2023

Relatório sobre o desenvolvimento da FORÇA DE TRABALHO DE CIBERSEGURANÇA em uma era de escassez de talentos e habilidades

OEA Más derechos para más gente

Cybersecurity Innovation Councils

CISCO

COPYRIGHT© (2022) Organização dos Estados Americanos. Todos os direitos reservados sob as Convenções Internacional e Pan-Americana. Nenhuma parte do conteúdo deste material pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, no todo ou em parte, sem a permissão expressa da Organização.

Preparado e publicado pelo Programa de Segurança Cibernética do Comitê Interamericano contra o Terrorismo (cybersecurity@oas.org)

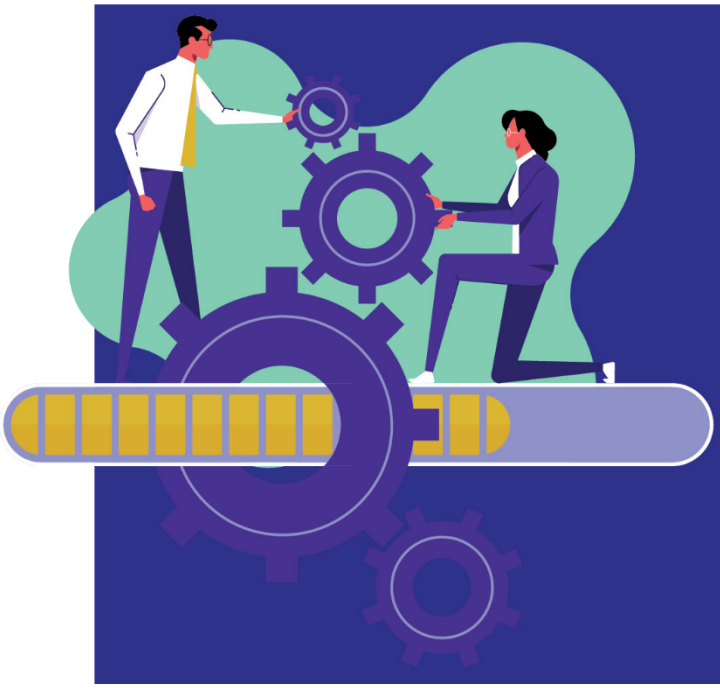
O conteúdo deste documento é apresentado apenas para fins informativos e não representa a opinião ou posição oficial da Organização dos Estados Americanos, de sua Secretaria Geral ou de seus Estados Membros.

SÍNTESE

A pandemia COVID-19 e a pós-pandemia geraram um forte impacto na economia global[1] , uma expansão do cenário do ameaça e risco[2] e uma grande mudança na forma como as organizações trabalham[3] . Há também um envelhecimento geral da população[4] , grandes problemas nas economias da região devido ao alto desemprego[5] e uma inversão geral no progresso da paridade de gênero[6].

O mercado de trabalho de cibersegurança criou uma lacuna (escassez) em sua força de trabalho no curto prazo[7] , gerando riscos devido não apenas à escassez de talentos nas organizações, mas também à escassez de habilidades na força de trabalho. Esta situação, embora global, é exacerbada na América Latina e no Caribe, gerando fortes pressões sobre organizações públicas e privadas com o conseqüente impacto sobre a segurança cibernética nos países da região.

Atualmente, o desenvolvimento da força de trabalho ciber-segurança é analisado sob duas abordagens: quantitativa e qualitativa, ou seja, no contexto da escassez de profissionais e no contexto da falta de habilidades tanto dos profissionais que desejam entrar na força de trabalho ciber-segurança quanto dos profissionais que já fazem parte da força de trabalho ciber-segurança. A análise da situação tanto do lado da demanda quanto do lado da oferta do mercado de trabalho de cibersegurança é crucial para identificar os desafios e os desafios que todos os multi-stakeholders precisam enfrentar a fim de fechar as lacunas nos países da região.



Por exemplo, no lado da oferta, para aqueles interessados em entrar no mercado de trabalho de segurança cibernética, a informação sobre o que uma carreira implica é esmagadora, confusa e contraditória. O caminho a seguir na preparação para uma carreira e progressão cibernética, uma vez na força de trabalho, pode ser um processo complexo. Para as organizações do lado da demanda, há dificuldades em identificar os requisitos necessários para preencher cargos em aberto, recrutando e retendo talentos, enquanto se tenta manter uma forte postura de segurança cibernética. Os governos têm adotado e implementado políticas e estratégias nacionais de cibersegurança que abordam questões relacionadas à falta de capacidades de cibersegurança, entretanto, as iniciativas estratégicas propostas em torno do desenvolvimento da força de trabalho de cibersegurança na região levará anos ou mesmo décadas para amadurecer.

1 De acordo com (WORLD BANK, 2022), após uma forte recuperação em 2021, a economia global está entrando em uma acentuada desaceleração em meio a novas ameaças de variantes da COVID-19 e ao aumento da inflação, da dívida e da desigualdade de renda que podem comprometer a recuperação das economias emergentes e em desenvolvimento. O crescimento na América Latina e no Caribe deverá desacelerar para 2,6% em 2022 antes de subir ligeiramente para 2,7% em 2023.

2 De acordo com (FORTINET, 2022), a região da América Latina e Caribe sofreu 137 bilhões de tentativas de ciberataques de janeiro a junho de 2022, um aumento de 50% em relação ao mesmo período do ano passado (com 91 bilhões). O México foi o país mais visado (com 85 bilhões), seguido pelo Brasil (com 31,5 bilhões) e pela Colômbia (com 6,3 bilhões).

3 De acordo com (FORBES, 2022), o futuro do trabalho será mais híbrido, mais colaborativo e mais automatizado.

4 De acordo com (Oxford Martin School, 2022), nos próximos cinqüenta anos, espera-se que o número de idosos seja superior ao de jovens em quase todos os países. Esta mudança na composição etária tem enormes implicações para todos os aspectos da sociedade e da economia.

5 De acordo com (OIT, 2022), o número total global de jovens desempregados é estimado em 73 milhões em 2022, uma ligeira melhoria em relação a 2021 (75 milhões), mas ainda seis milhões acima do nível pré-pandêmico de 2019.

6 De acordo com (WEF, 2022), serão necessários mais 132 anos para fechar a lacuna global de gênero.

7 De acordo com (ISC2, 2022a), há uma escassez global de 3,43 milhões de trabalhadores qualificados em cibersegurança.

O desenvolvimento da força de trabalho de cibersegurança é fundamental para que os países estejam preparados para conflitos no ciberespaço. Também cabe às organizações definir as habilidades e capacidades necessárias de sua força de trabalho para atender sua estratégia e objetivos comerciais, identificar as principais lacunas da força de trabalho atual e criar estratégias e programas inovadores para atrair, recrutar, contratar e desenvolver os melhores talentos.

A força de trabalho cibernética e a escassez de habilidades continuarão a crescer na América Latina e no Caribe, portanto, o ecossistema de cibersegurança na região deve trabalhar de forma holística e coordenada no desenvolvimento da força de trabalho, a fim de enfrentar uma combinação única de desafios e desafios, mas sempre passando da formulação de soluções à ação.

CRÉDITOS

Luis Almagro
Secretaria Geral da
Organização dos Estados Americanos

Luis Oliveira
Secretaria da Organização Multidimensional de
Segurança dos Estados Americanos

Alison August Treppel
Secretário Executivo
Comitê Interamericano contra o Terrorismo
Organização dos Estados Americanos

Equipe Técnica da Organização dos Estados Americanos
Kerry-Ann Barrett
Orlando Garcés
David Moreno
Mariana Cardona

Equipe Técnica da CISCO
Rebeca De La Vega
Mario De La Cruz
Ned Cabot
Frederico Vasconcelos
Vinita Venugopal

ÍNDICE

LISTA DE CARTÕES

LISTA DE TABELAS

INTRODUÇÃO

A América Latina e o Caribe continuam a maximizar os benefícios trazidos pelo uso das Tecnologias de Informação e Comunicação (TICs), pois são ferramentas poderosas que ajudam a transformar a vida de cada um de seus cidadãos. A criação de mais e melhor infra-estrutura que permite o acesso à Internet tem um impacto direto sobre o desenvolvimento econômico e social da região. É por isso que **os países da região devem elevar os níveis de confiança digital.**

Devido ao grande aumento das ameaças cibernéticas, os esforços para melhorar a capacidade de segurança cibernética têm crescido substancialmente na região. Entretanto, uma área que continua a ficar para trás é o desenvolvimento da força de trabalho de segurança cibernética. Ou seja, há uma escassez de pessoal treinado e qualificado no mercado de trabalho para trabalhar em funções de segurança cibernética que possam enfrentar essas ameaças e seus riscos relacionados.

As habilidades de cibersegurança podem ser adquiridas, alteradas e melhoradas **através da educação, treinamento ou coaching,** tornando a força de trabalho de cibersegurança um pool de talentos em evolução que as organizações públicas e privadas da região devem desenvolver e manter.

A escassez de profissionais e habilidades em segurança cibernética é uma questão política multidimensional que envolve múltiplas partes interessadas (setor público, setor privado, academia e sociedade civil) e é agravada por muitos fatores. Evitar os desafios relacionados a esta escassez colocaria problemas tanto para o desenvolvimento econômico quanto para a segurança nacional dos países da região da ALC.

luz do acima exposto, este documento apresenta uma **análise detalhada do mercado de trabalho de cibersegurança e sua força de trabalho na região** sob o atual contexto de cibersegurança, identificando uma questão que pode ser explicada por desafios que precisam ser abordados de forma abrangente por múltiplas partes interessadas, de acordo com as melhores práticas internacionais. A pesquisa envolveu uma revisão da literatura acadêmica e cinzenta, bem como outros materiais produzidos pelos governos e outras organizações para compreender as habilidades da força de trabalho de cibersegurança e a lacuna profissional.

Este documento está dividido em cinco (5) capítulos, sendo este o primeiro capítulo. O segundo capítulo apresenta o contexto atual de cibersegurança e identifica fatores que afetam o mercado de trabalho de cibersegurança e sua força de trabalho. O terceiro capítulo fornece uma descrição esquemática deste mercado de trabalho e das condições que o afetam tanto do lado da oferta quanto do lado da demanda de mão-de-obra, caracterizando a força de trabalho atual. Além disso, ele descreve o problema principal e identifica uma combinação única de desafios enfrentados pelo mercado de trabalho no contexto atual. O quarto capítulo propõe uma solução multi-stakeholder para ações que promovam o desenvolvimento da força de trabalho e resolvam o problema identificado. Finalmente, o quinto capítulo apresenta as referências bibliográficas consultadas.

SEGURANÇA CIBERNÉTICA NO CONTEXTO ATUAL

O desenvolvimento de uma economia digital contribui positivamente para a geração de prosperidade econômica e social nos países da região da América Latina e Caribe. Isto requer a construção de um ambiente digital seguro e confiável, em linha com a multiplicação das atividades digitais de governos, organizações e cidadãos. Atualmente, muitos dos desafios enfrentados pela economia digital se devem em grande parte à dependência da Internet e seu rápido crescimento tanto em usuários quanto em aplicações.

Esta situação exige que a região tenha capacidades suficientes para o gerenciamento adequado e oportuno dos riscos inerentes à cibersegurança, de modo que, embora haja um maior nível de exposição a riscos devido ao uso crescente do ambiente digital, as ações que são tomadas reduzem os incidentes digitais para evitar conseqüências econômicas ou sociais derivadas de ameaças cibernéticas, ataques e incidentes que deterioram a confiança digital e retardam a adaptação ao futuro digital. Respondendo adequadamente aos desafios atuais da cibersegurança, é possível aproveitar ao máximo a transformação digital e capitalizar novas oportunidades para indivíduos, organizações e a sociedade como um todo.

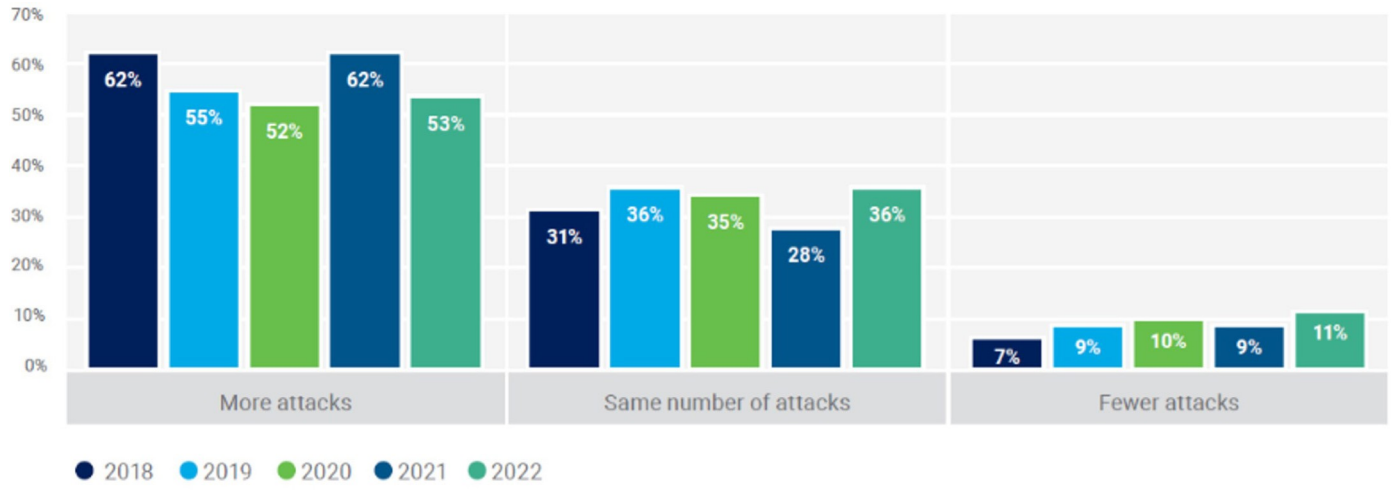
A situação econômica na América Latina e no Caribe nos últimos 3 anos tem sido complexa devido à pandemia da COVID-19. As restrições e outras intervenções de saúde pública implementadas para reduzir o contágio tiveram um forte impacto sobre a economia da região. Organizações e cidadãos mudaram-se em massa para canais online e digitais para contornar medidas de distanciamento social, continuar as operações comerciais, assegurar fluxos de receita e permanecer solventes durante a pandemia (BID, CEPAL & KAS, 2021). Entretanto, alguns setores econômicos, como o setor de TIC, experimentaram não apenas aumentos nas horas trabalhadas, mas também crescimento no emprego em comparação com os anos pré-pandêmicos (OCDE, 2021).

As organizações, especialmente as PME[8] da região, enfrentaram apressados processos de digitalização e transformação digital. Entretanto, a falta de habilidades digitais tornou-se um desafio transversal para este segmento empresarial e surgiu como um obstáculo-chave para abordar estes processos. Muitas dessas organizações carecem de uma cultura digital tanto no nível estratégico quanto operacional, onde os benefícios potenciais da digitalização são muitas vezes desconhecidos ou não totalmente compreendidos.

8 As PMEs compreendem 99,5% das empresas da região ALC (com quase 9 em cada 10 classificadas como microempresas) e geram 60% do emprego produtivo formal. Entretanto, as PMEs latino-americanas têm uma lacuna de produtividade particularmente significativa, representando apenas um quarto do valor total da produção da região (OCDE, 2022).

Há uma crescente expansão do cenário de ameaça e risco globalmente e na região da América Latina e Caribe. Como a dependência das tecnologias digitais continua a aumentar, o mesmo acontece com o crime cibernético. Os criminosos cibernéticos estão aproveitando todas as oportunidades para explorar vulnerabilidades contra pessoas e organizações através da tecnologia, adaptando rapidamente novas tecnologias e seus ataques usando novos métodos e cooperando estreitamente uns com os outros (WEF, 2022). De acordo com (ISACA, 2022), durante 2018 e 2022, entre 52% e 62% das organizações perceberam que receberam mais ataques[9] do que no ano imediatamente anterior.

Gráfico 1.
Comparação ano a ano dos relatórios de ataques de segurança cibernética



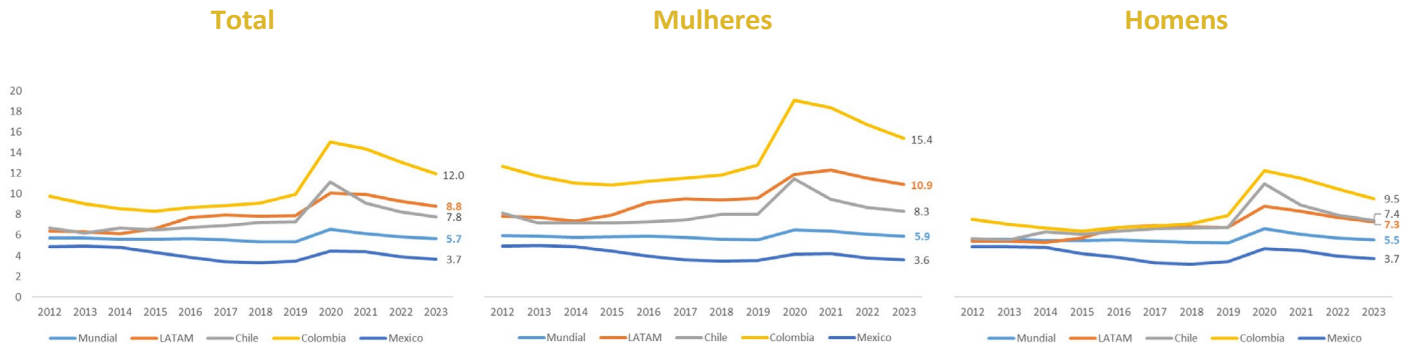
Fonte: (ISACA, 2022)

Os mercados de trabalho estão em um período de profunda transformação. Empregos e habilidades foram afetados pel a automaçao[10] , transformação da indústria e transição ecológica, coincidindo com mudanças nas práticas de trabalho que antes pareciam impossíveis[11]. Em particular, o papel da tecnologia cresceu
exponencialmente em todos os setores da economia, gerando novas ocupações e mudando as tarefas que os seres humanos desempenham e as habilidades de que necessitam para fazer seu caminho no mercado de trabalho (BID, 2021). Entretanto, a tecnologia pode gerar desemprego tecnológico e aumentar tanto a desigualdade quanto a polarização na região se os governos, organizações e indivíduos não responderem adequadamente (BID, 2020).

9 De acordo com (WEF, 2022), o resgate, a engenharia social e a atividade maliciosa de infiltrados são os três principais ataques cibernéticos com os quais as organizações estão mais preocupadas. Enquanto as falhas na infra-estrutura devido a ataques cibernéticos, roubo de identidade e resgate são os três principais ataques cibernéticos com os quais os líderes cibernéticos estão mais preocupados.
10 Quase metade (48%) dos entrevistados do Cyber Outlook do Fórum Econômico Mundial dizem que a automação e o aprendizado de máquinas introduzirão a maior transformação em segurança cibernética no futuro próximo (WEF, 2022).
11 https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/a-new-vision-for-jobs

Gráfico 2.

Evolução e projeção da taxa de desemprego na América Latina

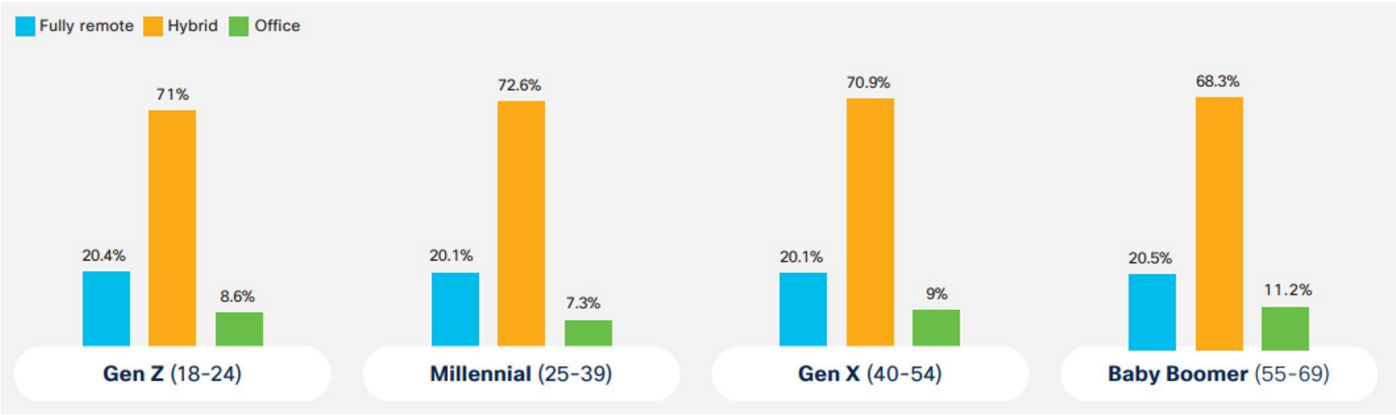


Fonte: Elaboração própria baseada em (OIT, 2022).

Houve mudanças importantes na forma de trabalho das organizações na região. De acordo com (MichaelPage, 2022), menos de 20% das organizações na América Latina e no Caribe atualmente continuam a trabalhar exclusivamente de casa, 37,5% voltaram ao modelo presencial e 44,3% dizem estar trabalhando em modo híbrido ou misto. De acordo com (WEF, 2022), 28% dos executivos organizacionais estimam que o ambiente de trabalho remoto/híbrido será uma das maiores influências na transformação da segurança cibernética nos próximos dois anos.

Gráfico 3.

Preferências de local de trabalho por geração



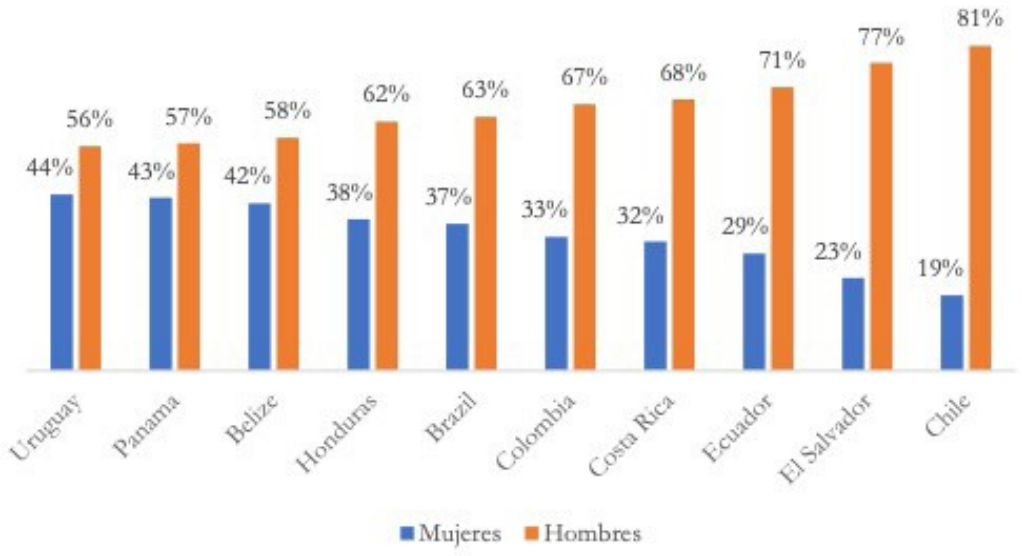
Fonte: (CISCO, 2022)

Em algumas regiões do mundo, fenômenos como *a Grande Resignação ou a Grande Renúncia*[12] *ou a Renúncia Silenciosa*[13] estão sendo experimentados. Um grande número de pessoas optando por deixar seus empregos em busca de papéis mais preenchidos com maior flexibilidade tem levado a um número recorde de vagas e escassez de pessoal em alguns setores[14]. Na esteira deste fenômeno, organizações globais estão reexaminando estratégias empresariais, modelos de força de trabalho, valores e cultura, freqüentemente guiadas por novas demandas dos próprios funcionários (LinkedIn, 2022).

O progresso na paridade de gênero na participação no trabalho foi revertido com importantes conseqüências para outras dimensões do emprego e na distribuição do trabalho não remunerado, afetando a forma como as mulheres acessam oportunidades na esfera econômica, bem como em outras esferas da vida. A brecha geral de gênero em 2022 foi fechada em 68,1%. Outro exemplo é que as mulheres estão sub-representadas nos mercados de trabalho relacionados aos campos STEM[15] e a brecha de gênero é mais prevalente no setor das TIC[16]. A América Latina e o Caribe fecharão sua brecha de gênero em aproximadamente 67 anos (WEF, 2022).

Gráfico 4.

Porcentagem de homens/mulheres formados no ensino superior dos programas STEM na América Latina



Fonte: Elaboração própria baseada em informações apresentadas em (WEF, 2022).

12 De acordo com (MERCER, 2022), a Grande Demissão certamente intensificou o foco na retenção dentro das organizações, que é uma das principais solicitações dos CEOs para seus líderes de RH este ano. Curiosamente, as razões dos funcionários para permanecerem em sua empresa não diferem muito por país e por indústria, mas diferem por geração. Os funcionários da Geração Z dão mais valor aos líderes inspiracionais, mas não aos salários competitivos. Para os Baby Boomers, as políticas de férias/tempo livre são a segunda razão pela qual eles permaneceram. A segurança no emprego é a número um em todos os grupos geracionais da força de trabalho.

13 Durante 2022, surgiu uma nova tendência no mercado de trabalho chamada Quiet Quitting, que consiste em rejeitar a noção de que o trabalho tem que tomar conta da vida e que os empregados devem ir além do que suas descrições de trabalho implicam.

14 https://www.weforum.org/agenda/2022/02/great-reshuffle-jobs-market-resignation/

15 O termo STEM é um acrônimo para Ciência, Tecnologia, Engenharia e Matemática.

16 A porcentagem de mulheres formadas em TIC no mundo inteiro é de 1,7%, comparada a 8,2% de homens formados (WEF, 2022).

O ritmo acelerado da digitalização e a mudança de hábitos de trabalho está impulsionando a resiliência cibernética[17]. Os executivos estão planejando melhorar a resiliência cibernética em suas organizações, fortalecendo as políticas, processos e padrões de resiliência sobre como engajar e gerenciar terceiros (WEF, 2022). Isto não está acontecendo apenas em organizações privadas, mas também no setor público.

Neste contexto, os países da América Latina e do Caribe têm adotado e implementado políticas e estratégias nacionais de cibersegurança[18] **,** no âmbito das quais estão desenvolvendo ações destinadas a gerar um ambiente digital mais confiável e adequado para alcançar seus objetivos de desenvolvimento econômico e social, para o qual a formulação e implementação de iniciativas para fomentar o desenvolvimento das capacidades das organizações e dos cidadãos para gerenciar os riscos da cibersegurança é particularmente importante.

De acordo com as melhores práticas[19] **, as políticas e estratégias nacionais na região abordam questões relacionadas ao treinamento e à conscientização sobre cibersegurança para entidades governamentais, cidadãos, empresas e outras organizações, que são** fundamentais para viabilizar a economia digital na região. As boas práticas incluem o estabelecimento de currículos e programas de conscientização sobre cibersegurança, a expansão de currículos de treinamento e programas de treinamento vocacional, a adoção de esquemas internacionais de certificação e a promoção de clusters de inovação e pesquisa e desenvolvimento (P&D). Por exemplo, várias iniciativas se destacam:

A *A Política Nacional de Confiança e Segurança Digital da Colômbia* (2020-2022)[20] estabelece como um de seus três objetivos específicos fortalecer as capacidades de segurança digital dos cidadãos, do setor público e do setor privado a fim de aumentar a confiança digital no país através da formulação de estratégias e ações para a formação profissional e o desenvolvimento de competências sob uma abordagem diferencial e inclusiva.

B A *Política Nacional de Segurança Cibernética do Chile (*2017-2022)[21] estabelece como um de seus cinco objetivos desenvolver uma cultura de segurança cibernética em torno da educação, boas práticas e responsabilidade no manuseio de tecnologias digitais através da implementação de iniciativas que promovam e desenvolvam uma cultura digital consciente, competente, informada e responsável que inclua todos os atores relevantes.

C A *Estratégia Nacional de Segurança Cibernética do México (*2017-2021)[22] estabelece como um de seus cinco eixos transversais o desenvolvimento de capacidades através do estabelecimento de ações destinadas a gerar e fortalecer as capacidades organizacionais, o capital humano e os recursos tecnológicos em segurança cibernética, o que permitirá que a sociedade, a academia, o setor privado e as instituições públicas tenham os recursos para gerenciar riscos e ameaças no ciberespaço, bem como para aumentar a resiliência nacional.

17 (WEF, 2022) define a resiliência cibernética como *"a capacidade de uma organização de transcender (antecipar, resistir, recuperar e adaptar-se a) qualquer estresse, falha, perigo e ameaça a seus recursos cibernéticos dentro da organização e seu ecossistema, de modo que a organização possa cumprir com confiança sua missão, possibilitar sua cultura e manter sua forma desejada de operar".*

18 Atualmente, um total de dezessete (17) Estados membros da Organização dos Estados Americanos (OEA) aprovaram suas políticas/estratégias nacionais de cibersegurança (OEA & GPD, 2022) e 14 deles puderam fazê-lo com o apoio técnico da OEA.

19 O *Guia* da União Internacional de Telecomunicações (UIT) *para o Desenvolvimento de uma Estratégia Nacional de Segurança Cibernética* apresenta as boas práticas nesta área (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/NCS%20Guide_s.pdf).

20 A Política Nacional de Confiança e Segurança Digital da Colômbia foi emitida através do Documento CONPES 3995 de 2020 (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf).

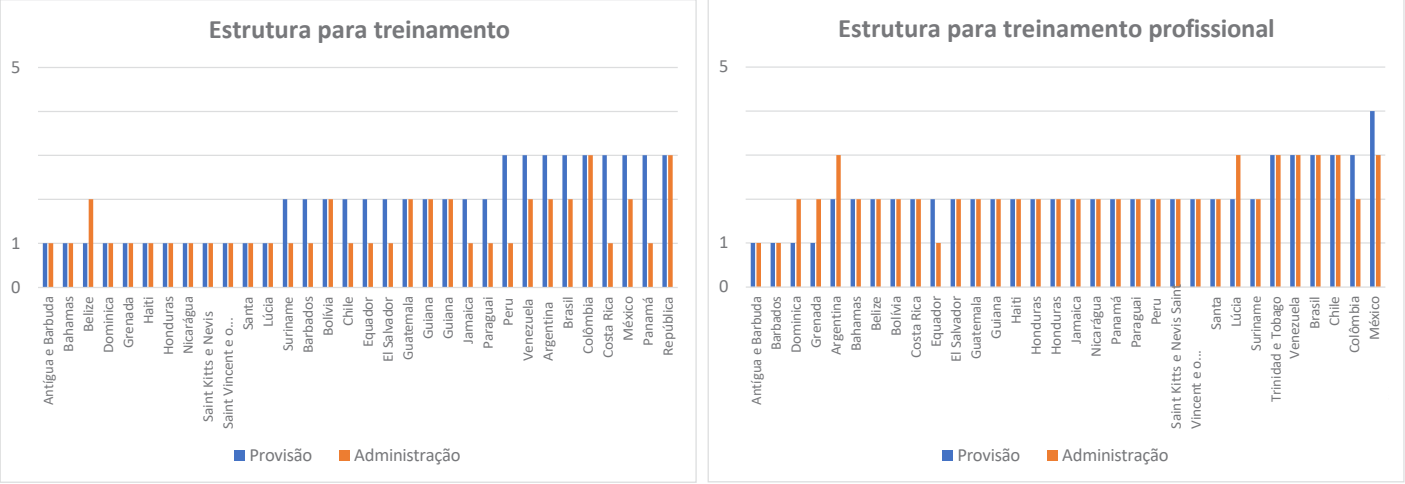
21 https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf

22 https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

Entretanto, tais iniciativas estratégicas relacionadas com o mercado de trabalho cibersegurança levarão anos ou mesmo décadas para amadurecer. De acordo com (OAS & GPD, 2022), levará muitos anos para desenvolver uma força de trabalho com conhecimento digital e habilidades voltadas para uma economia do conhecimento, devido às altas taxas de desgaste no setor público para empregos de cibersegurança e baixos índices de disponibilidade de oportunidades educacionais específicas na área. Por esta razão, os países da região devem priorizar as iniciativas de desenvolvimento da força de trabalho para alocar orçamento a fim de implementar programas o mais rápido possível.

Gráfico 5.

Nível de maturidade de habilidades na América Latina e no Caribe em relação à educação e treinamento vocacional



Fonte: Elaboração própria baseada em (OEA & BID, 2020).

Entretanto, o aumento da demanda por profissionais de cibersegurança[23] é acompanhado por um forte aumento nos salários[24] e alta competição entre profissionais qualificados. Neste tipo de mercado de trabalho, a curto prazo, a oferta de profissionais de segurança cibernética não responde a salários mais altos, pois leva tempo para treinar trabalhadores adicionais com as habilidades necessárias. Os esforços de treinamento e educação podem levar anos, mesmo que os trabalhadores individuais em outras ocupações, setores ou indústrias tenham o conjunto certo de habilidades para se tornarem profissionais de segurança cibernética, eles não podem mudar de ocupação imediatamente.

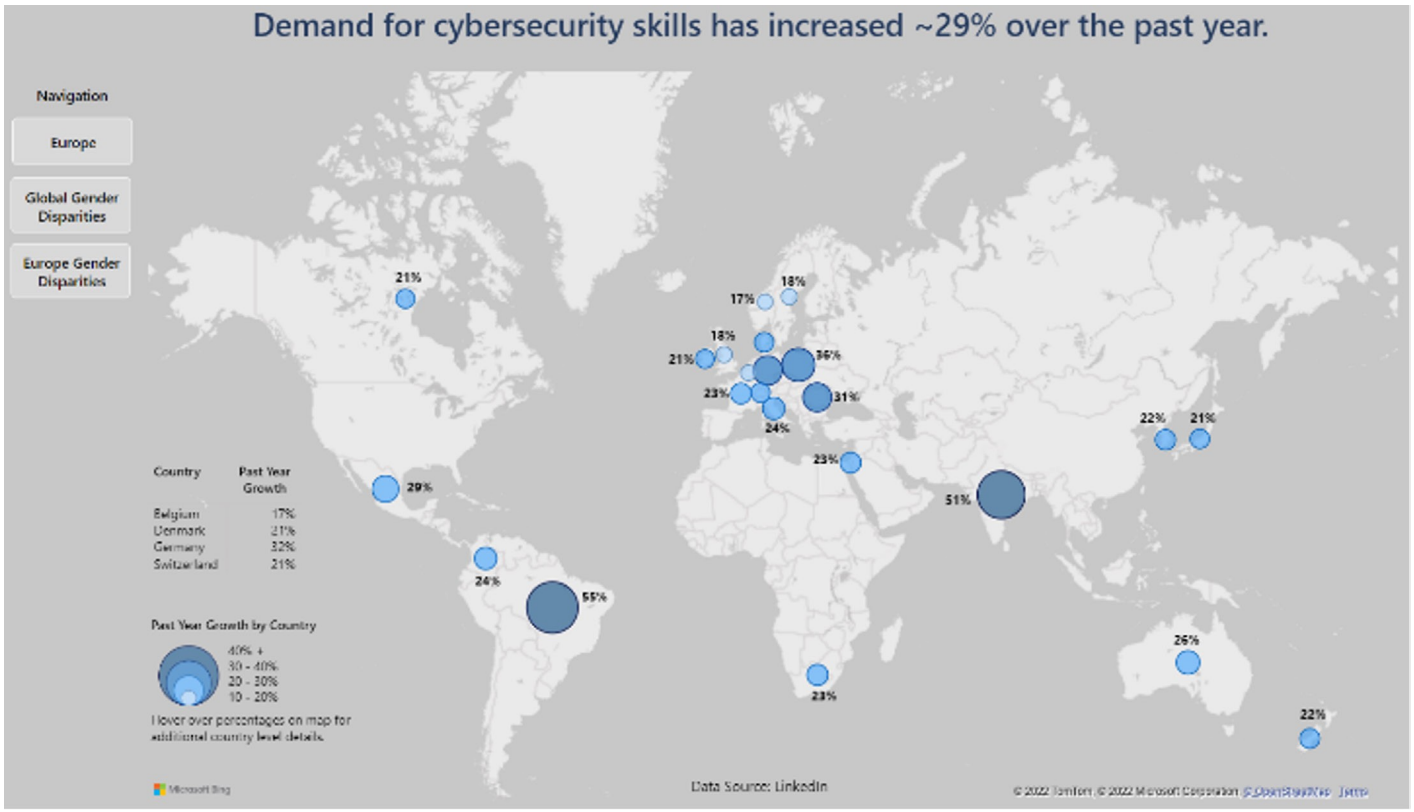
23 Aumento devido ao aumento da conectividade, maior vulnerabilidade e crescimento do crime cibernético, juntamente com choques exógenos ao mercado devido à pandemia da COVID-19.

24 De acordo com (DCMS & IPSOS, 2022), empregadores e equipes cibernéticas no Reino Unido continuam a sentir o impacto da pandemia. Em particular, isto pode ter levado a salários de mercado mais altos fora de Londres e do Sudeste, apresentando desafios para empregadores regionais menores.

Esta situação no mercado de trabalho de cibersegurança da região cria uma lacuna (escassez) na força de trabalho a curto prazo. De acordo com (ISC, 2021) e (ISC, 2022a), há uma escassez de entre 515.000 e 701.000 trabalhadores cibernéticos qualificados na região da ALC. De acordo com este estudo, a falta de mão-de-obra continua sendo a principal barreira para atender as necessidades de segurança das organizações, descobrindo que 60% dos entrevistados relatam que a falta de mão-de-obra ciber-segurança está colocando suas organizações em risco[25].

Mas não é apenas a escassez de talentos que cria riscos nas organizações, mas também a escassez de habilidades[26] na força de trabalho. Por exemplo, 59% de todos os entrevistados da pesquisa *Global Cybersecurity Outlook* 2022 responderam que teriam dificuldade em responder a um incidente de cibersegurança em suas organizações devido à escassez de habilidades dentro de sua equipe (WEF, 2022).

Gráfico 6.
Aumento da demanda por cybersecurity skills



Fonte: (MICROSOFT, 2022)

25 (ISC2, 2021) confirma, da perspectiva da força de trabalho cibersegurança global, que quando a força de trabalho cibersegurança é pequena, as conseqüências negativas são reais: sistemas mal configurados, ciclos de remendos lentos, implementações apressadas, tempo insuficiente para uma avaliação de risco adequada, supervisão insuficiente dos processos e procedimentos, e muito mais.

26 De acordo com a National Initiative for Cybersecurity Education (NICE) *Cybersecurity Personnel Framework of the US National* Institute of Standards and Technology (NIST), entende-se que as habilidades representam uma combinação de habilidades, conhecimento e experiência que permitem a um indivíduo completar bem uma tarefa em uma função de cibersegurança em uma organização.

Esta situação tem gerado fortes pressões sobre as organizações públicas e provadas[27] , pois elas devem, por um lado, identificar, atrair e recrutar os melhores talentos disponíveis e, por outro lado, retê-los implementando, entre outras, estratégias inovadoras de treinamento e coaching, como por exemplo:

i) *Capacitação* (processos de aprendizagem de novas habilidades ou de ensino de novas habilidades aos funcionários),

ii) *Requalificação* (processos de treinamento de funcionários em um conjunto completamente novo de habilidades para prepará-los para assumir um papel diferente dentro da empresa), e iii) *Novas habilidades* (processos de aprendizagem contínua para ajudar a desenvolver habilidades de alta demanda, quer um indivíduo esteja tentando atualizar as habilidades atuais ou precise de uma atualização completa para desenvolver habilidades completamente novas). Da mesma forma, incentivando programas de aprendizagem baseados no trabalho, incluindo aprendizados e estágios.

Estes problemas nas organizações podem potencialmente minar a segurança cibernética das nações e da região. Esta situação significa, portanto, que os múltiplos atores do ecossistema de cibersegurança que têm influência no desenvolvimento destes mercados de trabalho enfrentam uma combinação única de desafios que os países da América Latina e do Caribe devem enfrentar.

27 De acordo com (DCMS & IPSOS, 2022), especificamente no setor cibernético britânico, há evidência de um mercado de trabalho mais desafiador do ponto de vista do empregador. Mais da metade das empresas do setor cibernético (53%) tentaram contratar alguém nos 18 meses anteriores. De todas as vagas abertas durante este período, 44% das empresas foram relatadas como difíceis de preencher (comparado com 37% em 2021 e 35% em 2020). A razão mais comum dada para as vagas difíceis de preencher continua sendo a falta de habilidades técnicas e conhecimento dos candidatos (43% dos empregadores com vagas difíceis de preencher). Este ano, as menções à competência de outros empregadores aumentaram (de 9% em 2021 para 25% em 2022), e mais pessoas agora também mencionam uma falta geral de candidatos (de 13% para 25%).

O MERCADO DE TRABALHO DE CIBERSEGURANÇA ENFRENTA UMA COMBINAÇÃO ÚNICA DE DESAFIOS

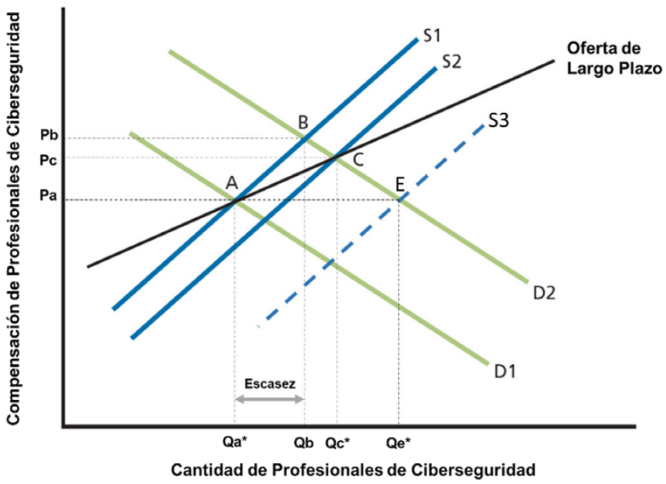
A análise dos desafios enfrentados pelo mercado de trabalho de cibersegurança ajuda os países a estarem preparados para conflitos no ciberespaço e as organizações a identificarem as principais lacunas na força de trabalho atual que podem ter impacto na realização dos objetivos empresariais e setoriais. As análises a seguir analisam este mercado de trabalho, fornecem uma caracterização geral e esquemática da oferta e demanda de trabalho cibersegurança, descrevem a força de trabalho cibersegurança e identificam uma questão e um conjunto de desafios que precisam ser abordados de forma abrangente por múltiplas partes interessadas, especialmente na região da América Latina e Caribe.

3.1. O MERCADO DE TRABALHO

De uma perspectiva econômica, o mercado de trabalho cibersegurança segue os mesmos princípios do mercado livre, onde se aplica a regra da oferta e da demanda. O mercado de trabalho é o lugar onde a oferta e a demanda de empregos se encontram, onde os trabalhadores ou a mão-de-obra fornecem os serviços exigidos pelos empregadores.

A figura abaixo apresenta uma visão simplificada do mercado de trabalho de cibersegurança. No passado recente, a oferta e a demanda foram atendidas no ponto A (vários profissionais de Qa* com remuneração de Pa). Como ficou evidente, a demanda por profissionais de segurança cibernética aumentou consideravelmente. Este aumento pode ser devido a múltiplos fatores, incluindo maior conectividade, maior digitalização, maior transformação digital, mais atividades econômicas no ambiente digital, aumento das vulnerabilidades, entre outros. Estes eventos empurraram a curva de demanda para a direita, de D1 a D2. O movimento da curva de demanda implica que, como observado no mercado atual, muitos empregadores estão dispostos a pagar mais (Pb) para contratar a mesma qualidade e tipo de profissional que contrataram anteriormente. O aumento da demanda nos últimos anos tem sido ainda mais exacerbado pela pandemia COVID-19, e é necessário tempo para desenvolver mais profissionais de cibersegurança em resposta ao aumento da demanda.

Gráfico 7.
Forças do mercado de trabalho de cybersecurity



Fonte: Adaptado de (RAND, 2014)

O treinamento e a educação podem levar anos para criar outra situação de equilíbrio no mercado de trabalho ciber-segurança. Mesmo que os trabalhadores individuais em outras ocupações e setores tenham o conjunto certo de habilidades para se tornarem profissionais de segurança cibernética, eles não podem mudar de ocupação ou setores imediatamente. Portanto, no curto prazo, a curva da oferta é bastante inelástica ou, em outras palavras, pouco responsiva ao preço. Esta situação também leva à escassez de profissionais, por exemplo (ISC, 2021) e (ISC, 2022a) estimam uma escassez entre 515.000 e 701.000 profissionais para a região da ALC. O ponto B pode ser visto como um equilíbrio de curto prazo e, a longo prazo, o mercado deve alcançar um novo equilíbrio no ponto C (um número de profissionais Qc* com uma compensação Pc).

Como mostrado na figura acima, a curva de fornecimento de longo prazo provavelmente será mais elástica (mais sensível ao preço) do que as curvas de fornecimento de curto prazo, porque é mais fácil para as pessoas entrarem e saírem de uma profissão a longo prazo. Por exemplo, um novo equilíbrio poderia ser encontrado no ponto E (um Qe* de quantidade com um Pa de compensação) quando a curva de fornecimento se move para a direita de S2 a S3, com mais profissionais ciber-segurança no mercado com menor compensação. Entretanto, os movimentos das curvas de oferta e demanda de mão-de-obra, juntamente com os efeitos sobre as lacunas e preços, dependem das ações tomadas por todos os múltiplos atores envolvidos no mercado de trabalho de cibersegurança.

A figura a seguir mostra uma caracterização geral e esquemática da oferta e demanda de mão-de-obra em ciber-segurança na região. Por um lado, a oferta de mão-de-obra é composta de: i) recém-formados, ii) profissionais de outros setores ou indústrias que podem ter experiência em tecnologia, e iii) aqueles que não têm formação técnica, mas possuem outras habilidades que podem ser aplicadas em um trabalho relacionado à ciber-segurança[28].

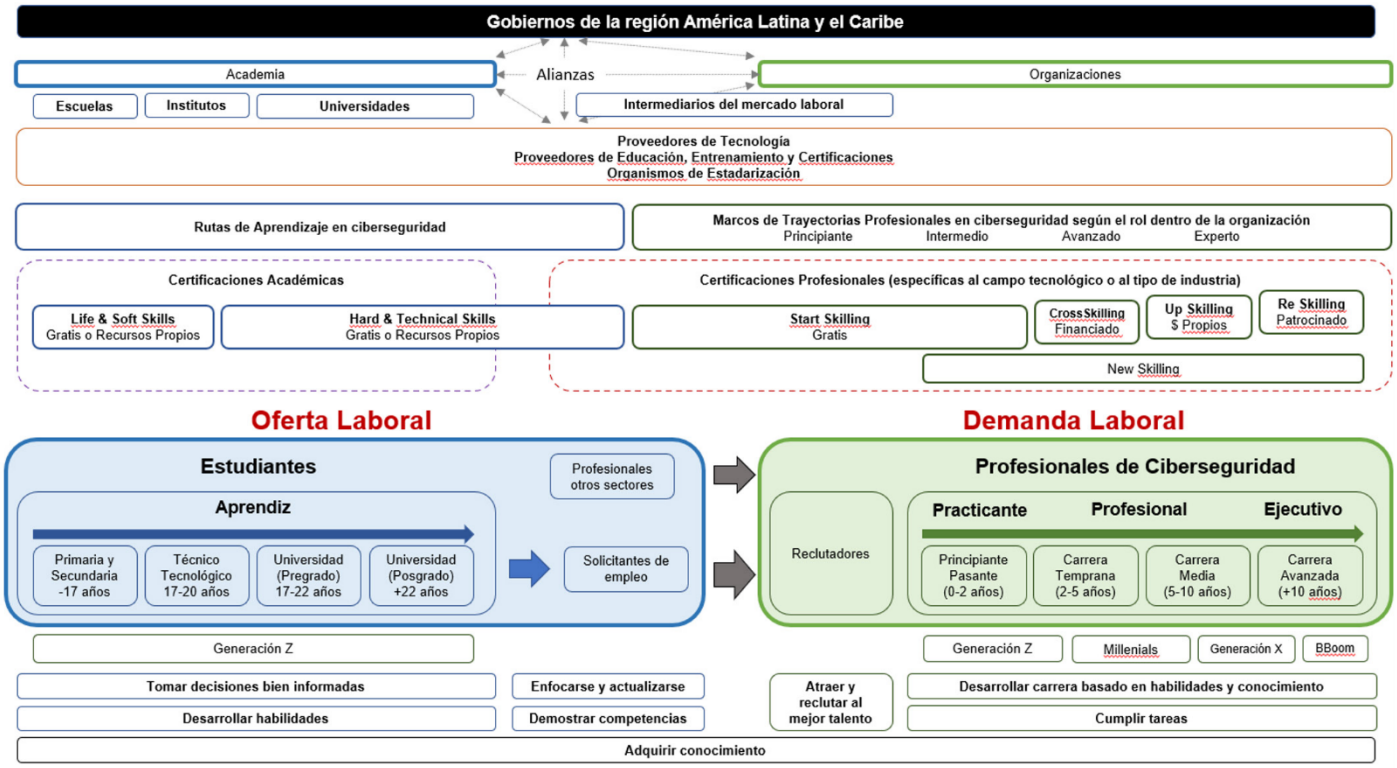
Também é importante considerar os estudantes atuais, que estão nos níveis primário, secundário e terciário dos sistemas educacionais da região. Alguns estão até nos níveis de pós-graduação. Em geral, estes estudantes pertencem à Geração Z ou *"Centenialls"*[29], pessoas que têm características diferentes das gerações anteriores porque nasceram sob novas normas, diretrizes e conceitos que correspondem ao mundo digital.

Estes estudantes devem desenvolver habilidades e tomar decisões bem informadas, enquanto os que procuram emprego devem demonstrar competência, foco e auto-aperfeiçoamento.

28 De acordo com (CSES, 2018), do lado da oferta de mão-de-obra há pelo menos seis caminhos para empregos de cibersegurança de nível básico: i) rota de aprendizagem (secundária com know-how),
ii) caminho da educação continuada (secundária com certificações), iii) primeiro caminho da formação STEM (graduação), iv) primeiro caminho da formação não-STEM (graduação), v) caminho da formação superior (pós-graduação), e vi) caminho da mudança de carreira.

29 Pessoas nascidas entre 1997 e 2010.

Gráfico 8.
Caracterização esquemática da oferta e demanda de mão de obra de cibersegurança na região



Fonte: Elaboração própria

O ator mais representativo e de maior impacto na oferta de mão-de-obra é a Academia, em particular escolas, faculdades e universidades. Dado que o estudante (futuro candidato a emprego) é o *vendedor* no mercado de trabalho de segurança cibernética, cujo valor é determinado pelas habilidades que ele possui, é muito importante que as instituições que representam a academia lhe dêem a oportunidade de desenvolver uma ampla gama de habilidades (habilidades para a vida, habilidades brandas, habilidades técnicas e habilidades duras) para entrar no campo cibernético.

Por outro lado, a demanda de mão-de-obra é representada por organizações que exigem profissionais de cibersegurança, que podem ser classificados como aprendizes ou estagiários[30] , profissionais e executivos, dependendo de há quanto tempo fazem parte da força de trabalho. Por exemplo, os estagiários geralmente
pertencem à Geração Z, os profissionais podem ser formados por pessoas pertencentes à Geração Z, Geração Y ou Millenials[31] ou Geração X[32] , e finalmente os executivos podem ser pessoas pertencentes à Geração X ou *Baby Boomers*[33].
Os profissionais da Cibersegurança na força de trabalho devem cumprir tarefas e desenvolver uma carreira baseada em habilidades e conhecimentos.

30 Segundo (DCMS & IPSOS, 2022), cerca de 1 em cada 3 empresas cibernéticas (27%) no Reino Unido relataram ter oferecido estágios ou colocações de trabalho desde o início de 2020 (aproximadamente por um período de 18 meses).
31 Pessoas nascidas entre 1981 e 1996, chamadas de nativos digitais e a primeira geração que é verdadeiramente global porque compartilham os mesmos valores em todos os países, graças à globalização e à conexão através da Internet.
32 Pessoas nascidas entre 1965 e 1980, que se adaptaram muito facilmente à chegada da Internet em suas vidas e ao desenvolvimento tecnológico subseqüente.
33 Pessoas nascidas entre 1946 e 1964, que tiveram que se adaptar às novas tecnologias e são, portanto, consideradas imigrantes digitais.

Os atores mais representativos com impacto na demanda de mão-de-obra são organizações públicas e privadas em todos os setores econômicos, que têm áreas de recursos humanos encarregadas de identificar, atrair e recrutar talentos. O *comprador do* mercado de trabalho representa o setor empregador, seja ele privado ou público, e entra no mercado de trabalho com a intenção de adquirir o serviço de uma pessoa que possa realizar as tarefas exigidas.

Finalmente, existem intermediários do mercado de trabalho, tais como agências de recrutamento e até mesmo plataformas de redes profissionais. Além disso, existem Provedores de Educação, Treinamento e Certificação e Provedores de Tecnologia que oferecem ferramentas, recursos e conteúdos para desenvolver habilidades tanto para estudantes quanto para profissionais, seja através de caminhos de aprendizado ou através de estruturas de carreira, concedendo certificações que podem ser acadêmicas[34] ou profissionais[35] , esta última específica para o campo tecnológico ou tipo de indústria[36.] Com o apoio desses provedores, as organizações podem implementar esquemas de *crosskilling, upskilling, reskilling* e *novas habilidades*, entre outros, a fim de reter e manter sua força de trabalho cibernética de segurança.

3.2. A FORÇA DE TRABALHO

De acordo com a Iniciativa Nacional de Educação em Segurança Cibernética (NICE*)* Iniciativa Nacional de Educação em Segurança Cibernética (NICE) Quadro de *Força de Trabalho em Segurança Cibernética*[37], a força de trabalho em segurança cibernética pode ser considerada como o conjunto de pessoas (possuindo conhecimentos e habilidades) para executar tarefas a fim de atingir os objetivos de gerenciamento de risco de segurança cibernética de uma organização. Essas pessoas podem ser internas ou externas à organização[38].

Um exemplo de definição de força de trabalho é fornecido pelo *Cyber Career Pathways Tool*[39] baseado no NICE *Cybersecurity Workforce Framework* e desenvolvido pela National Initiative for Cybersecurity Careers and Studies (NICCS*).* A força de trabalho cibernética é o conjunto de profissionais dentro de uma organização com as habilidades necessárias para: i) construir, proteger, operar, defender e proteger tecnologia, dados e recursos, ii) realizar atividades de inteligência relacionadas, iii) possibilitar operações futuras, e iv) projetar poder no ou através do ciberespaço.

34 As certificações acadêmicas Cybersecurity são projetadas para fornecer aos estudantes um treinamento profundo sobre algumas das questões atuais no campo da cibersegurança. Estes cursos são geralmente combinados com outros cursos e programas de certificação para fornecer aos estudantes as habilidades e a experiência necessárias para iniciar no crescente setor de cibersegurança.

35 As certificações profissionais de cibersegurança são projetadas para indivíduos que já trabalham no campo da cibersegurança (ou campos de TI e redes estreitamente relacionados) para treinar em algumas das mais recentes ferramentas e softwares para detectar, prevenir e combater problemas de cibersegurança. Estas certificações são utilizadas para demonstrar competência com tecnologias específicas.

36 Um roteiro de certificações de segurança cibernética pode ser consultado em: https://pauljerimy.com/security-certification-roadmap/

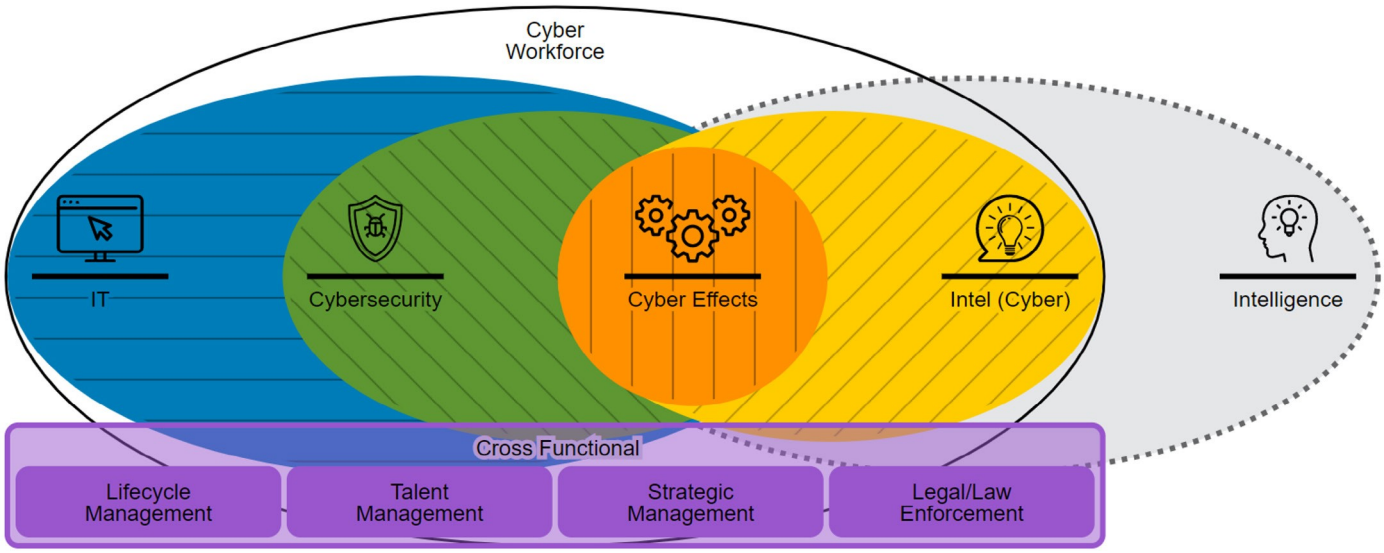
37 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1es.pdf

38 De acordo com (DCMS & IPSOS, 2022), cerca de um terço das empresas no Reino Unido terceirizam qualquer aspecto da segurança cibernética.

39 https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

Gráfico 9.

Representação esquemática da força de trabalho de uma organização e das comunidades de profissionais que a compõem



Fonte: (NICCS, 2022)

De acordo com (NICCS, 2022), a força de trabalho de uma organização pode ser composta pelas seguintes comunidades de profissionais, com habilidades distintas mas complementares:

A *Tecnologia da Informação (TI):* profissionais com habilidades necessárias para projetar, construir, configurar, operar e manter TI, redes e capacidades. Isto inclui ações para priorizar investimentos de portfólio; projetar, adquirir, implementar, avaliar e dispor de TI, bem como a gestão de recursos de informação; e a gestão, armazenamento, transmissão e visualização de dados e informações.

B *Ciber-segurança:* profissionais com habilidades necessárias para proteger, defender e preservar dados, redes, capacidades centradas em rede e outros sistemas designados, assegurando que controles e medidas de segurança apropriados sejam implementados e tomando medidas de defesa interna. Isto inclui o acesso a controles de sistema, monitoramento, gerenciamento e integração da ciber-segurança em todos os aspectos da engenharia e aquisição de capacidades cibernéticas.

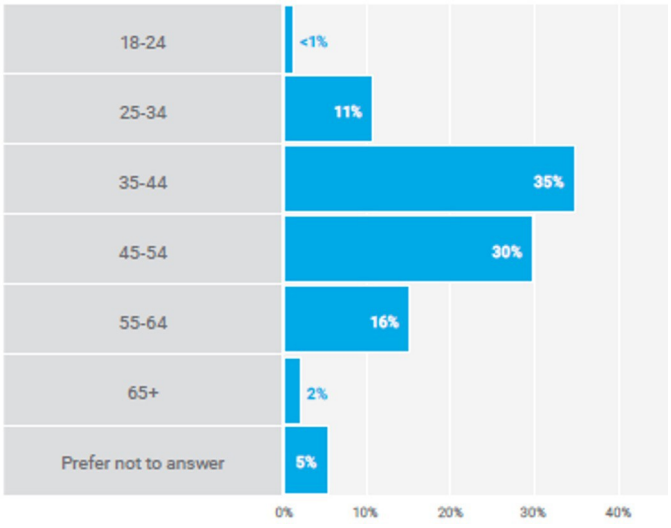
C *Efeitos cibernéticos:* profissionais com habilidades necessárias para planejar, apoiar e executar capacidades cibernéticas onde o objetivo principal é defender externamente ou conduzir projeção de força no ou através do ciberespaço.

D *Inteligência cibernética:* profissionais com habilidades necessárias para coletar, processar, analisar e divulgar informações de todas as fontes de inteligência sobre programas cibernéticos, intenções, capacidades, pesquisa e desenvolvimento e atividades operacionais de atores estrangeiros.

E *Transversal:* profissionais com habilidades necessárias para liderar, adquirir e gerenciar iniciativas cibernéticas; desenvolver o talento da força de trabalho cibernética; e conduzir atividades legais e policiais relacionadas com a cibernética.

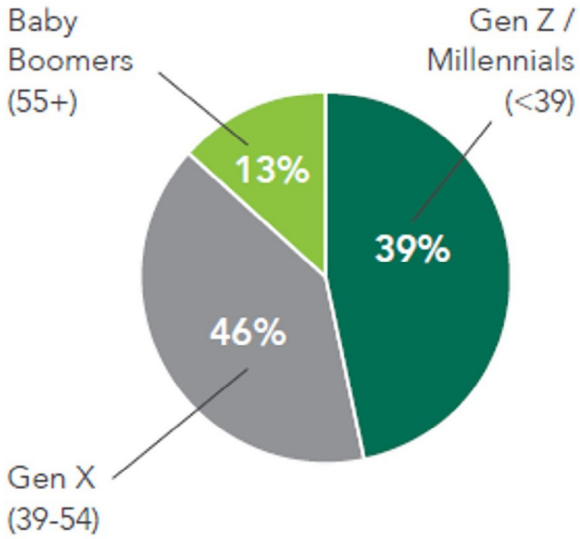
Atualmente, a força de trabalho é composta por profissionais entre 25 e 65[40] anos de idade. Em outras palavras, há diversidade geracional, pois as pessoas pertencem às quatro coortes demográficas (Gerações Z, Y, X e Baby Boomers). Estas quatro gerações de talentos não só devem coexistir dentro das organizações, mas, com suas próprias características e diferenças, devem se entender e se complementar mutuamente.

Gráfico 10.
Força de trabalho por idade



Fonte: (ISACA, 2022)

Gráfico 11.
Representação por gerações



Fonte: (ISACA, 2021)

Atualmente, os principais setores em demanda de profissionais de segurança cibernética são o setor de TIC, o setor financeiro e de seguros e o setor de telecomunicações. O recrutamento no setor público também responde por uma fatia maior do mercado nos últimos anos.

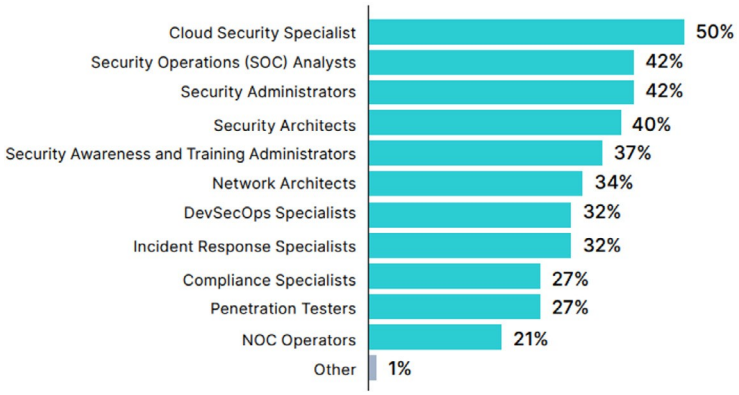
Gráfico 12.
Porcentagem de anúncios de emprego para as principais funções cibernéticas provenientes dede setores específicos no Reino Unido

Nota: De 8.426 anúncios de empregos cibernéticos de janeiro a dezembro de 2021. Fonte: (DCMS & IPSOS, 2022.

40 Observa-se que a maioria (35%) são pessoas com idade entre 35 e 44 anos. Destaca-se que esta situação pode impactar a força de trabalho cibernética de segurança já que, segundo (Cook, 2021), os funcionários entre 30 e 45 anos de idade têm impulsionado o fenômeno da *Grande Demissão*, já que tiveram o maior aumento nas taxas de demissão nos EUA, com um aumento médio de mais de 20% entre 2020 e 2021.

Há uma ampla gama de papéis e especializações de segurança cibernética (especialistas, analistas, entre outros) em demanda no mercado de trabalho[41]. Por exemplo, os seguintes papéis são demandados pelos empregadores no mercado de trabalho de cibersegurança nos EUA: analista de cibersegurança, desenvolvedor de software, consultor de cibersegurança, entre outros.

Gráfico 13.
Principais funções na ciber-segurança em demanda



Fonte: (FORTINET, 2022)

Gráfico 14.
Principais funções na área de cibersegurança em demanda nos Estados Unidos

Nota: A partir de setembro de 2022
Fonte: (CyberSeek, 2022)

Os principais requisitos de habilidades em soft skills nas descrições de cargos de cibersegurança no Reino Unido são: habilidades de comunicação, pensamento criativo, resolução de problemas, trabalho em equipe e atenção aos detalhes. De acordo com (MichaelPage, 2022), as 5 principais soft skills mais exigidas em 2022 na América Latina e no Caribe são: adaptabilidade, pensamento criativo, trabalho em equipe, inteligência emocional e resiliência.

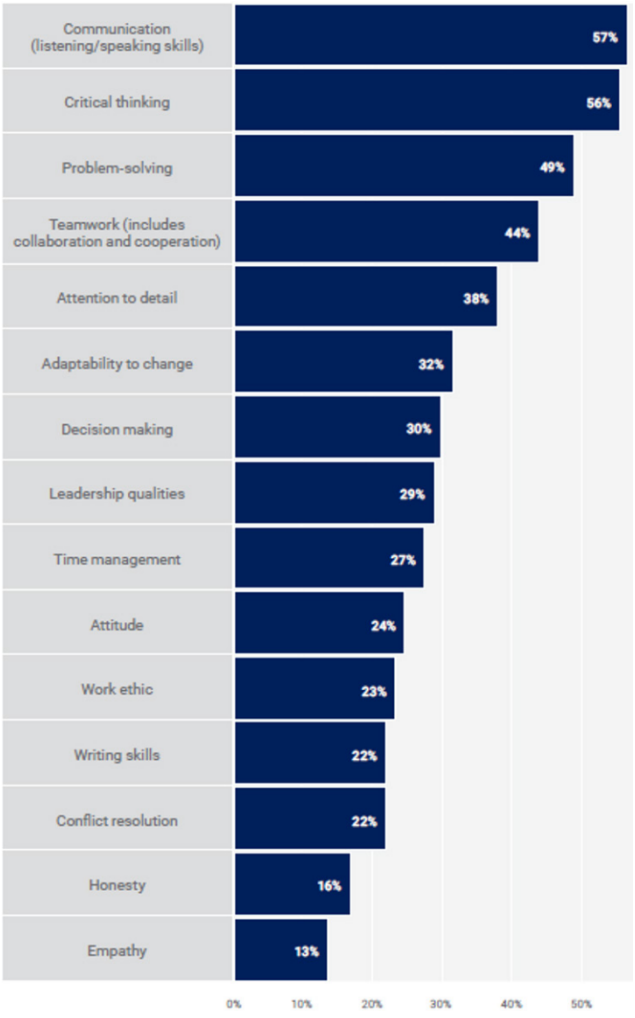
Gráfico 15.
Principais atributos necessários para o pessoal de segurança cibernética

Fonte: (ISC2, 2021)

41 De acordo com (CyberSeek, 2022), há 714.548 vagas de emprego on-line para posições relacionadas à cibersegurança nos Estados Unidos de maio de 2021 a abril de 2022. De acordo com (DCMS & IPSOS, 2022), entre janeiro de 2021 e dezembro de 2021, houve 153.192 vagas de empregos ciber-segurança no Reino Unido.

Gráfico 16.

Principais habilidades de soft skills para funções cibernéticas no setor de segurança cibernética

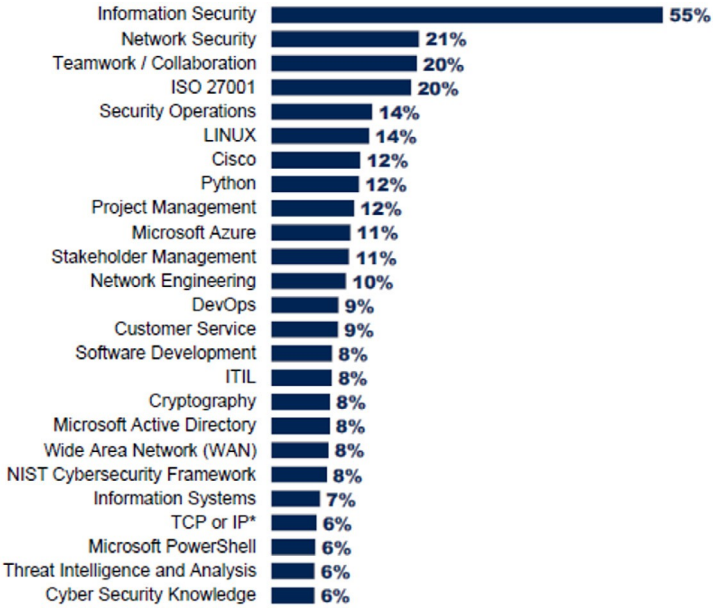


Fonte: (ISACA, 2022)

Os principais requisitos de habilidades técnicas nas descrições de cargos de segurança cibernética no Reino Unido são: habilidades de segurança da informação, habilidades de segurança de rede e habilidades em torno de padrões, tais como ISO 27001 (o padrão internacional de segurança da informação). Outras áreas de habilidades técnicas exigidas aos profissionais de segurança cibernética no mercado de trabalho incluem: computação em nuvem, desenvolvimento, segurança e operações (DevSecOps), gerenciamento de risco e controles técnicos, conhecimento de sistemas operacionais e virtualização, criptografia e programação.

Gráfico 17.

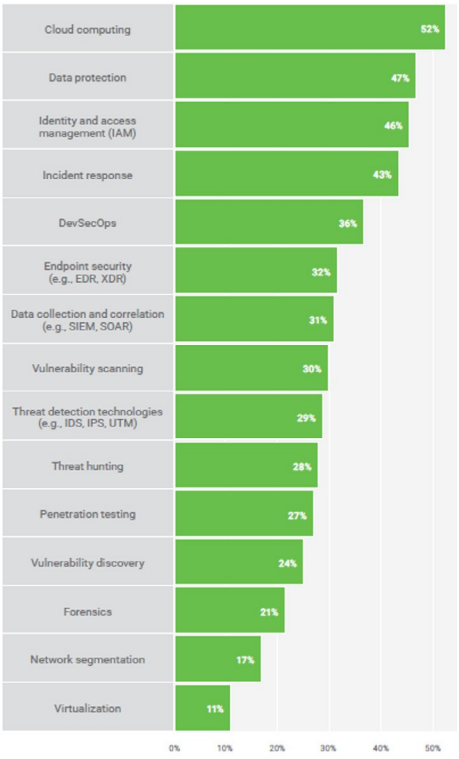
Principais habilidades técnicas em demanda para cargos cibernéticos de topo no Reino Unido



Nota: De 35.103 anúncios de empregos cibernéticos de janeiro a dezembro de 2021 solicitando pelo menos uma habilidade específica.
Fonte: (DCMS & IPSOS, 2022)

Gráfico 18.

Principais habilidades técnicas para funções de trabalho cibernético no setor de segurança cibernética

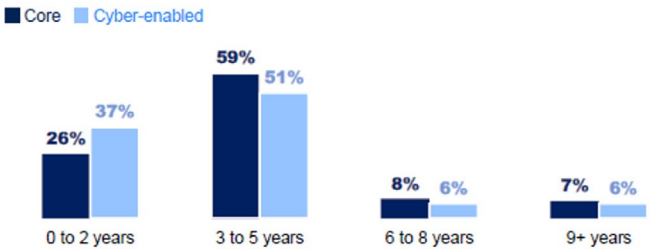


Fonte: (ISACA, 2022)

Nos últimos anos, as organizações têm procurado profissionais para funções de segurança cibernética com 3-5 anos de experiência, seguidos por candidatos a nível básico com um diploma de bacharelado ou equivalente.

Gráfico 19.

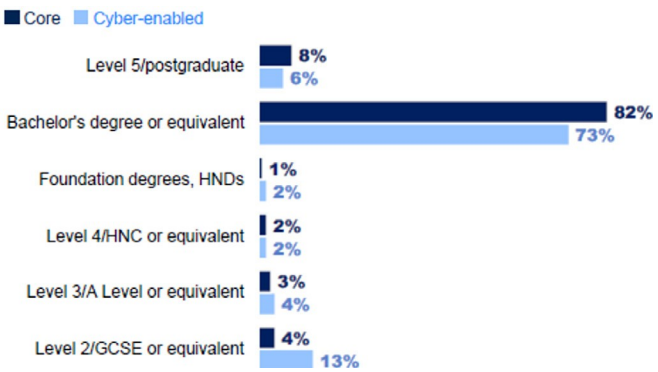
Níveis mínimos de experiência necessários para funções de trabalho cibernético no Reino Unido (principal e relacionado)



Nota: Com base em 31.307 publicações de obras cibernéticas (principais e relacionadas) de janeiro a dezembro de 2021.
Fonte: (DCMS & IPSOS, 2022)

Gráfico 20.

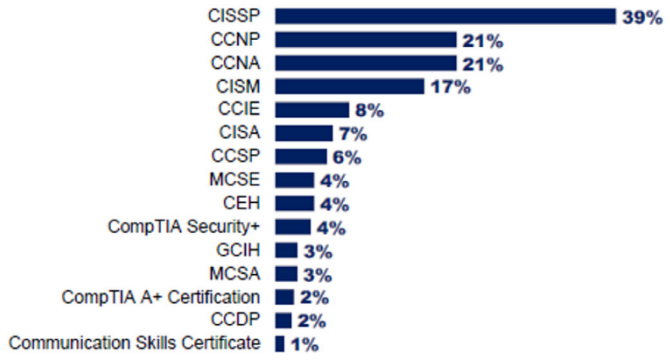
Níveis mínimos de educação necessários para funções de trabalho cibernético no Reino Unido (núcleo e afins)



Nota: Com base em 30.472 publicações ciber-paper (principais e relacionadas) de janeiro a dezembro de 2021.
Fonte: (DCMS & IPSOS, 2022)

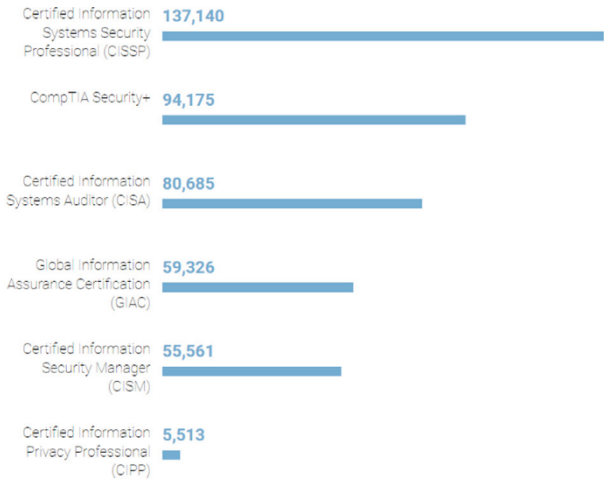
Além disso, a importância de ter certificações de TI e de segurança da informação na oferta de trabalho é destacada. É notado que a certificação *Certified Information Systems Security Professional (CISSP)* é a principal certificação procurada para funções cibernéticas importantes em todo o mundo. No Reino Unido, as certificações *Cisco Certified Network* continuam a ser muito solicitadas, por exemplo, Cisco Certified Network Professionals (CCNP) e Cisco Certified Network Associates (CCNA). No mercado de trabalho dos EUA, as certificações CompTIA Security+ e as da Information Systems Audit and Control Association (ISACA) são valorizadas.
-ISACA-) como o Auditor Certificado de Sistemas de Informação (CISA) e o Gerente Certificado de Segurança da Informação (CISM).

Gráfico 21.
As principais certificações procuradas para os principais papéis cibernéticos no Reino Unido



Nota: Com base em 11.086 anúncios de empregos cibernéticos de janeiro a dezembro de 2021.
Fonte: (DCMS & IPSOS, 2022)

Gráfico 22.
As principais certificações procuradas para os principais papéis cibernéticos nos EUA



Nota: A partir de setembro de 2022 Fonte: (CyberSeek, 2022)

Tabela 1.
Principais Certificações de Tecnologia da Informação e Segurança da Informação

Fornecedor		Certificação	Certificação
(ISC)² (ISC)² (ISC)² (ISC)² (ISC)² (ISC)²	CISSP	Profissional Certificado de Segurança de Sistemas de Informação	USD 749
ISACA	CISA	Auditor de Sistemas de Informação Certificado	USD 575 membros ISACA, USD 760 não-membros
ISACA	CISM	Gerente Certificado de Segurança da Informação	USD 575 membros ISACA, USD 760 não-membros
CompTIA	Segurança +	CompTIA Segurança+	USD 381
EC-Council	CEH	Hacker Ético Certificado	USD 950 a USD 1.199, dependendo da localização
GIAC	GSEC	Certificação GIAC Security Essentials	USD 2.499
(ISC)² (ISC)² (ISC)² (ISC)² (ISC)² (ISC)²	SSCP	Praticante Certificado de Segurança de Sistemas	US$ 249
CompTIA	CASP+	CompTIA Praticante Avançado de Segurança	480 USD
GIAC	GCIH	Tratador de Incidentes Certificado GIAC	USD 2.499
Segurança ofensiva	OSCP	Profissional Certificado de Segurança Ofensiva	USD 999 a USD 5.499

Fonte: Coursera (2022)[42] e ComputerScienceMS (2022)[43]

42 https://www.coursera.org/articles/popular-cybersecurity-certifications
43 https://computersciencems.com/resources/cyber-security/best-cybersecurity-certifications/

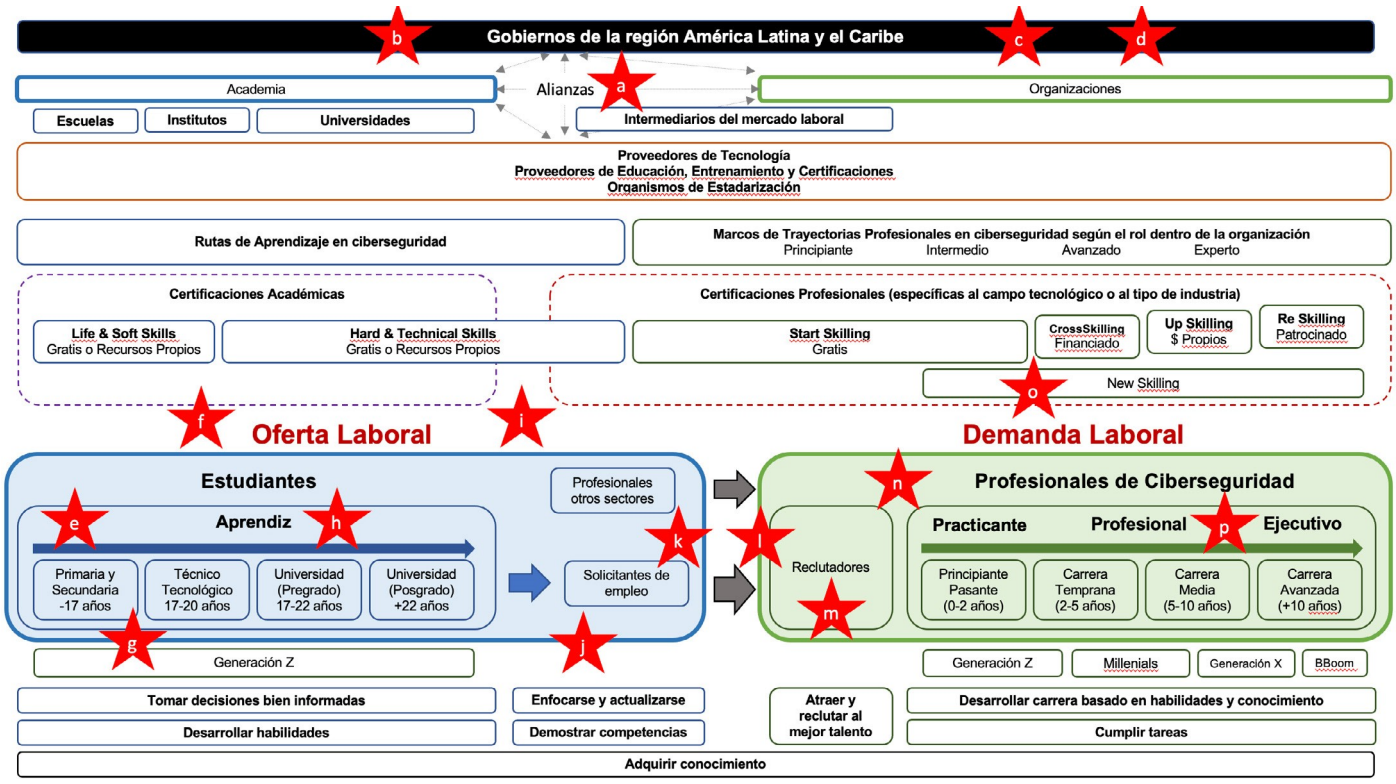
3.3. OS PRINCIPAIS DESAFIOS

Fortes habilidades e capacidades de segurança cibernética são um motor fundamental da atividade econômica na região da América Latina e do Caribe e são fundamentais para sua prosperidade futura. A escassez de profissionais de segurança cibernética e as habilidades deste talento humano podem ser causadas por uma combinação única de desafios para a região, onde estima-se que entre 515.000 e 701.000 profissionais adicionais possam ser necessários atualmente para cargos técnicos e não técnicos. A região é, portanto, identificada como enfrentando o seguinte problema:

> ***A demanda por profissionais de segurança cibernética na América Latina e no Caribe continua a superar a oferta, resultando em uma lacuna crescente (escassez) na força de trabalho de segurança cibernética.*** *Essas vagas em organizações públicas e privadas podem levar a ameaças, ataques e incidentes cibernéticos, com graves conseqüências econômicas ou sociais, e podem deixar países da região mal preparados para lidar com conflitos no ciberespaço.*

Os desafios no mercado de trabalho de cibersegurança em torno desta questão podem ser identificados tanto do lado da oferta quanto do lado da demanda de mão de obra. Alguns dos principais desafios enfrentados pelos países da região são identificados abaixo.

Gráfico 23.
Representação esquemática dos desafios no mercado de trabalho de cibersegurança na região



Fonte: Elaboração própria

São identificados os seguintes desafios para os governos da região:

- **A** Esforços isolados para o desenvolvimento da força de trabalho e promoção de parcerias nacionais e internacionais
- **B** Fraca estrutura regulatória e articulação institucional
- **C** Informações estratégicas insuficientes para a tomada de decisões a nível nacional
- **D** Sensibilização e disseminação insuficientes de recursos, ferramentas e informações para o desenvolvimento da força de trabalho cibernética de segurança

No lado da oferta de mão-de-obra da segurança cibernética, são identificados os seguintes desafios:

- **E** Desenvolvimento insuficiente das vocações STEM e baixa habilidade digital entre meninas e meninos na região
- **F** Baixa/moderada proficiência em inglês na região
- **G** Falta de conscientização e educação de segurança em idade precoce
- **H** Falta de conhecimento da oferta educacional por parte dos estudantes
- **I** Desconectar entre educação, treinamento e indústria
- **J** Falta de consciência dos percursos de aprendizagem entre os candidatos a emprego
- **K** Fraco entendimento da definição da profissão de segurança cibernética

No lado da demanda de mão-de-obra da ciber-segurança, são identificados os seguintes desafios

- **L** Falta de uma linguagem comum entre a demanda e a oferta de mão de obra
- **M** Preferência de o experiência sobre qualificações em organizações
- **N** Lacuna na diversidade, equidade e inclusão na força de trabalho
- **O** Dificuldades de acesso às estruturas de carreira
- **P** Fraco programas de retenção em organizações

ANÁLISE PARA O DESENVOLVIMENTO DA FORÇA DE TRABALHO NA REGIÃO

Apesar dos esforços dos países da região da América Latina e Caribe, um número substancial de posições cibersegurasvagas permanece por preencher porque as organizações não conseguem encontrar o talento certo. Em resposta a esta situação, os sistemas educacionais da região começaram a se mobilizar, com um grande número de instituições e entidades educacionais criando e lançando novos graus e cursos de cibersegurança. Da mesma forma, os *Provedores de Educação, Treinamento e Certificação* e os *Provedores de Tecnologia* estão fortalecendo suas ferramentas, recursos e conteúdo para desenvolver as capacidades e habilidades da força de trabalho cibernética de hoje.

No entanto, a falta de habilidades de cibersegurança da região está afetando o mercado de trabalho e continuará aguda a médio prazo. Para desenvolver defesas cibernéticas fortes, a região precisa construir e desenvolver uma força de trabalho de segurança cibernética mais diversificada, com mais e melhores habilidades técnicas e não técnicas. A melhoria do equilíbrio de gênero também ajudará esta força de trabalho a crescer e amadurecer. Fortalecer as ligações entre as habilidades oferecidas pelos sistemas educacionais e as necessidades do mercado de trabalho é uma prioridade para fechar as lacunas de capital humano na cibersegurança.

Por esta razão, são apresentadas abaixo considerações tanto do lado da oferta quanto do lado da demanda de mão-de-obra para profissionais da cibersegurança, a fim de que o ecossistema de cibersegurança trabalhe de forma abrangente no desenvolvimento da mão-de-obra na região. Para cada desafio identificado, é feita uma análise em três (3) partes: uma descrição da importância da questão tratada pelo desafio, algum apoio ou evidência da situação atual em nível global ou regional, e uma descrição de boas práticas para enfrentar o desafio. Além disso, são apresentadas algumas considerações para os governos da América Latina e do Caribe.

4.1. DAS OFERTA DE TRABALHO

A nova geração de estudantes e profissionais de outros setores precisa de habilidades pessoais e profissionais para prepará-los para as oportunidades atuais e futuras no mercado de trabalho de segurança cibernética.

A partir da análise dos desafios identificados no lado da oferta de mão-de-obra da ciber-segurança, são apresentadas as seguintes considerações a fim de

- Aumentar as vocações científicas entre as crianças e os jovens da região.
- Fortalecimento da proficiência em inglês na região
- Aumentar a conscientização e a sensibilização para a cibersegurança em uma idade precoce
- Promover o acesso à educação
- Conectando a educação ao treinamento e à indústria
- Promover o acesso a percursos de aprendizagem
- Esclareça o definição de o profissão em ciber-segurança

Aumentar as vocações científicas entre as crianças e os jovens da região.

Relevância

O desenvolvimento da força de trabalho de cibersegurança deve começar nas escolas primárias e secundárias. Quanto mais as escolas encorajam os alunos a considerar uma carreira em cibersegurança e quanto mais eles incentivam as primeiras habilidades, maior é a qualidade dos alunos no sistema de educação terciária. Isto significa que as escolas devem dar maior ênfase ao desenvolvimento de habilidades em cibersegurança nos programas curriculares e extracurriculares como caminhos para o ensino superior. As habilidades aprendidas na educação STEM são as mesmas habilidades necessárias para uma carreira em segurança cibernética. Praticamente todas as funções no mercado de trabalho de segurança cibernética exigem habilidades relacionadas com a STEM. Como mais trabalhadores com habilidades baseadas na STEM entram na força de trabalho em cibersegurança, as empresas e outras organizações provavelmente verão menos ataques cibernéticos bem sucedidos e sofrerão menos danos econômicos com esses ataques (WICKR, 2021).

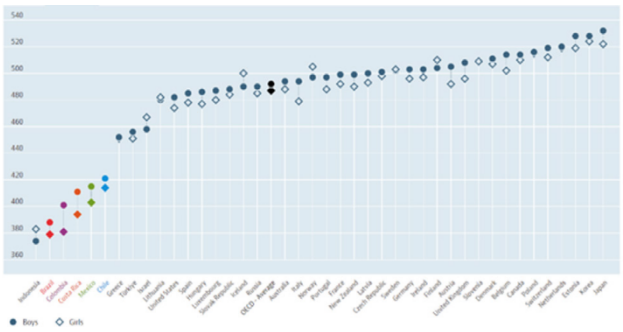
Desafi

Na América Latina e no Caribe, não há treinamento suficiente nas áreas de conhecimento STEM nos níveis de educação básica, média e secundária. Os resultados das últimas medições PISA confirmam que, em média, os estudantes de 15 anos na região estão três (3) anos atrás dos estudantes de leitura, matemática e ciências em comparação com os estudantes de um país da OCDE. Há também uma lacuna de gênero no desenvolvimento de habilidades STEM (Banco Mundial, 2019). Além disso, apenas 2,68% dos inscritos no ensino superior da região são estudantes em áreas relacionadas com matemática, ciências e estatística. Isto é problemático quando comparado à média dos países da OCDE, onde as matrículas em áreas relacionadas às mesmas áreas de conhecimento atingiram 6,24% (DNP, 2022).

Alguns

Gráfico 24.

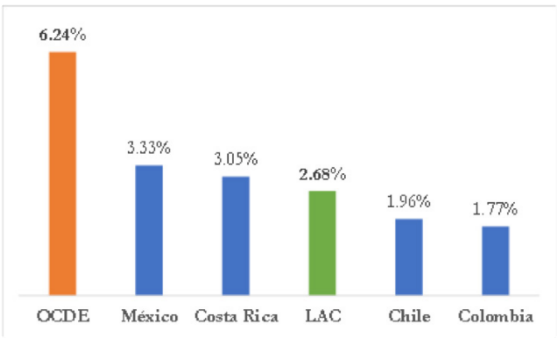
Desempenho (nota média) em habilidades matemáticas discriminadas entre meninos e meninas a partir do PISA 2018



Fonte: (OCDE, 2022)

Gráfico 25.

Proporção matriculada em programas universitários nos campos STEM



Fonte: (DNP, 2022)

Boas práticas

A educação STEM é um esforço global para melhorar as habilidades científicas, tecnológicas, de engenharia e matemáticas de crianças e jovens. Cada país do mundo tem uma abordagem diferente para implementá-la, alguns estão integrando-a em suas políticas educacionais, outros estão implementando-a através de organizações externas. A *Estratégia Educacional da Estônia (2021-2035)*[44] enfatiza as habilidades da STEM que criam mais valor agregado para melhorar a aprendizagem ao longo da vida e as oportunidades de reciclagem, incluindo a aprendizagem baseada no trabalho. Cingapura incorporou o *Programa de Aprendizagem Aplicada STEM (ALP)*[45] em suas escolas secundárias em conjunto com a STEM Inc, uma unidade do Centro de Ciências de Cingapura. A educação STEAM integrada na Coréia do Sul é uma abordagem para preparar uma força de trabalho STEM de qualidade e cidadãos alfabetizados para uma sociedade altamente tecnológica, integrando ciência, tecnologia, engenharia, artes e matemática na educação (Kang, 2019). A OEA oferece na região o *Diploma em Educação STEM-STEAM*[46] a professores e agentes educacionais para fortalecer a concepção e implementação de práticas, projetos ou programas de educação STEM. A Colômbia lançou o *Programa Ruta STEM 2022*[47] que procura fortalecer as capacidades de 5.000 professores e 100.000 alunos do ensino básico e secundário do país em tecnologia, ciência, engenharia e matemática.

44 https://www.hm.ee/sites/default/files/haridusvaldkonna_arengukava_2035_kinnittaud_vv_eng.pdf
45 https://www.science.edu.sg/stem-inc/about-us/about-stem-inc
46 https://www.oas.org/en/scholarships/professionaldev/Courses_2022/Anuncio-PDSP-Educacion_STEM-STEAM.pdf
47 https://www.mineducacion.gov.co/portal/salaprensa/Noticias/410966:Gobierno-nacional-lanza-Ruta-Stem-2022-para-fortalecer-las-capacidades-de-docentes-y-country-students-in-technology-science-engineering-and-mathematics

Fortalecimento da proficiência em inglês na região

Relevância

O inglês é agora o idioma padrão nos negócios internacionais, diplomacia, entretenimento, ciência, tecnologia e, em particular, segurança cibernética. O inglês é a língua mais usada no mundo tanto por falantes nativos como não-nativos. Estima-se que 1,45 bilhões de pessoas (18,2% da população total) falam inglês, enquanto aproximadamente 548 milhões (6,9% do total) falam espanhol e aproximadamente 258 milhões (3,2%) falam português (ETHNOLOGUE, 2022). Além disso, o inglês continua sendo a língua mais utilizada na Internet em 2022, sendo utilizado por 60,4% de todos os websites cujo idioma de conteúdo é conhecido, enquanto o espanhol representa apenas 4,1% dos websites na Internet (W3TECHS, 2022). No mundo da programação de computadores e da indústria de software, o inglês parece ser a *lingua franca*.[48] A maioria dos novos códigos é geralmente desenvolvida por falantes de inglês. A língua mais comumente usada nas principais certificações acadêmicas e profissionais em Tecnologia da Informação e Segurança da Informação é o inglês.

Desafi

Segundo (EF, 2022), as Américas Central e do Sul melhoraram consideravelmente sua proficiência em inglês na última década, mas em 2022 a proficiência em inglês continua muito baixa para o México e Haiti e baixa para a Colômbia, Equador, Panamá, Venezuela e Nicarágua. Além disso, a região tem a maior diferença de idade do mundo. Os resultados dos jovens da região caíram significativamente desde 2020. O fechamento de escolas durante a pandemia parece ser a causa mais provável. Finalmente, em 2022, a proficiência em inglês dos homens aumentou e a das mulheres diminuiu ligeiramente. Os machos têm pontuado melhor do que as fêmeas na região.

Alguns

Tabela 2.
Relevância global do idioma inglês

Lenguajes hablados	Sitios WEB por idioma *	Población por idioma **	Usuarios de Internet por idioma ***
Inglés	60.4%	18.2%	25.9%
Ruso	5.4%	3.2%	2.5%
Español	4.1%	6.9%	7.9%
Aleman	3.4%	1.7%	2.0%
Frances	3.1%	3.4%	3.3%
Japonés	2.8%	1.6%	2.6%
Chino	1.8%	14.0%	19.4%
Otros	19.0%	51.1%	36.4%
Total	**100.0%**	**100.0%**	**100.0%**

Fonte: Elaboração própria com base em * (W3TECHS, 2022), ** (ETNOLOGUE, 2022), * (INTERNETWORLDSTATS, 2022)**

Gráfico 26.
Ranking de proficiência em inglês na região

Fonte: (EF, 2022)

Boas práticas

Uma pessoa bilíngüe, que fala espanhol e inglês, pode compreender 1 em cada 3 pessoas que estão atualmente conectadas à Internet (25,9% dos internautas falam inglês e 7,9% falam espanhol). Como um caso de boas práticas, a Argentina implementou diferentes iniciativas e leis para melhorar o ensino de línguas nas escolas (Lei Nacional de Educação, Núcleos de Aprendizagem Prioritária - NAP- e programas como o Dia Ampliado em Buenos Aires)[49]. A fim de alcançar estes objetivos, foi desenvolvido um sistema de treinamento de professores de idiomas em metodologias comunicativas. Na Costa Rica, as disposições da Diretriz de Bilinguismo[50] e da Política Educacional para a Promoção das Línguas[51] destacam a importância da aprendizagem de uma segunda língua como uma ferramenta indispensável para a formação, desempenho, desenvolvimento pessoal e profissional dos cidadãos, e propõem melhorar o ensino do inglês aplicando-o a partir do nível pré-escolar.

48 https://preply.com/en/blog/b2b-english-for-software-engineers-developers-and-programmers/#:~:text=So%2C%20how%20importante%20is%20inglês,will%20still%20be%20in%20inglês.

49 https://www.ambito.com/informacion-general/ranking/la-argentina-es-el-pais-mejor-dominio-del-ingles-america-latina-n5149683

50 Diretiva N° DM-0004-2-2019 e Circular DVM-AC-004-2020 do Ministério de Educação Pública da Costa Rica, onde são estabelecidas disposições para implementar o ensino do inglês no nível pré-escolar.

51 http://cse.go.cr/sites/default/files/acuerdos/politica_educativa_para_la_promocion_de_idiomas.pdf

Aumentar a conscientização e a sensibilização para a cibersegurança em uma idade precoce

Relevância

A população com menos de 15 anos na América Latina e no Caribe representa 24% da população total, em comparação com 18% na América do Norte e 16% na Europa. A conscientização da cibersegurança em uma idade precoce é fundamental para o desenvolvimento da força de trabalho da região. Os ataques cibernéticos continuam a atingir todos os tipos de organizações, incluindo escolas, pois os estudantes e o pessoal trazem dispositivos conectados de casa e compartilham informações através de suas redes. É importante conscientizar e sensibilizar os estudantes desde cedo sobre os riscos que enfrentam on-line, mas também é importante oferecer-lhes a oportunidade de aprender sobre segurança cibernética em um nível mais profundo, permitindo-lhes ter habilidades cibernéticas para toda a vida. É imperativo preencher a crescente lacuna de conscientização e habilidades de segurança cibernética entre os jovens estudantes, assegurando que ela se torne uma área crítica para a educação.

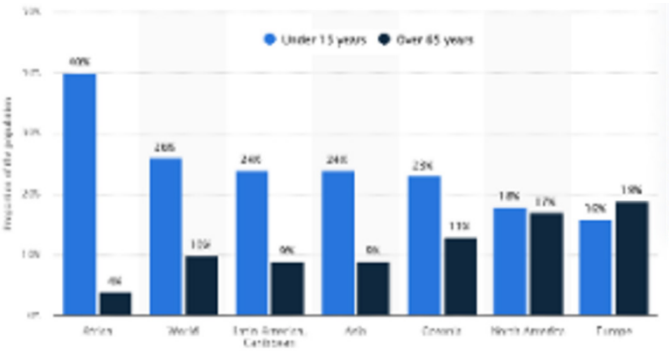
Desafi

Geralmente, nas escolas e outros tipos de instituições educacionais e vocacionais pré-universitárias, o conteúdo relacionado aos riscos da cibersegurança é agregado como parte de uma área temática de tecnologia, como ciência da computação/TI/ICT/ tecnologia (digital), e o conteúdo agregado com uma variedade de matérias não tecnológicas. De acordo com (GFCE, 2022), na educação infantil tende a haver uma falta de habilidades práticas de cibersegurança, uma falta de mentalidade de cibersegurança, uma falta de cobertura suficiente de conjuntos de habilidades incorporadas, rumo a uma carreira relacionada à cibersegurança e uma percepção geral de falta de interesse e consciência entre as crianças no desenvolvimento de habilidades cibernéticas e cibersegurança como uma carreira potencial.

Alguns

Gráfico 27.
População mundial com menos de 15 e mais de 65 anos de idade

Fonte: ESTATÍSTICA (2022)[52]



Boas práticas

Dentro de contextos internacionais e multinacionais, existe uma ampla gama de conteúdos educacionais de cibersegurança (através de programas, diretrizes e iniciativas) dentro de um contexto pré-universitário. Por exemplo, o programa *Child Online Protection (COP)*[53] da União Internacional de Telecomunicações -ITU- destinado a crianças, pais e educadores, indústria e formuladores de políticas. Também o conteúdo fornecido pela Agência da União Européia para Segurança Cibernética (ENISA) se concentra, por um lado, na conscientização e sensibilização em torno da segurança cibernética[54]. A European Cyber Security Organisation (ECSO) está desenvolvendo a iniciativa *Youth4Cyber*[55], que visa educar e conscientizar os jovens (de 6 a 26 anos) sobre cibersegurança. Também merece destaque o conteúdo do Fórum Global de Especialização Cibernética (GFCE)[56], que compartilha as melhores práticas e desenvolve iniciativas para melhorar a capacidade cibernética. Em nível nacional, existe o programa *SG Cyber Youth* em Cingapura, dirigido pela Cyber Security Agengy of Singapore (CSA) para orientar crianças e jovens (especialmente aqueles em escolas secundárias) para uma carreira em segurança cibernética, com o apoio da academia, da comunidade e da indústria. Além disso, o US Cybersecurity Education and Training Assistance Program (CETAP)[57] para apoiar a educação em segurança cibernética nas salas de aula K-12[58] através do desenvolvimento de currículos de segurança cibernética e treinamento de instrutores.

52 https://www.statista.com/statistics/265759/world-population-by-age-and-region/#:~:text=Globally%2C%20about%2026%20percent%20of%20the%20world%20is,19%20percent%20being%20over%2065%20years%20of%20age.
53 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx e https://www.itu-cop-guidelines.com/
54 https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport
55 https://www.ecs-org.eu/initiatives/youth4cyber
56 https://thegfce.org/working-groups/working-group-d/
57 https://niccs.cisa.gov/education-training/cybersecurity-teachers
58 K-12 ("k a doze" ou "k a doze") é a designação usada em alguns sistemas de educação para o ensino primário e secundário.

Promover o acesso à educação

Relevância

O ensino superior oferece uma gama considerável de conteúdos, cursos, módulos e oportunidades para explorar a segurança cibernética tanto em nível de graduação como de pós-graduação. Universidades e institutos de ensino superior estão expandindo rapidamente suas ofertas de programas de cibersegurança, concedendo diplomas ou títulos específicos como especialização ou mestrado em TI, TIC e segurança da informação. Como a demanda por profissionais de cibersegurança cresceu nos últimos anos, o ensino superior também respondeu fornecendo (i) cursos dedicados à cibersegurança, (ii) cursos gerais de TI ou computação com um ou mais módulos em cibersegurança e (iii) cursos não técnicos com módulos em cibersegurança. Além disso, os cursos multidisciplinares estão se tornando cada vez mais comuns.

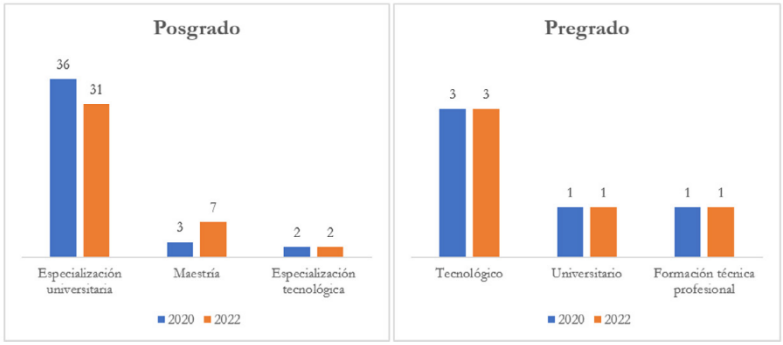
Desafi

Embora haja esforços isolados em vários países[59] , não há provisão educacional suficiente na região para gerar competências e habilidades adequadas de segurança cibernética[60]. A demanda por educação em segurança cibernética por estudantes pós-secundários não está aumentando suficientemente rápido. Além disso, a demanda por habilidades de segurança cibernética nos setores industriais também torna difícil para o meio acadêmico atrair acadêmicos, pesquisadores e professores, com conhecimento, experiência prática, histórico de pesquisa e aspirações acadêmicas. Há também dificuldades em atrair e reter professores qualificados em cibersegurança, em grande parte porque tais profissionais de alta qualidade exigem salários acima da média. Os provedores de ensino superior precisam garantir que a cibersegurança seja vista como uma opção de estudo desejável para atrair os melhores e mais motivados estudantes.

Alguns

Gráfico 28.
Evolução do número de programas de ensino superior relacionados à Segurança Cibernética e da Informação na Colômbia

Fonte: Dados de 2020 (DNP, 2020) e Dados de 2022[61] (MINEDUCACION, 2022).



Boas práticas

A fim de promover a oferta educacional, destacam-se iniciativas regionais para o desenvolvimento de habilidades em cibersegurança como o CYBERHEAD[62] da ENISA, tornando-se o maior banco de dados validado do ensino superior em cibersegurança (123 programas em 25 países) e o principal ponto de referência para todos os cidadãos da região que procuram melhorar seus conhecimentos e habilidades em cibersegurança. No Reino Unido, o National Cyber Security Centre (NCSC) certificou vários diplomas de bacharelado e mestrado no âmbito do programa de certificação. Ele também apoiou o desenvolvimento de Centros Acadêmicos de Excelência em Pesquisa em Segurança Cibernética (ACE-CSR) e Centros Acadêmicos de Excelência em Educação em Segurança Cibernética (ACE-CSE). Em Cingapura, existem vários programas voltados para os jovens, notadamente o *programa* o *SG Cyber Youth*[63] que os orienta a iniciar em cibersegurança, com o apoio do meio acadêmico, da comunidade e da indústria. Uma iniciativa chave é o Programa de *Exploração Cibernética da Juventude*[64] que introduz os estudantes do ensino médio aos fundamentos da cibersegurança e cultiva seu interesse em uma carreira na cibersegurança. O *Programa de Mentoria de Carreira em Segurança Cibernética (CCMP)* também fornece orientação de carreira e apoio de mentores da indústria. Outras iniciativas em Cingapura incluem o *Programa de Voluntariado Estudantil e Reconhecimento (SVRP)* e as *Jornadas de Aprendizagem sobre Cibersegurança.* Também o programa *SG Cyber Olympians* com o objetivo de ser preparado sob o SG *Cyber* Olympians através de sessões de guerra cibernética, treinamento mais aprofundado e competições internacionais.

59 Por exemplo, destaca-se o Diretório da Oferta Acadêmica 2022 do *Centro de Ciber-Segurança* da cidade de Córdoba na Argentina (https://corlab.cordoba.gob.ar/wp-content/ uploads/2022/09/oferta-educativa-ciberseguridad-cordoba.pdf).

60 Por exemplo, de acordo com (DNP, 2020) existe *"evidência de que a oferta de programas educacionais relacionados à segurança digital é baixa no nível acadêmico de graduação"* na Colômbia.

61 Destaca-se a atual oferta de programas de mestrado na Colômbia, tais como: Mestrado em Gestão e Segurança da Informação, Mestrado em Segurança Digital, Mestrado em Segurança da Informação, Mestrado em Segurança da Informática e Comunicações, Mestrado em Segurança Cibernética e Computação Forense ou Mestrado em Segurança Cibernética e Defesa Cibernética.

62 https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/

63 https://www.cyberyouth.sg/
64 https://www.csa.gov.sg/ycep

Conectando a educação ao treinamento e à indústria

Relevância

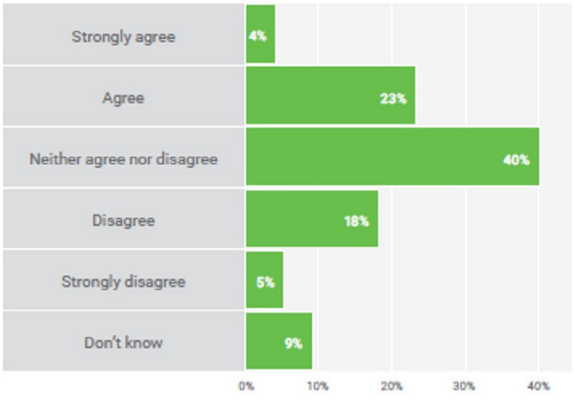
O desenvolvimento de currículos e programas de educação superior e contínua é de grande importância quando se trata de mitigar a escassez de mão de obra e a falta de habilidades em cibersegurança, pois eles incentivam os estudantes a buscar temas de cibersegurança, aumentam as capacidades operacionais da nova força de trabalho potencial e promovem e fomentam as relações entre o meio acadêmico e a indústria, bem como alinham o treinamento em cibersegurança com as necessidades reais da indústria. Os currículos devem ser multidisciplinares, pois estudantes e profissionais precisam compreender uma variedade de áreas de conhecimento em cibersegurança, desde tópicos mais técnicos até aspectos sociais e jurídicos. Além disso, os currículos e programas devem priorizar o treinamento prático em vez do treinamento teórico.

Desafi

Nos países da região, não há evidências da existência de estruturas específicas para definir currículos padronizados que sejam amplamente aceitos e alinhados com a indústria. Não há evidência da existência de alianças entre indústria e academia com o objetivo de gerar guias curriculares nacionais ou diretrizes para programas de graduação ou pós-graduação relacionados à ciber-segurança ou segurança da informação. Um conjunto de áreas temáticas centrais com práticas de cibersegurança associadas, nas quais se espera que todos os estudantes sejam competentes ao final do ensino médio e terciário, precisa emergir periodicamente dessas parcerias. Isto pode ter um impacto sobre a entrada dos estudantes na força de trabalho.

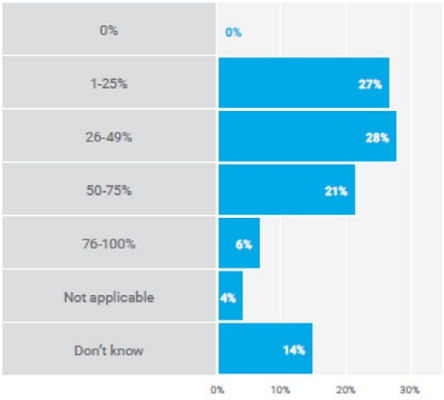
Alguns

Gráfico 29.
Os recém-formados universitários em segurança cibernética estão bem preparados para os desafios de segurança cibernética em sua organização?



Fonte: (ISACA, 2022)

Gráfico 30.
% de candidatos cibernéticos de segurança que são bem qualificados para o cargo ao qual se candidatam



Fonte: (ISACA, 2022)

Boas práticas

Há algumas iniciativas que visam contribuir para a criação de estruturas específicas ou um conjunto padronizado de diretrizes a serem seguidas pelos países para a educação pré-universitária e universitária. Com relação à educação pré-universitária, a *iniciativa Computing for All*[65] e seu *"Computing Curriculum Framework for Schools"*[66] lançada em 2022 é um bom exemplo de como diferentes partes interessadas em vários países podem trabalhar juntas para produzir currículos e diretrizes mais padronizados e amplamente adotados. Com relação à educação universitária, destaca-se a experiência nos Estados Unidos, onde há vários esforços de colaboração público-privada, mais notadamente a Joint Task Force (JTF) on Cybersecurity Education, que desde 2015 vem trabalhando para desenvolver um guia curricular que alinha os programas acadêmicos de graduação em cibersegurança com as necessidades da indústria. Especificamente, ele também destaca o projeto *Cyber2yr2020*[67] que se concentra nas diretrizes curriculares para programas de cibersegurança, incluindo programas de graduação de associados que devem se alinhar com a Iniciativa Nacional para Educação em Cibersegurança (NICE) da NIST.

65 https://www.informaticsforall.org/
66 https://www.informaticsforall.org/wp-content/uploads/2022/03/Informatics-Reference-Framework-for-School-release-February-2022.pdf
67 http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf

Promover o acesso a percursos de aprendizagem

Relevância

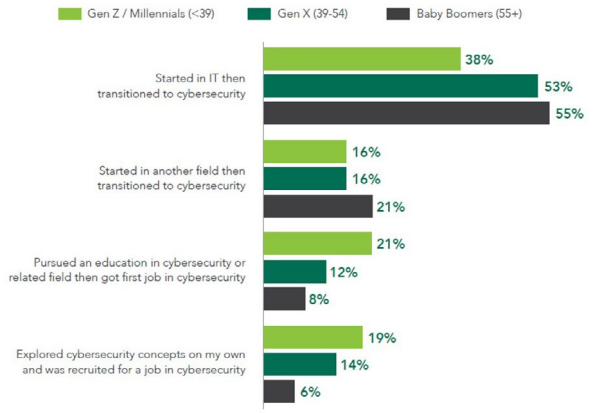
Ter uma sólida base de conhecimentos e habilidades é de suma importância no mercado de trabalho de segurança cibernética. Isso inclui habilidades brandas, tais como comunicação verbal e escrita, e habilidades técnicas validadas através de certificações acadêmicas ou profissionais. Estudantes e profissionais de outros setores que se tornarão candidatos a emprego podem desenvolver essas habilidades e competências através de caminhos de aprendizado focados especialmente para o nível básico ou de praticante dentro das organizações. Tanto os *Provedores de Educação, Treinamento e Certificação* quanto os *Provedores de Tecnologia* são atores-chave para preencher a lacuna entre a demanda e a oferta em habilidades de segurança cibernética. Estes caminhos, que compreendem cursos práticos que ensinam habilidades empresariais e tecnológicas, permitem que as habilidades sejam demonstradas aos empregadores potenciais. Programas de certificação acadêmica em cibersegurança são destacados para estudantes que já obtiveram um diploma em uma área relacionada e estão procurando mudar de carreira, ou para estudantes que desejam explorar o que seria se preparar para uma carreira em cibersegurança antes de se comprometerem com uma carreira mais longa.

Desafi

Iniciar e avançar uma carreira em cibersegurança não é tão simples como outras profissões mais tradicionais. Nos países da região, é importante gerar mais interesse nos estudantes e nas pessoas à procura de emprego, a fim de se mover para caminhos de aprendizagem autodidata. Pode haver uma incapacidade das partes interessadas de encorajar mais estudantes a entrar em caminhos acadêmicos que são mais facilmente associados a um trabalho de cibersegurança. Outro problema é que as habilidades necessárias estão mudando a um ritmo mais rápido do que o habitual dentro dos campos de tecnologia avançada, devido às mudanças introduzidas pela nova tecnologia digital e a rápida digitalização da sociedade.

Alguns

Gráfico 31.
Caminhos para carreiras em ciber-segurança



Fonte: (ISC2, 2021)

Gráfico 32.
Composição da equipe de segurança cibernética por nível de experiência por tamanho de organização

Fonte: (ISC2, 2022b)

Boas práticas

No mercado de trabalho, há atores-chave no lado da oferta do mercado de trabalho que impulsionam os caminhos do aprendizado. *Provedores de educação, treinamento e certificação* e *provedores de tecnologia* oferecem conteúdo de todos os níveis de complexidade para desenvolver habilidades e habilidades. Há um grande número de cursos no mercado sob as plataformas MOOC,[68] destinados a estudantes e profissionais. Exemplos de tais plataformas são: Coursera (https:// www.coursera.org/), LinkedIn Learning (https://www.lynda.com/), edX (http://www.edx.org/), PluralSight (https://www. pluralsight.com/), Cybrary (https://www.cybrary.it/), Udacity (https://www.udacity.com/), Udemy (https://www.udemy. com/), MiriadaX (https://miriadax.net/) ou Cyberwiser (https://www.cyberwiser.eu/). Também são dignas de nota as plataformas oferecidas pelos *Provedores de Tecnologia* para iniciar caminhos de aprendizagem, como a *Cisco Networking Academy* desenvolvendo *Skills for All*[69] , uma plataforma móvel e gratuita que oferece experiências de aprendizagem no próprio ritmo para impulsionar um futuro inclusivo para todos, incluindo o *Cybersecurity Learning Pathway*[70].

68 O termo MOOC é um acrônimo para *Massive Open Online Courses*, ou seja, refere-se a cursos online abertos, tanto gratuitos como pagos, que são acessíveis a um grande número de alunos.

69 https://skillsforall.com/

70 Alinhado com a nova certificação *Certiport Information Technology (IT) Specialist Cybersecurity*, os estudantes podem exercer funções como técnico de segurança cibernética, analista júnior de segurança cibernética e suporte de help desk. Os graduados também podem aproveitar o programa *Talent Bridge* da CISCO e usar o mecanismo de busca de emprego que inclui oportunidades em mais de 725 parceiros empregadores em 70 países.

Esclarecendo a definição da profissão de segurança cibernética

Relevância

O papel dos profissionais de segurança cibernética está em constante evolução e, portanto, é difícil definir a profissão de segurança cibernética. Além disso, a taxonomia em torno da segurança cibernética pode ser confusa e as rotas para e através das carreiras de segurança cibernética podem ser difíceis de navegar. É importante que os países abordem esta questão para garantir que haja uma profissão ciber-segurança estruturada e sustentável. A linguagem técnica e os acrônimos freqüentemente utilizados podem tornar este desafio particularmente pronunciado para aqueles estudantes ou candidatos a emprego que são novos ou não familiarizados com a cibersegurança. O atual cenário profissional também é complexo para as organizações profissionais existentes e para os *Provedores de Educação, Treinamento e Certificação*, que muitas vezes não conseguem articular a equivalência de suas ofertas na ausência de uma estrutura técnica comum. A cibersegurança é cada vez mais reconhecida como um tópico altamente interdisciplinar, abrangendo áreas de conhecimento como gestão de risco e governança, leis e regulamentos cibernéticos, fatores humanos, proteção da privacidade e direitos on-line e comportamentos adversos (GFCE, 2022).

Desafi

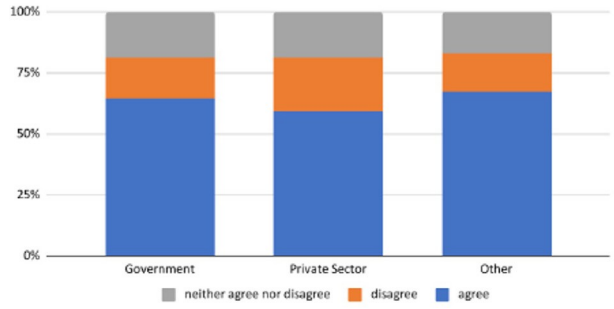
Na região, segurança informática e segurança da informação são termos que ainda são confundidos com o termo ciber-segurança. Isto também gera confusão entre estudantes e candidatos a emprego quanto ao escopo de tarefas e habilidades que eles precisam possuir para cumprir requisitos ou perfis quando procuram emprego. De acordo com (GFCE, 2022), mais da metade dos participantes entrevistados em um estudo sobre o desenvolvimento da cibersegurança como profissão mencionou globalmente que a definição da profissão não é clara e esta resposta foi praticamente a mesma em todos os grupos de participantes e foi ligeiramente superior entre os entrevistados de países desenvolvidos.

Alguns

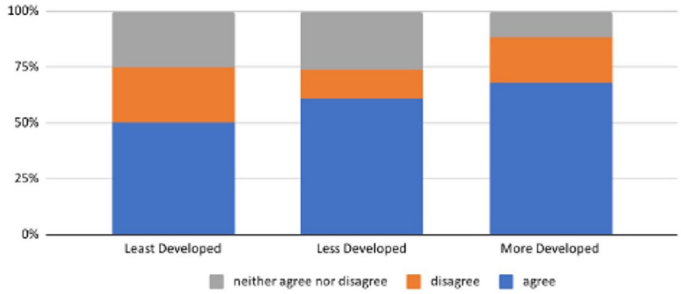
Gráfico 33.

Percepções sobre a definição da profissão de cibersegurança

(Até que ponto você concorda que a definição de um profissional cibernético de segurança não é clara?)



Fonte: (GFCE, 2022)



Fonte: (GFCE, 2022)

Boas práticas

No Reino Unido, o *UK Cyber Security Council e o Cyber Security Body Of Knowledge (CyBOK)*[71] estabeleceram uma categorização[72] das funções de segurança cibernética. O CyBOK é um recurso único, fornecendo um corpo de conhecimento de fundo que cobre a amplitude e profundidade da segurança cibernética em uma ampla gama de disciplinas. Por exemplo, de acordo com (DCMS & IPSOS, 2022), as funções mais requisitadas em cibersegurança no Reino Unido são engenheiros de segurança (35%), analistas de segurança (18%), gerentes de segurança (14%), arquitetos de segurança (11%) e consultores de segurança (9%). Há iniciativas para tópicos específicos, por exemplo, Cingapura emitiu um *Quadro de Competências de Cibersegurança de Tecnologia Operacional* (CSA, 2021) que fornece a base para atrair e desenvolver talentos para o emergente setor de cibersegurança de OT em Cingapura e fornece orientação sobre competências para equipar profissionais para desempenhar suas funções nos setores da indústria de OT. Há também iniciativas como o (ISC)² CBK[73] (Body of Knowledge) que é um compêndio desenvolvido por pares do que um profissional competente em cibersegurança deve saber, incluindo as habilidades, técnicas e práticas que são rotineiramente empregadas e estabelece uma estrutura comum de termos e princípios de segurança da informação que permite aos profissionais de cibersegurança e TI/TI em todo o mundo discutir, debater e resolver questões relacionadas à profissão com um entendimento comum, taxonomia e léxico.

71 https://www.cybok.org/

72 Por exemplo, de acordo com (DCMS & IPSOS, 2022), a força de trabalho cibernética britânica trabalha em funções ou especializações específicas: Um papel generalista de segurança cibernética (26%), governança da segurança, risco, conformidade e legalidade (14%), segurança de rede (redes e firewalls) (11%), arquitetura de segurança (11%), gerenciamento de incidentes, resposta e recuperação (10%), operações de segurança (por exemplo, detecção de intrusão) (9%), segurança de sistema (sistemas operacionais e patching) (9%) e testes de penetração (8%).

73 https://www.isc2.org/Certifications/CBK

4.2. DA DEMANA DE MÃO-DE- OBRA

As organizações têm se tornado cada vez mais dependentes da tecnologia e proteger sistemas, redes e dados contra ciberataques é mais desafiador do que nunca, já que ainda mais tecnologias e processos de segurança precisam trabalhar em conjunto. Portanto, as organizações precisam que sua força de trabalho de segurança cibernética seja maior e tenha uma gama de habilidades mais ampla do que nunca.

A partir da análise dos desafios identificados no lado da demanda de mão-de-obra da ciber-segurança, são apresentadas as seguintes considerações a fim de

- Assegurar que a demanda e a oferta falem uma língua comum
- Ajustando os requisitos de recrutamento para atrair os melhores talentos
- Promover a diversidade, a equidade e a inclusão na força de trabalho
- Impulsionar as estruturas dos caminhos de carreira
- Retenção da força de trabalho

Assegurar que a demanda e a oferta falem uma língua comum

Relevância

medida que o mercado de trabalho de segurança cibernética amadurece, tem havido uma necessidade local e regional de um léxico comum para descrever e organizar a força de trabalho de segurança cibernética. É importante que os países disponham de estruturas que gerem um entendimento comum dos papéis, competências, habilidades e conhecimentos utilizados por e para os indivíduos, empregadores e *Provedores de Educação, Treinamento e Certificação*, a fim de lidar com a falta de habilidades cibernéticas de segurança. Além disso, ajuda a facilitar ainda mais o reconhecimento de habilidades relacionadas à cibersegurança, impulsiona o emprego e a empregabilidade em posições relacionadas à cibersegurança. Essas estruturas, que em vários países se tornam padrões, fornecem orientação sobre quais papéis implementar na organização para alcançar as tarefas de cibersegurança necessárias e também maneiras de identificar os talentos certos, formulando descrições de cargos apropriadas que identifiquem corretamente as qualificações e deveres certos que podem ser atribuídos a cada papel.

Desafi

A região carece de esforços de padronização em torno da segurança cibernética, em termos de como as funções de segurança cibernética e as habilidades associadas a essas funções são definidas e descritas e como a força de trabalho é treinada. A falta de padrões unificados para o conhecimento, competência e habilidades que os estudantes devem desenvolver para atender às necessidades e que as organizações devem levar em conta ao criar seus perfis de busca de talentos pode levar a ineficiências no mercado de trabalho de cibersegurança, impactando a transação entre fornecedores e consumidores neste mercado.

Alguns

Gráfico 34.
Benefícios do Quadro Europeu de Habilidades de Segurança Cibernética

Fonte: (ENISA, 2022)

Boas práticas

Uma melhor prática nas Américas é a Iniciativa Nacional de Educação em Segurança Cibernética (NICE) do NIST, que fornece aos empregadores, empregados, educadores, estudantes e provedores de treinamento nos Estados Unidos uma linguagem comum para definir o trabalho em segurança cibernética. Definindo a força de trabalho cibernética de segurança e usando terminologia padrão, o meio acadêmico e os empregadores podem sincronizar educação, recrutamento e desenvolvimento para estabelecer um forte fluxo de talentos e manter uma força de trabalho altamente qualificada. Por exemplo, a *Iniciativa Nacional para Carreiras e Estudos de Segurança Cibernética* desenvolveu a *Ferramenta Caminhos de Carreira Cibernética*[74] , baseada na estrutura NICE, que descreve a força de trabalho descrevendo em detalhes os principais atributos entre cada uma das 52 funções de trabalho definidas[75] em segurança cibernética. Outra boa prática é o desenvolvimento de um Quadro *Europeu de Habilidades de Segurança Cibernética*[76] pela ENISA. A Austrália desenvolveu um *Cyber Skills Framework*[77] que permite o recrutamento direcionado de especialistas cibernéticos, fornece um caminho de desenvolvimento para o pessoal cibernético atual e futuro e alinha habilidades, conhecimentos e atributos com os padrões nacionais e internacionais da indústria.

74 Além disso, o NIST emitiu documentação (Versão preliminar do NISTIR 8193) sobre indicadores de capacidade destinados a ajudar as organizações a determinar se um trabalhador cibersegurança pode desempenhar uma função de segurança cibernética. Os indicadores de capacidade são recomendados para educação, certificação, treinamento, aprendizagem experimental e aprendizagem ao longo da vida que poderiam indicar um aumento da capacidade de desempenhar uma determinada função de trabalho.

75 https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles

76 https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

77 https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework

Ajustando os requisitos de recrutamento para atrair os melhores talentos

Relevância

Os processos de recrutamento são métodos passo a passo para encontrar, recrutar e contratar novos funcionários. Um bom processo de contratação ajuda a atrair e reter funcionários de alta qualidade na força de trabalho cibersegurança. Os elementos específicos de um processo de contratação são exclusivos para cada organização. Os gerentes de contratação dependem de uma ampla gama de táticas e recursos para recrutar todo o pessoal de nível básico e júnior. Enquanto as empresas de recrutamento e os órgãos de certificação se destacam em todos os países, os estágios e aprendizados são mais populares no Reino Unido e na Índia (ISC2, 2022b).

Desafi

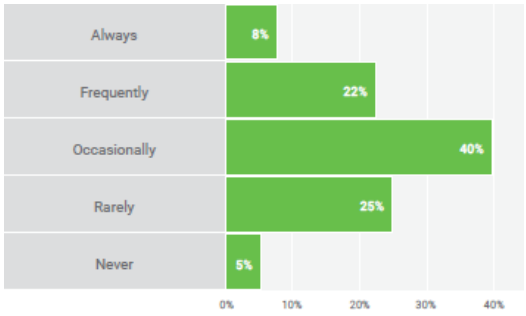
O recrutamento de talentos para funções de segurança cibernética continua sendo um desafio para muitas organizações. Problemas de comunicação continuam a ser observados entre os gerentes organizacionais e seus departamentos de recursos humanos (ISACA, 2022). Além disso, as especificações de trabalho são diferentes se as organizações operam fora da indústria de segurança cibernética. Há também grandes expectativas que os empregadores têm quanto ao nível de habilidade dos candidatos. Em muitos casos, as organizações estão à procura de profissionais de segurança cibernética para empregos de nível básico, mas pedem, inconscientemente, por vários anos de experiência [78]. Além disso, as suposições de alguns empregadores de que os candidatos devem ter um certo grau acadêmico ou certificação para se qualificar para um emprego ou papel de segurança cibernética ou que as promoções devem ser baseadas no tempo em serviço e não nas competências são barreiras para atrair os melhores talentos. Outros problemas são que às vezes é solicitado talento que não é necessário e que os empregadores freqüentemente dispensam pessoas que não possuem credenciais formais, apesar das provas de aquisição de conhecimentos e habilidades de cibersegurança. De acordo com (DCMS & IPSOS, 2022), os recrutadores no Reino Unido dizem que comumente viram especificações de trabalho mal escritas que tentavam recrutar várias funções em uma só, não refletiam os requisitos reais para a função que estava sendo oferecida, ou minimizavam benefícios importantes, como treinamento.

Alguns

Gráfico 35.

Entendendo as necessidades de recrutamento de recursos humanos

Com que freqüência você acha que seu departamento de recursos humanos compreende plenamente suas necessidades de recrutamento cibernético de segurança a fim de pré-selecionar adequadamente os candidatos?



Fonte: (ISACA, 2022)

Gráfico 36.

Status da relação entre ciber-segurança e outras organizações funcionais

Fonte: (ESG, 2021)

Boas práticas

A descrição das funções deve ser uma responsabilidade compartilhada. É importante melhorar continuamente a relação entre segurança cibernética e RH para criar descrições de cargos realistas para funções de nível básico e júnior que estabeleçam expectativas claras para novos funcionários e empregadores (ISC2, 2022b). É importante criar postos de trabalho que sejam atraentes para aqueles que estão saindo de programas de treinamento e educação em segurança cibernética ou que são autodesenvolvidos. As organizações devem redefinir os requisitos mínimos para obter um trabalho básico de cibersegurança e adotar canais de treinamento não-tradicionais. A CISCO desenvolveu um motor de correspondência *Talent Bridge*[79] que automatiza a conexão entre os estudantes da *Cisco Networking Academy* e uma rede de parceiros em todo o mundo, sem custo para empregadores ou estudantes. O motor combina as qualificações dos estudantes com as necessidades dos empregadores, facilitando a contratação de gerentes para identificar rapidamente os melhores candidatos.

78 Por exemplo, uma das certificações mais procuradas é o CISSP, que exige que os candidatos passem no exame e tenham pelo menos cinco anos de experiência acumulada de trabalho remunerado em dois ou mais dos oito domínios do ISC2. Ao se candidatar a esta certificação, os empregadores realmente exigem cinco anos de experiência para um cargo de nível básico.

79 https://www.netacad.com/es/careers/matching-engine

Promover a diversidade, a equidade e a inclusão na força de trabalho

Relevância

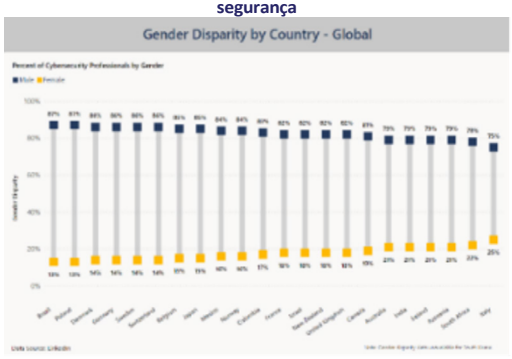
Segundo (FORTINET, 2022), o desafio atual no mercado de trabalho não é apenas contratar mais pessoas, mas também construir equipes mais capazes e diversificadas. Enquanto as empresas precisam de talentos qualificados para uma variedade de funções diferentes, 89% das empresas globais também têm objetivos explícitos de diversidade como parte de seu plano de contratação. Uma equipe de cibersegurança mais diversificada é uma equipe de cibersegurança melhor, porque neste campo multidisciplinar, diferentes perspectivas são críticas. Quando as ameaças mudam a cada dia, os diversos pontos de vista da força de trabalho ajudam a contrariar, trazendo novas idéias para as situações. A este respeito, há países como o Reino Unido onde a força de trabalho cibernética se tornou mais diversificada nos últimos 3 anos, em termos do número de mulheres e minorias étnicas que trabalham em papéis cibernéticos[80].

Desafi

De acordo com o último relatório do centro de política de tecnologia digital da ASPEN, grupos sub-representados como os afro-americanos (9%), hispânicos (4%) e asiáticos (8%) constituem uma porcentagem decrescente da indústria. Na mesma linha, as mulheres constituem 51% da população, mas representam apenas 24% da força de trabalho da cibersegurança (ASPENDIGITAL, 2021). De acordo com (FORTINET, 2022), globalmente, 70% dos gerentes de TI vêem a contratação de mulheres e recém-formados como um dos três maiores desafios. Embora as organizações na América Latina (93%) e na América do Norte (90%) tenham metas de diversidade, provavelmente como resultado de maiores dificuldades no recrutamento dessas populações.

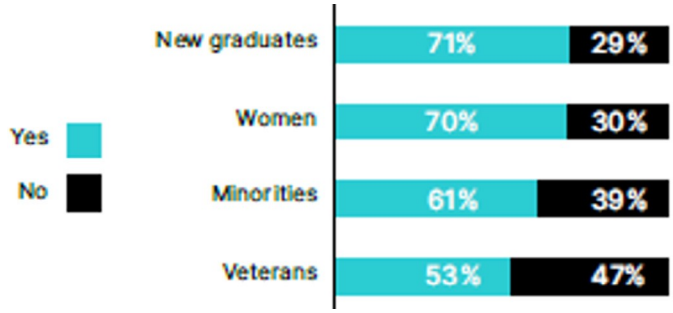
Alguns

Gráfico 37.
Disparidade de gênero na ciber-segurança



Fonte: (MICROSOFT, 2022)

Gráfico 38.
O recrutamento dessas populações é um dos três maiores desafios de sua organização?



Fonte: (FORTINET, 2022)

Boas práticas

No Reino Unido, a importância de ter campeões para o recrutamento cibernético diversificado, dentro das organizações e em toda a indústria, é destacada para ajudar a mudar a cultura entre os empregadores e aumentar a consciência das necessidades dos diversos candidatos (DCMS & IPSOS, 2022). Outra boa prática em organizações é acrescentar linguagem inclusiva nas descrições de cargos que indique explicitamente o interesse em grupos minoritários, tais como pessoas de cor e membros da comunidade LGBTQIA+[81]. Estas práticas promovem ambientes acolhedores para a força de trabalho e o desenvolvimento pessoal e profissional de talentos cibernéticos de segurança. Cingapura tem iniciativas como a SG Cyber Women,[82] com o objetivo de aproveitar o pool de talentos sub-representados e incentivar as mulheres, desde a juventude até a educação terciária, a ingressar na profissão de cibersegurança, que abundam no campo. No nível regional, a CISCO está atualmente oferecendo treinamento gratuito em três (3) fases para toda a comunidade de mulheres chilenas sob o *Programa Chilenas Conectadas y Seguras*[83], visando acelerar a transformação digital e a inclusão de gênero no Chile. Também merece destaque o WOMCY[84], uma iniciativa que busca aumentar a diversidade em cibersegurança na região da América Latina e Caribe, minimizando a lacuna de conhecimento e aumentando as oportunidades para as mulheres na indústria da cibersegurança.

80 De acordo com (DCMS & IPSOS, 2022), há evidências de que a força de trabalho cibernética do Reino Unido se tornou mais diversificada nos últimos 3 anos, tanto em termos de gênero (22% são mulheres, contra 15% em 2020) quanto de etnia (25% são de minorias étnicas, contra 16% em 2020). A força de trabalho sênior (normalmente com 6 ou mais anos de experiência) tende a ser um pouco menos diversificada do que aqueles que ocupam funções mais jovens, em termos de gênero, etnia e status de deficiência. Por exemplo, apenas 13% dos cargos seniores são ocupados por mulheres. Houve um aumento nos esforços para recrutar pessoas com condições neurodiversivas (23% dos empregadores cibernéticos fizeram mudanças para este grupo em comparação com 15% em 2021). Entretanto, ainda é uma minoria que faz adaptações para encorajar qualquer um desses diversos grupos a se candidatar.

81 O termo LGBTQIA+ é um acrônimo para Lésbica, Gay, Bissexual, Transgênero, Intersexual, Queer/Questioning, Asexual.

82 https://www.csa.gov.sg/programmes/sgcybertalent/sgcyberwomen

83 https://www.cisco.com/c/m/es_cl/cda/chilenas-conectadas-y-seguras.html

84 https://womcy.org/

Impulsionar as estruturas dos caminhos de carreira

Relevância

Há muitas oportunidades para os trabalhadores iniciarem e avançarem em suas carreiras de segurança cibernética dentro das organizações. Como os empregados em funções de cibersegurança valorizam empregos que lhes permitem crescer e se desenvolver, os empregadores que não podem oferecer salários generosos ainda podem competir por talentos, oferecendo estruturas de carreira que demonstram potencial de crescimento e aprendizagem. Essas estruturas ajudam os profissionais de cibersegurança a se prepararem para empregos-chave dentro da organização, para oportunidades comuns de transição entre eles e para informações detalhadas sobre salários, credenciais e conjuntos de habilidades associadas a cada função de cibersegurança. Estas estruturas são geralmente seqüências bem articuladas de ofertas educacionais e de treinamento e serviços de apoio que ajudam os profissionais a avançar em sua carreira em um determinado setor ou ocupação.

Desafi

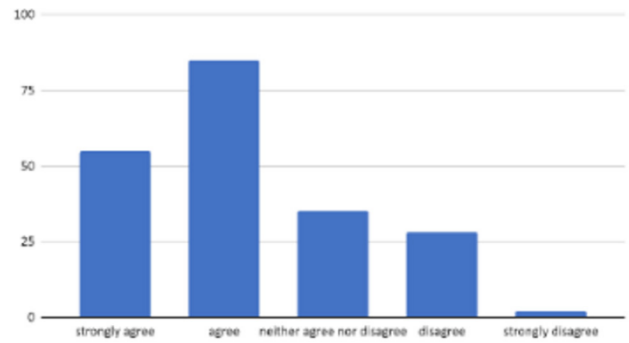
De acordo com (DCMS & IPSOS, 2022), pouco mais de 6 em cada 10 empresas cibernéticas (63%) no Reino Unido informam que empregam pessoal que tem ou está trabalhando para obter qualificações relacionadas à cibersegurança (isto é, no ensino superior, aprendizados ou outro treinamento certificado)[85]. Além disso, os preços de assinatura de algumas associações profissionais, bem como os preços de alguns programas nas estruturas de carreira podem ser superiores ao salário médio mensal de alguns profissionais da cibersegurança nos países em desenvolvimento (GFCE, 2022). Além disso, dois terços das partes interessadas pesquisadas em um estudo sobre o desenvolvimento da cibersegurança como profissão concordaram globalmente que os caminhos de carreira da cibersegurança não são claros e, desses, a maioria achou que essa falta de clareza desencorajava as pessoas de ingressar ou permanecer na profissão de cibersegurança. Esta visão era mais forte entre as pessoas que trabalham no governo (6%) e menos forte entre as pessoas que trabalham no setor privado (40%) (GFCE, 2022).

Alguns

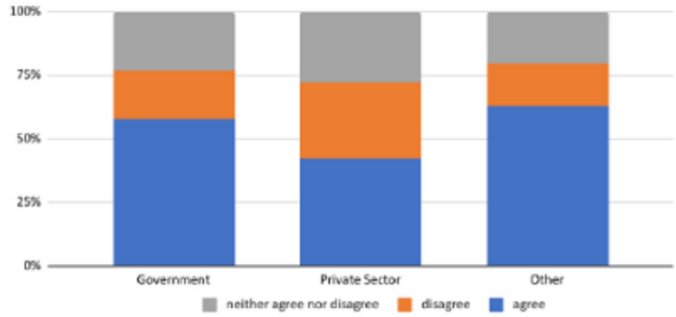
Gráfico 39.

Percepções das estruturas de trajetórias de carreira

Até que ponto você concorda que as estruturas da carreira não são claras?



Fonte: (GFCE, 2022)



Fonte: (GFCE, 2022)

Boas práticas

O site interativo Cyberseek.org[86] contém diversas ferramentas destinadas a ajudar os profissionais a planejar percursos de carreira que mostram os principais empregos de segurança cibernética, oportunidades comuns de transição entre eles e informações detalhadas sobre salários, credenciais e conjuntos de habilidades associadas a cada função. Por exemplo, a *Iniciativa Nacional para Carreiras e Estudos em Segurança Cibernética* desenvolveu a *ferramenta Career Pathway Roadmap*[87] , uma forma interativa para profissionais que trabalham (cibernéticos e não cibernéticos), empregadores para explorar e construir seu próprio roadmap de carreira através das 52 diferentes funções no NICE Framework. Apoiar os caminhos de carreira e criar valor econômico e de emprego a longo prazo requer programas de reciclagem através de aprendizagem transformacional. Muitos fornecedores de certificação oferecem caminhos de carreira a seguir, com cada credencial representando um nível diferente de especialização. Entre os fornecedores de certificação notáveis estão (ISC)2 (https:// www.isc2.org/), CompTIA (https:// www.comptia.org/), ISACA (https://www.isaca.org/), GIAC (https://www.giac.org/), EC-Council (https:// www.eccouncil.org/) e SANS (https://www.sans.org/).

85 A certificação mais freqüentemente solicitada pelos empregadores cibernéticos é o *Certified Information Systems Security Professional (CISSP)*, que foi encontrado em 39% dos postos de trabalho on-line em 2021 que solicitaram uma certificação específica. As certificações *Cisco Certified Network Professional* e *Cisco Certified Network Associate* também foram muito solicitadas no Reino Unido, com 21% das postagens de empregos solicitando cada uma delas.

86 https://www.cyberseek.org/pathway.html

87 https://niccs.cisa.gov/workforce-development/career-pathway-roadmap

Retenção da força de trabalho

Relevância

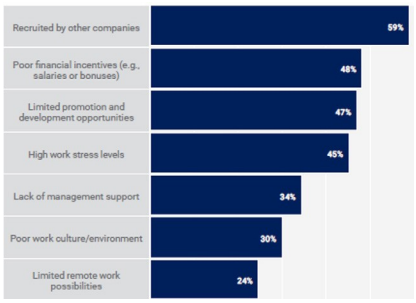
Os departamentos de recursos humanos das organizações devem implementar estratégias de desenvolvimento da força de trabalho cibersegurança para atender às demandas atuais e futuras da força de trabalho. Quando há escassez de profissionais qualificados, as organizações devem inovar para aumentar sua força de trabalho. Para que as empresas se protejam de forma confiável a longo prazo, a coisa mais importante que elas podem fazer é se concentrar na retenção de seus melhores funcionários. De acordo com (WEF, 2022), retenção e equilíbrio entre trabalho e vida pessoal também são fatores que amplificam a escassez de talentos, descobrindo que 6% dos líderes cibernéticos expressam que suas organizações carecem de pessoas e habilidades críticas, 6% dependem de terceiros e recursos externos, 37% têm as pessoas e habilidades de que precisam hoje, e 47% têm falta de treinamento e habilidades em algumas áreas. As organizações devem melhorar sua capacidade de reter pessoas, permitindo que os funcionários atualizem suas habilidades, se tornem certificados e continuem seu desenvolvimento profissional.

Desafi

Há uma série de problemas para as organizações na retenção de talentos da força de trabalho cibernética de segurança. A incapacidade de adquirir e reter os talentos cibernéticos de segurança necessários para enfrentar os desafios atuais é um fator limitante fundamental tanto para o setor privado quanto para o público. Há uma falta de programas de treinamento suficientes e apropriados para os funcionários, especialmente nas PMEs. Além disso, este segmento enfrenta riscos devido à existência de treinamento de cibersegurança de baixa qualidade no mercado de treinamento externo, já que a maioria das organizações compra treinamento principalmente com base no custo e na velocidade, sem inicialmente reconhecer o valor de [cursos] mais [longos][88]. De acordo com (LinkedIn, 2022), as organizações devem agora priorizar o sucesso pessoal dos funcionários através do desenvolvimento profissional. De acordo com (ISACA, 2022), 60% das respostas à pesquisa apontam para a dificuldade de reter talentos em empresas do setor de cibersegurança, sendo as principais causas o recrutamento por outras empresas, baixos incentivos e promoção limitada.

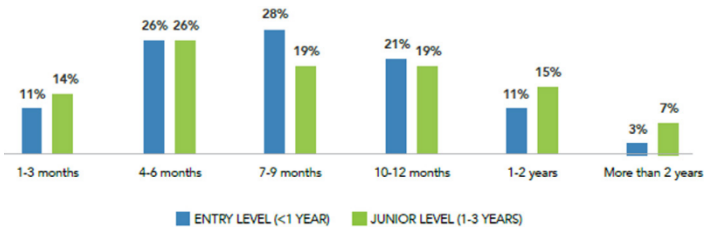
Alguns

Gráfico 40.
Principais causas de demissão entre os profissionais de segurança cibernética



Fonte: (ISACA, 2022)

Gráfico 41.
Quanto tempo leva para treinar o pessoal de nível básico e júnior?



Fonte: (ISC2, 2022b)

Boas práticas

As organizações devem implementar estratégias inovadoras para reter mão-de-obra e talentos, combinando vários incentivos, tais como salário, treinamento, reputação e oportunidades de progresso. De acordo com (MERCER, 2022), as organizações devem considerar diferentes estruturas de recompensa para diferentes modelos de trabalho, por exemplo, uma mudança para uma remuneração baseada em habilidades é uma solução. Também menciona que diferenças geracionais notáveis devem ser consideradas[89], por exemplo, a Geração X e os Baby Boomers valorizam mais o sentimento de pertencer, enquanto os Millennials valorizam mais oportunidades para aprender novas habilidades. De acordo com (ISC2, 2022b), mentoria, certificações e orientação profissional estão entre as ferramentas e recursos que os participantes dos estudos oferecem para ajudar os recém-chegados a ganhar experiência, desenvolver suas habilidades e alcançar novos marcos de carreira. De acordo com (ESG, 2021), algumas ações que a organização poderia tomar para reter a força de trabalho e enfrentar o impacto da falta de habilidades cibernéticas de segurança são: aumentar o compromisso com o treinamento, aumentar os níveis de remuneração, oferecer incentivos tais como pagamento por certificações e participação em eventos, criar/aperfeiçoar programas de estágio cibernético de segurança.

88 De acordo com (DCMS & IPSOS, 2022), isto havia incentivado a entrada no mercado de cursos de treinamento de má qualidade, o que, por sua vez, havia tornado difícil para as organizações distinguir entre treinamento bom e treinamento ruim. Este relatório também menciona que as universidades e os provedores de ensino superior também haviam distorcido o mercado nesta direção ao favorecerem cursos de curta duração ministrados externamente que tinham altas taxas de aprovação. Um indicador disto foi a grande diferença de preços entre os provedores de treinamento mais baratos e mais caros.

89 Um exemplo disso é visto no relatório *Global Recruitment Trends 2022* (LinkedIn, 2022), onde 66% dos entrevistados da Geração Z em sua pesquisa global dizem que gostariam de ver mais investimento em saúde mental e bem-estar para melhorar a cultura da empresa, enquanto 51% dos Millenials, 41% da Geração X e apenas 31% dos Baby Boomers apóiam a idéia.

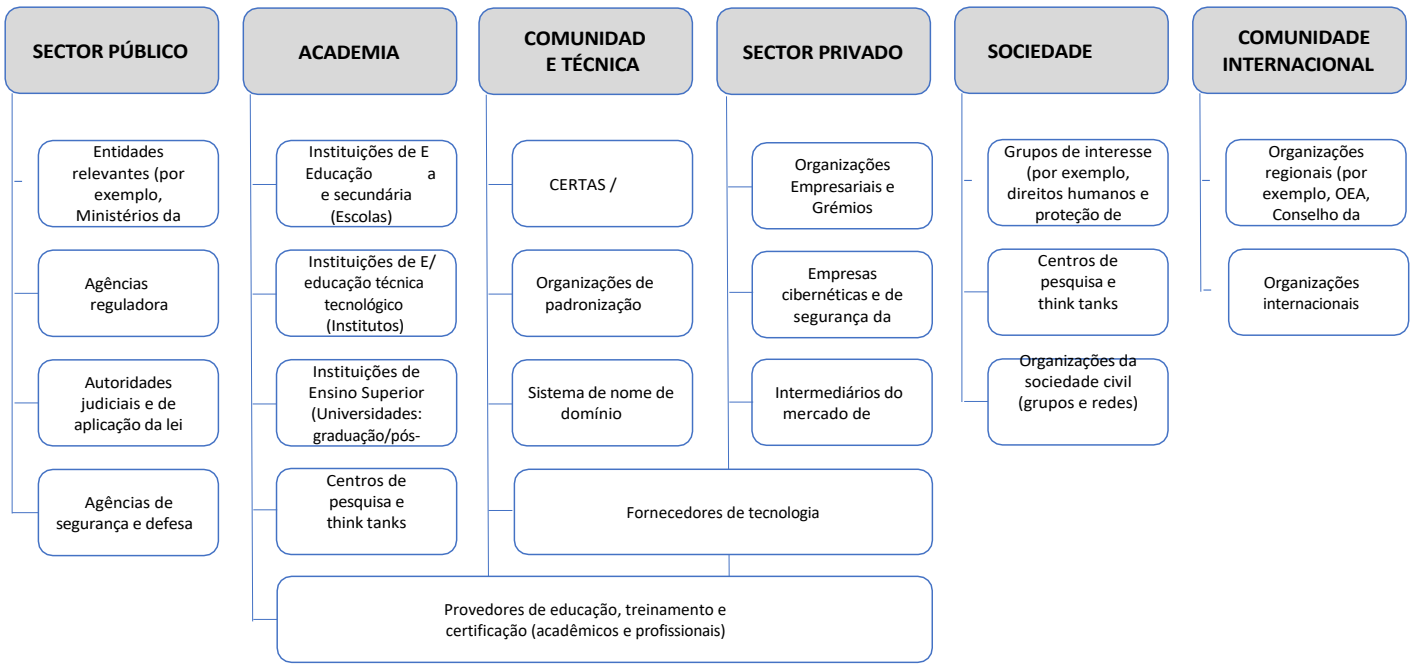
OS MÚLTIPLOS ATORES DA REGIÃO PRECISAM TOMAR MEDIDAS

As condições atuais do mercado de trabalho de cibersegurança e os desafios analisados exigem nos países da América Latina e do Caribe, por um lado, o desenvolvimento e a implementação de novos caminhos em educação e treinamento para o fornecimento de um maior número de candidatos a empregos de cibersegurança com as habilidades necessárias e , por outro lado, o investimento em estratégias inovadoras de recrutamento, treinamento e coaching da força de trabalho atual por parte das organizações.

O problema identificado relacionado à escassez de mão de obra e de habilidades em cibersegurança na região pode ser resolvido trazendo múltiplos interessados (setor público, academia, comunidade técnica, setor privado, sociedade civil e comunidade internacional) para a ação. Internacionalmente, a prática mais comum para resolver o problema identificado é abordar de forma abrangente os desafios no mercado de trabalho de cibersegurança através de abordagens inclusivas e colaborativas que incentivem a participação de múltiplas partes interessadas no ecossistema de cibersegurança.

Gráfico 42.

Representação esquemática das múltiplas partes interessadas envolvidas no desenvolvimento da força de trabalho cibersegurança[90]



Fonte: Elaboração própria

90 Este gráfico ilustra os grupos de partes interessadas relevantes, incluindo uma lista não exaustiva de partes interessadas potenciais em cada grupo. É importante reconhecer que qualquer agrupamento de partes interessadas deve ser abordado com flexibilidade e cautela, pois as categorias e subcategorias podem mudar de acordo com o contexto local de cada país da região e a auto-identificação das partes interessadas. Como regra geral, a estrutura para identificar as partes interessadas relevantes deve ser tão ampla e flexível quanto necessário, de modo a não restringir a participação efetiva das partes interessadas relevantes.

5.1. RECOMENDAÇÕES PARA OS GOVERNOS DA REGIÃO

O problema da cibersegurança e da escassez de profissionais é uma questão política multidimensional que envolve múltiplos interessados e é exacerbada por muitos fatores. Os governos da região desempenham um papel fundamental no desenvolvimento da força de trabalho para proporcionar às pessoas educação, desenvolvimento de habilidades e melhor acesso ao emprego e ao avanço no mercado de trabalho para alcançar o máximo crescimento econômico sustentável em geral.

Em primeiro lugar, recomenda-se que os governos desenvolvam estratégias e planos de ação nacionais para o desenvolvimento da força de trabalho de cibersegurança, tomando pelo menos as seguintes ações:

- Criar um modelo de governança para a articulação e harmonização de múltiplas partes interessadas para fortalecer as capacidades do país em torno do desenvolvimento da força de trabalho de segurança cibernética.
- No lado da oferta de mão-de-obra, desenvolver e incluir um plano de ação para a educação em segurança cibernética[91], abordando os desafios identificados abaixo.
- Do lado da demanda de mão-de-obra, elaborar e incluir um plano de ação para promover o recrutamento, retenção, treinamento e coaching da força de trabalho de segurança cibernética atual, abordando os desafios identificados abaixo.
- Financiar estratégias nacionais e planos de ação relacionados ao desenvolvimento da força de trabalho cibernética de segurança.
- Criar centros de competências e de emprego / fundos (possíveis esquemas de subsídios para segmentos específicos da população).

Em segundo lugar, os governos devem estabelecer estruturas de liderança e coordenação em nível nacional e regional, tomando pelo menos as seguintes ações:

- Reunir todas as partes interessadas em altos níveis de tomada de decisão e em grupos de trabalho.
- Promover a máxima colaboração e cooperação entre as múltiplas partes interessadas, levando em conta o papel e o grau de responsabilidade pelo treinamento e desenvolvimento da força de trabalho.
- Promover o diálogo social e as parcerias multi-stakeholder para o desenvolvimento das habilidades da força de trabalho.
- Facilitar a implementação de iniciativas regionais conjuntas para enfrentar a escassez de mão-de-obra e a lacuna de habilidades de segurança cibernética.
- Desenvolver ecossistemas para treinamento em segurança cibernética que motivem estudantes e profissionais a desenvolver sua carreira em segurança cibernética.

45 Veja a proposta desenvolvida pelo Programa de Segurança Cibernética da OEA e Amazon Web Services (AWS) na edição 9 da série de livros brancos de 2020 *"Cybersecurity Education - Planning for the Future through Workforce Development"* (OAS & AWS, 2020).

Em terceiro lugar, são apresentadas considerações para que os governos abordem os desafios especificamente identificados no desenvolvimento de parcerias público-privadas, atualização das estruturas legislativas e regulatórias, coleta e avaliação contínua de dados relacionados, e conscientização e disseminação de recursos, ferramentas e informações para o desenvolvimento da força de trabalho cibernética de segurança.

1) Estabelecendo estratégias para desenvolver parcerias público-privadas

O desenvolvimento da força de trabalho de cibersegurança depende de uma estreita coordenação entre governos, setor privado e fornecedores de educação ou treinamento. Em particular, os governos deveriam:

- Envolver as organizações de empregadores no lançamento de novos programas de treinamento.
- Atualização dos currículos e programas existentes para melhorar os programas de aprendizagem baseados no trabalho para atender às necessidades do mercado de trabalho.
- Conceber uma estratégia abrangente de desenvolvimento da força de trabalho cibernética que não só abranja políticas voltadas para o sistema de educação, treinamento e habilidades, mas também promova o desenvolvimento de parcerias público-privadas.

2) Atualização ou adaptação das estruturas legislativas e regulamentares para promover o desenvolvimento da força de trabalho

(OEA & BID, 2020) destaca a importância para os países da região da ALC de ter estruturas legais e regulamentares eficazes, a fim de melhorar o nível de maturidade das capacidades de cibersegurança. Uma vez que uma estrutura legislativa estabelece a linha de base mínima de comportamento sobre a qual podem ser construídas mais capacidades de cibersegurança, o objetivo é que os países tenham legislação suficiente para harmonizar as práticas em nível regional/internacional. Os governos devem, portanto:

- Adaptar, adaptar e/ou harmonizar a estrutura jurídica e regulatória nacional em torno da dinâmica da economia digital e suas incertezas inerentes, pois em muitos casos essas estruturas nacionais estão dispersas e desatualizadas em muitas áreas relacionadas à ciber-segurança, incluindo aspectos relacionados aos desafios identificados na análise do mercado de trabalho e que impactam o desenvolvimento da força de trabalho na região.

3) Promover a contínua coleta e avaliação dos dados do mercado de trabalho e da força de trabalho cibersegurança

Em geral, o pessoal de desenvolvimento da força de trabalho cibernética carece de dados precisos para medir e compreender o impacto dos diferentes esforços e intervenções políticas sobre a força de trabalho cibernética de segurança. O fechamento de lacunas no mercado de trabalho de segurança cibernética requer um conhecimento detalhado da força de trabalho de segurança cibernética nos países da região, portanto, os governos da região deveriam:

- Incentivar a cooperação de múltiplas partes interessadas na coleta e compartilhamento de informações[92].

46 Nos Estados Unidos, é destacada a iniciativa CyberSeek, que apresenta empregadores locais, educadores, orientadores e conselheiros de carreira, estudantes, trabalhadores atuais, formuladores de políticas e outras partes interessadas com ferramentas tais como: (i) um mapa de calor interativo que fornece um status instantâneo e granular da oferta e demanda de empregos de cibersegurança em nível estadual e de área metropolitana, (ii) uma proposta de caminhos de carreira que mostra os principais empregos de cibersegurança, oportunidades comuns de transição entre eles e informações detalhadas sobre salários, credenciais e conjuntos de habilidades associadas a cada função, e (iii) uma ferramenta que informa sobre diferentes programas de educação e treinamento, bem como provedores de treinamento no país.

- Promover a colaboração de múltiplas partes interessadas para pesquisar e disseminar resultados sobre fatores que influenciam o impacto da educação, treinamento e desenvolvimento da força de trabalho em cibersegurança.[93]

- Usar os resultados da pesquisa para informar os programas e o desenho do currículo, promover oportunidades de aprendizagem ao longo da vida, impactar o sucesso dos estudantes e garantir acesso eqüitativo.

- Estabelecer e manter um diretório de programas e atividades de projetos, iniciativas e recursos relacionados à conscientização, exploração, preparação, colocação, manutenção e orientação de carreiras cibernéticas de segurança.

- Promover a análise das necessidades do mercado de cibersegurança e tendências relacionadas através da identificação de métricas que mostrem a extensão do problema e possíveis medidas para resolvê-lo.

4) Aumentar a conscientização e disseminar recursos, ferramentas e informações para o desenvolvimento da força de trabalho de segurança cibernética.

Os países da região precisam tornar a população em geral mais consciente de sua segurança pessoal, mas também aumentar a conscientização das oportunidades profissionais em cibersegurança, o que ajudaria a colocar os futuros profissionais de cibersegurança no caminho da carreira. Os governos deveriam:

- Aumentar a conscientização e disseminar recursos, ferramentas e informações de desenvolvimento de força de trabalho cibersegurança para ajudar as organizações a recrutar profissionais qualificados de forma mais eficiente e eficaz, e para fornecer a essa força de trabalho crítica descrições claras de cargos e oportunidades de desenvolvimento.

- Adotar e promover o projeto e desenvolvimento de bancos de dados educacionais, especialmente no setor de ensino superior, sobre cibersegurança e bancos de dados para promover a demanda de mão-de-obra tanto no setor privado quanto no público.

- Trabalhar com a indústria para aumentar a conscientização sobre qualificações, certificações, diplomas e padrões de aprendizagem, alcançando tanto empregadores quanto profissionais de segurança cibernética (GFCE, 2022).

93 Destaca-se a experiência do Reino Unido na realização de pesquisas, estudos e relatórios detalhados sobre o mercado de trabalho cibersegurança, que reúnem dados sobre lacunas e carências de habilidades através da análise da oferta e demanda de mão de obra cibernética. Tais relatórios destacam os desafios de atender as necessidades de contratação e treinamento dos empregadores, por um lado, e a perspectiva dos indivíduos que entram ou são ativos no mercado de trabalho de cibersegurança, por outro, ilustrando as dificuldades que eles enfrentam para encontrar os caminhos certos de carreira e treinamento, e a crescente necessidade de um conjunto de habilidades holísticas em várias funções.

5.2. RECOMENDAÇÕES SOBRE O LADO DA OFERTA DE MÃO-DE- OBRA

A fim de aumentar as vocações científicas entre crianças e jovens da região, as entidades do setor público relacionadas juntamente com o meio acadêmico (instituições de ensino primário e secundário) deveriam:

- Avaliar e atualizar as políticas nacionais de educação que enfatizam as habilidades STEM para professores e alunos.
- Incentivar a alfabetização digital na população infantil e juvenil, promovendo vocações científicas e ênfase na STEM.
- Organizar eventos de massa para explorar o pool de talentos e investir na construção de capacidades e práticas de desenvolvimento de habilidades da STEM.

A fim de fortalecer a proficiência em inglês na região, as entidades do setor público relacionadas juntamente com o meio acadêmico (instituições de ensino primário, secundário e superior) deveriam:

- Avaliar e atualizar as políticas nacionais de educação em andamento para a promoção das línguas e do bilingüismo e identificar as principais dificuldades que afetam as oportunidades para alcançar o domínio da língua inglesa tanto entre os estudantes quanto entre os professores dos sistemas educacionais da região.
- Atualizar programas e/ou estratégias nacionais de bilingüismo incorporando o uso de novas tecnologias para o aprendizado.
- Criar conteúdo educacional complementar relacionado ao gerenciamento de risco de cibersegurança em língua inglesa e treinar estudantes do ensino básico e secundário, bem como estudantes do ensino superior.

A fim de aumentar a conscientização e a sensibilização da cibersegurança em uma idade precoce, as entidades relacionadas do setor público juntamente com o meio acadêmico (instituições de ensino primário e secundário) deveriam:

- Identificar e compartilhar práticas eficazes para promover a conscientização de crianças e jovens e a descoberta de carreiras cibernéticas de segurança.
- Fornecer informações e ferramentas sobre opções de carreira relacionadas à cibersegurança para aqueles que influenciam as escolhas de carreira (por exemplo, professores, conselheiros escolares, orientadores de carreira, mentores, pais ou tutores).
- Aumentar a consciência de privacidade e segurança cibernética entre os usuários de tecnologia, especialmente os usuários jovens, através de treinamento em massa e exercícios de capacitação.

A fim de promover o acesso à oferta educacional, as entidades do setor público relacionadas juntamente com o meio acadêmico (instituições de educação técnica/tecnológica e de ensino superior) deveriam:

- Desenvolver e utilizar ferramentas e recursos para identificar e atrair as pessoas com maior probabilidade de sucesso no mercado de trabalho.
- Diversificar e atualizar os currículos de educação básica, secundária e superior para incluir conteúdo cibernético de segurança.
- Promover e facilitar o acesso a programas acadêmicos relacionados.
- Disponibilizar mais bolsas de estudo e esforços mais ativos e focados na diversidade para aumentar as matrículas.
- Promover e incentivar temas específicos como criptografia nos currículos de educação básica, secundária e superior.

Para conectar a educação com o treinamento e a indústria, o setor público, o setor privado, a comunidade técnica (organizações de padronização) e o meio acadêmico devem:

- Promover o uso de abordagens unificadas das funções, competências, habilidades e conhecimentos de segurança cibernética.
- Desenvolver currículos padronizados que estabeleçam uma taxonomia e um léxico comum para a cibersegurança, de modo que as instituições educacionais alinhem seus currículos com os padrões estabelecidos.
- Integrar o conhecimento da indústria sobre cibersegurança nos vários cursos que compõem a oferta acadêmica, de modo que a desconexão entre o meio acadêmico e a indústria possa ser gradualmente superada.
- Atualização do conteúdo educacional sobre cibersegurança a ser aplicado em ambos os setores: educação de alto nível e indústria relevante.
- Promover casos de uso confiáveis na academia para o desenvolvimento de habilidades.
- Promover desafios e competências no mundo dos negócios para o desenvolvimento de habilidades de segurança cibernética.
- Promover uma estratégia nacional de certificação de segurança cibernética.

A fim de promover o acesso a vias de aprendizagem, o setor público, o setor privado e o meio acadêmico, juntamente com os *Provedores de Educação, Treinamento e Certificação* e os *Provedores de Tecnologia,* deveriam:

- Fomentar a democratização do conhecimento para o desenvolvimento de habilidades.
- Assegurar ligações claras entre escolas, universidades, indústria e o mercado de trabalho de cibersegurança.
- Aumentar a compreensão dos estudantes e das pessoas à procura de emprego sobre os caminhos de aprendizagem e as certificações acadêmicas.
- Trabalhar para garantir que programas de graduação acadêmica e certificações reconhecidas pela indústria meçam efetivamente as competências de segurança cibernética.
- Aumentar o investimento dos parceiros do setor privado na força de trabalho da segurança cibernética.

A fim de esclarecer a definição da profissão de cibersegurança, o setor público, o setor privado e o meio acadêmico, juntamente com os *Provedores de Educação, Treinamento e Certificação*, os *Provedores de Tecnologia,* a Comunidade Técnica (Organismos de Normalização) e a Comunidade Internacional, deveriam:

- Promover iniciativas de padronização nacional (e se possível, regional) de currículos e programas de estudo para estabelecer uma definição de linguagem comum do trabalho de segurança cibernética e a categorização das funções de segurança cibernética.
- Promover o uso de linguagem comum e a categorização de papéis de segurança cibernética na região da ALC.

5.3. RECOMENDAÇÕES SOBRE O LADO DA DEMANDA DE MÃO - DE - OBRA

A fim de garantir que a demanda e a oferta falem uma língua comum, o setor público, o setor privado e o meio acadêmico, juntamente com os *Provedores de Educação, Treinamento e Certificação*, os Provedores de Tecnologia, a Comunidade Técnica (Organismos de Normalização) e a Comunidade Internacional, deveriam:

- Desenvolver estruturas para a geração de um léxico e linguagem comum para gerar incentivos e promover a força de trabalho da segurança cibernética.
- Fornecer clareza sobre funções, papéis e responsabilidades para o desenvolvimento da força de trabalho de segurança cibernética.
- Utilizar tecnologias novas e emergentes para aumentar as conexões e a correspondência entre empregadores e pessoas à procura de emprego.

A fim de ajustar os requisitos de recrutamento para atrair os melhores talentos, as entidades do setor público e as organizações do setor privado devem:

- Melhorar a capacidade de recrutar e contratar efetivamente os talentos necessários para gerenciar os riscos relacionados à cibersegurança.
- Promover o estabelecimento de mais posições e oportunidades de nível básico que proporcionem caminhos para o crescimento e o avanço.
- Promover a comunicação entre as áreas de recursos humanos e de segurança cibernética, a fim de acordar os perfis exigidos pela organização.

A fim de promover a diversidade, equidade e inclusão na força de trabalho, o setor público, o setor privado, a academia, a comunidade técnica, a sociedade civil e a comunidade internacional devem:

- Promover a diversidade na força de trabalho em todos os níveis, melhorar o equilíbrio de gênero e criar programas que levem em conta a diversificação da força de trabalho.
- Identificar e promover métodos de aprendizagem, práticas e programas educacionais eficazes que cresçam e desenvolvam uma força de trabalho cibernética de segurança diversificada e inclusiva.
- Garantir financiamento para treinamento, aperfeiçoamento e reciclagem, especialmente para mulheres, grupos desfavorecidos e os setores mais afetados.

A fim de impulsionar as estruturas dos caminhos de carreira, o setor público, o setor privado e o meio acadêmico, juntamente com os *Provedores de Educação, Treinamento e Certificação* e os *Provedores de Tecnologia,* deveriam:

- Aumentar a acessibilidade e a acessibilidade econômica das estruturas de carreiras de segurança cibernética.
- Expandir orçamentos nos esforços existentes de desenvolvimento da força de trabalho de segurança cibernética.
- Incentivar práticas eficazes de reciclagem de desempregados, subempregados, trabalhadores em atividade para prepará-los para carreiras em segurança cibernética.
- Tomar medidas específicas para incentivar a oferta e a participação em programas de aprendizagem baseados no trabalho, incluindo estágios e aprendizagens.
- Identificar, medir e disseminar oportunidades bem-sucedidas de aprendizagem baseada no trabalho em segurança cibernética.
- Fornecer motivação às organizações através de vários mecanismos para desenvolver cursos e certificações internas, produtos, estruturas, etc.

A fim de manter a força de trabalho, as entidades do setor público e as organizações do setor privado deveriam:

- Identificar, atrair e recrutar os melhores talentos disponíveis e retê-los, implementando estratégias inovadoras de treinamento e coaching, tais como: i) Upskilling (processos de aprendizagem de novas habilidades ou ensino de novas habilidades aos funcionários), ii) Reskilling (processos de treinamento de funcionários em um conjunto completamente novo de habilidades para prepará-los para assumir um papel diferente dentro da empresa), e iii) New Skilling (processos de aprendizagem contínua para ajudar a desenvolver habilidades de alta demanda, quer uma pessoa esteja tentando melhorar as habilidades atuais ou precise de uma atualização completa para desenvolver habilidades completamente novas).
- Promover programas de aprendizagem baseados no trabalho, incluindo estágios e colocações de trabalho.
- Fornecer incentivos para desenvolver funcionários de nível inicial em talentos de meia-carreira e talentos de carreira avançada.
- Incentivar e permitir o desenvolvimento e treinamento contínuo dos funcionários, incluindo programas rotativos e de intercâmbio, para fomentar a retenção de talentos atuais com diversas habilidades e experiências.

06

REFERÊNCIAS BIBLIOGRÁFICAS

ASPENDIGITAL (setembro de 2021). Diversidade, Equidade e Inclusão na Ciber-segurança. Obtido em https://www.aspeninstitute.org/wp- content/uploads/2021/09/Diversity-Equity-and-Inclusion-in-Cybersecurity_9.921.pdf

BID. (2020). O futuro do trabalho na América Latina e no Caribe - Qual é o impacto da automação no emprego e nos salários? Obtido em https://publications.iadb.org/publications/spanish/document/El-futuro-del-trabajo-en-America-Latina-y-el-Caribe-Cual- es-el-impacto-de-la-automatizacion-en-el-empleo-y-los-salarios.pdf

BID. (2021). *O impacto da automação, além das fronteiras.* Obtido em https://blogs.iadb.org/trabajo/es/el-impacto-de-la-automatização-mas-alla-las-fronteras/

BID, ECLAC & KAS (2021). Recuperação econômica após a pandemia COVID-19 - Capacitando a América Latina e o Caribe a tirar melhor proveito do comércio eletrônico e do comércio digital. Obtido em https://publications.iadb.org/publications/spanish/document/Recuperacion-economica-tras-la-pandemia-COVID-19-empoderar-a-America-Latina-y-el-Caribe-para-un-mejor-aprovechamiento-del-comercio-electronico-y-digital.pdf

CISCO (2022). *Os funcionários estão prontos para o trabalho híbrido, você está? Cisco Global Hybrid Work Study 2022*. Obtido em https://www.cisco.com/c/ dam/m/en_us/solutions/global-hybrid-work-study/reports/cisco-global-hybrid-work-study-2022.pdf

Informática (2022). Obtido de Women in Computer Science: Getting Involved in STEM: https://www.computerscience.org/resources/women-in-computer-science/

Cook, I. (15 de setembro de 2021). "(T. H. Review, Editor) Obtido do site https://hbr.org/2021/09/ who-is-driving-the-great-resignation.

CSA. (2021). Quadro de Competência de Tecnologia Operacional Cybersecurity. Obtido do site https://www.csa.gov.sg/News/Publications/ - estrutura de competência operacional-tecnologia-segurança-certeza-competência-(otccf)

CSES. (2018). Identificando o Papel da Educação Superior e Avançada no Desenvolvimento de Habilidades de Segurança Cibernética. Obtido do site https://www.gov.uk/ governo/publicações/publicações/o papel da educação avançada e superior em segurança cibernética - habilidades

CyberSeek (agosto de 2022). *Cybersecurity supply/demand heat map.* Obtido em https://www.cyberseek.org/heatmap.html

DCMS & IPSOS (2022). Habilidades de segurança cibernética no mercado de trabalho do Reino Unido 2022 - Relatório de resultados. Obtido em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf

DELOITTE (2020). Desenvolvimento da força de trabalho: Equipar a força de trabalho para o futuro. Obtido em https://www2.deloitte.com/us/en/pages/ human-capital/articles/workforce-development-strategies.html

DNP. (2020). Política Nacional de Confianza y Seguridad Digital de Colombia (Documento CONPES 3995 de 2020). Obtido em https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

DNP. (2022). Política Nacional de Ciencia, Tecnología e Innovación de Colombia 2022-2031 (Documento CONPES 4069 de 2022). Obtido em https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%c3%b3micos/4069.pdf

ENISA (2022). European Cybersecurity Skills Framework ECSF - Draft v0.5. Obtido de https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills framework/ecsf-profiles-v-0-5-draft-release.pdf

ESG (2021). ESG Infográfico: a Vida e Tempos dos Profissionais de Segurança Cibernética 2021. Obtido em https://www.esg-global.com/research/ esg-infographic-the-life-and-times-of-cybersecurity-professionals-2021

FORBES. (31 de julho de 2022). *O Futuro do Trabalho: Mais Híbrido, Mais Colaborativo, Mais Automatizado.* Obtido em https://www.forbes. com/sites/danielnewman/2022/07/31/the-future-of-work-more-hybrid-more-collaborative-more-automated/?sh=77896d589c46

FORTINET. (18 de agosto de 2022). Obtido em https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-register-137-billion-cyberattack-attempts-e

FORTINET. (2022). 2022 Cybersecurity Skills Gap - Global Research Report. Obtido em https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

GFCE. (julho de 2022). Developing Cyber Security as a Profession - A Report by the Global Forum on Cyber Expertise. Obtido em https://thegfce.org/wp-content/uploads/2022/08/GFCE-Report-Developing-Cyber-Security-as-a-Profession-July-2022-1.pdf

GFCE. (2022). Pre-University Cyber Security Education: A report on developing cyber skills among children and young people. Obtido em https://thegfce.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

PARCEIROS GLOBAIS DIGITAL (2018). *Abordagens Multistakeholder Approaches to National Cybersecurity Strategy Development (Abordagens Multistakeholders para o Desenvolvimento da Estratégia Nacional de Segurança Cibernética).* Obtido de Multistakeholder Approaches to National Cybersecurity Strategy Development: https://www.gp-digital.org/publication/multistakeholder- approaches-to-national-cybersecurity-strategy-development/

OIT (11 de agosto de 2022). *Tendências globais de emprego para a juventude.* Obtido em https://www.ilo.org/global/about-the-ilo/newsroom/news/ WCMS_853078/lang--en/index.htm

OIT (2022). ILOSTAT. Obtido em https://ilostat.ilo.org/es/data/

ISACA (2022). Estado de Segurança Cibernética 2022. Obtido em https://www.isaca.org/go/state-of-cybersecurity-

2022 ISC2. (2021). Estudo da força de trabalho da Cybersecurity. Obtido em

https://www.isc2.org/Research/Workforce-Study

ISC2 (2022a). Estudo da força de trabalho da Cybersecurity. Obtenido de https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx

ISC2 (2022b). Melhores Práticas para Contratação e Desenvolvimento de Entrada e Práticas Cibernéticas de Nível Júnior de Segurança. Obtido em https://www. isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ashx

Kang, N. (2019). Uma revisão do efeito da educação integrada STEM ou STEAM (ciência, tecnologia, engenharia, artes, artes e matemática) na Coréia do Sul. *Asia Pac. Sci. Educ.* doi: https://doi.org/10.1186/s41029-019-0034-y

LinkedIn (2022). A Reinvenção da Cultura da Empresa - Tendências Globais de Talentos 2022. Obtido em https://business.linkedin.com/content/ dam/me/business/en-us/talent-solutions-lodestone/body/pdf/global_talent_trends_2022.pdf

LinkedIn (2022). A Transformação da L&D - Aprendizagem abre o caminho através da Grande Reorganização. Obtido em https://learning.linkedin. com/content/dam/dam/me/learning/en-us/pdfs/workplace-learning-report/LinkedIn-Learning_Workplace-Learning-Report-2022-pt.pdf

MERCER (2022). Rise of the relatable organization - Global Talent Trends 2022 Study. Obtido em https://www.mercer.com/our-thinking/career/global-talent-hr-trends.html

MichaelPage. (2022). Estudo LATAM Outlook 2022. Obtido de https://www.michaelpage.com.co/estudios-y-tendencias/ perspectivas-2022

MICROSOFT. (23 de março de 2022). *Fechando a lacuna de habilidades cibernéticas de segurança - A Microsoft expande os esforços para 23 países.* Obtido em https:// blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

MINEDUCACION (setembro de 2022). *Sistema Nacional de Informação do Ensino Superior -SNIES-.* Obtido em https://hecaa.mineducacion.gov.co/consultaspublicas/programas

NICCS (2022). *Ferramenta Cyber Career Pathways.* Obtido em https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

OAS & AWS (2020). Cybersecurity Education - Planejamento para o futuro através do desenvolvimento da força de trabalho. Obtido em https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OEA E BID. (2020). Cybersecurity Report 2020 - Risks, Progress and the Way Forward in Latin America and the Caribbean (Relatório de Segurança Cibernética 2020 - Riscos, Progressos e o caminho a seguir na América Latina e no Caribe). Obtido em https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

OEA & GPD. (2022). National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions (Estratégias Nacionais de Segurança Cibernética: Lições Aprendidas e Reflexões das Américas e Outras Regiões). Obtido em https://www.gp-digital.org/publication/national-cybersecurity-strategies-lessons-learned-and-reflections-from-the-americas-and- outras regiões/

OCDE (2021). OECD Employment Outlook 2021: Navigating the COVID-19 Crisis and Recovery (Perspectivas de Emprego da OCDE 2021: Navegando na Crise e Recuperação da COVID-19). Paris: OECD Publishing. Obtido em https:// read.oecd-ilibrary.org/employment/oecd-employment-outlook-2021_5a700c4b-en#page1

OCDE (2022). Obtido de OECD Data - Mathematics performance (PISA): https://data.oecd.org/pisa/mathematics-performance-pisa. htm

OCDE (2022). *Apoio ao desenvolvimento das PMEs na América Latina e no Caribe.* Obtido de https://www.oecd.org/latin-america/regional-programa/produtividade/meio-desenvolvimento/

Oxford Martin School (2022). *Oxford Institute of Populating Ageing (Instituto do Envelhecimento Populacional de Oxford).* Obtido em https://www.oxfordmartin.ox.ac.uk/ageing/

RAND (2014). Procura-se Hackers: Um exame da Ciber-segurança. Obtido em https://www.rand.org/pubs/research_reports/RR430. html.

WEF. (2022). Global Cybersecurity Outlook 2022. Obtido em https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

WEF. (2022). Relatório sobre a Lacuna Global de Gênero 2022. Obtido de https://www.weforum.org/reports/global-gender-gap-report-2022/.

WICKR (18 de fevereiro de 2021). Obtido de The Future of Cybersecurity Depende da Educação STEM: https://wickr.com/the-future-of-cybersecurity-depends-on-stem-education/

Banco Mundial (2019). Obtido de Quais são as principais lições dos últimos resultados do PISA 2018 para a América Latina?: https://blogs. worldbank.org/latinamerica/what-are-the-main-results-pisa-2018-latin-america

BANCO MUNDIAL (2022). *Crescimento Global para Abrandar até 2023, Somando ao Risco de 'Aterragem Difícil' em Economias em Desenvolvimento.* Obtido em https:// www.worldbank.org/en/news/press-release/2022/01/11/global-recovery-economics-debt-commodity-inequality

2023

Relatório sobre o desenvolvimento da FORÇA DE TRABALHO DE CIBERSEGURANÇA em uma era de escassez de talentos e habilidades

OEA Más derechos para más gente

Cybersecurity Innovation Councils

CISCO