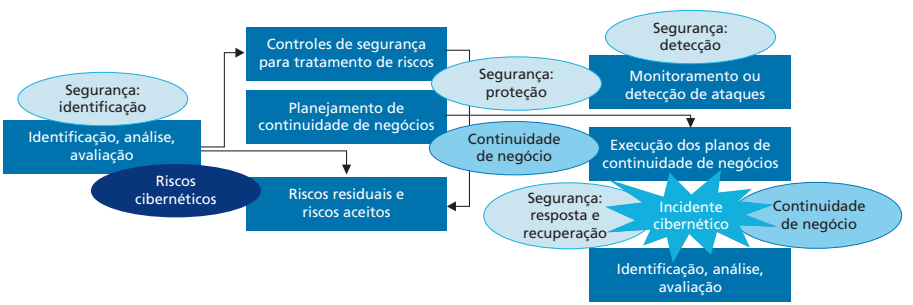
GRÁFICO 1
Principais riscos considerados para 2023
(Em %)



Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.

Esses riscos de segurança da informação, tratados pela norma ABNT NBR ISO/IEC 27005 (ABNT, 2019), possuem relação direta com a segurança da informação, tratada pela norma ABNT NBR ISO/IEC 27001 (ABNT, 2022a), e a continuidade de negócios, tratada pela norma ABNT NBR ISO 22301 (ABNT, 2020), como pode ser visto na figura 2. Os controles de segurança são implantados para o tratamento dos riscos identificados, analisados e avaliados, promovendo a proteção. O planejamento da continuidade de negócios é um controle de segurança cibernética, fazendo parte também da continuidade de negócios. Ele é executado em caso de incidente de segurança.

FIGURA 2
Relação entre riscos cibernéticos, segurança da informação e continuidade de negócios

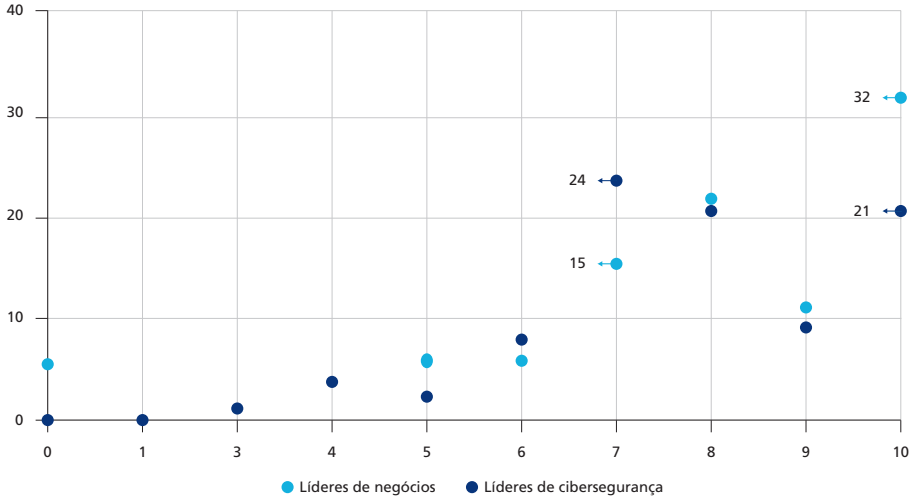


Elaboração do autor.

Os riscos devem ser identificados, analisados e avaliados, para que possam ser tratados em cada contexto específico, com a implantação de controles de segurança da informação. Dessa forma, a gestão de riscos cibernéticos direciona os investimentos em segurança da informação. Como há limites para os investimentos, além dos riscos não identificados, aceitos e residuais, a preparação das organizações para um incidente de segurança é uma das funções essenciais da cibersegurança, com a continuidade de negócios, que trata da resiliência cibernética.

O relatório de cibersegurança do FEM (2023a) indicou que 43% dos líderes de organizações acreditam que serão afetados por ataques cibernéticos nos próximos dois anos, o que tem direcionado os investimentos nos controles de segurança, incluindo a continuidade de negócios. O reflexo é um alinhamento cada vez maior entre a cibersegurança e a alta gestão das organizações, como pode ser visto no gráfico 2.

GRÁFICO 2
Integração dos riscos cibernéticos na estratégia corporativa
(Em %)

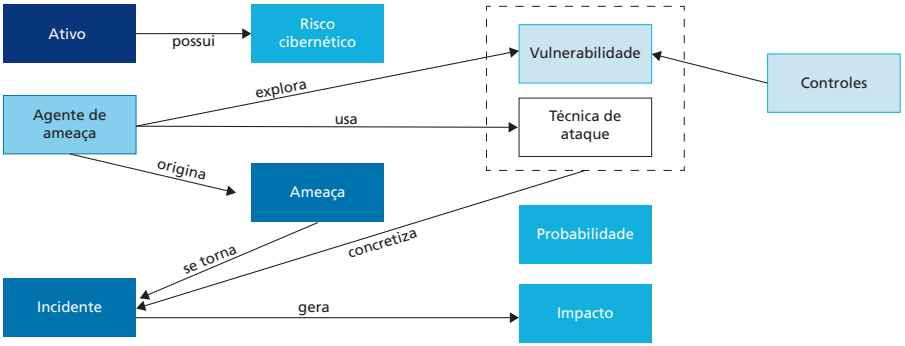


Fonte: WEF (2023a).
Elaboração do autor.

Um incidente de segurança é decorrente de um risco cibernético que se concretiza, ou seja, da efetivação da ameaça com a exploração de vulnerabilidades de um ativo do ambiente por um agente de ameaça, causando impactos para a organização. Os controles de segurança, que podem ser tecnológicos, processuais ou físicos, devem ser implantados para que as vulnerabilidades sejam eliminadas. A figura 3 apresenta os elementos dos riscos cibernéticos que devem ser gerenciados com identificação, análise, avaliação, tratamento, comunicação e

monitoramento. Um risco cibernético é o produto da probabilidade e do impacto potencial causado por um incidente de segurança.

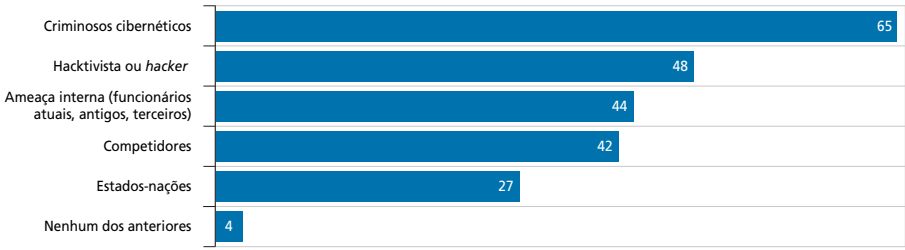
FIGURA 3
Elementos do risco cibernético



Elaboração do autor.

O gráfico 3 apresenta os principais agentes de ameaça considerados para 2023, segundo uma pesquisa realizada globalmente. De acordo com o estudo, 65% dos respondentes estão preocupados com criminosos cibernéticos, com outras preocupações com *hackers*, agentes internos, como funcionários e terceiros, competidores e países.

GRÁFICO 3
Principais agentes de ameaça considerados para 2023
(Em %)



Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.

Os riscos cibernéticos são dinâmicos e evoluem sintonizados com os avanços no mundo, tais como o trabalho remoto, a adoção acelerada da nuvem computacional, o aumento do volume de dados, a convergência entre as tecnologias da informação e operacional, o lançamento de novos produtos e serviços, o aumento do uso de internet das coisas (*internet of things* – IoT), o aumento da digitalização de mecanismos de entregas e de cadeia de suprimentos, o aumento da

digitalização das operações de *back-office* e a entrada em novos mercados. O gráfico 4 mostra que menos que 3% das organizações tratam os riscos em sua completude, em todas as iniciativas. De uma forma geral, menos de 40% tratam totalmente os riscos cibernéticos de cada contexto individual, segundo a pesquisa.

GRÁFICO 4
Riscos cibernéticos associados a diferentes contextos e o nível de tratamento
(Em %)

Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.
Obs.: NA – não se aplica.

O fator humano deve ser considerado cada vez mais no universo digital, uma vez que as pessoas são os principais atores em qualquer contexto e representam ativos que podem ser explorados, com fraquezas ou vulnerabilidades, como ganância, desconhecimento, inocência e distração ou outras características e situações. Os ativos humanos, incluindo usuários, alta gestão, desenvolvedores, administradores, clientes ou parceiros, são cada vez mais utilizados como ponto inicial de ataques cibernéticos, permitindo o acesso e possibilitando as movimentações que levam a impactos relacionados à indisponibilidade, à perda de confidencialidade ou à perda de integridade.

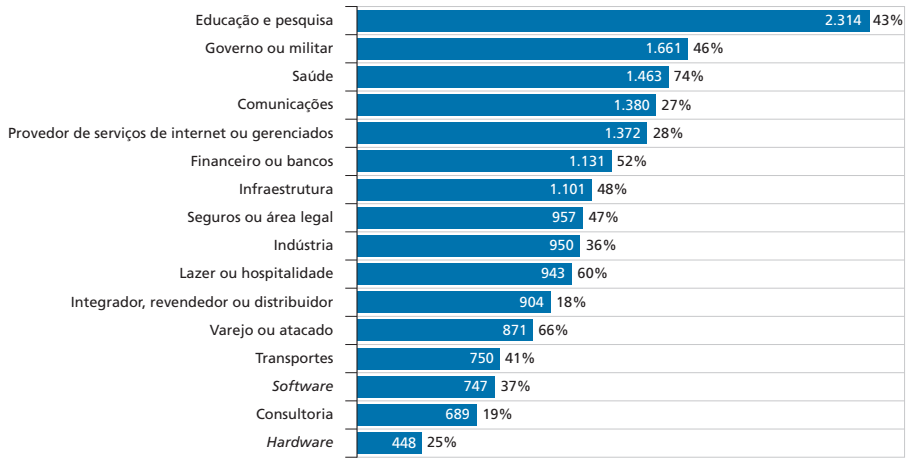
2.2 Incidentes de segurança crescendo em todo o mundo

Os ataques cibernéticos vêm crescendo no Brasil e no mundo, grande parte como reflexo da evolução da conectividade, das integrações e da digitalização, que aumentam naturalmente a superfície de ataques e a complexidade para a segurança cibernética. A criticidade pode ser vista na IoT (melhor abordada nas subseções 3.1 e 3.2) e nas infraestruturas críticas (subseção 3.4), que, com as cidades inteligentes, a Indústria 4.0 e setores como o elétrico e a saúde, podem sofrer impactos cada vez maiores devido à interdependência. Com esta, um incidente em uma parte da cadeia pode ser suficiente para afetar o todo. Exemplo disso é um ataque a um sistema do ambiente operacional de uma distribuidora

elétrica decorrente do acesso indevido com o uso de credenciais de um funcionário vítima de um ataque. Esse ataque inicial resulta na instalação de um código malicioso, que tem como consequência a interrupção ou picos de energia que acabam afetando outros setores, como a indústria, o financeiro ou a saúde.

Ataques cibernéticos à indústria que afetam a produção têm ocorrido com mais frequência (Arctic Wolf, 2023), especialmente no setor de energia (IEF, 2022). Em um contexto militar, os incidentes cibernéticos também são utilizados e demonstram, cada vez mais, a importância da segurança da área, conhecida como defesa cibernética nesse contexto. O gráfico 5 apresenta os setores mais atacados em 2022. Os destaques estão, nos últimos anos, nos âmbitos da educação e do governo, que têm sofrido a maior quantidade de ataques semanais. Uma série de aspectos devem ser considerados para esses destaques, como o aumento da superfície de ataques, decorrente, por exemplo, da necessidade de maior distribuição das plataformas de ensino, dos próprios alunos e dos dados de pesquisa no setor da educação. Outro aspecto é o nível de investimentos em cibersegurança de cada setor, que possui momentos diferentes e reforça a importância de uma articulação setorial para as ações de cibersegurança. Além disso, os agentes de ameaça atuam naquele alvo em que as condições de sucesso e recompensa dos ataques são maiores, o que indica uma necessidade de análise mais profunda nos setores de saúde, lazer e varejo, que tiveram os maiores índices percentuais de aumento de ataques semanais.

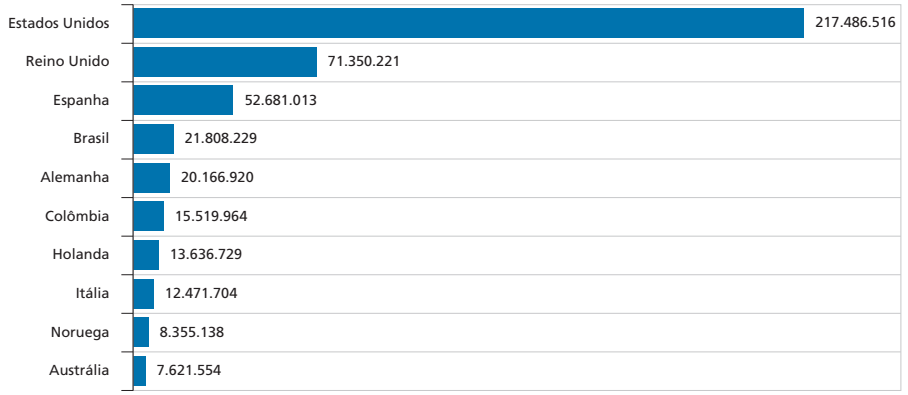
GRÁFICO 5
Setores mais atacados em 2022



Fonte: Check Point, 2023. Disponível em: https://go.checkpoint.com/2023-cyber-security-report/.
Elaboração do autor.

O Brasil possui uma posição de destaque entre os países que mais sofrem ataques cibernéticos. Em 2022, o Brasil continuou entre os países com maior volume de ataques de *ransomware*, como mostra o gráfico 6 (Sonicwall, 2023). Nesse tipo de incidente de segurança, há o sequestro de dados sensíveis com o uso de criptografia, paralisando as vítimas que não possuem *backups* e que não pagam o resgate para o acesso aos dados cifrados. Nos ataques mais recentes de *ransomware*, há pedidos de resgate também para evitar o vazamento dos dados, tornando os incidentes ainda mais custosos.

GRÁFICO 6
Países com maior quantidade de ataques cibernéticos (*ransomware*)



Fonte: Sonicwall (2023).
Elaboração do autor.

Os crimes cibernéticos impactam os negócios e trazem à tona discussões sobre regulamentações e mecanismos para minimizar os prejuízos das vítimas, incluindo os aspectos financeiros envolvidos com pagamento de resgates. Há muito ainda a evoluir nesse aspecto, mas um ponto de consenso é a importância de se tratar o fator humano, que tem sido explorado nos ataques de *ransomware*, principalmente para a instalação do código malicioso.

O gráfico 7 mostra os principais vetores de ataques que resultam em vazamentos de dados, com destaque para o roubo de credenciais de acesso e o *phishing*. Erros e mau uso de recursos e sistemas também podem resultar em vazamento de dados, mas não foram considerados nessa ilustração. Os erros representam 13% dos vazamentos, por exemplo, uma configuração errada do armazenamento em nuvem. As pessoas estão sendo mais exploradas em ataques cibernéticos do que as vulnerabilidades de sistemas e uso de *botnets*, com cerca de 82% dos incidentes de vazamento relacionados ao fator humano (Verizon, 2022).

GRÁFICO 7
Principais vetores de ataques cibernéticos[1]
(Em %)

Fonte: Verizon (2022).
Elaboração do autor.
Nota: [1] Valores aproximados.

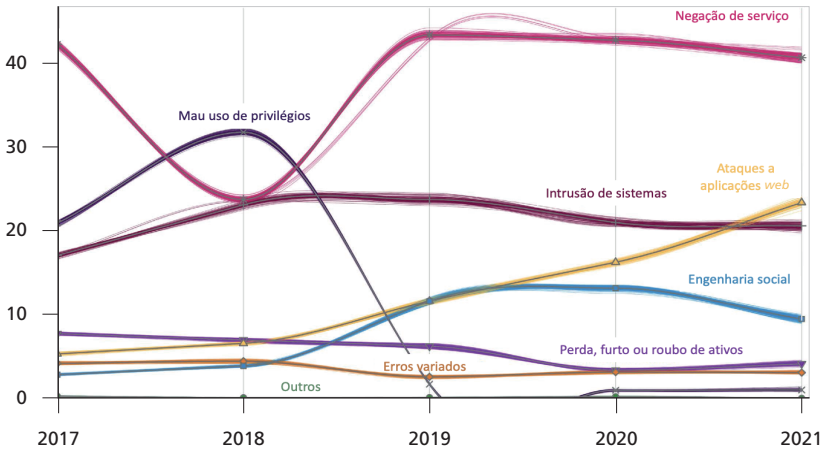
Os atacantes buscam otimizar os ataques cibernéticos, visando os ativos mais expostos e vulneráveis. Com isso, as pessoas parecem ser um dos alvos preferidos, mais até mesmo do que os sistemas vulneráveis. Mesmo os ataques direcionados, realizados por campanhas, visam as pessoas, que podem iniciar os ataques com a instalação de códigos maliciosos em sistemas internos. Um exemplo é o Stuxnet, que afetou usinas nucleares do Irã por meio de código malicioso instalado a partir de dispositivos de armazenamento que foram levados para dentro da usina por seus próprios funcionários (Fruhlinger, 2022).

Nesse contexto de otimização de ataques cibernéticos, os vazamentos de dados possuem grande relevância, já que aumentam a assertividade dos ataques direcionados, com o uso de dados pessoais para aumentar a verossimilidade de mensagens contendo conteúdo maliciosos, por exemplo. Esses casos reforçam a importância de leis como a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018a), que visam evitar vazamentos de dados que podem e estão sendo utilizados em outros ataques cibernéticos e outros tipos de fraudes.

2.3 Principais ataques cibernéticos

Os ataques cibernéticos podem ocorrer em diferentes camadas, das redes às aplicações, passando pelas infraestruturas e pelas pessoas. O gráfico 8 mostra os principais ataques realizados em 2022 (Verizon, 2022), com destaque para os incidentes relacionados aos ataques de negação de serviço (DDoS), que resultam em indisponibilidade dos serviços. Os ataques em aplicações *web* tiveram crescimento em 2022, ultrapassando as intrusões em sistemas, muito devido à própria evolução da internet como uma das principais plataformas para a realização de negócios, o que atrai naturalmente o interesse de criminosos. Muitos desses ataques exploram vulnerabilidades técnicas com o emprego de diferentes táticas, incluindo o uso de vulnerabilidades humanas, por exemplo, para a obtenção de credenciais. Entre os vetores de ataques, dois estão ligados diretamente às pessoas, que são a engenharia social e os erros. Há também os ataques que visam ao ativo físico, como os casos de perda, furto ou roubo.

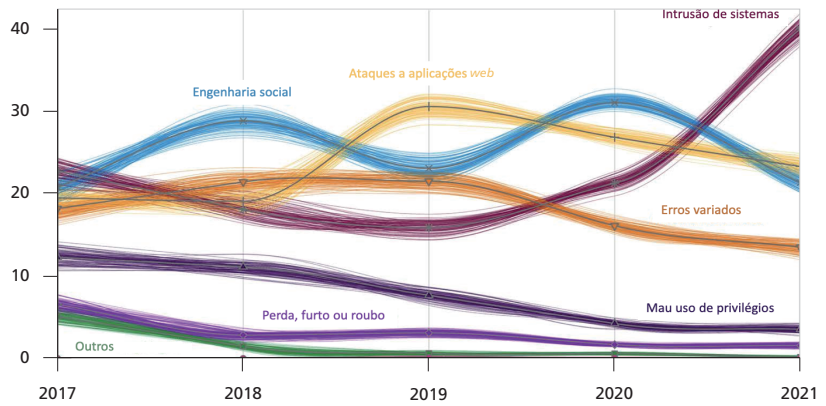
GRÁFICO 8
Principais vetores de ataques cibernéticos



Fonte: Verizon (2022).
Elaboração do autor.

O gráfico 9 apresenta as principais ameaças relacionadas ao vazamento de dados (Verizon, 2022), com destaque para a intrusão de sistemas. Deve-se considerar que as intrusões são realizadas para a instalação de códigos maliciosos que enviam dados para os criminosos a partir de diferentes vetores, incluindo o uso de credenciais de acesso obtidas ilicitamente, o *phishing* e os *ransomware*s. Esses vetores envolvem o fator humano, bem como as ameaças de engenharia social e os erros variados, que permitem aos criminosos o acesso a dados de forma indevida.

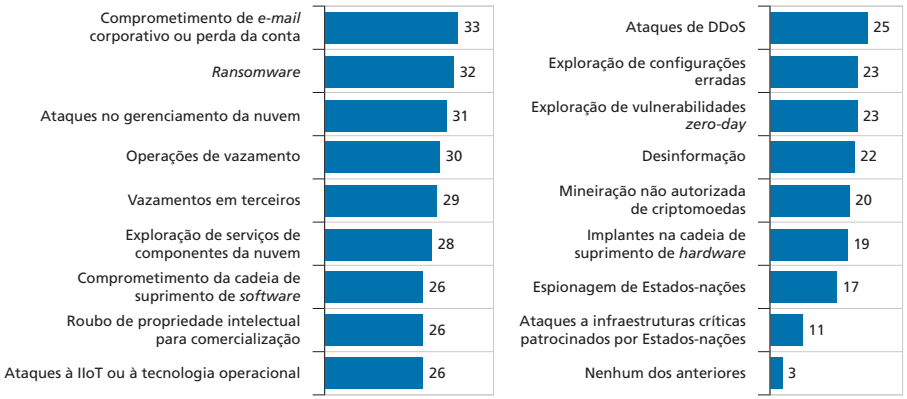
GRÁFICO 9
Principais ameaças relacionadas ao vazamento de dados



Fonte: Verizon (2023).
Elaboração do autor.

Uma dimensão da complexidade da cibersegurança pode ser vista nas preocupações para 2023 sobre as ameaças e eventos cibernéticos, no gráfico 10. Há um receio quanto às informações internas e ao roubo de credenciais de acesso, além da manipulação de informações e de ataques mais sofisticados relacionados ao uso de nuvem computacional, cadeia de suprimentos e internet industrial das coisas (*industrial internet of things* – IIoT).

GRÁFICO 10
Principais ameaças em 2023
(Em %)



Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.

O gráfico 10 mostra a amplitude de alvos e objetivos e a complexidade de ataques. Além disso, reflete o papel da cibersegurança no universo digital, ao envolver elementos como as pessoas, a cadeia de suprimentos, a nuvem computacional, as infraestruturas críticas, a desinformação, a propriedade intelectual e o furto de poder computacional, e engloba indivíduos, organizações de diferentes naturezas e tamanhos, além de países.

3 DIMENSÕES DA SEGURANÇA CIBERNÉTICA

A cibersegurança está se tornando cada vez mais complexa porque diferentes dimensões devem ser consideradas. Além dos diferentes vetores de ataques, com variados agentes de ameaças visando o ativo mais vulnerável, as ameaças envolvem a confidencialidade, a integridade e a disponibilidade, resultando em impactos diversos, que podem escalar e alcançar grandes proporções. Há escopos, focos, camadas e funções diferentes na cibersegurança.

3.1 Escopos da cibersegurança

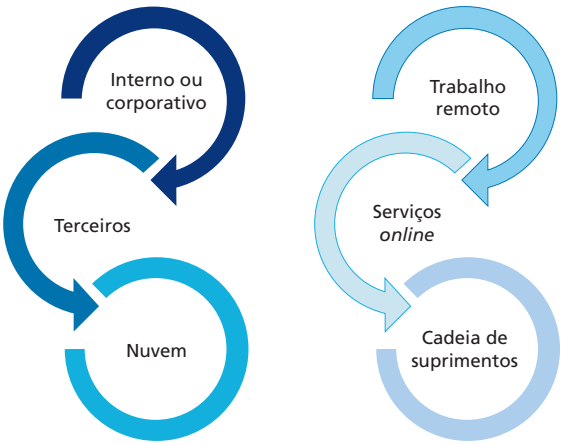
No universo digital, todos estão suscetíveis aos ataques cibernéticos. Um indivíduo, um cidadão aleatório de um país ou um colaborador de uma organização que possuem a sua identidade digital são alvos importantes, que devem ser considerados. A relevância das pessoas na cibersegurança é grande porque elas são, muitas vezes, utilizadas como entrada ou parte do fluxo de ataques cibernéticos em empresas, instituições ou organizações de diferentes tamanhos e setores.

Além das pessoas, há o parque tecnológico, que inclui sistemas, equipamentos ou plataformas que são alvos constantes de ataques cibernéticos. Adicionalmente, há os ativos físicos, que também representam riscos cibernéticos. O escopo da cibersegurança em uma empresa normalmente consiste em sua rede interna ou corporativa. Mas o provisionamento de serviços para clientes ou mesmo para os usuários internos já expande o escopo e, principalmente, a superfície de ataques.

Com o trabalho remoto, a cadeia de suprimentos e o uso intensivo de nuvem computacional, o ambiente se torna cada vez mais distribuído e heterogêneo, influenciando no escopo a ser trabalhado. Nesse ambiente, um incidente pode ocorrer na casa de um colaborador e se espalhar pela empresa, da mesma forma que a vulnerabilidade de uma aplicação no provedor de nuvem pode ser explorada em um ataque e os dados de todos os clientes, por exemplo, podem ser expostos. As possibilidades de ataques, que tiram proveito de uma superfície maior, aumentam e exigem uma estratégia de cibersegurança mais abrangente e complexa.

A figura 4 sintetiza os diferentes escopos que devem ser considerados em cibersegurança, sob o ponto de vista do contexto para a gestão dos riscos cibernéticos.

FIGURA 4
Escopos da cibersegurança

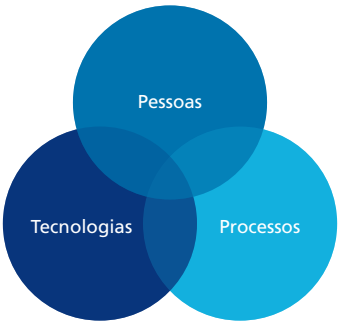


Elaboração do autor.

3.2 Focos da cibersegurança

Uma estratégia efetiva de cibersegurança deve considerar, além dos diferentes escopos, que são particulares para cada organização, os focos, que estão nas pessoas, nos processos e nas tecnologias (figura 5). Esses focos aparecem em diferentes elementos do risco cibernético, principalmente nos ativos e nos controles de segurança.

FIGURA 5
Focos da cibersegurança



Elaboração do autor.

Os ativos são os elementos que podem ter vulnerabilidades. Há aqueles físicos, mas também as pessoas, os processos e as tecnologias, que podem ser explorados em ataques cibernéticos. Não é suficiente tratar somente o foco tecnológico em cibersegurança, porque muitos ataques exploram o fator humano. Além disso, processos podem conter falhas ou vulnerabilidades em aspectos relacionados com as responsabilidades, atividades e pontos de controle. Os processos também envolvem diferentes áreas das organizações e todos os seus relacionamentos e interações que fazem parte dos negócios, incluindo entidades externas e a cadeia de suprimentos. Como a informação flui o tempo todo, os processos considerando a cibersegurança são imprescindíveis no universo digital.

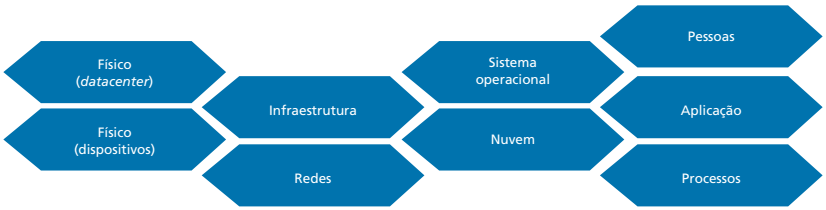
Os controles de segurança, que podem ser físicos, tecnológicos, humanos ou organizacionais, segundo a norma ABNT NBR ISO/IEC 27002 (ABNT, 2022b), devem ser assim definidos, de acordo com os riscos cibernéticos, para tratar dos diferentes focos.

3.3 Camadas da cibersegurança

A cibersegurança é complexa também devido às suas camadas, que devem ser tratadas e estão sempre em mudança. Agentes de ameaça podem explorar vulnerabilidades nas pessoas, nos processos e nas tecnologias. Da mesma maneira, há os elementos físicos, como as informações em papel ou em *hardware*, que podem ter a confidencialidade comprometida. E, na tecnologia, há as camadas de *software*,

como o sistema operacional, a infraestrutura, como virtualização, os serviços e as aplicações *web* ou móvel. Além disso, há a camada de redes ou de nuvem, que também representam riscos cibernéticos. Sendo assim, como um ataque a uma dessas camadas pode resultar em um incidente cibernético, elas devem ser tratadas de forma ampla e integrada. A figura 6 apresenta algumas camadas da cibersegurança que devem ser consideradas.

FIGURA 6
Camadas da cibersegurança

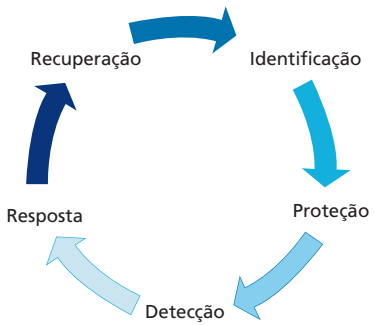


Elaboração do autor.

3.4 Funções da cibersegurança

As funções da cibersegurança envolvem as capacidades de identificação, proteção, detecção, resposta e recuperação, segundo o Nist Cybersecurity Framework, como pode ser visto na figura 7. Essas funções reforçam a visão de que as gestões de riscos cibernéticos, de segurança da informação e de continuidade de negócios devem ser trabalhadas de forma integrada. As capacidades de segurança estão aumentando a integração, o que tem solidificado o entendimento da complexidade da cibersegurança e a visão de que todos têm que procurar evitar incidentes, mas devem estar preparados para o caso de uma ocorrência, em uma perspectiva holística que consolida a resiliência cibernética.

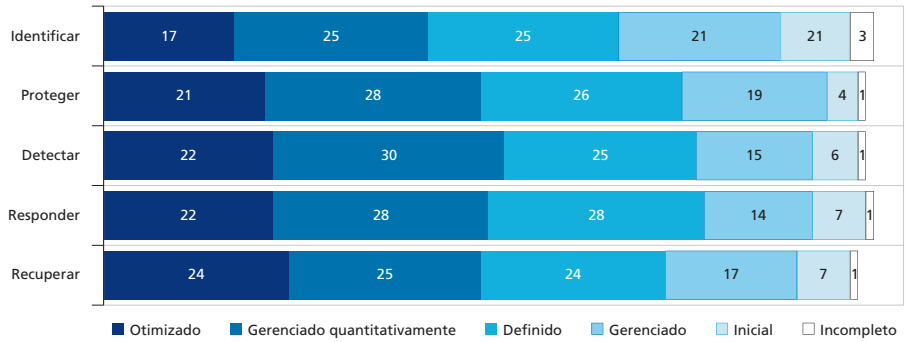
FIGURA 7
Funções ou capacidades da cibersegurança



Fonte: Nist, 2023. Disponível em: https://www.nist.gov/cyberframework.
Elaboração do autor.

Atualmente, poucas organizações atingiram um nível otimizado em todas as capacidades de cibersegurança. Apenas 3% dos que participaram da pesquisa realizada pela PwC estão com as funções de identificação, proteção, detecção, resposta e recuperação em nível otimizado, como pode ser visto no gráfico 11. A maioria está no nível gerenciado quantitativamente, muitas em nível definido, e uma quantidade menor no nível gerenciado. A minoria está em nível inicial ou incompleto, indicando que as ações em cibersegurança estão em andamento, mas com avanços necessários para elevar o nível de maturidade.

GRÁFICO 11
Nível de maturidade nas funções de cibersegurança
(Em %)



Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.

4 DINAMISMO E EVOLUÇÃO DA CIBERSEGURANÇA

Além das dimensões da cibersegurança, há o dinamismo da própria evolução do mundo em que vivemos, seja no aspecto tecnológico, seja no da própria sociedade. As influências na velocidade dessa evolução são extremamente relevantes para a cibersegurança, porque um ataque emergente pode exigir que se tornem indisponíveis as operações ou o funcionamento da vítima, para que os controles de segurança adequados possam ser implantados e até mesmo desenvolvidos. Esse assincronismo entre os ataques e as proteções é decorrente de avanços tecnológicos, como a computação quântica e o uso intensivo de inteligência artificial, que alteram a dinâmica tradicional, sendo potencializado pelo uso de dados pessoais obtidos por vazamentos decorrentes de outros ataques.

4.1 Novas tecnologias, novos riscos

As novas tecnologias, como novos protocolos, serviços ou plataformas, de diferentes setores, são os pilares do universo digital, as quais viabilizam e criam

ondas de desenvolvimento econômico. Desde o surgimento dos computadores, passando pela internet, por *blockchain* e outras aplicações, os avanços têm possibilitado a fusão entre o físico e o digital (fidigital), o que reflete cada vez mais nos aspectos humanos. Os riscos cibernéticos vêm junto, potencializando os impactos na medida em que as interdependências aumentam.

O FEM cita avanços em inteligência artificial, computação quântica e biotecnologia, entre outras, como elementos que trazem novos riscos, relacionados à desinformação, ao enfraquecimento da soberania individual e do direito à privacidade, além de ataques às infraestruturas de agricultura, água, sistemas financeiros, segurança pública, transporte, energia e comunicações domésticas (FEM, 2023b).

Uma medida da dimensão do dinamismo dos novos riscos cibernéticos pode ser vista pelo breve histórico de códigos maliciosos, como vírus, *worms* e outros, com as principais características que mostraram a evolução, a seguir descritos.

1) 1971: Creeper, que não era malicioso.
2) 1974: Wabbit (Rabbit), que era malicioso e replicante.
3) 1975: Animal/Prevade, que era um cavalo de Troia, um código malicioso que aparentava ser legítimo.
4) 1986: Brain, que era um código malicioso de *boot*, em disquetes de 5.2 polegadas.
5) 1989: AIDS Trojan ou PC Cyborg, que pode ser considerado o primeiro *ransomware*. Foram 20 mil disquetes distribuídos na Conferência da Organização Mundial da Saúde, com a exigência de um resgate de US$ 189,00 para o Panamá, após noventa *boot*s. Escondia diretórios e cifrava nomes de arquivos no *drive* C.
6) 2000: LoveLetter/ILOVEYOU, que aplicou a engenharia social para a instalação de código malicioso.
7) 2001: Code Red, *worm* em memória que se espalhou rapidamente em todo o mundo conectado.
8) 2013: CryptoLocker, *ransomware* em anexo de *e-mails* que afetou cerca de 500 mil computadores e disponibilizava a chave de recuperação em um portal.
9) 2014: Heartbleed, código malicioso que explorava a implementação de um protocolo de segurança *web*, o OpenSSL.

10) 2014: Shade/Troldesh, *ransomware* que explorava o *phishing* como vetor de ataque e estabelecia uma comunicação direta com as vítimas, com possibilidade de negociações. Foi desativado em 2020, com o criador liberando 750 mil chaves em sinal de arrependimento.

11) 2016: Jigsaw, *ransomware* que apagava arquivos originais e substituía a extensão por .fun, .kkk, .gws e .btc. Utilizava um *cookie* como *timer* para os pagamentos.

12) 2016: Locky, *ransomware* que explorava o *phishing* e tinha como alvos profissionais de *software*, como arquitetos, desenvolvedores, engenheiros e testadores.

13) 2016-2017: Petya/GondenEye, *ransomware* que utilizava um *link* infectado do Dropbox e, uma vez instalado, aplicava criptografia no Master File Table (MFT) da vítima, o que a deixava sem acesso ao disco.

14) 2016: Mirai/DYN Attack, ataque DDoS a partir de dispositivos IoT, que paralisou a internet.

15) 2017: Bad Rabbit, *ransomware* que era instalado a partir de *websites* comprometidos (*malware dropper*).

16) 2017: WannaCry, *ransomware* que explorava vulnerabilidades do Windows e comprometeu cerca de 230 mil computadores, causando cerca de US$ 4 bilhões em prejuízos.

17) 2018: GandCrab, *ransomware* que ameaçava divulgar os hábitos de pornografia das vítimas. Um dos primeiros códigos maliciosos a partir do Ransomware as a Service (RaaS), em um modelo de atuação distribuído no qual o lucro está na criação dos códigos, que são usados para os ataques pelos clientes. Agências governamentais implementaram e disponibilizaram uma ferramenta de decifragem que devolvia o acesso aos dados cifrados e sequestrados.

18) 2018: Ryuk, *ransomware* que desabilitava a função de recuperação do Windows, atacando também os discos de rede.

19) 2019: Maze, *ransomware* que realizava a dupla extorsão, ou seja, além de cifrar os dados, promovia o seu vazamento, com ameaças de divulgação pública.

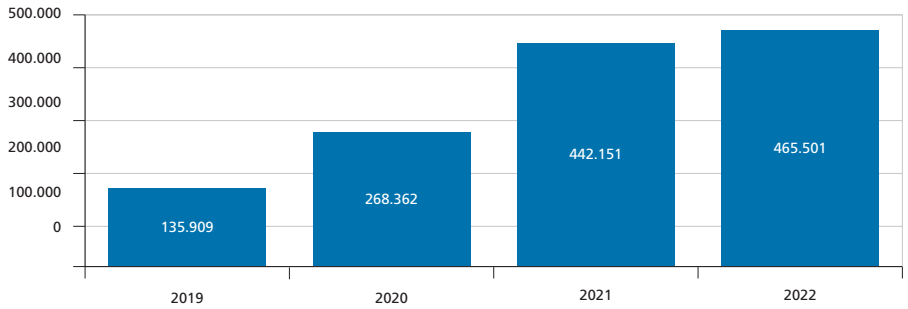
20) 2019: REvil/Sodinokibi, *ransomware* que afetou a cadeia de suprimentos a partir da contaminação de um *software* utilizado por outras empresas.

21) 2020: DarkSide, *ramsomware* direcionado a componentes da infraestrutura crítica.

Os ataques de *ransomware* continuam evoluindo, se tornando mais sofisticados e agregando outras técnicas de ataques para dificultar a sua detecção. O relatório *Global Threat Landscape Report* (FortiGuard Labs, 2023) apresenta algumas das técnicas mais adotadas. Adicionalmente, os atacantes têm utilizado a inteligência artificial para automação e efetividade das campanhas de ataques. Além disso, as extorsões cibernéticas, que começaram com pedidos de resgate para o acesso aos dados cifrados, passaram pelo resgate para não publicar dados vazados, em uma dupla extorsão. Recentemente, técnicas de DDoS também passaram a fazer parte dos ataques, paralisando mais criticamente as vítimas, em uma tripla extorsão. Uma quarta extorsão, com casos em que os criminosos entram em contato com clientes e parceiros das vítimas, também tem sido observada.

Adicionalmente, a integração entre grupos criminosos e tecnologias tende a possibilitar a evolução do grau de sofisticação dos ataques. O gráfico 12 mostra, por exemplo, o crescimento do número de códigos maliciosos (Sonicwall, 2023).

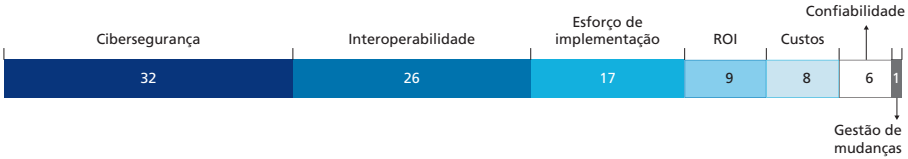
GRÁFICO 12
Crescimento da identificação de novos códigos maliciosos



Fonte: Sonicwall (2023).
Elaboração do autor.

Novas tecnologias trazem consigo novos riscos, incluindo os cibernéticos. Além disso, as integrações também incorporam complexidade, resultando em novas vulnerabilidades. A integração tecnológica com o universo físico, representada pela IoT ou a internet de tudo (*internet of everything* – IoE), mostra o potencial tecnológico e os riscos cibernéticos associados, que têm feito com que a segurança cibernética seja cada vez mais central no desenvolvimento de novos serviços, aplicações ou sistemas. Isso justifica o aumento contínuo dos investimentos na área. Uma pesquisa mostra (figura 8), de fato, que a cibersegurança é considerada o maior obstáculo para a adoção da IoT, maior do que a interoperabilidade, que esforços de implementação, retorno sobre o investimento (ROI), custos, confiabilidade e gestão de mudanças (Caso *et al.*, 2023).

FIGURA 8
Os maiores impeditivos para a adoção da IoT



Fonte: Caso ***et al***. (2023).
Elaboração do autor.

O universo digital também traz implicações diretas na Indústria 4.0, na saúde digital, no governo digital e nas infraestruturas críticas. Nesses contextos, os impactos ultrapassam o mundo digital, chegando diretamente ao mundo físico, com paralisações de serviços essenciais e operações de fábricas, chegando às vidas humanas. As pessoas passam a ter riscos relacionados à vida a partir de ataques cibernéticos, decorrentes tanto da digitalização do setor de saúde quanto do uso de dispositivos de saúde conectados.

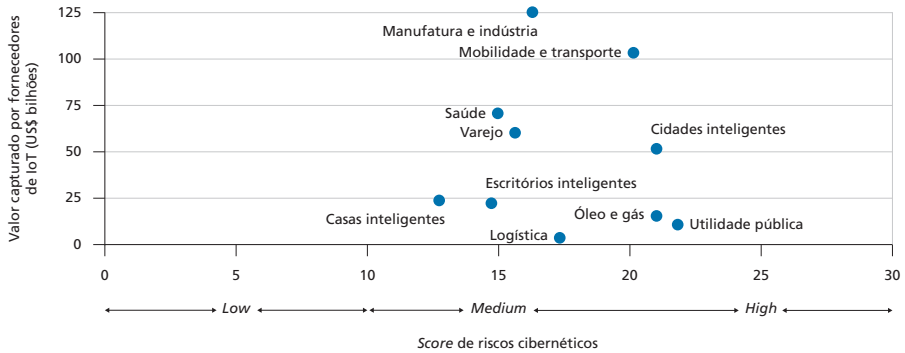
Outro escopo está nos países, com elementos cibernéticos sendo utilizados cada vez mais em conflitos e guerras como arma e no meio militar, com muitos dos países possuindo exércitos cibernéticos.

4.2 Segurança na Indústria 4.0

Os impactos relacionados aos incidentes cibernéticos fazem parte também das preocupações na Indústria 4.0. Um dos desafios relacionados à IoT eram as atualizações dos dispositivos para correções de vulnerabilidades, que poderiam tornar inviável o futuro de um produto. Na Indústria 4.0, as implicações ultrapassam fronteiras, já que os processos de produção estão distribuídos. Modelos, dados de personalização, composições de produtos e propriedade intelectual são transmitidos entre os componentes, e as fábricas passam a depender de tecnologias da informação e de comunicação, que precisam ser seguras.

A importância da cibersegurança na IoT, em diferentes casos de uso, se reflete nos valores capturados por fornecedores. O gráfico 13 apresenta uma projeção da relação entre os valores de cada caso de uso de IoT e os riscos cibernéticos esperados para 2030. A cibersegurança oferece um potencial maior de valor para setores com riscos cibernéticos mais altos. A Indústria 4.0 possui um valor maior do que outros casos de uso de IoT, com um índice de risco cibernético médio, enquanto os setores de utilidades públicas e de infraestrutura crítica de óleo e gás possuem risco cibernético alto, com valor menor para os fornecedores de IoT (Caso *et al.*, 2023).

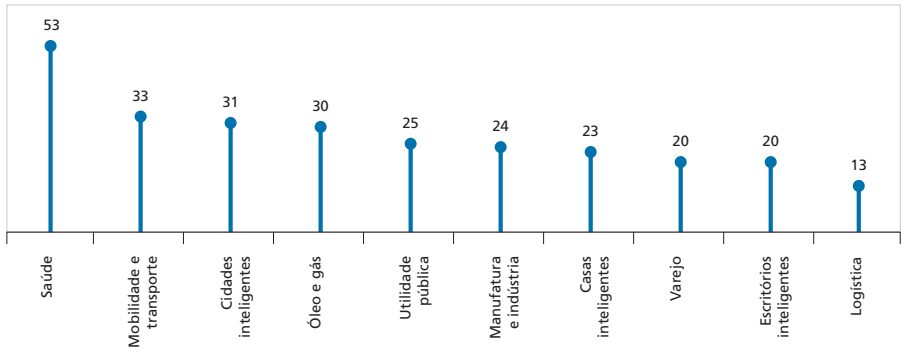
GRÁFICO 13
Valores e os riscos de cibersegurança em 2023 para IoT



Fonte: Caso *et al*. (2023).
Elaboração do autor.

Entender e gerenciar os riscos cibernéticos é fundamental, pois isso potencializa a adoção de IoT em diferentes casos de uso. O percentual de aumento de gastos em caso de maior segurança pode ser visto no gráfico 14, com o setor de manufatura e indústria tendo um aumento de gastos de 24%, enquanto a saúde possui um aumento de 53% (Caso *et al*., 2023).

GRÁFICO 14
Aumento em gastos com IoT em cada caso de uso devido à cibersegurança
(Em %)

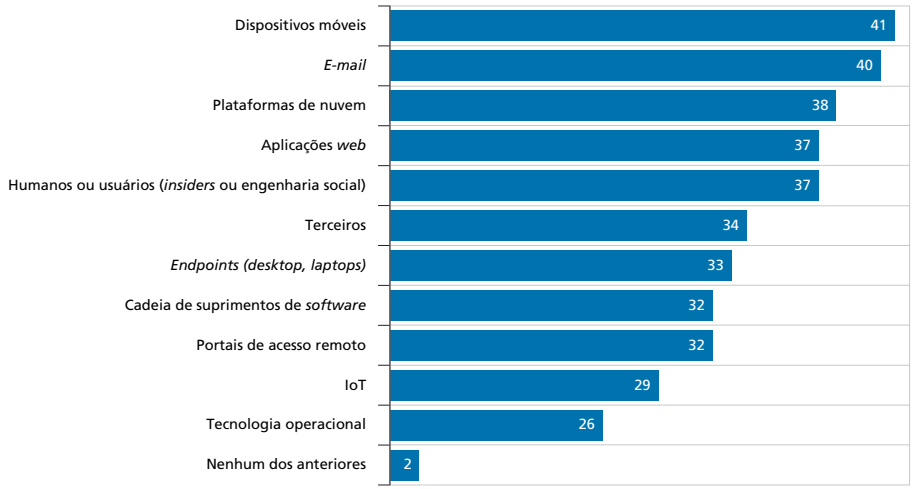


Fonte: Caso *et al*. (2023).
Elaboração do autor.

A necessidade de gerenciamento de riscos cibernéticos é reforçada pelos vetores de ataques, que incluem também a tecnologia operacional e IoT. Para 2023, 29% das organizações que participaram da pesquisa do PwC possuem expectativa de aumento dos ataques à IoT, enquanto 26% esperam ataques à tecnologia operacional (gráfico 15). A principal razão são as vulnerabilidades em sistemas

legados da indústria, potencializados pela cadeia de suprimentos e uso de IoT, que representam uma superfície de ataques maior. Há um destaque também para os dispositivos móveis, citado como o principal vetor de ataque, com 41% das organizações tendo essa preocupação para 2023. Além disso, o vetor humano é citado por 37% das organizações.

GRÁFICO 15
Expectativa de ataques em 2023 pelas organizações
(Em %)

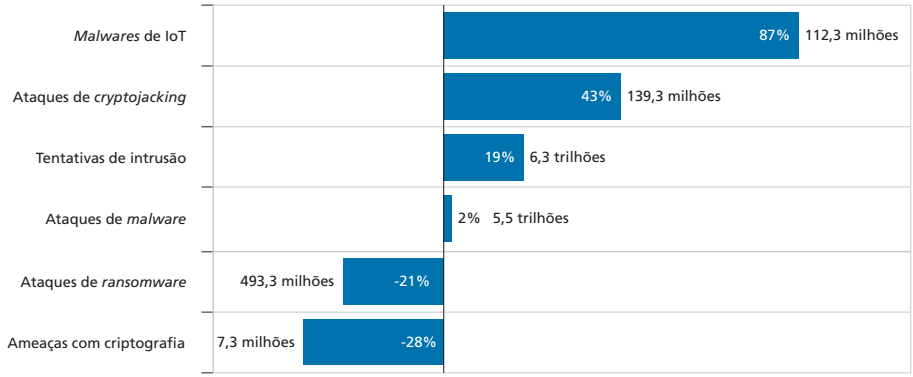


Fonte: PwC, 2023. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html.
Elaboração do autor.

Os esforços das organizações com relação à IoT e à tecnologia operacional estão relacionados a um conjunto de necessidades nas funções de segurança cibernética. Há a limitação da cibersegurança na cadeia de suprimentos, na capacidade de detecção e de resposta nesses ambientes, na falta de especialistas, na insuficiência de documentação e na ineficiência de recuperação do ambiente operacional após um incidente de segurança.

Essas limitações devem ser tratadas com urgência, pois o aumento do volume de *malware*s para IoT foi o mais significativo em 2022, se comparado com outras ameaças cibernéticas, incluindo os ataques de *ransomware*, de *malware*s, de *cryptojacking* e tentativas de intrusões. Os *malware*s de IoT tiveram um crescimento de 87% em 2022 se comparado com o ano anterior, com 112,3 milhões de incidências. As tentativas de intrusão também continuaram crescendo em 2022 (19%), como pode ser visto no gráfico 16 (Sonicwall, 2023).

GRÁFICO 16
Panorama das ameaças cibernéticas em 2022



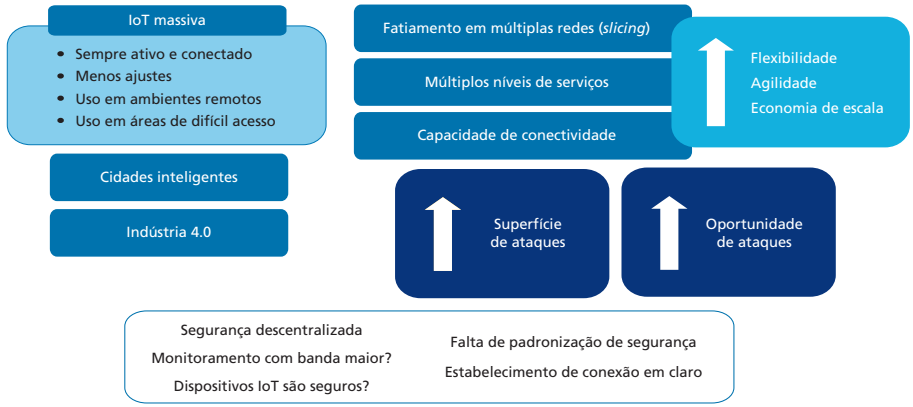
Fonte: Sonicwall (2023).
Elaboração do autor.

4.3 Segurança em 5G

Mesmo com as redes de comunicação tendo sido consolidadas no aspecto de segurança cibernética, principalmente com a proteção de perímetros, os avanços tecnológicos continuam acontecendo, trazendo consigo novas implicações de segurança. Se tradicionalmente os principais riscos nas redes estão relacionados à DDoS e ao acesso indevido aos dados em transmissão, novas tecnologias, como a 5G, incorporam novos desafios. As integrações e as migrações que exigem uma coexistência tecnológica entre gerações diferentes já trazem complexidades que criam condições para novas vulnerabilidades. Além disso, as características da 5G, como a conectividade permanente, maior responsividade, maior confiabilidade de conexão, IoT com maior número de dispositivos, menor consumo de energia e maior largura de banda, representam uma superfície de ataque mais extensa que pode ser explorada, principalmente como meio para um ataque maior e direcionado.

A IoT massiva e a viabilização de casos de uso, como cidades inteligentes e Indústria 4.0, criam condições para a conectividade em ambientes remotos, em áreas de difícil acesso e com conexão sempre ativa. Criam também uma oportunidade para os ataques cibernéticos, como pode ser visto na figura 9. Os desafios de cibersegurança envolvem o tratamento de aspectos específicos das redes 5G, tais como a descentralização e a distribuição de componentes, uma largura de banda maior, a diversidade de dispositivos IoT, a falta de padronização de segurança e o estabelecimento de conexões em claro, sem uma proteção de confidencialidade. São desafios que exigem uma abordagem de segurança cibernética holística, com estratégia, processos, arquitetura, capacidades e tecnologias de segurança complementares e integradas, que também direcionam os avanços necessários no setor.

FIGURA 9
Características de redes 5G e as implicações de segurança

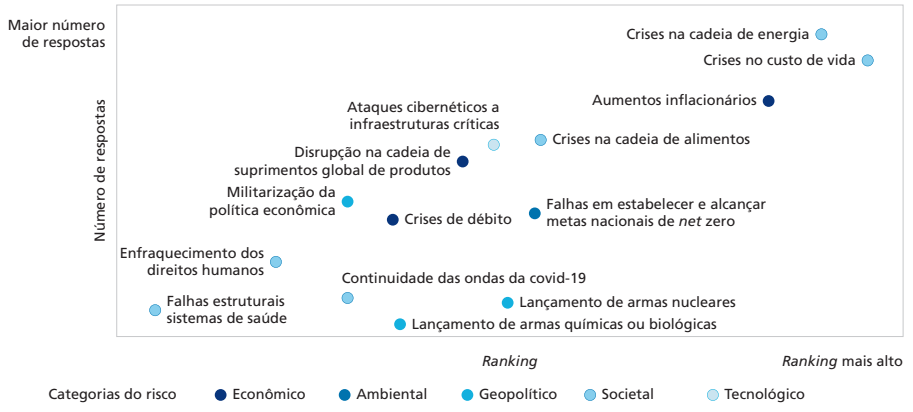


Elaboração do autor.

4.4 Proteção de infraestrutura crítica

A segurança cibernética possui um papel fundamental também no escopo dos países: com os avanços gerados pela digitalização, proporcionou o estabelecimento de uma área particular, a proteção de infraestrutura crítica. Os ataques cibernéticos às infraestruturas críticas são considerados um dos principais riscos globais de 2023, segundo o FEM, como pode ser visto no gráfico 17 (FEM, 2023b), que sintetiza a visão de cerca de 1.200 especialistas, que responderam sobre os cinco principais riscos. Os riscos globais envolvem riscos econômicos, ambientais, geopolíticos, societais e tecnológicos.

GRÁFICO 17
Ataques cibernéticos a infraestruturas críticas são um dos principais riscos globais



Fonte: WEF (2023b).
Elaboração do autor.

No Brasil, a definição de infraestruturas críticas vem do Decreto nº 9.573 (Brasil, 2018b), que estabeleceu a Política Nacional de Segurança de Infraestruturas Críticas, complementada pelo Decreto nº 10.569, que define a Estratégia Nacional de Segurança de Infraestruturas Críticas (Brasil, 2020b). As infraestruturas críticas são instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoca sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade. Além disso, a segurança das infraestruturas críticas é um conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados a essas infraestruturas.

As infraestruturas críticas estão associadas, assim, a setores críticos, sob o ponto de vista dos países, em que incidentes de diferentes naturezas podem resultar em impactos para a população, principalmente devido à interrupção de serviços essenciais. No Brasil, as áreas de águas, energia, transporte, comunicações, finanças, biossegurança e bioproteção e defesa fazem parte das infraestruturas críticas, de acordo com o Decreto nº 11.200 (Brasil, 2022), que estabelece o Plano Nacional de Segurança de Infraestruturas Críticas.

Um dos elementos do plano nacional é a capacidade de resposta a incidentes cibernéticos, com a necessidade de uma estrutura capaz de minimizar os impactos decorrentes de ataques. A Rede Federal de Gestão de Incidentes Cibernéticos, instituída pelo Decreto nº 10.748 (Brasil, 2021), tem a finalidade de aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação.

5 O FATOR HUMANO NA SEGURANÇA CIBERNÉTICA

As pessoas representam, cada vez mais, o elo mais fraco da segurança cibernética. Seja como alvo principal dos ataques que vêm ocorrendo em todo o mundo, em diferentes contextos, seja na incorporação de conceitos de segurança cibernética no desenvolvimento tecnológico, o fator humano possui o foco para se criar um universo digital mais seguro.

5.1 Vulnerabilidades humanas exploradas em ataques cibernéticos

O gráfico 18 mostra o nível de preocupação com os ataques cibernéticos (Sonicwall, 2022), e nele é possível observar que a grande maioria dos ataques possui relação com a exploração de vulnerabilidades humanas. Os ataques envolvem aspectos humanos, que são explorados em *phishing*, *ransomware*, vazamentos de dados e de *e-mails* corporativos, e ataques relacionados à cadeia de suprimentos, à

espionagem interna e a falhas no uso de criptografia de mensagens e informações. Da lista de preocupações, todas envolvem o fator humano.

GRÁFICO 18
Nível de preocupação sobre tipos de ataques cibernéticos
(Em %)

Fonte: Sonicwall (2022).
Elaboração do autor.

O elemento humano sempre teve papel relevante em ataques cibernéticos e continua direcionando os vazamentos de dados. Em 2022, 82% dos vazamentos envolveram o elemento humano, nas credenciais roubadas, em *phishing*, no mau uso de recursos ou em erros (Verizon, 2022). Nesses ataques, são exploradas vulnerabilidades humanas, como a curiosidade ou a empatia, que fazem com que uma mensagem com *phishing* seja aberta, ou a ganância, a desatenção ou a preguiça, que fazem com que as credenciais de acesso caiam na mão de criminosos.

5.2 Conscientização, treinamento e cultura de segurança da informação

A educação, em todos os sentidos, deve incorporar, cada vez mais, os riscos cibernéticos, já que a distância entre a vida digital e a realidade tende a desaparecer. A segurança cibernética, assim, deve ser um dos requisitos para a educação de cada indivíduo, desde cedo. Preservar e cuidar da identidade digital, que representa o próprio indivíduo nas suas atividades cotidianas, é primordial. As fraudes e ataques de *phishing*, que podem levar ao roubo de identidades e à inserção de códigos maliciosos com impactos ainda mais diretos, devem ser tratados com programas de conscientização em segurança da informação e fazer parte da educação de todos. Saber como lidar com as situações no universo digital é fundamental para a formação de cidadãos conscientes e educados sobre a segurança cibernética. Esse é o início do fortalecimento de uma cultura de segurança da informação.

O desenvolvimento tecnológico, de produtos a sistemas e aplicações, também deve ser feito, de uma forma essencial, com uma visão de segurança

cibernética, ou seja, de maneira a não criar condições de serem atacados, com o mínimo de vulnerabilidades. E isso exige cada vez mais uma visão de segurança de profissionais de diferentes áreas, para que o processo de desenvolvimento tecnológico incorpore a segurança, resultando em produtos e serviços mais confiáveis e menos suscetíveis a ataques cibernéticos. O treinamento em segurança da informação, desse modo, é fundamental para todos os profissionais.

Como toda cultura, a de segurança e privacidade também é desafiadora, incluindo elementos como hábitos, conhecimento e habilidades, além das crenças (figura 10). O fortalecimento de culturas passa por ações que reforçam os hábitos e crenças, incrementando ainda o conhecimento e as habilidades constantemente.

FIGURA 10
Elementos da cultura de segurança da informação

Elaboração do autor.

5.3 Complexidade da segurança eleva a necessidade de especialistas

No início da internet, o profissional de segurança precisava se preocupar mais fortemente com os aspectos de redes de computadores, que possibilitavam a conectividade e exigiam arquiteturas seguras com perímetros, zonas desmilitarizadas (*demilitarized zones* – DMZs), redes privadas virtuais (*virtual private networks* – VPNs) e *firewalls*. Os processos eram importantes para manter o ambiente atualizado e livre de vulnerabilidades. Além desse perfil de segurança de redes, havia o perfil para a gestão de identidades e controle de acesso, que tratava dos usuários, nas primeiras versões das identidades digitais.

Com a evolução da internet, o advento de novas plataformas e serviços, os ambientes mais distribuídos com a nuvem computacional e as camadas tecnológicas

com integrações cada vez maiores com diferentes componentes, a segurança cibernética também passou a ser feita por equipes especializadas e multidisciplinares. Atualmente, há diferentes perfis profissionais para a segurança cibernética.

Há perfis técnicos, como o de segurança de redes e o de segurança de TI. Os profissionais que analisam riscos cibernéticos e vulnerabilidades podem ser considerados analistas de segurança ofensiva, realizando ações como testes de penetração em sistemas, plataformas e ambientes. Esses profissionais são também conhecidos como integrantes de Red Team. Os profissionais que trabalham com arquiteturas de segurança e definição e implantação de controles de segurança fazem parte da segurança defensiva ou do Blue Team. Existem, por sua vez, os profissionais de cibersegurança que trabalham especificamente com controle de acesso, enquanto outros trabalham com segurança nas aplicações, ou desenvolvimento seguro. Há ainda os especialistas em criptografia e os analistas de operações de segurança. Todas as capacidades de segurança cibernética, que envolvem identificação, proteção, detecção, resposta e recuperação, podem ter perfis específicos de profissionais. O profissional de resposta a incidentes complementa os demais perfis, tratando diretamente dos ataques cibernéticos que já aconteceram, após a exploração de vulnerabilidades pelos agentes de ameaça.

Como a segurança cibernética é holística, há também os perfis que não são essencialmente tecnológicos, como os de governança, riscos e conformidade, que implementam os sistemas de gestão de riscos, de segurança da informação e de continuidade de negócios. Outro perfil, cada vez mais necessário, é o de profissionais especializados em conscientização de usuários. Processos e políticas de segurança podem igualmente envolver profissionais específicos, bem como para a gestão de projetos de segurança cibernética.

No universo digital, com as integrações em diferentes níveis e com o advento de novas tecnologias, as atividades de cibersegurança se tornaram mais complexas e mais intensas. A questão da velocidade dos avanços tecnológicos, das necessidades de segurança e da capacidade de atendimento a essas necessidades revelou uma assimetria que resulta no crescimento do número de incidentes cibernéticos e fica evidente no âmbito dos recursos humanos especializados.

O International Information System Security Certification Consortium (ISC2) estima que a força de trabalho em segurança cibernética seja de 4,6 milhões no mundo todo, sendo que no Brasil há 687 mil profissionais especializados. O déficit de profissionais é de 3,4 milhões em todo o mundo, sendo de 312 mil no Brasil. Esses números podem ser vistos na figura 11 (ISC2, 2022). Os Estados Unidos são o país com maior número de profissionais de cibersegurança, com mais 1,2 milhão. O déficit nos Estados Unidos é de cerca de 410 mil profissionais. Os países

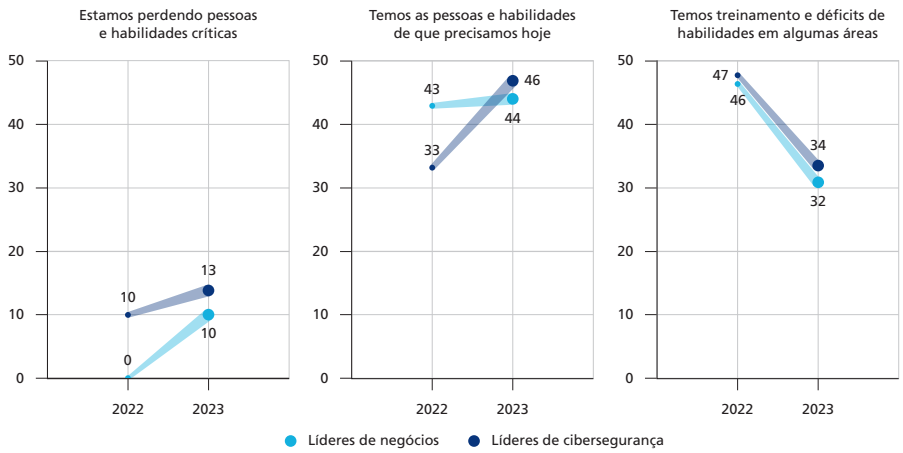
que possuem maiores déficits são a China, com 1,4 milhão, e a Índia, com cerca de 560 mil profissionais especializados faltando.

FIGURA 11
Força de trabalho em cibersegurança no mundo e no Brasil

Fonte: ISC2 (2022).
Elaboração do autor.

A complexidade da cibersegurança e os desafios de negócios têm aproximado as visões entre os líderes de negócios e os especialistas. Estudo do FEM (2023a) mostra que há a preocupação com as habilidades e as capacidades de cibersegurança (gráfico 19), sendo que a diferença de visões entre os líderes de negócios e os de cibersegurança diminuiu. O maior alinhamento é imprescindível para que o problema de competências em segurança e privacidade sejam tratados adequadamente.

GRÁFICO 19
Visões sobre habilidades e capacidades de cibersegurança
(Em %)

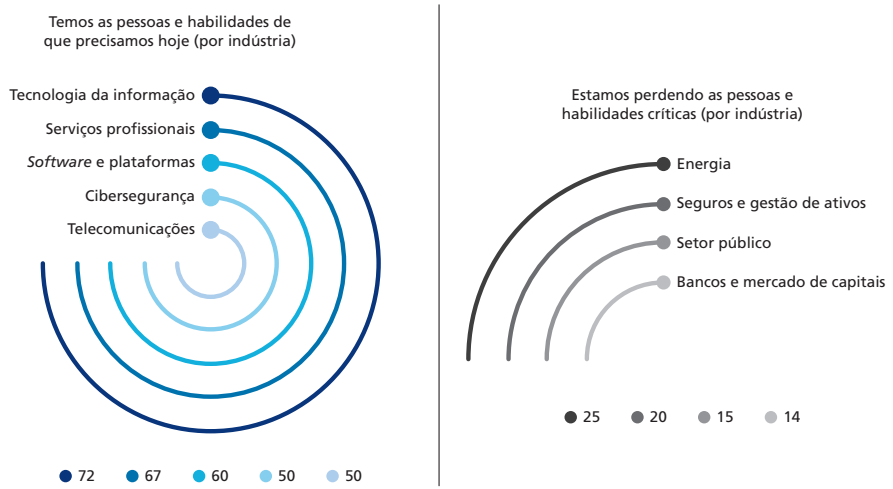


Fonte: WEF (2023a).
Elaboração do autor.

O desenvolvimento de competências em cibersegurança é essencial e um desafio global, e seu tamanho varia de acordo com o setor. Há aqueles que sofrem mais ou menos ataques cibernéticos, bem como aqueles que estão em estágios

diferentes de maturidade, que se refletem nos esforços necessários, incluindo os de investimentos. A figura 12 apresenta essa diferença existente em setores, com 72% do setor de tecnologia de informação possuindo as pessoas e habilidades de cibersegurança necessárias atualmente, enquanto 25% do setor de energia passa por perda de pessoas e habilidades críticas de cibersegurança (FEM, 2023a).

FIGURA 12
Setores com lacunas em cibersegurança



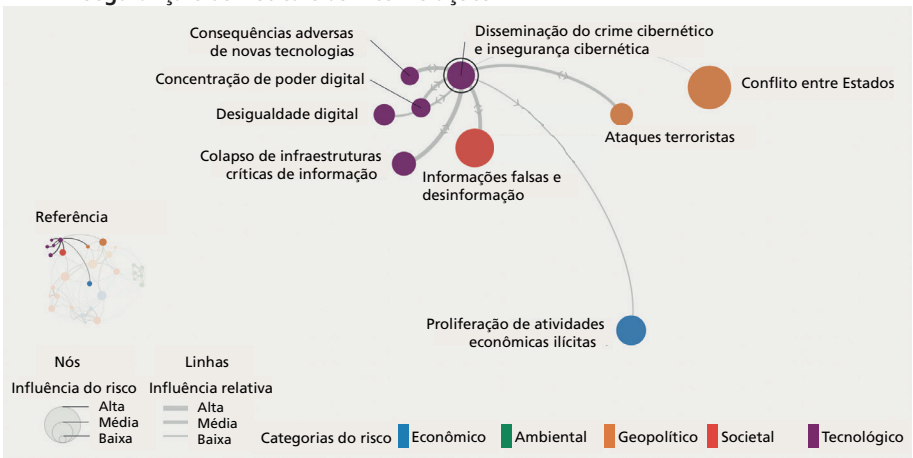
Fonte: WEF (2023a).
Elaboração do autor.

6 TENDÊNCIAS E ESTRATÉGIA PARA O FATOR HUMANO NA SEGURANÇA CIBERNÉTICA

No universo digital, vem ocorrendo um aumento do número de incidentes cibernéticos, ataques cada vez mais sofisticados e impactos cada vez maiores, que se espalham por diferentes atores na medida em que crescem a interdependência e a cadeia de suprimentos. Com uma superfície de ataques cada vez maior e distribuída, a complexidade da cibersegurança repercute em diferentes dimensões, relacionadas ao escopo, ao foco, às camadas e às funções de segurança cibernética.

A importância da segurança cibernética tende a crescer ainda mais, refletindo em outros contextos. Isso pode ser observado no fortalecimento das interconexões com outros riscos a partir dos riscos cibernéticos. A figura 13 mostra que a insegurança cibernética pode levar a conflitos, ataques terroristas, desinformação, colapso de infraestruturas críticas, concentração de poder digital, desigualdade digital e impactos tecnológicos negativos (FEM, 2023b).

FIGURA 13
Insegurança cibernética e as inter-relações



Fonte: WEF (2023b).
Elaboração do autor.

A complexidade da cibersegurança exige cada vez mais ações organizadas, integradas e holísticas. Adicionalmente, a velocidade das necessidades e dos avanços digitais tem criado um descompasso que se reflete nos ataques cibernéticos que exploram o vetor humano e, adicionalmente, resultam em déficit global de profissionais especializados em cibersegurança. Nesse cenário, duas principais tendências devem ser consideradas: o desenvolvimento tecnológico em cibersegurança e o desenvolvimento de competências e capacidades de segurança cibernética.

O fator humano em cibersegurança vem sendo tratado como política pública e de Estado em muitos países. No Brasil, há a Estratégia Nacional de Segurança Cibernética – E-Ciber (Brasil, 2020a), estabelecida pelo Decreto nº 10.222, de 5 de fevereiro de 2020, que é oriunda do Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação (PNSI) (Brasil, 2018c). A PNSI priorizou a segurança cibernética como o primeiro módulo a ter a sua estratégia elaborada, que terá sequência com a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados.

A E-Ciber define como visão para o Brasil que se torne um país de excelência em segurança cibernética, com objetivos de: i) tornar o Brasil mais próspero e confiável no ambiente digital; ii) aumentar a resiliência brasileira às ameaças cibernéticas; e iii) fortalecer a atuação brasileira em segurança cibernética no cenário internacional. As ações envolvem: i) governança cibernética; ii) modelo

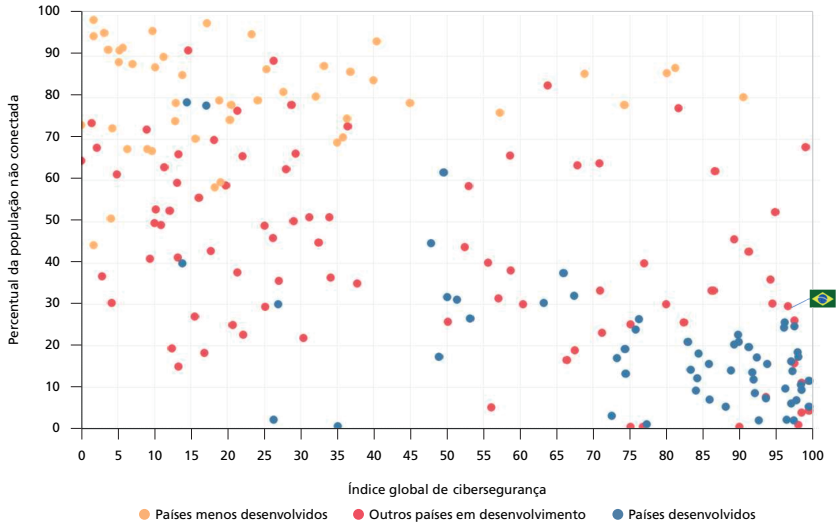
centralizado de governança no âmbito nacional; iii) promoção de um ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; iv) elevação do nível de proteção do governo; v) elevação do nível de proteção das Infraestruturas Críticas Nacionais; vi) aprimoramento do arcabouço legal sobre segurança cibernética; vii) incentivo à concepção de soluções inovadoras em segurança cibernética; viii) ampliação da cooperação internacional do Brasil em segurança cibernética; ix) ampliação da parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade; e x) elevação do nível de maturidade da sociedade em segurança cibernética.

A E-Ciber busca proporcionar às infraestruturas críticas maior resiliência, visando à contínua prestação de serviços essenciais, por meio de iniciativas que envolvem a interação entre as agências reguladoras de infraestruturas críticas, adoção de ações de segurança cibernética pelas infraestruturas críticas, políticas de segurança cibernética, equipes de resposta a incidentes, notificação de incidentes cibernéticos ao CTIR Gov e exercícios cibernéticos.

O fator humano em cibersegurança também faz parte do Índice Global de Cibersegurança (Global Cybersecurity Index – CGI), que é medido pela International Telecommunication Union (ITU) e engloba 194 países, considerando medidas legais, técnicas, organizacionais, de desenvolvimento de capacidades e de cooperação (ITU, 2020). O CGI reforça o papel dos países em cibersegurança, principalmente porque, no universo digital, tudo está interligado, e os avanços econômicos e sociais dependem cada vez mais do gerenciamento apropriado dos riscos cibernéticos.

É importante notar que a superfície de ataque, que se inicia com a conectividade, direciona as ações dos países, indicando o papel das nações na construção de pilares que envolvem uma política em cibersegurança e estrutura de apoio às organizações. Há, assim, uma correlação direta entre a conectividade e a cibersegurança. O gráfico 20 mostra que os países com maiores índices globais de cibersegurança são aqueles que possuem a maior parte da população conectada. A maioria dos países desenvolvidos possui um alto índice de cibersegurança e de população conectada. Já entre os países em desenvolvimento, há um equilíbrio entre os dois índices, com países com percentual da população desconectada média ou alta possuindo um bom CGI e vice-versa. Entre os países pouco desenvolvidos, há o desafio de conectar a população, o que se reflete nos índices globais de cibersegurança mais baixos.

GRÁFICO 20
Relação entre conectividade e o CGI



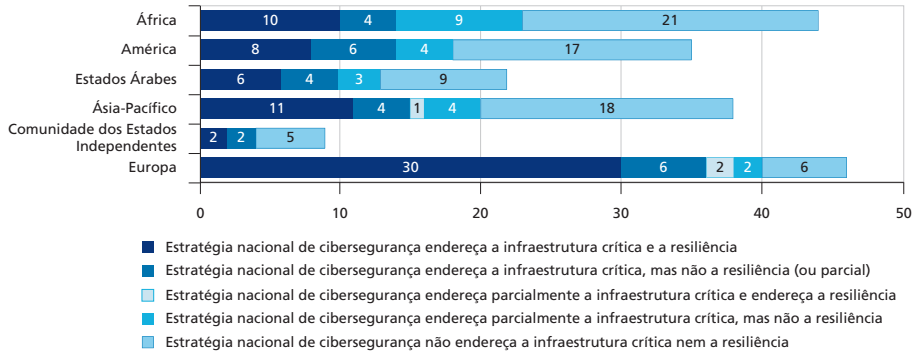
Fonte: ITU (2020).
Elaboração do autor.

A E-Ciber do Brasil trata das questões relevantes e é um exemplo das estratégias nacionais de cibersegurança (National Cybersecurity Strategy – NCS), que possuem uma visão de proteção dos serviços essenciais que são providos para a sociedade, tratando principalmente da proteção de infraestrutura crítica e da resiliência, visando minimizar as interrupções dos serviços e proporcionar o retorno mais efetivo às operações. O gráfico 21 mostra que os países europeus estão mais avançados nas estratégias nacionais de cibersegurança, mas ainda é grande o número de países, em todos os continentes, que não tratam da infraestrutura crítica e da resiliência.

A figura 14 mostra que 95% dos usuários de internet estão em países que possuem uma estratégia nacional de cibersegurança e uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (Etir), ou Computer Security Incident Response Team (CSIRT), nacional. O Brasil está entre os países com maior número de usuários de internet (Morgan, 2019) e possui uma estratégia nacional de cibersegurança (Brasil, 2020a) e CSIRTs nacionais, como o Centro de Atendimento a Incidentes de Segurança (Cais), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).[2]

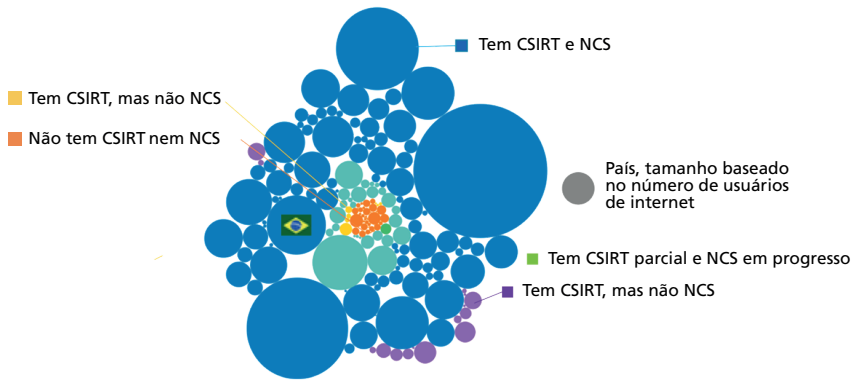
2. Disponíveis em: https://cais.rnp.br; https://cert.br; e https://www.gov.br/ctir.

GRÁFICO 21
Número de países que tratam a infraestrutura crítica e a resiliência cibernética



Fonte: ITU (2020).
Elaboração do autor.

FIGURA 14
Relação entre usuários de internet e estruturação de resposta a incidentes e estratégia nacional



Fonte: ITU (2020).
Elaboração do autor.

A estratégia nacional de cibersegurança é um fator importante para que os países tenham um CSIRT nacional, como mostra a tabela 2, que indica um relacionamento direto com um grande número de países que não possuem a estratégia nacional, portanto também não apresentam um CSIRT.

A construção de uma estratégia nacional de cibersegurança e a sua execução, com os mecanismos adequados para o tratamento das dimensões da cibersegurança, abrange aspectos multidisciplinares e exige capacidades especializadas e um trabalho integrado. Os desafios passam ainda pelo desenvolvimento de cooperações e parcerias internacionais, visando à construção conjunta de capacidades,

competências, conscientização, recursos tecnológicos, processos, mecanismos e medidas para gerenciar os riscos cibernéticos, incluindo a prevenção contra os ataques e a resposta adequada em caso de incidentes de segurança.

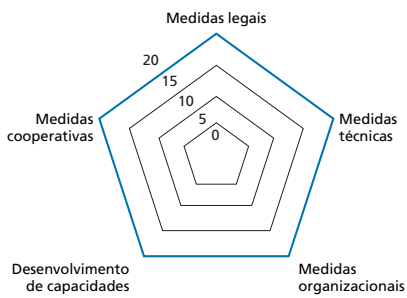
TABELA 2
Relação entre estratégia nacional de cibersegurança e estruturação de resposta a incidentes

	Possui NCS (países)	NCS em andamento ou > 5 anos (países)	Não possui NCS (países)
CSIRT nacional	90	29	18
Não possui CSIRT nacional	7	1	49

Fonte: ITU (2020).
Elaboração do autor.

De acordo com o CGI, o Brasil está em 18º lugar entre 184 países, sendo o terceiro nas Américas, atrás de Estados Unidos e Canadá. O Brasil é um país em desenvolvimento, com força nas medidas legais e potencial de crescimento nas medidas técnicas e organizacionais. No desenvolvimento de capacidades, que mede as campanhas de conscientização, treinamentos, educação e incentivos para criar capacidades de segurança cibernética, são avaliadas as iniciativas, os programas de pesquisa e desenvolvimento (P&D) em cibersegurança e a existência de uma indústria nacional em segurança. A composição do CGI do Brasil pode ser vista na figura 15 (ITU, 2020).

FIGURA 15
Composição do CGI do Brasil



Nível de desenvolvimento: país em desenvolvimento

Área(s) de força relativa: medidas legais

Área(s) com potencial de crescimento: medidas técnicas e organizacionais

Índice geral	Medidas legais	Medidas técnicas	Medidas organizacionais	Desenvolvimento de capacidades	Medidas cooperativas
96.60	20.00	18.73	18.98	19.48	19.41

Fonte: ITU (2020).
Elaboração do autor.

Além do CGI, há outros índices, tais como o National Cyber Security Index (NCSI) e o Cybersecurity Exposure Index (CEI). Neles, o Brasil está em uma posição inferior, se comparado ao CGI. No NCSI, o Brasil está em 71º, com índice de 51,95 de possíveis 100. O NCSI utiliza dados públicos para a composição do índice e considera elementos como política de segurança cibernética, análise de ameaças cibernéticas, educação e desenvolvimento profissional, contribuição para a cibersegurança global, proteção de serviços digitais, proteção de serviços essenciais, serviços de confiança e identificação digital, proteção de dados pessoais, resposta a incidentes cibernéticos, gerenciamento de crises cibernéticas, medidas contra crimes cibernéticos e operações cibernéticas militares.[3]

No CEI, o Brasil ocupa a 46ª posição no *ranking* global e o quinto lugar na América do Sul, atrás de Uruguai, Paraguai, Chile e Argentina. No entanto, esse índice utiliza uma métrica diferente do CGI, considerando dados sobre *malware*, *ransomware*, mineração de criptomoedas, ataques relacionados a provedores de nuvem e nível de comprometimento com cibersegurança, de 2018 a 2020.[4]

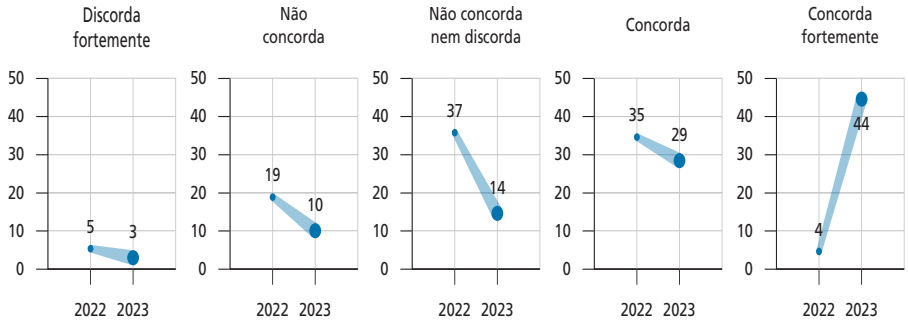
As medidas legais possuem uma importância em cibersegurança, ao promoverem um direcionamento das ações, principalmente na priorização feita por organizações de diferentes naturezas. O Brasil conta com a Estratégia Nacional de Segurança Cibernética (Brasil, 2020a), a Política Nacional de Segurança da Informação (Brasil, 2018c), a Política Nacional de Segurança de Infraestruturas Críticas (Brasil, 2018b), a LGPD (Brasil, 2018a) e outros decretos relacionados ao Plano Nacional de Segurança de Infraestruturas Críticas (Brasil, 2022) e à Rede Federal de Gestão de Incidentes Cibernéticos (Brasil, 2021), que têm pautado um conjunto de ações importantes para a evolução da cibersegurança no país.

A relevância das medidas legais pode ser conferida no relatório do FEM, que abordou o panorama global em segurança cibernética (FEM, 2023a) e indicou que tem aumentado o entendimento de que o arcabouço regulatório em cibersegurança e privacidade é um elemento efetivo para melhorar a resiliência cibernética com o tratamento dos riscos, como apresentado no gráfico 22.

Um exemplo de medida regulatória envolve os incidentes de segurança à infraestrutura crítica e IoT industrial nos Estados Unidos. O Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) estabelece que organizações em dezesseis infraestruturas críticas devem reportar ataques cibernéticos e vazamentos em até 72 horas, e 24 horas para qualquer pagamento de *ransomware* feito (Cisa, 2022).

3. Disponível em: https://ncsi.ega.ee.
4. Disponível em: https://passwordmanagers.co/cybersecurity-exposure-index/.

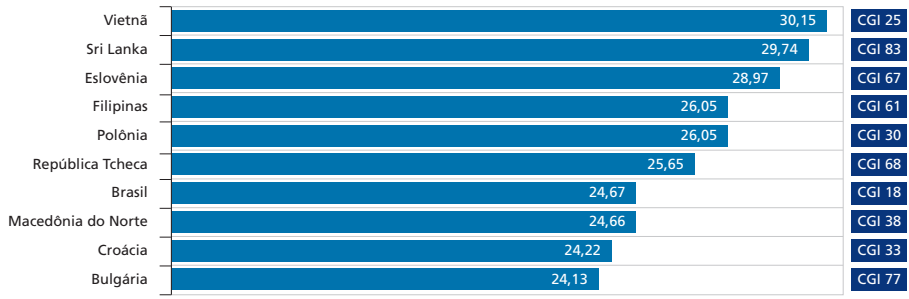
GRÁFICO 22
O papel do arcabouço regulatório para o tratamento dos riscos cibernéticos
(Em %)



Fonte: WEF (2023a).
Elaboração do autor.

Em 2022, o Brasil continuou entre os países com maiores chances de serem alvos de códigos maliciosos (Sonicwall, 2023). Como os principais vetores de ataques relacionados a códigos maliciosos envolvem o fator humano, as campanhas e os alvos nesses países indicam que há a necessidade de conscientização e fortalecimento de uma cultura de segurança cibernética. Os principais países podem ser vistos no gráfico 23, juntamente com a posição no *ranking* do CGI.

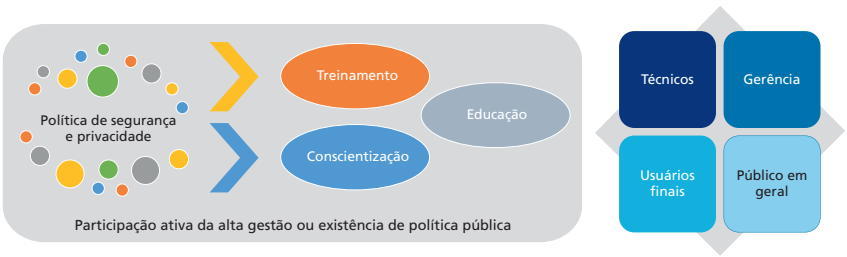
GRÁFICO 23
Países com maiores chances de serem alvos de um *malware*
(Em %)



Fonte: Sonicwall (2023); ITU (2020).

O fortalecimento geral de uma cultura de segurança e privacidade exige a formalização de políticas que direcionam ações de treinamento, conscientização e educação para diferentes perfis, da população em geral até a alta gestão, passando pelos profissionais técnicos e usuários das empresas, organizações e órgãos, como mostra a figura 16.

FIGURA 16
Fortalecimento de cultura de segurança e privacidade

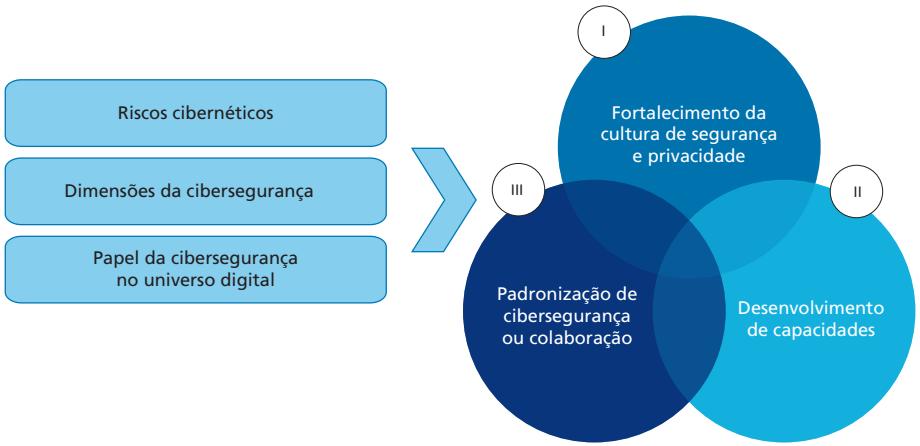


Elaboração do autor.

Uma estratégia para o fator humano em cibersegurança deve, assim, considerar o fortalecimento da cultura de segurança e privacidade. Outros pilares importantes da estratégia são o desenvolvimento de capacidades e a padronização de cibersegurança e colaborações. Eles refletem as necessidades atuais, decorrentes de fatores como o déficit de profissionais de cibersegurança, os avanços dos incidentes cibernéticos, os avanços na área, a estratégia nacional de cibersegurança, as ações realizadas pelos CSIRTs e a forma como o CGI é calculado (medidas legais, técnicas, organizacionais, de desenvolvimento de capacidades e de cooperação).

A figura 17 apresenta uma proposta de estratégia para o fator humano em cibersegurança com esses três pilares, que devem ser tratados devido ao contexto representado pelos riscos cibernéticos que faz parte da vida de todos, a complexidade resultante das dimensões da cibersegurança, e do papel da cibersegurança no universo digital.

FIGURA 17
Uma estratégia para o fator humano em cibersegurança



Elaboração do autor.

Os três pilares da estratégia para o fator humano em cibersegurança são baseados em públicos distintos, em frentes de ações complementares e em escopos de visões diferentes. Os públicos são os receptores das ações e possuem perfis diferentes que necessitam de ações próprias. Os públicos são: jovens e alunos, profissionais de cibersegurança, dirigentes e gestores, usuários e clientes e público em geral.

O pilar de fortalecimento da cultura de segurança e privacidade é voltado principalmente para os perfis de usuários e clientes, além do público em geral. O pilar de desenvolvimento de capacidades é voltado mais para os jovens e alunos, além dos profissionais de cibersegurança. Já o pilar de padronização de cibersegurança e colaboração está mais relacionado aos dirigentes e gestores.

Cada pilar possui um conjunto de frentes de ações, voltado para cada um dos perfis. As frentes de ações para cada um dos pilares da estratégia são descritas a seguir.

1) Pilar do fortalecimento da cultura de segurança e privacidade:
    a) campanhas de conscientização: levar ao público informações a respeito de segurança cibernética e de riscos cibernéticos;
    b) conscientização para a educação: após conscientização sobre os riscos, abrange avanços nos comportamentos do público e nas medidas que precisam ser tomadas;
    c) currículo acadêmico incluindo a cibersegurança: com o universo digital, todas as profissões possuem aspectos de cibersegurança que devem ser conhecidos desde a formação para serem adotados por todos; e
    d) treinamentos incluindo a cibersegurança: qualquer ação profissional de qualquer área, em algum ponto dos processos, envolve aspectos de cibersegurança, que devem ser abordados.
2) Pilar do desenvolvimento de competências:
    a) programas de P&D em cibersegurança: desenvolvimento tecnológico de cibersegurança, reforçando o ecossistema de inovação e a ligação com o mercado;
    b) currículo acadêmico especializado: conjunto de disciplinas alinhado com o mercado, para a formação profissional de diferentes perfis necessários no mercado, incentivando ainda o desenvolvimento tecnológico;
    c) programas de iniciação científica em cibersegurança: projetos práticos de cibersegurança, com aproximação com o setor privado;

d) programas de pós-graduação: especialização em cibersegurança, com melhor preparação para o mercado de trabalho, proporcionando também o desenvolvimento tecnológico; e

e) treinamentos especializados: treinamentos acessíveis para a formação em cibersegurança, de diferentes perfis necessários no mercado.

3) Pilar da padronização de cibersegurança e colaboração:

a) mecanismos de colaboração: espaços de conexão entre atores do ecossistema, para sinergias e desenvolvimento de ações em conjunto;

b) padronização técnica: desenvolvimento de padrões de modelos, processos e tecnologias para serem adotados pelas organizações, acelerando a cibersegurança;

c) estrutura da área responsável: modelagem de estruturas da área de cibersegurança, incluindo mecanismos de viabilidade, para serem adotados pelas organizações, acelerando a estruturação; e

d) padronização de perfis de cibersegurança: sintonia com o mercado e os currículos de formação, para organizar o desenvolvimento de capacidades de forma mais sinérgica, como o realizado na Europa (Enisa, 2023).

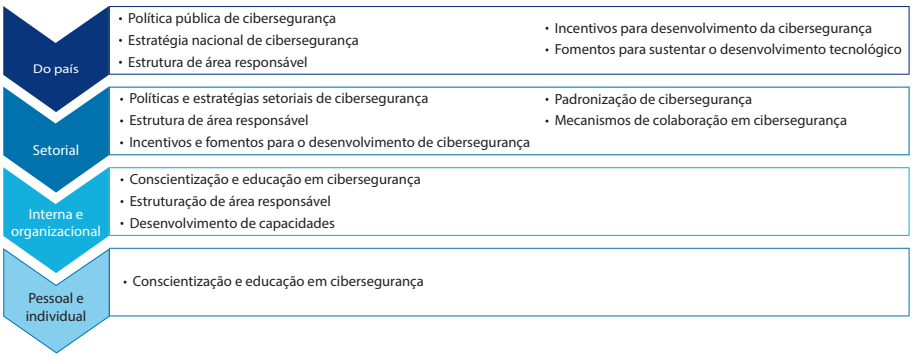
Cada frente de ações para os três pilares pode ser aplicada para os perfis específicos, como pode ser visto na figura 18. Para os jovens e alunos, podem ser desenvolvidas frentes de ações relacionadas à educação em cibersegurança, programas de P&D, currículo acadêmico especializado, programas de iniciação científica, programas de pós-graduação e mecanismos de colaboração. Os profissionais de cibersegurança possuem frentes de ações específicas, bem como os dirigentes e gestores, os usuários e clientes e o público em geral.

Para o planejamento e a execução das frentes de ações, é importante que diferentes escopos de visões sejam considerados (figura 19). Há o escopo do país, que pode contribuir com uma política pública de cibersegurança, com uma estratégia nacional, que já existe no Brasil, com incentivos para o desenvolvimento da cibersegurança e com os fomentos para sustentar o desenvolvimento tecnológico, por exemplo. A visão setorial envolve também a contribuição para os setores, com políticas e estratégias setoriais, envolvendo incentivos e fomentos, além da padronização e de mecanismos de colaboração. A visão interna organizacional é corporativa, com ações específicas de conscientização, estruturação e desenvolvimento de capacidades para que os desafios do universo digital possam ser enfrentados. A visão pessoal representa a evolução da própria sociedade digital, com conscientização e educação em cibersegurança como essenciais para o fortalecimento da cultura.

FIGURA 18
Frentes de ações para diferentes perfis na estratégia

Elaboração do autor.

FIGURA 19
Visões e escopos para planejamento e execução



Elaboração do autor.

Uma estratégia para o fator humano em cibersegurança envolve o fortalecimento da cultura de segurança e privacidade, alavancado por estratégias e políticas nacionais, que direcionam e reforçam o foco nos riscos cibernéticos. Adicionalmente, o apoio e o incentivo ao desenvolvimento tecnológico em cibersegurança, que fortalece toda uma indústria, envolve programas de pesquisa e desenvolvimento na área, os quais, naturalmente, incrementam as capacidades de segurança cibernética. Isso ocorre tanto sob o ponto de vista de recursos humanos quanto de recursos tecnológicos que compõem as arquiteturas de segurança e são adotados como funções de segurança cibernética, para identificação de riscos, proteção, detecção de ataques, resposta a incidentes e recuperação dos ambientes.

Como medidas de incentivo para o desenvolvimento de capacidades de cibersegurança, há possibilidades como o estabelecimento de programas de educação e treinamento por governos, empresas ou setores. As capacitações podem ser realizadas em diferentes níveis, desde o básico até os especializados, voltados para perfis profissionais específicos em cibersegurança. O mercado, de forma geral, pode contribuir com o provimento de residências tecnológicas, que possibilitam aos alunos aplicarem os conhecimentos teóricos e práticos em um ambiente real, o que auxilia também na diminuição do déficit de profissionais da área. A educação em cibersegurança passa também pela inclusão do assunto no currículo acadêmico nacional dos ensinos fundamental e médio, e a definição de um currículo padrão para cursos de graduação e pós-graduação.

As ações para o desenvolvimento de capacidades de segurança cibernética ganham força com políticas públicas, que são necessárias no contexto do universo digital. Adicionalmente, incentivos governamentais para o desenvolvimento da cibersegurança, como impostos ou a inclusão de padrões de segurança em contratos, podem beneficiar a todos.

7 CONCLUSÃO

Enquanto as vantagens das tecnologias digitais resultam em imensos benefícios econômicos e sociais, os riscos cibernéticos podem afetar negativamente as consequências da digitalização. Com os novos desafios profissionais relacionados à construção e à evolução do universo digital, o estabelecimento dos pilares da confiança no universo digital passa pela segurança cibernética. Os riscos cibernéticos, assim, devem ser entendidos e gerenciados, com as funções de identificação, análise, avaliação, tratamento, comunicação e monitoramento efetivas.

Além da estratégia nacional de cibersegurança, que trata de aspectos como proteção de infraestrutura crítica, resiliência e resposta a incidentes cibernéticos, há um importante fator para o avanço digital dos países: a segurança do domínio cibernético, principalmente com a construção de capacidades de cibersegurança. Relacionadas ao fator humano, as capacidades de cibersegurança são a chave para o universo digital e conectado, necessário para que os países possam construir infraestruturas críticas resilientes e, assim, criar as condições para proteger cidadãos e negócios, fortalecendo as comunidades digitais. Desse modo, as capacidades de cibersegurança contribuem diretamente para a redução de problemas como exclusão digital e riscos cibernéticos.

A percepção de distância é outra no universo digital, e tudo passa a estar conectado. E as conexões, em todos os níveis – do tecnológico aos modelos de negócios – se traduzem em complexidades que, naturalmente, elevam os riscos, inclusive os cibernéticos. Assim, com os avanços do universo digital, a

segurança cibernética está evoluindo, deixando de ser uma capacidade técnica e se transformando em uma capacidade das empresas, organizações e países. Os riscos cibernéticos avançam na agenda de todos, fazendo parte da vida de pessoas, empresas, organizações e países.

Os progressos da cibersegurança e o fortalecimento da cultura de segurança e privacidade envolvem o papel do governo e a necessidade de políticas públicas, em conjunto com a continuidade da aproximação entre a alta gestão e os líderes de negócios com os profissionais de cibersegurança. As ações podem incluir mudanças na estrutura organizacional para que haja maior fluidez nas comunicações e mais efetividade do gerenciamento dos riscos cibernéticos. São importantes também a evolução da linguagem, para possibilitar que essa integração ocorra com uma melhor comunicação e um melhor entendimento dos aspectos de cibersegurança por todos, e a aceitação das responsabilidades e deveres pelos requisitos de cibersegurança necessários como capacidade intrínseca da organização.

O aumento da interdependência das infraestruturas críticas e a busca por maior conectividade e novas tecnologias continuam, com o universo digital evoluindo constantemente. Com o uso intensivo da inteligência artificial, os ataques tendem a ser ainda mais sofisticados, com o fator humano representando um elemento-chave, tanto para os atacantes quanto para a proteção das organizações. Os ataques direcionados ganham força e eficiência, principalmente com o uso cruzado de dados, muitas vezes provenientes de outros ataques cibernéticos. Além disso, o volume de ataques aumenta, enquanto os mecanismos de monitoramento e defesa ganham em eficiência e efetividade. Nesse contexto, o fator humano é imprescindível, principalmente sob o aspecto profissional e para diminuir o déficit de profissionais especializados, que irão direcionar as ações de cibersegurança necessárias.

O universo digital, com todos os riscos cibernéticos intrínsecos, faz também com que as habilidades em cibersegurança se expandam para os profissionais de todas as áreas. Todos devem ter uma visão mais crítica sobre o funcionamento de qualquer elemento, para que as vulnerabilidades e os cenários de ataques sejam visualizados para, assim, serem evitados. É a natureza dos riscos cibernéticos, que afeta todas as pessoas, empresas, organizações e países. A segurança cibernética é de responsabilidades de todos. Com uma educação em cibersegurança, que fortalece uma cultura de segurança e privacidade, com ações de desenvolvimento de capacidades e de padronização de cibersegurança e com o estabelecimento de mecanismos de colaboração, a sociedade pode avançar com mais confiança no universo digital, com benefícios tecnológicos e maior conformidade legal. O reflexo é o próprio avanço econômico.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005**: tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação. [s.l.]: ABNT, 2019.

_____. **ABNT NBR ISO 22301**: segurança e resiliência – sistema de gestão de continuidade de negócios – requisitos. [s.l.]: ABNT, 2020.

_____. **ABNT NBR ISO/IEC 27001**: segurança da informação, segurança cibernética e proteção à privacidade – sistemas de gestão da segurança da informação – requisitos. [s.l.]: ABNT, 2022a.

_____. **ABNT NBR ISO/IEC 27002**: segurança da informação, segurança cibernética e proteção à privacidade – controles de segurança da informação. [s.l.]: ABNT, 2022b.

ARCTIC WOLF. **The top 10 manufacturing industry cyber attacks**. Arctic Wolf, 12 mar. 2023. Disponível em: https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks/. Acesso em: 13 maio 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, p. 59, 15 ago. 2018a. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 14 maio 2023.

_____. Decreto nº 9.573, de 22 de novembro de 2018. Política Nacional de Segurança de Infraestruturas Críticas. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**, Brasília, p. 40, 23 nov. 2018b. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-9-573-de-22-de-novembro-de-2018-51525032. Acesso em: 14 maio 2023.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**, Brasília, p. 23, 27 dez. 2018c. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em: 21 mar. 2023.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, p. 6, 6 fev. 2020a. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 21 mar. 2023.

_____. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**, Brasília, p. 8, 10 dez. 2020b. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.569-de-9-de-dezembro-de-2020-293251357. Acesso em: 14 maio 2023.

_____. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. **Diário Oficial da União**, Brasília, p. 2, 19 jul. 2021. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022. Acesso em: 14 maio 2023.

_____. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**, Brasília, p. 9, 16 set. 2022. Seção 1. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-11.200-de-15-de-setembro-de-2022-430035293. Acesso em: 14 maio 2023.

CASO, Jeffrey *et al*. Cybersecurity for the IoT: how trust can unlock value. **McKinsey & Company**, 7 Apr. 2023. Disponível em: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value. Acesso em: 14 maio 2023.

CISA – CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **Cyber Incident Reporting for Critical Infrastructure Act of 2022** (CIRCIA). Arlington: Cisa, Mar. 2022. Disponível em: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. Acesso em: 15 maio 2023.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. **European Cybersecurity Skills Framework (ECSF)**. Athens: Enisa, 2023. Disponível em: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework. Acesso em: 20 jun. 2023.

FEM – FÓRUM ECONÔMICO MUNDIAL. **Global Cybersecurity Outlook 2023**. Colony/Geneva: World Economic Forum, 18 Jan. 2023a. Disponível em: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/. Acesso em: 13 maio 2023.

_____. **The Global Risks Report 2023**. 18th ed. Colony/Geneva: World Economic Forum, 11 Jan. 2023b. Disponível em: https://www.weforum.org/reports/global-risks-report-2023/. Acesso em: 13 abr. 2023.

FORTIGUARD LABS. **Global threat landscape report**: a semianual report by FortiGuard Labs – February 2023. Sunnyvale: Fortinet, 2023. Disponível em: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-2023-threat-landscape.pdf. Acesso em: 14 maio 2023.

FRUHLINGER, Josh. Stuxnet explained: the first known cyberweapon. **CSO**, 31 Aug. 2022. Disponível em: https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html. Acesso em: 13 maio 2023.

IEF – INTERNATIONAL ENERGY FORUM. Energy is the top target for cyberattacks. How can the sector respond? **IEF**, 25 Aug. 2022. Disponível em: https://www.ief.org/news/energy-is-the-top-target-for-cyberattacks-how-can-the-sector-respond. Acesso em: 13 abr. 2023.

ISC2 – INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM. **(ISC)² Cybersecurity workforce study**: a critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution – 2022. Alexandria: ISC2, 2022. Disponível em: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf. Acesso em: 15 maio 2023.

ITU – INTERNATIONAL TELECOMMUNICATION UNION. **Global cybersecurity index**: 2020. Geneve: ITU Publications, 2020. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em: 21 mar. 2023.

MORGAN, Steve. Humans on the internet will triple from 2015 to 2022 and hit 6 billion. **Cybercrime Magazine**, Sausalito, 18 July 2019. Disponível em: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/. Acesso em: 20 jun. 2023.

SONICWALL. **2022 Sonicwall cyber threat report**. Milpitas: Sonicwall, 2022. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf. Acesso em: 14 maio 2023.

_____. **2023 Sonicwall cyber threat report**: charting cybercrime's shifting frontlines. Milpitas: Sonicwall, 2023. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf. Acesso em: 13 maio 2023.

VERIZON. **2022 DBIR Data Breach Investigations Report**. New York: Verizon, 2022. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 14 maio 2023.