APRESENTAÇÃO

EDIÇÃO ESPECIAL: REFERENCIAIS DE FORMAÇÃO EM CIBERSEGURANÇA

POR

Aldri Luiz dos Santos (UFMG), Altair Olivo Santin (PUCPR) e
Marcos Antonio Simplicio Jr (USP)
aldri@dcc.ufmg.br, santin@ppgia.pucpr.br, mjunior@larc.usp.br

Em um mundo cada vez mais tecnológico, a computação tornou-se imprescindível no cotidiano da sociedade, exigindo o aprendizado e domínio sobre novas áreas quase que imediatamente. Esse movimento tem levado, ao mesmo tempo, ao surgimento de novas profissões e também à carência de profissionais qualificados para preencher as vagas criadas. A Ciber-Segurança (escrito propositalmente com ´S´ maiusculo para destacar a área de segurança) é uma destas áreas que exige atenção especial e urgência devido a sua ampla abrangência, devendo ser incorporada por outras áreas que estão passando por transformação digital ou ainda se encontram em desenvolvimento.

A CiberSegurança é vista de modo estratégico e fundamental pelos principais países do mundo, que precisam enfrentar um crescimento contínuo no número de incidentes de segurança. O Brasil não é uma exceção a essa tendência, pelo contrário: o país apresenta uma situação particularmente preocupante. Por exemplo, um relatório recente da Trend Micro (ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE, 2024) mostra que o Brasil continua entre os principais alvos de ciberataques no mundo, contando com mais de 100 bilhões de registros de tentativas de ataque em 2023; o setor governamental está entre os alvos preferenciais dos atacantes, que também miram em áreas como educação, mercado financeiro, e varejo. Preocupações similares são apresentadas em outro relatório de 2023, que mostra que um aumento expressivo de incidentes de segurança tendo o Brasil como protagonista no últimos anos, incluindo casos de roubo e vazamento de dados, ataques de *ransomware*, e personificação de sites brasileiros via *phishing* (SOCRADAR, 2023).

Agravando essa expansão do número e variedade de ameaças, o mundo ainda apresenta um grave déficit de profissionais capacitados e treinados para construir sistemas computacionais mais resilientes, testar sua segurança de forma efetiva, e reagir rapidamente a eventuais ataques. Segundo estimativas do Consórcio Internacional de Certificações em Segurança da Sistemas de Informação (*International Information System Security Certification Consortium* - ISC2), em 2023 havia uma necessidade de quase dobrar a força de trabalho especializada em cibersegurança no mundo: embora o número atual de profissionais da área seja da ordem de 5,5 milhões, estima-se que seja necessário formar cerca de 4 milhões adicionais para satisfazer as crescentes demandas do mercado (INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM, 2023).

É nesse cenário que, ao se planejar o uso de tecnologia para melhorar a qualidade de vida nas cidades, deve-se pensar também em como promover a proteção dessa infraestrutura tecnológica, prevenindo a ação de agentes maliciosos e coibindo abusos. Essa não é, entretanto, uma tarefa fácil: ela exige profissionais com experiência e conhecimento sólido, capazes de aplicar boas práticas e evitar erros comuns, além de inovar quando necessário. Assim, para fazer frente ao desafio de construir e operar sistemas tecnológicos resilientes a ataques, é recomendado que entidades governamentais, nas suas diferentes esferas, considerem em seus planos de trabalho a inclusão de equipes especializadas em CiberSegurança. Isso pode ser feito de forma específica, criando grupos dedicados a uma região ou sistema alvo, ou de forma integrada, com a criação de equipes que possam prestar suporte a múltiplos sistemas e jurisdições. Em qualquer dos casos, o ideal é haver profissionais atuando nas diferentes fases de cada projeto tecnológico, incluindo (1) sua concepção, para permitir a construção de sistemas mais robustos, e (2) sua operação, para permitir melhoria contínua do sistema e uma

resposta rápida a eventuais incidentes de segurança.

A implantação dessa ação pode se apoiar não apenas em parcerias público-privadas, envolvendo empresas do setor de CiberSegurança, mas também em programas já existentes no Brasil para promover a formação de profissionais na área. De fato, existem algumas iniciativas alinhadas com as diretivas da Política Nacional de CiberSegurança (PNCiber), lançada pelo governo federal em 26 de dezembro de 2023. Um exemplo é o Programa Hackers do Bem, coordenado pela Softex e executado pela Rede Nacional de Ensino e Pesquisa (RNP) e pelo Senai-SP, que visa à capacitação profissional em larga escala e de forma contínua em cibersegurança, contemplando estudantes de ensino técnico, médio e superior, e profissionais que buscam uma especialização no tema (REDE NACIONAL DE ENSINO E PESQUISA - RNP, 2024). Outra iniciativa abrangente, lançada pela Sociedade Brasileira de Computação (SBC), consiste em Referenciais de Formação para o curso de bacharelado em CiberSegurança (RF-BCS), que tem por objetivo nortear e promover a criação de cursos de graduação voltados especificamente a essa área (SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 2023).

O RF-BCS foi construído com base no relatório do grupo de trabalho CSEC2017, que coloca CiberSegurança como uma nova área da Computação no GRCC - Guia de Referência Curricular de CiberSegurança (ACM/IEEE/AIS SIGSEC/IFIP, 2017). Este guia foi desenvolvido pela principais entidades da área no mundo: *Association for Computing Machinery* (ACM), IEEE *Computer Society* (IEEE-CS), *Association for Information Systems Special Interest Group on Information Security and Privacy* (AIS SIGSEC) e *International Federation for Information Processing Technical Committee on Information Security Education* (IFIP WG 11.8). Portanto, ele parte de uma base sólida, de qualidade internacional.

No GRCC foi definido que "CiberSegurança é uma área baseada na Computação que envolve tecnologia, pessoas, informações e processos para possibilitar operações com garantias de segurança. Envolve a criação, operação, análise e teste de sistemas computacionais seguros. Cursos de CiberSegurança têm natureza interdisciplinar, incluindo aspectos da lei, política, fatores humanos, ética e gestão de risco, com o objetivo de considerar contextos adversariais". A conceituação de CiberSegurança do GRCC evidência, assim, suas principais diferenças em relação a áreas correlatas, como Segurança da Informação, que "se preocupa em prover segurança a informações armazenadas, em trânsito ou em processamento, escolhendo controles condizentes com o valor da informação e do risco observado frente às ameaças do ambiente". Nesse contexto semântico, é também interessante notar que, em alguns casos, é feita no Brasil a tradução livre de *CyberSecurity* (CiberSegurança em português) para Segurança Cibernética – termo que, em tradução livre para o inglês, seria *Cybernetics Security*. Porém, a Cibernética (do inglês *Cybernetics*) na realidade está fora do escopo da compu-

tação, como discutido, por exemplo, no artigo de Filev, Zhao e Brine (2013). Assim, embora o termo Segurança Cibernética seja compreensível, CiberSegurança remete melhor ao contexto de Segurança do Ciberespaço, constituído pela conectividade da Internet, sendo esta a razão pela sua adoção neste documento.

Consciente dos desafios na área, e a comunidade científica brasileira dedicada ao tema de CiberSegurança tem se reunido na última década no Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), evento anual promovido pela Comissão Especial de CiberSegurança (CESeg) da SBC. As discussões e ações promovidas neste fórum têm por objetivo consolidar as áreas que exigem CiberSegurança, demonstrando a interdisciplinaridade do tema a partir da proposição de workshops temáticos. Além disso, várias das discussões conduzidas nas reuniões plenárias da CESeg versam sobre o escopo da área. Como um desdobramento da maturidade desta comunidade, há um entendimento geral da necessidade de formação específica em CiberSegurança em nível de graduação. Tal constatação vem do fato de que oferecer cursos de especialização para profissionais da área da Computação (e.g., por meio de certificações) tem como consequência subtrair recursos humanos da própria área de Tecnologia da Informação (TI), que já é carente de pessoal. Ao mesmo tempo, essa estratégia não proporciona a formação ampla, consolidada e interdisciplinar necessária para profissionais de CiberSegurança. Na prática, o que ainda se observa é que a disponibilidade de vagas na área permanece maior do que o número de profissionais qualificados o suficiente para preenchê-las, indicando um cenário de demanda reprimida.

Os referencias da Sociedade Brasileira de Computação (2023) são resultado da atuação da CESeg, que participou em 2015 no *International Security Education Workshop* pela primeira vez, e depois em muitos eventos ligados à concepção do RF-CS. A CESeg também tem atuado no sentido de defender a necessidade de CiberSegurança como uma área autônoma, como um fator crítico de sucesso, para desenvolver um quadro de profissionais necessários na sociedade para proteger seus ativos. Ela se alinha, assim, a entidades internacionais relevantes na área de CiberSegurança, que recentemente passaram a promover iniciativas voltadas à educação específica envolvendo essas habilidades. Exemplos incluem o *National Institute of Standards and Technology* (NIST), por meio da *National Initiative for Cybersecurity Education* (NICE); a *National Security Agency* (NSA), por meio de iniciativas como a *National Centers of Academic Excellence in Cybersecurity* (NCAE-C); e, a *European Union Agency for Cybersecurity* (ENISA).

Como parte dessas iniciativas educacionais, é comum que seja promovida a formação na área contemplando-se 8 eixos: (i) Segurança de Dados, (ii) Segurança de Sistemas, (iii) Segurança de Conexão, (iv) Segurança de Software, (v) Segurança de Componentes, (vi) Segurança Organizacional, (vii) Fatores Humanos em Segurança e (viii) Segurança e

Sociedade. Cada eixo de formação relaciona os conhecimentos que são importantes no desenvolvimento das competências dos egressos do curso. Não por acaso, na RF-BCS as 12 competências específicas para o Bacharel em CiberSegurança foram sumarizadas nestes oito eixos de formação.

Assim, nesta edição especial, convidamos profissionais da academia, setor público (regulamentação e polícia), comitê gestor da internet, indústria de defesa, representação civil em autarquias e um convidado internacional para falar sobre temas relacionados a esses oitos eixos contemplados pelos referenciais da Sociedade Brasileira de Computação (2023).

No eixo 1, Segurança de Dados, a discussão concentra-se na proteção de dados armazenados, no seu processamento e em trânsito. Para tal, o prof. Dr. Ricardo Dahab da Unicamp vai falar sobre "**O papel basilar da Criptografia na segurança de dados**", explicando as técnicas e mecanismos de criptografia em uma linguagem acessível, enfatizando a função essencial da criptografia para atender requisitos de segurança de dados. Para abordar a lacuna significativa de conhecimento nessa área, ele enfatiza a necessidade urgente de educar estudantes e profissionais para lidar com a complexidade e da profundidade matemática da criptografia, cuja relevância cotidiana é cada vez mais notável, por exemplo, para mitigar riscos como violações de dados e fraudes financeiras.

No eixo 2, Segurança de Sistemas, o foco é nos aspectos dos sistemas compostos por componentes e conexões, e os softwares em uso. Os prof. Dr. Ewerton Madruga e prof. Dr. Luiz Rust, ambos do InMetro abordam "**Formando Profissionais sob a Perspectiva da Evolução na Adoção de Sistemas em Nuvem**", falando sobre a segurança desses sistemas, especialmente na era da Inteligência Artificial Generativa e computação em nuvem, demanda novas abordagens de ensino. Da necessidade de compreensão dos modelos de serviço em nuvem (IaaS, PaaS, SaaS), responsabilidade compartilhada, normas (ISO 27001, NIST CSF, ISO/IEC 15408), e catálogos de vulnerabilidades, entre outros. Eles destacam que o ensino de cibersegurança torna a compreensão de cada um destes aspectos um novo desafio acadêmico que requer adaptações curriculares e o uso de novas plataformas educacionais para sala de aula e laboratórios.

No eixo 3, Segurança de Conexão, que se concentra em aspectos de rede e comunicação das ligações lógicas e físicas entre os componentes, a profa. Dra. Michele Nogueira da UFMG nos instiga a pensar sobre a "**Segurança na Conectividade: Protegendo Redes e Conexões**", discorrendo sobre os desafios e as principais técnicas no campo da segurança na conectividade em um cenário global hiperconectado. Ela também destaca a necessidade de uma abordagem integrada e atualizada para a segurança na conectividade, que inclui não apenas tecnologias avançadas, mas também práticas de governança e políticas de segurança que acompanhem a evolução contínua das ameaças cibernéticas.

No eixo 4, Segurança de Software, que aborda o desenvolvimento e uso de software que preserva confiavelmente as propriedades de segurança da informação e sistemas que a protegem, o prof. Dr. Nuno Neves da Universidade de Lisboa indaga se "**A Segurança de Software necessita de atualização quando confrontada com a realidade da aprendizagem automática distribuída?**". No texto, ele nos diz que a aprendizagem federada (FL) é um método de aprendizagem distribuída no qual os modelos são treinados em vários dispositivos sem compartilhar dados para manter sua privacidade. No entanto, a FL é suscetível a ameaças à cibersegurança, como ataques de envenenamento de dados e modelos que comprometem a integridade dos dados. Neste caso, a filtragem de dados e a privacidade diferencial são estratégias de mitigação essenciais. Para que o estudante esteja pronto para o mercado, é essencial integrar o conhecimento dessas ameaças aos currículos de segurança de software e oferecer aos alunos uma experiência prática.

No eixo 5, Segurança de Componentes, o foco é o projeto, aquisição, teste, análise e manutenção de componentes integrados em um sistema maior. Nesse cenário, o Dr. Roberto Gallo, da Kryptus, fala sobre "**Os desafios da componentização para a segurança e a formação de equipes**", refletindo sobre a exploração de fatores teóricos e práticos que influenciam a cibersegurança em sistemas baseados em componentes e seu impacto na formação de equipes. Ele destaca os desafios enfrentados pelos recém-formados, que têm entrado em um cenário caracterizado pela abstração excessiva no software e por sistemas descartáveis. Essas condições inibem o desenvolvimento de uma perspectiva ampla de engenharia, o que é fundamental para o projeto e a manutenção de sistemas seguros. Para enfrentar esses desafios, o artigo apresenta práticas recomendadas e metodologias para o aprimoramento da educação em cibersegurança individual e em equipe.

No eixo 6, Segurança Organizacional, que envolve a proteção da organização contra ameaças e gestão de risco para apoiar os objetivos da organização, o prof. Dr. Flúvio Garcia da Polícia Federal fala sobre "**Cibersegurança, Compliance Digital e Custo Reputacional**", defendendo que a conformidade digital é o processo que visa proteger os direitos e a privacidade do usuário e, ao mesmo tempo, busca preservar a reputação corporativa por meio da conformidade com requisitos legais e padrões éticos no ambiente digital. Ela é essencial não só legalmente, mas também para proteger a reputação e a confiança na empresa, demandando uma mudança cultural e engajamento organizacional contínuo para garantir o sucesso do programa de conformidade digital.

No eixo 7, Fatores Humanos em Segurança, que contempla proteção de dados no contexto da vida pessoal e sua interação com as organizações, a Dra. Cristine Hoepers, do CERT.br/NIC.br faz uma reflexão sobre "**Importância dos Fatores Humanos para a Cibersegurança**" considerando a necessidade de assumir que o ser humano é o elo principal da cadeia, que possui pontos fortes e fracos, mas

não necessariamente é o elo mais fraco. Ela aponta que para sermos profissionais melhores e atingirmos os objetivos de transformar o comportamento dos usuários, de forma a aumentar a proteção de dados pessoais e organizações, precisamos entender além da tecnologia, também os aspectos de psicologia e evolução da espécie que possam nos trazer insights sobre como pensamos e porque agimos de determinadas maneiras.

No eixo 8, Segurança e Sociedade, que aborda cibercrimes, privacidade e aspectos legais, éticos e políticos, a Profa. Dra. Patricia Peck, da Peck Advogados, aborda o tema "**Cibersegurança, sociedade e futuro**" onde comenta que a crescente sofisticação do crime cibernético ressalta a necessidade de conformidade com a cibersegurança corporativa, o que requer diversas estratégias para enfrentar os desafios técnicos. A IA aumenta os riscos de segurança, motivando a validação de identidade e respostas regulatórias, como LGPD e PNCiber. A cibersegurança eficaz requer uma cultura proativa, cooperação internacional e considerações éticas.

Esta edição oferece uma breve abordagem sobre temas da atualidade da cibersegurança, de modo a orientar os estudantes, entusiastas e profissionais da área. A área da CiberSegurança é essencial para qualquer país em razão do seu impacto em todos os setores, desde o social ao econômico, passando pelo educacional. A Comissão de Educação da CESeg, no seu papel de apoiadora, disseminadora e promotora das diretrizes de educação em CiberSegurança da SBC, se coloca à disposição daqueles que queiram nos contactar para saber mais sobre o assunto (COMISSÃO ESPECIAL DE CIBERSEGURANÇA, 2024).

Referências

1. Comissão Especial de CiberSegurança. [on-line] www.ceseg.org. Acessado em maio de 2024.
2. Associação Brasileira das Empresas de Software. Brasil permanece na lista dos países mais atacados por malware, aponta Trend Micro. [on-line] https://abes.com.br/brasil-permanece-na-lista-dos-paises-mais-atacados-por-malware-aponta-trend-micro/. Acessado em maio de 2024.
3. Rede Nacional de Ensino e Pesquisa - RNP. Programa Hackers do Bem. [online] https://conteudo.hackersdobem.org.br. Acessado em maio de 2024.
4. International Information System Security Certification Consortium. How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. Cybersecurity Workforce Study. [online] https://www.isc2.org/Research, 2023. Acessado em maio de 2024.
5. SOCRadar. Brazil Threat Landscape Report - Unmasking Stealer Malware Dominance in Brazil. [online] https://socradar.io/wp-content/uploads/2023/06/Brazil-Threat-Landscape-Report.pdf, 2023. Acessado em maio de 2024.
6. ACM/IEEE/AIS SIGSEC/IFIP. Cybersecurity Curricular Guideline. 2017. [online] https://cybered.hosting.acm.org/wp/ ou https://cybered.acm.org/. Acessado em maio de 2024.
7. Sociedade Brasileira de Computação. Referenciais de Formação para o Curso de Bacharelado em Cibersegurança. [on-line] sol.sbc.org.br/livros/index.php/sbc/catalog/book/125, 2023. Acesso em maio de 2024.
8. Filev, D. P.; Zhao, Q. e Brine, J. Cybernetics: Where shall we go?.IEEE International Conference on Cybernetics (CYBCO), Lausanne, Switzerland, 2013, pp. 25-31, doi: 10.1109/CYBConf.2013.6617433.

ALDRI LUIZ DOS SANTOS é Professor Titular do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG). É Doutor em Ciência da Computação (2004) pela Universidade Federal de Minas Gerais, Mestre em Informática (1999) e Bacharel em Informática (1995) pela UFPR. É membro sênior do Institute of Electrical and Electronics Engineers (IEEE) em reconhecimento à sua liderança e contribuições técnicas e profissionais. Tem se dedicado a pesquisas voltadas à área de gerência de redes, tolerância a falhas, segurança, disseminação de dados, redes sem fio ad hoc e redes de sensores. É líder do grupo de pesquisa NR2 (Núcleo de Redes Sem Fio e Redes Avançadas) e membro do grupo CCSC. Foi coordenador da Comissão Especial em Segurança da Informação e de Sistemas Computacionais (CESeg) da SBC no biênio (2014-2016) e vice-coordenador no biênio (2012-2014). É membro do comitê técnico de segurança da informação e da comunicação da Sociedade de Comunicação (ComSoc) da IEEE, da SBC, do IEEE e da ACM. Membro da comissão da SBC para Proposição do Referencial de Formação aos cursos de Bacharelado em Cibersegurança.

ALTAIR OLIVO SANTIN é Engenheiro da Computação, Doutor em CiberSegurança e Professor Titular do PPGIa da PUCPR. Trabalha há muito tempo com big data (incluindo streaming) e aprendizagem de máquina (incluindo adversarial settings) para CiberSegurança. Aplica estas e outras técnicas à CiberSegurança para IoT, smart grid, computação em nuvem, spam de e-mail, detecção de intrusão etc. Também usa o aprendizado profundo para detecção de pornografia (incluindo abuso sexual infantil) em controle paterno. Trabalha com Gerenciamento de Identidade e Controle de Acesso há muitos anos, atualmente aplicando-o a Sistema Crítico Industrial (ICS).

MARCOS ANTONIO SIMPLICIO JR. possui graduação em Engenharia Elétrica (2006), com Ênfase em Computação, pela Escola Politécnica da Universidade de São Paulo (Poli-USP). Possui o título de Master of Science (2006) pela Ecole Centrale Paris (França, 2006) e de Mestre (2008), Doutor (2010) e Livre Docente (2017) em Engenharia Elétrica/Sistemas Digitais, pela Poli-USP. É Professor Associado e Pesquisador do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politecnica da Universidade de São Paulo e Vice-coordenador da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (CESeg-SBC). Atua em projetos relacionados a criptografia e cibersegurança desde 2007, cobrindo aspectos como projeto e análise de primitivas e protocolos criptográficos e de sistemas de segurança em geral.