2020

White paper series
Publicação 5

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do desenvolvimento da força de trabalho

OEA Mais direitos para mais pessoas | aws

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do desenvolvimento da força de trabalho

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

CRÉDITOS

Luis Almagro
Secretário-Geral
da Organização dos Estados
Americanos (OEA)

Equipe técnica da OEA
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Gabriela Montes de Oca Fehr
Babara Marchiori de Assis
Rolando Ramirez

Equipe técnica da AWS
Abby Daniell
Melanie Kaplan
Jordana Siegel
Andres Maz

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do
desenvolvimento da força de trabalho

ÍNDICE

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do
desenvolvimento da força de trabalho

Qual o objetivo deste documento?

À medida que aumenta o número de atividades maliciosas no ciberespaço, cresce também a necessidade de uma força de trabalho treinada em segurança cibernética. São habilidades indispensáveis para essa força de trabalho a capacidade de projetar e operar adequadamente aplicativos e sistemas para identificar as ameaças cibernéticas e responder a elas, bem como a capacidade de formular políticas públicas eficazes para combater essas ameaças. Os desafios futuros só podem ser enfrentados promovendo-se carreiras em segurança cibernética. A disparidade entre a oferta e a demanda de profissionais qualificados nessa área exige ações imediatas de treinamento dos profissionais atuais, enquanto as políticas para educar a próxima geração de profissionais de segurança cibernética estão sendo elaboradas. Sem políticas para melhorar as habilidades em segurança cibernética da força de trabalho, os países não poderão aproveitar plenamente os benefícios da economia digital. Este documento delineia os passos para a concepção de um plano de ação de educação em segurança cibernética (Cybersecurity Education Action Plan, CEAP), do qual constam mecanismos para integrar a educação em segurança cibernética à formulação de políticas e currículos escolares, a fim de lidar com a escassez dessa qualificação na América Latina e no Caribe. Ele também oferece um conjunto de iniciativas e mecanismos no nível nacional para gerar interesse em carreiras relacionadas com a segurança cibernética.

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do
desenvolvimento da força de trabalho

Por que a educação em segurança cibernética é importante na América Latina?

A Quarta Revolução Industrial é alimentada pela mais profunda interconectividade do mundo (Schwab, 2016, p. 3). A América Latina tem adotado rapidamente os serviços digitais possibilitados pela computação em nuvem, pelos dispositivos móveis e pelas redes de banda larga, permitindo uma transformação profunda dos governos e das empresas, inclusive com a incorporação do processamento de dados para a tomada de decisões integradas e eficazes por parte dos formuladores de políticas. Com a adoção dessas tecnologias na América Latina, o novo cenário também implicou uma transformação na natureza e nas operações do crime. Na América Latina e no Caribe, o custo do crime cibernético foi estimado entre US$ 15 bilhões e US$ 30 bilhões em 2017, ou seja, entre 0,28% e 0,57% do PIB da região (Lewis, 2018, p. 7). Os países da região não são apenas alvo dos ataques online, mas também fonte ativa deles (Lewis, 2018, p. 20). O aumento dos riscos cibernéticos exige que as empresas e os governos incorporem a segurança cibernética no tecido de seus processos, na aquisição de tecnologia e no recrutamento de pessoal.

Apesar dessas ameaças, ainda existe uma escassez global de profissionais de segurança cibernética, a qual se estima ser aproximadamente 4,07 milhões de pessoas. Somente na região da América Latina, ela é de aproximadamente 600.000 pessoas ((ISC)², 2019, p. 8). Esse número representa um aumento significativo em comparação com 2018, quando a escassez foi estimada em cerca de 136.000 profissionais ((ISC)², 2018, p. 4). Tanto as empresas de médio como de grande porte têm alta demanda por profissionais de segurança cibernética, o que requer uma força de trabalho preparada para projetar, construir e operar as mais recentes tecnologias, principalmente no nível técnico (Fórum Econômico Mundial , WEF, 2015, p. 20).

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do
desenvolvimento da força de trabalho

Educação em segurança cibernética

Na América Latina e no Caribe, a lacuna na demanda de mão de obra em segurança cibernética aumentou, especialmente em empresas de médio porte ((ISC)2, 2019). De acordo com o relatório de 2019 do (ISC)2, "é provável que os profissionais de segurança cibernética tenham pelo menos um diploma de bacharelado — pouco mais de um terço tem mestrado ou doutorado/pós-doutorado". Enquanto a maioria nessa área obtém seus diplomas em informática e ciências da informação (40%), outros obtêm diplomas que não são focados em TI, como engenharia (19%) e negócios (10%). Mais especificamente sobre a região, o relatório indica que as organizações são mais propensas a recrutar profissionais formados em instituições educacionais e fornecedores de segurança. A realidade é que a grande maioria dos profissionais de segurança cibernética não começou nessa área, mas seguiu outra trilha de carreira, e muitos começaram até em áreas não relacionadas a TI. Os formuladores de políticas devem adotar uma abordagem nacional para a educação em segurança cibernética fim de construir um pipeline de profissionais e pensar estrategicamente a forma de posicionar a educação na estrutura nacional de segurança cibernética.

O pilar da educação

Numerosas ferramentas foram criadas para ajudar a avaliar o estado da capacidade de segurança cibernética de um país. Dois exemplos são o Modelo de Maturidade da Capacidade em Segurança Cibernética das Nações (Cybersecurity Capacity Maturity Model for Nations, CMM) e o Índice Global de Segurança Cibernética. Essas ferramentas enfatizam a importância da educação em segurança cibernética para a capacidade cibernética de uma nação e incluem a essa educação como um pilar fundamental da estratégia nacional.

O CMM, criado pelo Global Cyber Security Capacity Centre (GCSCC),[1] é uma métrica que avalia o estado nacional das capacidades de segurança cibernética em um país. O CMM inclui uma seção dedicada à educação, treinamento e habilidades em segurança cibernética, que destaca a educação em segurança cibernética como um pilar-chave a ser considerado pelos formuladores de políticas na avaliação das capacidades em segurança cibernética através da preparação, qualidade e aceitação de ofertas educacionais e de treinamento para vários grupos, incluindo representantes governamentais, setor privado e a população como um todo (Cybersecurity Capacity Portal, 2020). Essa seção é dividida em três componentes principais: (1) conscientização dos cidadãos, (2) estrutura para a educação e (3) estrutura para o treinamento profissional. Enquanto o primeiro se concentra na existência de campanhas de conscientização para um público geral, o segundo refere-se a programas

1. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

credenciados no nível universitário, iniciativas de pesquisa e desenvolvimento (P&D) e um currículo nacional de segurança cibernética. O terceiro componente destaca a importância das certificações em segurança cibernética e os programas de treinamento para apoiar o desenvolvimento de habilidades ao longo do tempo.

Da mesma forma, o Global Cybersecurity Index 2018 (CGI), criado pela União Internacional de Telecomunicações (UIT),[2] ressalta a importância de se combinarem diferentes abordagens, técnicas e ferramentas para fechar a lacuna educacional da segurança cibernética. Como o CMM, o CGI tem indicadores similares no pilar "capacitação", que abrange "campanhas de conscientização pública, estrutura para a certificação e credenciamento de profissionais de segurança cibernética, cursos de treinamento profissional em segurança cibernética, programas educacionais ou currículo acadêmico em segurança cibernética, investimento em programas de P&D em segurança cibernética, mecanismos de incentivo e indústria de segurança cibernética doméstica" (UIT, 2019, p. 8). Ambos os modelos também destacam a importância dos programas educacionais, que podem influenciar as mudanças sociais e o crescimento econômico.

Esses modelos e índices de maturidade cibernética demonstram que a educação também deve ser destacada na estratégia nacional de segurança cibernética de um país. Na América Latina, os governos da Argentina, Brasil, Chile, Colômbia, Costa Rica, Guatemala, México, Panamá, Paraguai e República Dominicana publicaram ou atualizaram suas estratégias nacionais de segurança cibernética. Constam dessas estratégias uma estrutura de capacitação e linhas de ação para fortalecer a educação em segurança cibernética no âmbito nacional. Os dois primeiros objetivos da estratégia nacional da Argentina, por exemplo, concentram-se na conscientização e educação em segurança cibernética[3]. Quatro dos sete objetivos da Política Nacional de Segurança da Informação do Brasil estão relacionados a P&D, capacitação da força de trabalho, desenvolvimento de habilidades e uma cultura de segurança da informação.[4] Da mesma forma, o escopo das estruturas nacionais de segurança cibernética do Chile e da Colômbia tem a educação como uma característica fundamental para melhorar a maturidade da segurança cibernética; as referidas estruturas também identificam ações específicas a serem realizadas, estabelecendo um cronograma e determinando os atores responsáveis pelas tarefas. Os planos de ação de educação em segurança cibernética podem fortalecer e nortear as políticas de segurança cibernética a fim de abordar as deficiências da força de trabalho individual e dos sistemas educacionais.

No momento da finalização deste documento, a COVID-19 havia-se tornado uma pandemia global e transformado a educação mundial. Os ministérios e departamentos federais, estaduais e provinciais de educação tiveram de se adaptar rapidamente e migrar seu conteúdo educacional para a nuvem a fim de garantir acesso ininterrupto ao ensino a distância para milhões de estudantes e educadores. As universidades públicas e privadas, as faculdades e as escolas de ensino fundamental e médio fizeram o mesmo. O ensino a distância tornou-se cada vez mais predominante, o que desencadeou a necessidade de abordar questões de segurança cibernética na conectividade para permitir o aprendizado. Exercícios de treinamento on-line e mecanismos de apoio para professores e estudantes sobre educação em segurança cibernética são agora mais prioritários na adaptação ao aprendizado virtual.

---

2. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

3. Argentina (2019). Estrategia Nacional de Ciberseguridad. Disponível em: http://www.enre.gov.ar/web/bibliotd.nsf/203df3042bad9c40032578f6004ed613/1e2bd1ba24f72e9b03258408003abee3/$FILE/anexo%201pdf.

4. Brasil (2018). Política Nacional de Segurança da Informação. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm.

A construção de um plano de ação de educação em segurança cibernética

Um plano de ação de educação em segurança cibernética (CEAP) é um plano para que os formuladores de políticas elaborem políticas públicas eficazes destinadas a fortalecer suas estratégias nacionais de segurança cibernética e desenvolver a força de trabalho em segurança cibernética.

O diagrama abaixo demonstra como um CEAP se integra aos objetivos globais da estratégia nacional de segurança cibernética como uma linha de ação específica para abordar o pilar da educação.

Estratégia Nacional de Segurança Cibernética

Plano de ação de educação em cibernética

A elaboração de um CEAP deve considerar o seguinte:

1. Estabelecimento de metas.

2. Integração das partes interessadas.

3. Estabelecimento de objetivos e métricas.

4. Criação de um plano de implementação.

5. Identificação dos recursos necessários para a implementação.

A Iniciativa Nacional para Educação em Segurança Cibernética (NICE),[5] liderada pelo Instituto Nacional de Normas e Tecnologia (NIST) nos Estados Unidos, é um exemplo de iniciativa política que pode ser replicada na elaboração de um CEAP. A NICE opera como uma parceria entre o governo, o setor privado e a sociedade civil para enfrentar a escassez de mão de obra, aumentando a capacidade do país de enfrentar os desafios atuais e futuros da segurança cibernética. Considerando a natureza multidisciplinar da segurança cibernética e as principais recomendações recebidas das partes interessadas, tanto acadêmicas e privadas como governamentais, o Quadro NICE define claramente os papéis e as funções das partes interessadas no aprimoramento das capacidades de segurança cibernética nos Estados Unidos (NIST, 2017, pp. 1-2). A partir de agosto de 2020, o NIST realizará uma consulta pública com o objetivo de atualizar o quadro Nice, devendo lançar a última versão em novembro de 2020.[6]

O NIST, por meio do quadro NICE, fornece aos formuladores de políticas exemplos da importância de se adaptarem as atividades de segurança cibernética a cada etapa do ciclo de desenvolvimento da força de trabalho. A estrutura pode ser usada como um guia para as organizações prepararem programas de treinamento e educação em segurança cibernética, que podem ser adaptados por cada país. Mundialmente, esse é o único quadro que procura padronizar as funções necessárias para a força de trabalho em segurança cibernética, abrangendo tanto as funções técnicas quanto as não técnicas. Países como Austrália, Cingapura e Japão usaram a iniciativa NICE como base para a criação de suas próprias estruturas e as difundiram em seus setores público, privado e acadêmico. Atualmente, nenhum país da América Latina e do Caribe adotou formalmente o quadro NICE.

As seções a seguir descrevem os cinco passos cruciais para a criação de um CEAP em conformidade com o quadro NICE. A primeira seção, estabelecimento de metas, fixa metas específicas que definirão os resultados do plano de ação no longo prazo. A segunda seção, integração das partes interessadas no plano de ação de educação em segurança cibernética, descreve a importância de identificar adequadamente os atores que participarão da concepção e implementação do plano de ação. A terceira seção, estabelecimento de objetivos e métricas, descreve a importância de selecionar objetivos que sejam mensuráveis e aplicáveis ao contexto no qual o plano de ação será aplicado. A quarta seção, implementação de um plano de educação em segurança cibernética, identifica ações detalhadas que podem ser incorporadas em cada etapa da educação e ciclo de desenvolvimento da força de trabalho. Por fim, a última seção traz uma lista abrangente de recomendações práticas para tornar o Plano de Educação em Segurança Cibernética uma realidade.

5. Consulte o Anexo para obter mais detalhes.

6. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-draft-revision

Estabelecimento de metas

Nos estágios iniciais do projeto de CEAP, os formuladores de políticas devem selecionar um número limitado de objetivos e considerar o contexto social e econômico do país para estruturar um plano de ação bem-sucedido. Ao selecionar algumas metas relevantes e alcançáveis, os formuladores de políticas podem definir melhor o CEAP.

Para garantir sua eficácia, um CEAP deve concentrar-se em: (a) lidar com a escassez de educação e habilidades em segurança cibernética e (b) aumentar a conscientização sobre as lacunas em segurança cibernética e a importância dessa área. Como exemplo, o quadro NICE delineia três objetivos para enfrentar a escassez de educação e habilidades em segurança cibernética. Estes são objetivos não exclusivos, embora sejam abrangentes e completos, e podem ser úteis quando adaptados aos objetivos específicos que os formuladores de políticas procuram atingir.

1. Acelerar a aprendizagem e o desenvolvimento de habilidades: Descreve a importância de criar consciência sobre a necessidade de educação em segurança cibernética entre os atores públicos e privados. Especificamente, recomenda o engajamento de trabalhadores deslocados que possam estar disponíveis para desempenhar funções de segurança cibernética, bem como a experimentação do uso de programas de educação cooperativa onde os indivíduos podem se tornar parte da força de trabalho e ganhar um salário enquanto ainda aprendem as habilidades necessárias.

2. Nutrir uma comunidade de aprendizagem diversificada: Procura garantir que a educação em segurança cibernética enfatize o aprendizado contínuo, seja mensurável e incorpore a diversidade. Para promover a diversidade, a iniciativa NICE recomenda incentivar ativamente os membros de minorias sub-representadas para que aproveitem as oportunidades de aprendizagem em segurança cibernética. Este objetivo também encoraja os setores público e privado a inspirar a consciência da carreira de segurança cibernética, começando no nível do ensino fundamental, para facilitar o desenvolvimento de carreiras acadêmicas.

3. Orientar o desenvolvimento de carreira e o planejamento da força de trabalho: Especifica a necessidade de apoiar os empregadores no recrutamento, retenção e desenvolvimento contínuo de sua força de trabalho. Defende medidas como o auxílio aos profissionais de recursos humanos no desenvolvimento de ferramentas para gerentes e a análise das fontes de dados para realizar um recrutamento direcionado.

Os formuladores de políticas devem levar em consideração as opiniões daqueles direta e indiretamente envolvidos na criação e implementação do CEAP. Graças à participação das partes interessadas nesse processo, os formuladores de políticas podem reforçar a eficácia da estratégia e atingir as metas estabelecidas. A seção seguinte oferece uma visão geral sobre como identificar e envolver as partes interessadas da melhor forma possível.

Integração das partes interessadas no plano de ação de educação em segurança cibernética

A colaboração de múltiplas partes interessadas é essencial durante a formulação e implementação de um CEAP. Durante a fase de formulação, a parceria entre o governo, o setor privado e a sociedade civil ajuda a avaliar as necessidades atuais de mão de obra e a identificar iniciativas relevantes já em andamento do ensino fundamental ao superior.

Os governos da América Latina e do Caribe podem começar pelo mapeamento das principais partes interessadas da indústria, do meio acadêmico e da sociedade civil para convidá-las imediatamente a participar do processo de formulação do CEAP. Para tanto, é essencial comunicar claramente o seguinte às partes interessadas: (1) os objetivos e o escopo do plano de ação nacional de educação em segurança cibernética, (2) o cronograma, os marcos e os resultados do processo de formulação e (3) os mecanismos de tomada de decisões no processo de formulação (por exemplo, como o plano de ação será aprovado e como os comentários e contribuições das diferentes partes interessadas serão considerados, analisados e, finalmente, incorporados). Os formuladores de políticas podem envolver as partes interessadas criando comitês, realizando oficinas e emitindo consultas públicas, entre outros mecanismos. Os países que desenvolveram suas estratégias nacionais de segurança cibernética por meio de processos que envolveram a participação de várias partes interessadas podem aplicar essa experiência à formulação de seus CEAPs próprios.[7]

Além disso, para implementar um plano de ação nacional de educação em segurança cibernética, os formuladores de políticas devem considerar a criação de um comitê ou comissão de órgãos governamentais para coordenar a implementação de políticas educacionais, bem como grupos de trabalho abertos a contribuições e recomendações de vários setores. O caso NICE é um bom exemplo de mecanismos de coordenação, incluindo o Conselho Coordenador Interagência NICE (ICC) e o Grupo de Trabalho. Enquanto o primeiro compreende os órgãos governamentais que lideram a implementação do plano de ação, o segundo procura reunir representantes de diferentes setores. Ambas as estruturas devem ser consideradas na implementação de um CEAP nacional. É importante salientar que muitos países da América Latina e do Caribe desenvolveram um modelo similar para a implementação de suas estratégias nacionais de segurança cibernética,[8] adotando um comitê ou comissão conformada por órgãos governamentais bem como grupos de trabalho que atraem representantes de outros setores para participar voluntariamente. Esse modelo de governança poderia ser replicado para apoiar o CEAP nacional.

7. Documentos que descrevem como a abordagem com várias partes interessadas pode ser utilizada no desenvolvimento de estratégias nacionais de segurança cibernética são um bom começo na formulação de uma estrutura nacional de educação em segurança cibernética. (Ver relatórios Global Partners Digital, como Framework for Multistakeholder Cyber Policy Development e Multistakeholder Approaches to National Cybersecurity Strategy Development).

8. O Chile, por exemplo, criou o Comitê Interministerial de Segurança Cibernética, composto por vários órgãos governamentais. O Comitê pode convidar representantes do meio acadêmico, da sociedade civil e do setor privado para participar de suas sessões. Da mesma forma, o Paraguai criou uma Comissão Nacional de Segurança Cibernética com membros do governo, e podem ser criados grupos de múltiplas partes interessadas para definir questões específicas.

Setor privado

O setor privado é uma parte interessada crucial e um parceiro na implementação do CEAP nacional. Com um papel de liderança na condução do desenvolvimento tecnológico, o setor privado está ciente das necessidades da indústria e pode fornecer ferramentas para treinar a força de trabalho, bem como providenciar recursos para melhorar a oferta educacional.

Além das estruturas de governança, as parcerias público-privado-acadêmicas também têm um papel importante em um CEAP. As instituições de educação públicas e privadas podem aproveitar a experiência do setor privado, inclusive de empresas de tecnologia, para melhorar o conteúdo e a eficiência e garantir a sustentabilidade geral da educação em segurança cibernética. Facilitar essas parcerias pode proporcionar o acesso a recursos e oportunidades e torná-los acessíveis a um maior número de estudantes.

A iniciativa Educate Cloud Degree da Amazon Web Services (AWS), por exemplo, ajuda a "nuvenizar" os currículos existentes das instituições participantes, conferindo diplomas e credenciais com especialização ou concentração em computação em nuvem. No Brasil e na Colômbia, tanto o Serviço Nacional de Aprendizagem Industrial (SENAI)[9] quanto o Serviço Nacional de Aprendizagem (SENA)[10] fizeram uma parceria com a AWS para treinar estudantes em inteligência artificial, internet das coisas (IoT) e computação em nuvem, a qual inclui ferramentas e módulos sobre segurança cibernética. Por intermédio dessa parceria, o SENAI e o SENA treinaram 3.000 e 10.000 alunos em 2019, respectivamente. Da mesma forma, o Governo da Argentina também estabeleceu uma parceria com a AWS, oferecendo a seus cidadãos o programa AWS Educate no portal do Ministério da Modernização, juntamente com um currículo de computação em nuvem com módulos de segurança cibernética, por meio da AWS Educate, para 28 instituições educacionais do país.[11]

Além disso, a CISCO e a Trend Micro também fornecem recursos para auxiliar estudantes e instituições do ensino superior. A CISCO Networking Academy, por exemplo, fornece aprendizagem on-line e presencial sobre diversos temas técnicos, como segurança cibernética, que também é disponibilizada em português e espanhol.[12] A Trend Micro, por meio do programa de educação em segurança cibernética para universidades,[13] trabalha com essas instituições de ensino superior no treinamento de educadores, alinhando o currículo de segurança cibernética e fornecendo seminários técnicos e webinários para estudantes e professores.

9. https://noticias.portaldaindustria.com.br/noticias/educacao/senai-e-amazon-web-services-se-unem-para-incentivar-a-educacao-no-brasil/
10. https://aws.amazon.com/blogs/publicsector/president-of-colombia-joins-aws-in-bogota-talks-innovation-across-the-region/
11. https://aws.amazon.com/es/blogs/aws-spanish/aws-announces-amazon-cloudfront-edge-location-in-argentina/
12. https://www.netacad.com/
13. https://www.trendmicro.com/en_us/initiative-education/cybersecurity-education-universities.html

Setor acadêmico

Por meio de universidades, grupos de reflexão e outras instituições acadêmicas, o meio acadêmico reúne múltiplos especialistas que, com suas pesquisas, continuam os avanços no campo da segurança cibernética. A integração de acadêmicos em parcerias público-privado-acadêmicas pode proporcionar análises objetivas, científicas e revisadas por pares para o desenvolvimento de políticas. O meio acadêmico pode muitas vezes ser a fonte de inovação e avanço de tecnologias.

A Universidade de Oxford, por meio do Global Cyber Security Capacity Centre (GCSCC), se firmou como centro de pesquisa internacional líder em segurança cibernética, promovendo a escala, ritmo, qualidade e impacto da segurança cibernética. A universidade e o GCSCC subscreveram parcerias com organizações como a Organização dos Estados Americanos (OEA) e o Banco Interamericano de Desenvolvimento (BID) a fim de fornecer modelos para uma avaliação objetiva do estado da segurança cibernética na região. A primeira dessas parcerias ocorreu em 2016 com a publicação Segurança cibernética: Estamos prontos na América Latina e no Caribe? (2016)[14]. Essa publicação permitiu aos formuladores de políticas e às partes interessadas do setor privado identificar o progresso em segurança cibernética no país, além de destacar áreas-chave de engajamento e o apoio necessário para atingir um nível mais alto de maturidade.

A integração do setor acadêmico deve incentivar os formuladores de políticas a usarem os conselhos e dados disponíveis para construir políticas eficazes que possam assegurar a integração dos princípios de segurança cibernética na educação. E o que é ainda mais importante: estas são entidades primárias que devem ser apoiadas financeiramente para continuarem inovando e avançando no trabalho de segurança cibernética e educação.

Sociedade civil

La sociedad civil y muchas asociaciones de seguridad de la información (por ejemplo, (ISC)², CompTIA, ISACA y SANS) han desarrollado programas de educación en ciberseguridad que podrían ayudar a los Gobiernos a aprovechar las habilidades de ciberseguridad en diferentes instituciones y regiones del país. Además, en proyectos orientados a mejorar la educación y la empleabilidad de los jóvenes, las alianzas público-privadas tienden a ser neutrales y tener una duración definida y, a menudo, involucran a la sociedad civil (BID, 2018, pág. 4). Las organizaciones sin fines de lucro ayudan a los Gobiernos y actores del sector privado en el monitoreo y la rendición de cuentas de estos proyectos y aseguran que se cumplan los objetivos. Además, las organizaciones no gubernamentales, las comunidades y las instituciones académicas también encajan necesariamente en esta ecuación, al aportar sus propias ventajas comparativas, su voz y su posicionamiento (WEF, 2014, pág. 11). Además, en América Latina es más probable que las organizaciones contraten profesionales en ciberseguridad de instituciones académicas ((ISC)², 2019, pág. 27), lo que acentúa la importancia de las alianzas público-privadas-sociedad civil para mejorar las habilidades y el conocimiento de los profesionales de la ciberseguridad de la región.

Todas las partes interesadas deben apoyar el desarrollo de una fuerza laboral cualificada en ciberseguridad, ya que esos diferentes actores desempeñan roles únicos en diferentes instancias del ciclo educativo. Las siguientes secciones presentan algunos ejemplos en los que el sector público, el sector privado y la sociedad civil pueden participar en lograr la concienciación acerca de la ciberseguridad y de la preparación de la fuerza laboral que se necesita para ir cerrando la brecha.

14. Tradução livre da publicação disponível em inglês e espanhol: https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

Estabelecimento de objetivos e métricas

Ter objetivos mensuráveis e métricas apropriadas para avaliar continuamente o progresso e fornecer feedback para seu melhoramento ajuda diretamente na produção de CEAPs eficazes e direcionados. Para que funcionem corretamente, entretanto, os objetivos devem ser SMART: específicos, mensuráveis, alcançáveis, relevantes e oportunos.

Os governos também poderiam considerar o uso de indicadores de recursos (relacionados aos recursos necessários, como treinamento de professores e pedagogia na sala de aula), indicadores de resultados (referentes ao impacto da atividade realizada, por exemplo, conhecimentos e habilidades dos estudantes), indicadores educacionais e socioeconômicos nacionais (como índices de matrícula escolar) e indicadores de custo (comparação dos resultados de uma iniciativa com seus custos por meio de uma análise de custo-benefício, por exemplo) (Wagner et al., 2005, pp. 21-30).

Os formuladores de políticas também poderiam considerar a adaptação de indicadores de tecnologias da informação e das comunicações (TICs) para medir o impacto da educação em segurança cibernética. A Parceria para a Medição das TICs para o Desenvolvimento[15] da UIT, por exemplo, consiste de uma lista de indicadores acordados por meio de um processo de consulta com diversos atores e inclui uma série de indicadores para as TICs na educação que poderiam ser ajustadas e em seguida utilizadas para avaliar a implementação geral do CEAP nacional. Alguns indicadores nacionais incluem, a título de exemplo:

- Proporção de escolas de ensino fundamental e médio com programas educacionais de segurança cibernética.
- Proporção de alunos do ensino superior matriculados em cursos relacionados à segurança cibernética.
- Proporção de educadores cibernéticos qualificados nas escolas.[16]

Os governos e outras partes interessadas devem considerar não apenas utilizar as ferramentas tradicionais — como pesquisas especializadas — para medir o impacto, mas também explorar outras fontes de dados (OCDE, 2019, p. 18). Por exemplo, graças ao progresso tecnológico, os formuladores de políticas podem combinar diferentes fontes de dados, identificar correlações e até mesmo fazer análises preditivas.

15. https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/partnership/default.aspx

16. Preparados em conformidade com a lista principal de indicadores da Parceria para a Medição das TICs para o Desenvolvimento, disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/coreindicators/default.aspx

Implementação de um plano de educação em segurança cibernética

Esta seção fornece informações sobre aspectos fundamentais a serem considerados na implementação de um CEAP em cada fase do ciclo de desenvolvimento da força de trabalho, bem como as melhores práticas de todo o mundo.

Ensino fundamental e médio – A educação da próxima geração

O plano estratégico NICE é um bom exemplo de como delinear um plano de ensino fundamental e médio. O Plano Nacional de Implementação da Educação em Segurança Cibernética K-12[17] tem por objetivo: (1) incentivar os estudantes a se envolverem em atividades relacionadas à segurança cibernética, (2) ajudar os educadores a incorporarem conceitos de segurança cibernética nas aulas e, por fim, (3) ajudar os estudantes do ensino fundamental e médio a identificarem oportunidades de carreira na área de segurança cibernética. O referido plano também promove o engajamento da comunidade no estabelecimento de uma campanha de conscientização sobre a carreira cibernética, dirigido a "educadores, estudantes, pais, administradores e orientadores". Esses objetivos são um excelente exemplo do que os governos poderiam alcançar com a educação da próxima geração de profissionais de segurança cibernética.

Para ajudar os alunos do nível K-12 (fundamental e médio), o National Integrated Cyber Education Research Center (NICERC)[18] nos Estados Unidos oferece cursos gratuitos para que os educadores possam incorporar conceitos de segurança cibernética na sala de aula e os professores possam aproveitar oportunidades de desenvolvimento profissional.

Com vistas a educar a força de trabalho da próxima geração, os formuladores de políticas devem considerar a criação de um plano de ação específico com atividades para educadores e estudantes. Para os educadores, o treinamento deve fornecer recursos e ferramentas inovadoras que os professores possam adicionar às suas aulas para captar a atenção dos alunos. Para os alunos do ensino fundamental e médio, é essencial considerar as preocupações com a segurança, potenciais trilhas de carreira e como alavancar jogos e competições no processo. Os governos também devem considerar parcerias com o setor privado, organizações sem fins lucrativos e universidades quando da formulação e implementação das iniciativas educacionais. Muitas ferramentas podem ser usadas para educar as crianças sobre segurança cibernética, desde a adaptação de currículos — ou desenvolvimento de novos currículos — até competições promovidas pelo setor privado.

Estudo de caso

AAWS estabeleceu uma parceria com o Code.org, uma organização sem fins lucrativos dedicada a ampliar o acesso à informática nas escolas e aumentar a participação das mulheres e minorias sub-representadas. Graças ao apoio da AWS, a visão do Code.org é que cada estudante de cada escola tenha a oportunidade de aprender informática, assim como biologia, química ou álgebra. Especificamente, a AWS apoia o site Code.org durante todo o ano, aprimorando sua capacidade de receber milhões de professores e alunos de mais de 180 países durante a Hora do Código, uma campanha anual que envolve 15% dos alunos de todo o mundo em atividades de codificação introdutória de uma hora de duração. Além disso, o Code.org protege milhões de

17. https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

18. https://nicerc.org/student/

registros e guardas de estudantes contra ataques cibernéticos usando AWS Infrastructure Event Management, AWS Shield Advanced, AWS WAF - Web Application Firewall, e AWS GuardDuty. Nos últimos três anos, milhares de funcionários da Amazon foram voluntários durante a Hora do Código em salas de aula de San Miguel, Chile, à Cidade do Cabo, África do Sul, e em 2019, esses funcionários conduziram 280 eventos em mais de 20 países e 160 cidades.

Ensino superior e cursos técnicos

Durante essa fase educacional, os estudantes frequentemente dão o primeiro grande passo para uma carreira em segurança cibernética. No ensino superior, a educação em segurança cibernética poderia ser incluída tanto no caso dos estudantes que buscam empregos técnicos quanto daqueles que buscam carreiras em áreas não técnicas, tais como direito, políticas públicas, negócios, defesa e forças armadas. Muitos dos profissionais de segurança cibernética de hoje têm formação de outra área que não TI, sendo 30% deles egressos de negócios, marketing, finanças e contabilidade ou do exército. Na América Latina, 18% dos profissionais de segurança cibernética começaram em carreiras não técnicas ((ICS)^2, 2017, p. 5).

Muitos programas de informática e engenharia ainda não foram atualizados para atender às mudanças suscitadas pela Quarta Revolução Industrial, e fazer um apelo por sua modernização poderia ser um dos primeiros passos nesse processo. Os cursos de segurança cibernética também devem tornar-se parte integrante dos programas de ciência da computação e engenharia de software para garantir que os desenvolvedores incorporem a segurança por defeito no processo de desenvolvimento.

As respostas educacionais devem considerar a inclusão de cursos mais interdisciplinares, bem como currículos dinâmicos e responsivos, para acompanhar os avanços tecnológicos (Gleason, 2018, p. 223). Precisa-se, por exemplo, de profissionais com conhecimentos tanto do setor da saúde quanto da segurança cibernética. Como resultado, algumas universidades começaram a oferecer programas educacionais que combinam política de saúde com segurança cibernética.[19]

Após os cursos de graduação, os estudantes têm a opção de se especializarem em segurança cibernética no nível de pós-graduação. Há uma série de programas de pós-graduação em segurança cibernética, incluindo mestrados profissionais e mestrados acadêmicos em saberes desde ciência da computação até política e administração. De fato, alguns países da América Latina oferecem estudos de pós-graduação em segurança cibernética, como o Instituto Tecnológico e de Estudos Superiores de Monterrey no México[20] e a Escola Superior de Guerra na Colômbia.[21]

A Agência da União Europeia para a Cibersegurança (ENISA) criou um mapa educacional de diplomas relevantes de segurança cibernética em seus Estados membros, incluindo programas de graduação e pós-graduação.[22] Além de ajudar os estudantes a tomarem decisões informadas a respeito dos programas de segurança cibernética, com um mapa educacional de segurança cibernética os governos podem ter uma melhor compreensão da disponibilidade desses programas no ensino superior.

19. Por exemplo, a Universidade de Sydney está oferecendo um Mestrado em Segurança da Saúde. https://sydney.edu.au/courses/courses/pc/master-of-health-security.html.

20. https://maestriasydiplomados.tec.mx/posgrados/maestria-en-ciberseguridad

21. https://ciber.esdegue.edu.co/course/index.php?categoryid=6

22. https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

Os governos podem desempenhar um papel essencial na promoção da disponibilidade e qualidade desse tipo de programa, estabelecendo um padrão para uma boa educação em segurança cibernética no âmbito nacional. Por exemplo, o National Cybersecurity Center (NCSC) no Reino Unido certifica os diplomas de bacharelado e mestrado em segurança cibernética no país.[23] Assim, os estudantes podem tomar decisões informadas referente à educação superior escolhida, e os empregadores são capazes de recrutar mais indivíduos qualificados.

Cursos técnicos em segurança cibernética

Os estudantes podem se envolver em segurança cibernética após o ensino médio por meio de cursos técnicos. Especificamente, os programas desse tipo voltados para técnicas emergentes, como aprendizagem de máquina e inteligência artificial (IA), são cruciais para o futuro da força de trabalho, uma vez que essas tecnologias estarão presentes em quase todos os novos produtos de software e se tornaram uma prioridade máxima de investimento para os chief information officers (CIOs)[24]. Uma pesquisa realizada com 800 especialistas e executivos de altas tecnologias estimou que até 2025 haveria uma extensa integração da tecnologia de IA e, desse modo, haveria também funções e empregos de IA em diferentes partes das organizações. Ao mesmo tempo, muitas empresas de segurança de alta tecnologia estão interessadas em desenvolver cursos técnicos que combinem segurança cibernética e inteligência artificial.[25]

Muitos cursos técnicos na América Latina já começaram a treinar estudantes em segurança cibernética, como os programas já referidos do SENAI, no Brasil, e do SENA, na Colômbia. Da mesma forma, a National Research Foundation (NRF) em Cingapura, por exemplo, criou um programa nacional de IA intitulado AI Singapore, que inclui um curso técnico de IA (AI Apprenticeship Program, AIAP)[26] para preparar os talentos locais de IA. Na Alemanha[27] e na Coreia do Sul,[28] os governos têm aplicado um modelo duplo, que combina treinamento prático por meio de parcerias com empregadores com educação tradicional (Deloitte, 2018b, p. 23). Esse sistema de aprendizagem dual pode ser um bom mecanismo para facilitar a contratação por parte de empresas de tecnologia com altos níveis de demanda de trabalhadores qualificados.

Educação continuada e certificações

Os avanços tecnológicos e as mudanças no cenário das ameaças à segurança cibernética exigem um contínuo aperfeiçoamento e requalificação. Isso não é mais uma opção, mas uma necessidade para que os trabalhadores do século XXI continuem sua formação. Os treinamentos de curto prazo e os cursos on-line ajudam a preencher rapidamente as lacunas de conhecimento e habilidades. Na América Latina, há algumas oportunidades de treinamento presencial e on-line de curto prazo, além de muitas oportunidades de bolsas de estudo financiadas por governos, pelo setor privado e por organizações internacionais, tais como a OEA.

O Instituto Nacional de Segurança Cibernética (INCIBE) da Espanha e a OEA, por exemplo, organizam todos os anos o evento Cybersecurity Summer Bootcamp em León, Espanha, que consiste de um programa

23. https://www.ncsc.gov.uk/information/ncsc-certified-degrees

24. Gartner (julho 2017). A Gartner diz que a tecnologia AI estará em quase todos os novos produtos de software até 2020. Disponível em https://www.gartner.com/en/newsroom/press-releases/2017-07-18-gartner-says-ai-technologies-will-be-in-almost-every-new-software-product-by-2020.

25. Associação Americana de Faculdades Comunitárias (janeiro de 2019). Desenvolver aprendizados para a cibersegurança. Disponível em http://www.ccdaily.com/2019/01/developing-apprenticeships-cybersecurity/.

26. Mais informações disponíveis em https://www.aisingapore.org/industryinnovation/aiap/.

27. https://www.make-it-in-germany.com/en/study-training/training/vocational/system/

28. http://ncee.org/what-we-do/center-on-international-education-benchmarking/top-performing-countries/south-korea-overview/south-korea-school-to-work-transition/

de duas semanas ministrado em espanhol para técnicos, profissionais policiais e pessoas interessadas no desenvolvimento de estratégias nacionais de segurança cibernética.[29] A OEA oferece bolsas de estudo para profissionais da América Latina e do Caribe participarem do Summer Bootcamp, as quais ajudam a arcar com os custos de participação. Esse programa está se tornando uma iniciativa líder em segurança cibernética, com a participação de mais de 100 profissionais da América Latina em 2019, com o apoio de bolsas de estudo concedidas pela OEA. A Florida International University (FIU) também organiza um certificado executivo de segurança cibernética com duração de dois dias e apoio da OEA.[30] Em 2020, o Cybersecurity Summer Bootcamp transformou-se em um evento virtual de que participaram mais de 800 estudantes de 80 países.

Muitas organizações privadas também oferecem oportunidades de treinamento e certificação com módulos de segurança cibernética, tais como a AWS,[31] a Microsoft[32] e a CISCO.[33] Embora um diploma de ensino superior seja uma indicação de maior conhecimento em segurança cibernética, os empregadores podem considerar uma certificação como uma melhor maneira de adquirir as habilidades (McAfee, 2017, p. 4). De fato, o treinamento e a certificação em segurança cibernética podem proporcionar experiência em áreas práticas (Catota; Morgan; Sicker, 2019). Além disso, as certificações podem ter um impacto direto sobre as expectativas salariais. O salário médio dos profissionais de segurança cibernética com certificação é maior do que a média daqueles que não a possuem. Enquanto os primeiros ganham cerca de US$ 21.000, os últimos ganham uma média de US$ 16.000 na América Latina ((ISC)^2, 2019, p. 17).

A educação continuada e a certificação são um mecanismo tão importante para promover a adaptabilidade de uma força de trabalho em segurança cibernética que a iniciativa NICE nos Estados Unidos criou um subgrupo de trabalho sobre o tema. O Subgrupo de Treinamento e Certificação desenvolveu uma matriz de mapeamento que relaciona as certificações existentes ao quadro NICE de funções de cargos de segurança cibernética em uma organização.[34] São certificações reconhecidas:

- Hacker Ético Certificado (CEH), oferecida pelo Conselho Internacional de Consultores de E-Commerce (EC-Council). [35]
- Gerente Certificado em Segurança da Informação (CISM), oferecida pelo ISACA [36]
- CompTIA Security+[37]
- Profissional Certificado em Segurança de Sistemas de Informação (CISSP), oferecida pelo (ISC)^2 [38]
- Sans GIAC Security Essentials (GSEC)[39]
- NIST Cybersecurity Framework (NCSF), Foundation and Practitioner[40]
- Tratamento de Incidentes de Segurança Informática (CERT), oferecida pela Carnegie Mellon University[41]

29. https://www.incibe.es/en/summer-bootcamp
30. https://gordoninstitute.fiu.edu/executive-education/cls/
31. https://www.aws.training/
32. https://www.microsoft.com/en-us/learning/default.aspx
33. https://www.cisco.com/c/en/us/training-events/training-certifications.html
34. https://www.nist.gov/itl/applied-cybersecurity/nice/illustrative-mapping-certifications-nice-framework
35. https://cert.eccouncil.org/application-process-eligibility.html
36. http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
37. https://certification.comptia.org/certifications/security
38. https://www.isc2.org/Certifications/CISSP
39. https://www.giac.org/certification/security-essentials-gsec
40. https://niccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-boot-camp-foundation-practitioner
41. https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=14324

As oportunidades contínuas de treinamento e certificação possibilitam que os profissionais se mantenham atualizados e preencham rapidamente quaisquer lacunas de conhecimento.

Pesquisa e desenvolvimento (P&D) em segurança cibernética

Os pesquisadores podem ajudar os governos e a indústria na formulação de soluções inovadoras para enfrentar os desafios atuais e futuros referentes à segurança cibernética e na identificação das habilidades necessárias para racionalizar os planos de treinamento. Há pesquisas em vários âmbitos, a saber: (1) programas de doutorado em estudos de segurança cibernética, (2) centros de excelência com pesquisa em segurança cibernética e (3) programas de P&D específicos estabelecidos por acordos entre o setor acadêmico, a indústria ou o governo, entre outros.

O Gabinete do Primeiro-Ministro de Cingapura, por exemplo, lançou o Programa Nacional de P&D em Segurança Cibernética, que procura fortalecer a resiliência e a preparação da infraestrutura cibernética crítica. Entre suas iniciativas estão o Laboratório Nacional de P&D em Segurança Cibernética (NCL), o Consórcio de Segurança Cibernética bem como subsídios de pesquisa e bolsas de estudo para cursos de pós-graduação. Para ilustrar como esses programas incentivam a educação em segurança cibernética, a NCL estabeleceu recentemente uma parceria com o iTrust Labs da Universidade de Tecnologia e Design de Cingapura para "oferecer experiências e serviços integrados aos órgãos governamentais, academia e indústria para apoiar seus sistemas de TI e operações de pesquisa, avaliação de tecnologia e treinamento em segurança cibernética".[42]

Outro exemplo é o National Cybersecurity Center of Excellence (NCCoE), nos Estados Unidos. O NCCoE faz parte do NIST e consiste em "um centro colaborativo onde organizações da indústria, órgãos governamentais e instituições acadêmicas trabalham em conjunto para tratar das questões mais urgentes de segurança cibernética das empresas". Esta parceria público-privada permite a criação de soluções práticas de segurança cibernética para indústrias específicas, bem como para desafios tecnológicos amplos e intersetoriais.[43] O NCCoE está empreendendo muitos projetos como segurança da camada de transporte (TLS), gerenciamento de certificados de servidores, segurança de dispositivos móveis, segurança de dados, entre outros.[44]

Liderados por governos com uma visão nacional para a P&D em segurança cibernética, as partes interessadas — universidades, indústria, sociedade civil e governo — podem se reunir para colaborar no desenvolvimento de pesquisas e ferramentas para resolver as necessidades mais urgentes dos países em matéria de segurança cibernética. Os centros de P&D podem ser criados quando as partes interessadas de diferentes setores combinam esforços.

42. https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

43. https://www.nccoe.nist.gov/about-the-center

44. thttps://www.nccoe.nist.gov/projects

Criação de uma cultura de segurança cibernética

Hoje, grande parte de nossa vida pessoal e profissional se faz on-line. Todos os cidadãos — mesmo aqueles que não seguem uma carreira de segurança cibernética — precisam de um nível de proficiência em segurança para proteger seus dados pessoais e os dados da organização para a qual trabalham. De acordo com um relatório da McKinsey, o erro humano é identificado como uma das principais causas de violação de dados nas organizações: 50% das violações de dados entre 2012 e 2017 tinham um componente de ameaça interna (McKinsey, 2018, p. 3). Os profissionais de todas as carreiras podem e devem aprender as melhores práticas de segurança cibernética.

O **Kit de Ferramentas da Campanha de Conscientização sobre Segurança Cibernética da OEA** recomenda que as campanhas sejam simples e fáceis, evitando especificidades técnicas.[45] As mensagens de conscientização devem ter uma perspectiva positiva para capacitar o público na aplicação de medidas de proteção (OEA, 2016, p. 14). Os governos devem considerar a realização de pesquisas sobre como os jovens utilizam a tecnologia e o que eles sabem sobre segurança e privacidade on-line. Há uma série de ferramentas que poderiam ser aplicadas para aumentar a conscientização sobre segurança cibernética, tais como assembleias escolares, competições, lições em sala de aula, material informativo disponível em websites, campanhas de mídia social, entre outras.

As parcerias entre governo, indústria e sociedade civil também podem contribuir para aumentar a conscientização no tema. A campanha **STOP.THINK.CONNECT**[46] foi criada pela National Cybersecurity Alliance (NCSA) e pelo Grupo de Trabalho Anti-Phishing (APWG) em colaboração com empresas privadas, organizações sem fins lucrativos e organizações governamentais. Em 2014, a OEA reconheceu o mês de outubro como Mês de Conscientização sobre a Segurança Cibernética e tem celebrado essa ocasião todos os anos desde então. A OEA também incentivou seus Estados membros a aumentar seus esforços referentes às políticas nacionais de segurança cibernética e a aderir à iniciativa STOP.THINK.CONNECT "no estabelecimento de um esforço mundial coordenado e unificado para criar uma conscientização pública sobre segurança cibernética".[47]

Na América Latina, o Governo do Chile lançou uma campanha nacional de conscientização sobre segurança cibernética, que inclui várias recomendações para o público em geral e para funcionários de escritórios.[48] Da mesma forma, a campanha nacional de conscientização sobre segurança cibernética da Colômbia, chamada EnTIConfío, fornece informações e recursos a um amplo público, particularmente às crianças[49]. Países como Argentina, México, Panamá e Uruguai, entre outros, criaram suas próprias campanhas de conscientização para apoiar os esforços de construção de sociedades mais ciber-resilientes.

45. https://www.thegfce.com/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit.

46. https://www.stopthinkconnect.org/

47. OEA (outubro de 2014). A OEA se une ao reconhecimento de outubro como "Mês de Conscientização sobre a Segurança Cibernética". Disponível em https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-474/14 .

48. https://www.concienciadigital.gob.cl/

49. https://www.enticconfio.gov.co/

Recomendações práticas

Esta seção fornece um esboço das diferentes ferramentas e programas que os formuladores de políticas e educadores na América Latina e no Caribe podem desenvolver para melhorar o conhecimento e as habilidades da força de trabalho atual da região e atingir as metas e objetivos do plano de educação em segurança cibernética.

Palestras e discussões em sala de aula

Aulas inovadoras e dinâmicas sobre segurança cibernética, que incentivam a discussão de conceitos básicos e introduzem conceitos mais complexos durante o ciclo educacional, ajudarão a preparar os alunos para o trabalho. Os educadores poderão introduzir conceitos de segurança cibernética nas aulas existentes ou organizar oficinas específicas sobre o tema. Por exemplo, a OEA, em parceria com a Citi Foundation, desenvolveu o projeto intitulado Criando uma Trajetória Profissional em Segurança Digital, "Pathways2Progress", que oferece um curso técnico de segurança digital com 48 horas de duração para estudantes universitários de 17 a 25 anos de idade. O Instituto Nacional de Segurança Cibernética (INCIBE) da Espanha também organiza os "Espaços de Segurança Cibernética", um curso técnico prático de três horas para entre 20 e 30 estudantes, com idades de 16 a 18 anos. Esses são alguns exemplos de cursos que ajudam a incentivar os jovens a seguir uma carreira em segurança cibernética.

Feiras de carreira

As feiras de carreira e as campanhas informativas sobre uma trilha de carreira em segurança cibernética devem ser incentivadas, pois a maioria dos estudantes do ensino médio não tem acesso a cursos relacionados, nem tem conhecimento das oportunidades nessa área em muitos países da América Latina (Catota; Morgan; Sicker, 2019). As feiras de carreira devem envolver não apenas os estudantes, mas também os pais, pois eles podem ajudar seus filhos na escolha das trilhas de carreira. A iniciativa NICE nos Estados Unidos, por exemplo, organiza a NICE K-12 Cybersecurity Education Conference, que reúne educadores, profissionais, pesquisadores, organizações sem fins lucrativos e estudantes para discutir possíveis estratégias para aumentar a conscientização sobre as possibilidades da carreira de segurança cibernética entre estudantes e pais.

Treinamento on-line e laboratórios

Há uma série de programas on-line e webinários que oferecem uma série de aulas de segurança cibernética para vários públicos e em vários níveis. Em muitos países da América Latina, as pessoas se conectam por meio de laboratórios públicos de inovação, e o treinamento on-line poderia ser disponibilizado nesses laboratórios. Os governos devem combinar seus projetos de acesso às TICs com treinamentos de segurança cibernética on-line.

Plataformas como a AWS Educate e a CISCO Academy mencionadas acima, são bons exemplos de treinamento disponíveis on-line. A Microsoft também oferece um programa profissional de segurança cibernética que funciona por três meses a cada trimestre. Os cursos on-line abertos e massivos (MOOCs) também se tornaram uma ferramenta essencial para a capacitação em segurança cibernética. Plataformas como Coursera, edX, Udacity e Pluralsight oferecem muitos cursos, e até mestrados, de universidades reconhecidas em espanhol. Em resumo, o treinamento on-line e os laboratórios são uma opção animadora para estudantes de países onde o treinamento em segurança

cibernética não está amplamente disponível ou tem custos proibitivos. Por intermédio de parcerias público-privadas, os governos nacionais e locais devem aproveitar a oportunidade de usar essas plataformas on-line para treinar sua força de trabalho em temas de segurança cibernética. Muitas das plataformas mencionadas foram desenvolvidas com base no que eles procuram em um funcionário.

Competição/Gamificação

As competições podem contribuir para aumentar a conscientização, incentivar o trabalho em equipe e permitir que os participantes enfrentem um incidente cibernético do mundo real em um ambiente controlado, sob a supervisão de especialistas. Essas simulações podem ser estruturadas para se aproximarem dos ataques do mundo real enfrentados pelas organizações. Além disso, essa é uma oportunidade para que os participantes trabalhem em rede e compartilhem informações, até mesmo para encorajar a diversidade no campo da segurança cibernética.

No Reino Unido, o NCSC está organizando o Concurso CyberFirst Girls para meninas no país, que visa incentivar a próxima geração de mulheres a seguir uma carreira no campo da segurança cibernética. Na América Latina, a OEA organiza o desafio CyberWomen Challenge em parceria com a Trend Micro, que estabelece equipes somente de mulheres para mitigar efetivamente os ataques cibernéticos . Jogos on-line e quizzes também são uma forma interativa de captar a atenção do público em geral para aprender boas práticas de segurança cibernética.

Não faltam políticas para promover a integração da segurança cibernética na educação. A implementação efetiva de políticas educacionais pode resultar em uma maior priorização da segurança cibernética em geral. Como este livro branco destacou, o primeiro passo para os formuladores de políticas é identificar a necessidade de integração da segurança cibernética na educação. Em seguida, é importante criar um plano de ação de educação em segurança cibernética para racionalizar o processo de estabelecimento de metas, objetivos e métricas. Uma vez estabelecido esse plano, os formuladores de políticas podem optar pela integração de atores como o setor privado, a academia e até mesmo a sociedade civil por meio de parcerias público-privado-acadêmicas. Esses atores envidarão diferentes esforços com o objetivo global de educar o público sobre segurança cibernética e assegurar a emergência de uma população mais cibernética. Alguns exemplos envolvem o ensino fundamental e médio, incentivando os estudantes a continuarem com estudos superiores em segurança cibernética ou a buscarem cursos técnicos, educação continuada e certificações. As políticas voltadas para o nível micro, tais como palestras em sala de aula, discussões, feiras de carreira e laboratórios de treinamento, também devem ser levadas em consideração para uma rápida integração.

Conclusão

Para formular e implementar um plano de ação de educação em segurança cibernética (CEAP), os governos da América Latina e do Caribe devem coordenar esforços com o setor privado, a sociedade civil e o setor acadêmico. A escassez de profissionais qualificados em segurança cibernética exige ação imediata para treinar os profissionais atuais e formar a próxima geração. Para fechar a lacuna da força de trabalho — 600.000 pessoas na América Latina e 4 milhões em todo o mundo — os governos precisam adotar uma abordagem estratégica e colaborar com os setores privado e acadêmico para formular e implementar um CEAP. Esse plano auxilia a elaboração de políticas públicas eficazes destinadas ao fortalecimento de estratégias nacionais e ao desenvolvimento da força de trabalho de segurança cibernética a fim de que os profissionais estejam mais preparados e as pessoas mais conscientes sobre o tema. Os principais componentes de um CEAP encontram-se a seguir:

(1) objetivos claros e definidos para priorizar a educação em segurança cibernética e integrá-la em todos os níveis que orientam as ações dos formuladores de políticas.

(2) envolvimento de diversas partes interessadas.

(3) mecanismos de monitoramento e indicadores para avaliar o progresso na consecução dos objetivos.

Os formuladores de políticas dispõem de diversas ferramentas para implementar o CEAP e podem criar uma programação adequada para as diversas idades a fim de aumentar a conscientização e a educação sobre segurança cibernética, desde o ensino fundamental até a educação continuada para profissionais interessados. A programação varia de laboratórios on-line a competições, jogos, feiras de carreira e palestras e discussões em sala de aula. À medida que os alunos amadurecem, há oportunidades de aprendizagem em segurança cibernética, programas de pós-graduação, treinamento adicional e certificações.

O plano estratégico NICE é um bom exemplo de como delinear um plano para o ensino fundamental e médio. O Plano Nacional de Implementação da Educação em Segurança Cibernética K-12 tem por objetivo: (1) incentivar os estudantes a se envolverem em atividades relacionadas à segurança cibernética, (2) ajudar os educadores a incorporarem conceitos de segurança cibernética nas aulas e, finalmente, (3) ajudar os estudantes do ensino fundamental e médio a identificarem oportunidades de carreira na área de segurança cibernética. O desenvolvimento da educação e da força de trabalho tem muitas etapas, e a expansão de qualquer plano de educação em segurança cibernética deve levar isso em conta. O ensino fundamental, médio e superior, os programas de educação continuada e a P&D desempenham um papel significativo no aumento da força de trabalho cibernética. Várias ferramentas poderiam ser desenvolvidas para fomentar a educação em segurança cibernética em cada etapa do ciclo de desenvolvimento da força de trabalho. A capacitação pode ser melhorada no âmbito nacional em todos os estágios da educação e

do desenvolvimento dos profissionais, incluindo componentes específicos de educação cibernética durante cada fase. Do ensino fundamental e médio à pesquisa e desenvolvimento, todos podem se beneficiar da promoção de habilidades objetivas e subjetivas na educação cibernética.

Os países da América Latina poderão colher os benefícios da Quarta Revolução Industrial se investirem tanto em tecnologia quanto em sua população. A inovação por meio de novas oportunidades de negócios e interações sociais só ocorre quando há o encontro da tecnologia com trabalhadores qualificados. A América Latina, como qualquer região do mundo, requer uma força de trabalho que tenha o conhecimento e as habilidades para construir e operar as tecnologias emergentes e futuras, bem como a capacidade de fazer esse trabalho de forma segura.

Referências

Banco Interamericano de Desenvolvimento (2016). Caminho para as Smart Cities. Da Gestão Tradicional para a Cidade Inteligente. Disponível em: https://publications.iadb.org/publications/portuguese/document/Caminho-para-as-smart-cities-Da-gest%C3%A3o-tradicional-para-a-cidade-inteligente.pdf

Banco Interamericano de Desenvolvimento (2018). Factores de éxito y aprendizajes obtenidos de la formación de alianzas público-privadas. Disponível em: https://publications.iadb.org/es/factores-de-exito-y-aprendizajes-obtenidos-de-la-formacion-de-alianzas-publico-privadas

Catota, F. E., Morgan, M.G. y Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, Vol. 5, No. 1. Disponível em: https://doi.org/10.1093/cybsec/tyz001.

Cybersecurity Ventures (2019). 2019 Official Annual Cybercrime Report. Disponível em: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Deloitte (2019). Tech Trends 2019. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Deloitte (2018a). The jobs are here, but where are the people? Disponível em: https://www2.deloitte.com/us/en/pages/manufacturing/articles/future-of-manufacturing-skills-gap-study.html

Deloitte (2018b). Preparing tomorrow's workforce for the Fourth Industrial Revolution. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-preparing-tomorrow-workforce-for-4IR.pdf.

ENISA (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. Disponível em: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA (2015). Status of Privacy and NIS course curricula in Member States. Disponível em: https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states

Fórum Econômico Mundial (2014). Creating New Models: Innovative Public-Private Partnerships for Inclusive Development in Latin America. Disponível em: http://www3.weforum.org/docs/GAC/2014/WEF_GAC_LatinAmerica_InnovativePublicPrivatePartnerships_Report_2014.pdf

Fórum Econômico Mundial (2015a). Bridging the Skills and Innovation Gap to Boost Productivity in Latin America. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/finance/201501-Competitiveness_Lab_Latin_America_final.pdf

Fórum Econômico Mundial (2015b). Deep Shift: technology tipping points and societal impact. Disponível em: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Gleason, N. W. (Ed.). (2018). Higher education in the era of the fourth industrial revolution. Singapore: Palgrave Macmillan.

Global Cyber Security Capacity Centre (2016). Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition. Disponível em: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

IBM (2018). IBM X-Force Threat Intelligence Index 2018. Disponível em: https://www.ibm.com/downloads/cas/MKJOL3DG

(ISC)2 (2019). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study, 2019. Disponível em: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

(ISC)2 (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. (ISC)2 Cybersecurity Study, 2018. Disponível em:: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

(ISC)2 (2017). Global Information Security Workforce Study. Disponível em:: https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

Kelly, K. (2016). The inevitable: understanding the 12 technological forces that will shape your future. New York, NY: Penguin Books.

Lewis, J. (2018). Economic Impact of Cybercrime – No Slowing Down. Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

McAfee (2017). Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

McKinsey & Company (2018). Insider Threat: The human element of cyberrisk. Disponível em: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

National Cybersecurity Alliance (2017). Securing our Future: Cybersecurity and the Millennial Workforce. Disponível em: https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

National Initiative for Cybersecurity Education (2017). National K-12 Cybersecurity Education Implementation Plan. Disponível em: https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

National Institute of Standards and Technology (2017). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Open Web Application Security Project (2016). Security by Design Principles. Disponível em: https://www.owasp.org/index.php/Security_by_Design_Principles

Organização para a Cooperação e o Desenvolvimento Econômico (2012). The Protection of Children Online: Recommendations of the OECD Council.

Organização para a Cooperação e o Desenvolvimento Econômico (2016). Startup América Latina 2016. Construyendo un futuro innovador. Disponível em: https://www.oecd.org/innovation/startup-america-latina-2016-9789264265141-es.htm

Organização para a Cooperação e o Desenvolvimento Econômico (2017). Perspectivas económicas de América Latina 2017. Juventud, competencias y emprendimiento. Disponível em: https://www.oecd.org/economy/perspectivas-economicas-de-america-latina-20725183.htm

Organização para a Cooperação e o Desenvolvimento Econômico (2019). Measuring Innovation in Education 2019: What has changed in the classroom?

Organização dos Estados Americanos (2016). Ciberseguridad. Kit de herramientas para la campaña de concientización. Disponível em: https://www.sites.oas.org/cyber/Documents/2015%20OEA%20-%20Ciberseguridad%20Kit%20de%20Herramientas%20para%20la%20Campa%C3%B1a%20de%20Concientizaci%C3%B3n%20(Espa%C3%B1ol).pdf

Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview. Disponível em: https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute (2019). Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection. Disponível em:: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Schwab, K. (2016). The Fourth Industrial Revolution. New York, NY: Crown Business

Symantec (2018). Internet Security Threat Report. Disponível em: http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Symantec (2019). Internet Security Threat Report. Disponível em: https://img03.en25.com/Web/Symantec/%7Bdfc1cc41-2049-4a71-8bd8-12141bea65fd%7D_ISTR_24_2019_en.pdf

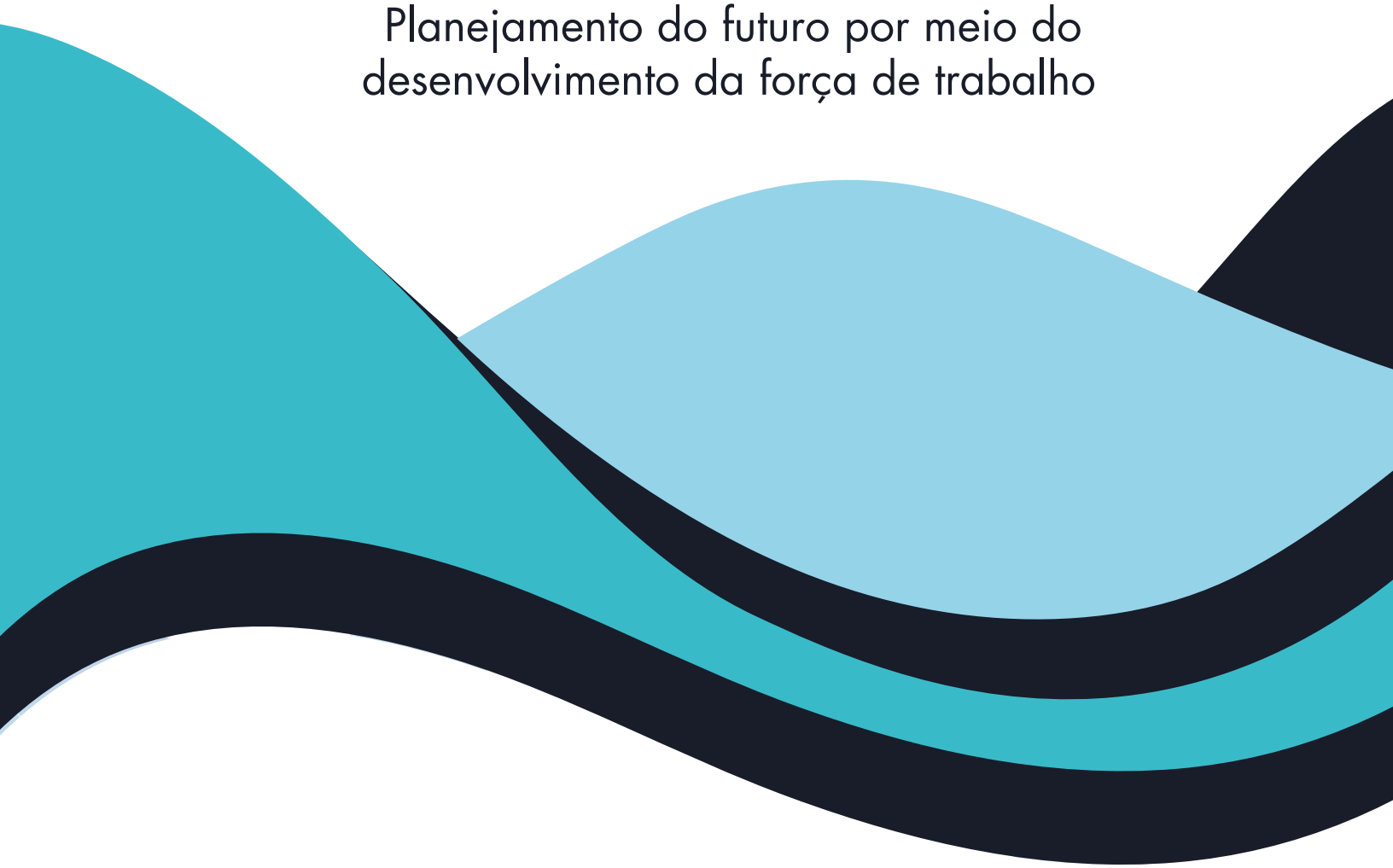
União Internacional das Telecomunicações (2019). Global Cybersecurity Index (GCI) 2018. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Wagner, D. A., et al. (2005). Monitoring and evaluation of ICT in education projects: a handbook for developing countries. Washington, D. C.: InfoDev.

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do desenvolvimento da força de trabalho



CICTE01316E05

OEA Mais direitos para mais pessoas | aws

— EDUCAÇÃO EM SEGURANÇA —

CIBERNÉTICA

Planejamento do futuro por meio do desenvolvimento da força de trabalho

White paper series
Publicação 5

2020