junho/2024 • n. 52

COMPUTAÇÃO BRASIL

REVISTA DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO

ISSN: 2965-9728

Referenciais de Formação em CiberSegurança

SBC
Sociedade Brasileira de Computação

EDITORIAL

THAÍS VASCONCELOS BATISTA
Presidente da Sociedade Brasileira de Computação (SBC)

É com grande entusiasmo que lançamos a primeira edição da Computação Brasil de 2024! .

No último Congresso da Sociedade Brasileira de Computação (CSBC 2023), realizado no mês de agosto em João Pessoa – PB, iniciamos uma nova gestão na Diretoria da SBC. Ao longo de quase um ano de gestão, realizamos ações relacionadas com o Ensino de Computação na Educação Básica, reforçamos o compromisso da SBC com a Ciência Aberta e planejamos uma nova edição do Seminário dos Grandes Desafios da Computação. Diante do crescente avanço da Inteligência Artificial (IA) e as demandas decorrentes desse contínuo progresso, criamos uma Comissão de Inteligência Artificial para trabalhar na definição do Plano de IA da SBC e representar a SBC na elaboração de propostas de política de IA para o Brasil. Ademais, visando desenvolver um plano de ação e executar atividades que permitam ampliar os esforços de inclusão, diversidade e equidade na SBC, criamos a Comissão para Inclusão, Diversidade e Equidade (CIDE).

Além das ações supracitadas, prosseguimos na elaboração de referenciais de formação curricular, concluindo o referencial de formação para os Cursos de Bacharelado em Inteligência Artificial. Em 2023, a gestão da Diretoria anterior publicou os referenciais de formação para os Cursos de Bacharelado em Ciência de Dados e para os Cursos de Bacharelado em CiberSegurança.

Esta primeira edição da Computação Brasil de 2024 é dedicada ao tema *Referenciais de Formação em CiberSegurança*. Em uma sociedade cada vez mais interconectada, a proteção de dados e sistemas contra ameaças cibernéticas é uma prioridade global. Nesta edição, o leitor encontra contribuições de especialistas renomados, cuja visão abrangente e atualizada oferece uma base sólida para orientar a formação na área. Agradecemos aos editores, Professores Altair Santin, Aldri Santos e Marcos Simplicio, e aos autores que escreveram os artigos presentes nesta edição, pelo esforço e pela excelente qualidade de seus trabalhos. Boa leitura!

junho/2024 • **n**. 52

COMPUTAÇÃO BRASIL

REVISTA DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO

Caixa Postal 15012
CEP: 91.501-970 – Porto Alegre/RS
Av. Bento Gonçalves, 9.500 - Setor 4 – Prédio 43412 – Sala 219
Bairro Agronomia - CEP: 91.509-900 - Porto Alegre/RS
Fone: (51) 3308.6835 | Fax: (51) 3308.7142
marketing@sbc.org.br | sbc.org.br

Editor Responsável | Alirio Sá (UFBA)
Editores Convidados | Aldri Luiz dos Santos (UFMG), Altair Olivo Santin (PUCPR) e Marcos Antonio Simplicio Jr (USP)
Equipe de Comunicação | Gracy Medeiros, Cris Felix e Wangles Oliveira

Diagramação: Priscila Krüger | priscilahbk@gmail.com | 84 99112-7473
Revisão: Carla Simões de Azevedo
Imagens Ilustrativas: Unsplash.com

SBC OPEN LIB

Uma das principais formas de difundir o conhecimento científico é por meio de sua publicação, após a revisão por pares. Uma boa publicação pressupõe o comportamento ético, honesto e responsável dos autores e dos revisores.

Conheça o novo código de Conduta para Publicações da SBC!

ACESSE O CÓDIGO NA SOL,
A BIBLIOTECA DIGITAL DA SBC.
https://bit.ly/codigodecondutasol

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO
SBC@SBC.ORG.BR
FONE: +55 51 3308-6835

facebook.com/sbcbrasil instagram.com/sbcoficial (51) 99252-6018

COMPUTAÇÃO BRASIL

ÍNDICE

Referenciais de Formação em CiberSegurança

Computação Brasil | Junho 2024

> 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.
>
> *- Aldri Luiz dos Santos, Altair Olivo Santin e Marcos Antonio Simplicio Jr, p. 07*

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.

ARTIGO

O PAPEL BASILAR DA CRIPTOGRAFIA NA SEGURANÇA DE DADOS

POR
Ricardo Dahab (Unicamp)
rdahab@unicamp.br

Começamos por uma questão de nomenclatura: o termo "segurança da informação" sempre teve a preferência em relação a "segurança de dados", na literatura da área. Em consonância com o currículo de referência da SBC, vamos adotar aqui a segunda forma, "segurança de dados", mesmo porque os dados de interesse podem ser totalmente desprovidos de informação, no sentido matemático da palavra. .

Os textos modernos trazem, como requisitos básicos de segurança de dados, o sigilo, a integridade, a autenticidade e a irretratabilidade. *Sigilo* refere-se à capacidade de leitura de um dado somente pelas partes autorizadas para tal. Integridade é a garantia de que um dado não tenha sido modificado desde a sua gênese. *Autenticidade* é a propriedade de que o dado seja, não somente íntegro, como também tenha sua origem comprovada. Finalmente, a *irretratabilidade* refere-se à impossibilidade de que a autoria de um dado possa ser negada posteriormente pelo seu autor. Dentre esses requisitos, a autenticidade (e integridade) é necessária com maior frequência, já que protege usuários contra dados falsos ou corrompidos. Sigilo nem sempre é necessário, assim como a irretratabilidade.

Há um grande número de outros requisitos de segurança, que são variações ou combinações desses quatro. A disponibilidade também é um requisito desejável de qualquer sistema de informação, mas envolve uma discussão mais ampla do que o nosso foco aqui, restrito à segurança.

Técnicas criptográficas para o provimento de requisitos básicos

Classicamente, o termo "Criptografia" refere-se à transformação da grafia original de um dado em outra, que oculte a informação nele contida. Mais recentemente, no entanto, a partir da década de 1970, esse termo designa todo um conjunto de técnicas matemáticas nas quais se baseia a maioria das aplicações para provimento de segurança de dados. Assim, a expressão "cifração de dados" tem a preferência sobre "criptografia de dados", evitando a ambiguidade. Alguns autores também usam a expressão "encriptação", em vez de cifração, pela sua proximidade com o termo *encryption*, em inglês.

A Criptografia dispõe de três técnicas, também básicas, para o provimento dos requisitos de segurança descritos acima: cifração de dados, resumo (*hash*) criptográfico, e assinaturas digitais.

A *cifração* consiste em substituir os caracteres (bits) de um dado, por outros, cuja relação com os caracteres originais seja impossível de se obter na prática, exceto pelos possuidores de um dado crucial, chamado de chave, que torna possível a *decifração* do dado cifrado. No caso da *cifração simétrica*, a *chave secreta* é única e de conhecimento restrito aos autorizados a cifrar/decifrar o dado. No caso da *cifração assimétrica*, ou de *chave pública*, a chave de cifração é diferente da chave de decifração- a primeira é pública, de conhecimento generalizado, e a segunda, a *chave privada*, é de conhecimento exclusivo do seu dono. A despeito de haver uma relação matemática entre as duas, é claro que a chave privada não deve ser facilmente dedutível a partir da chave pública. Primariamente, a cifração provê o requisito de sigilo, mas também pode ser usada para prover integridade e autenticidade.

Resumo (ou *hash*) é uma técnica oriunda da área de estruturas de dados. Trata-se de comprimir um texto (dado) de comprimento arbitrário, produzindo um texto de comprimento fixo, um resumo, portanto, com certa garantia de que dados diferentes resultem em resumos diferentes. É importante notar que dois ou mais textos podem ter o mesmo resumo; tais *colisões* são inevitáveis, pela grande diferença entre a dimensão do espaço de textos e a do espaço de resumos. Se colisões puderem ser evitadas, um resumo funcionará como um identificador curto de um dado arbitrariamente longo, o que é muito útil em buscas em estruturas de dados. No contexto da Criptografia, um resumo deve ter propriedades adicionais, de forma que sejam computacionalmente inviáveis: (i) produzir um texto a partir do seu resumo; e (ii) obter colisões, isto é, dois textos com o mesmo resumo, por qualquer meio. Resumos criptográficos provêm os requisitos de integridade e autenticidade.

A *assinatura digital* é a única técnica que provê irretratabilidade. A partir de um dado e da sua chave privada, um usuário *U* produz (sua) assinatura *S* do dado. Essa assinatura pode ser verificada por meio de um procedimento que combina o dado, a assinatura *S* e a chave pública de *U*, produzindo verificação positiva se, e somente se, *S* tenha sido produzida como esperado, conjugando o dado e a chave privada de *U*. O fato de a chave privada ser de conhecimento exclusivo do seu dono traz a garantia necessária para a irretratabilidade do ato da assinatura.

Algoritmos e protocolos

As técnicas descritas acima são implementadas por meio de algoritmos, que trazem em si as garantias matemáticas para o provimento dos requisitos de segurança. Tais algoritmos são combinados, na forma de um protocolo criptográfico que envolve, na maioria dos casos, duas ou mais partes realizando uma troca de mensagens. Em alguns casos a troca é muito simples; em outros, toma a forma de uma longa sequência de mensagens trocadas entre várias partes, algumas delas seres humanos e, outras, meros processos sendo executados por um dispositivo computacional.

Assim como algoritmos criptográficos derivam sua força de resultados matemáticos que necessitam ser demonstrados rigorosamente, protocolos criptográficos também devem ter sua robustez atestada, por técnicas que envolvem, muitas vezes, algum tipo de jogo entre as partes na presença de um adversário cujo objetivo é burlar o requisito de segurança em questão. O atestado de robustez deve demonstrar que a vitória do adversário só pode ocorrer com probabilidade infinitamente pequena. A isso chamamos de *segurança demonstrável* de um protocolo.

Protocolos criptográficos estão no cerne da maioria das soluções para provimento de cibersegurança. Além de proteger requisitos básicos de segurança, são usados em aplicações de suporte, como o estabelecimento, distribuição, gerenciamento e certificação de chaves criptográficas, ou requisitos mais elaborados como identificação/autenticação de entidades, e anonimato, controle de acesso e autorização, entre outros.

A matemática das técnicas criptográficas

A Criptografia clássica, sinônimo de cifração simétrica, é baseada em métodos que combinam texto e chave secreta principalmente por meio de substituições de caracteres e/ou permutações das suas posições no texto. Isso se mantém até hoje. Mesmo o método padrão dessa classe, o *AES (Advanced Encryption Standard)* usa tais operações, mas de forma muito mais sofisticada do que seus antecessores e, mais importante, usando chaves muito mais longas, de pelo menos 128 bits: o esforço computacional para encontrar a chave correta, tentando todas as possibilidades, é tarefa impensável, exigindo um número de operações da ordem de 2^{128}. Assim, os esforços de *criptoanálise*, isto é de tentativas de análise (ou "quebra") desses métodos tornando-os não efetivos, são quase sempre voltados

à redução desse esforço computacional imenso, por meio da identificação de atalhos no projeto usando técnicas como a criptoanálise *diferencial e linear*. É, em si, um trabalho também hercúleo, como buscar uma agulha num palheiro.

Algoritmos para resumos criptográficos surgiram concomitantemente ao advento da cifração de chave pública, como técnica de suporte às assinaturas digitais. Desde então encontraram um sem-número de aplicações, muito além do seu uso inicial, como a aleatorização de eventos, simulação de moedas, entre outras. Os métodos para construção de funções de resumo evoluíram nos últimos anos, dos métodos iterativos envolvendo funções de compressão, para os atuais *métodos esponja*. Seja qual for o caso, sua construção tampouco depende de conceitos matemáticos profundos. Sua criptoanálise se resume à redução da complexidade da busca por colisões.

Sem dúvida, a grande revolução nas técnicas criptográficas e teorias subjacentes foi produzida pelo advento da criptografia de chave pública na segunda metade da década de 1970, com a introdução do método RSA (das iniciais de Rivest, Shamir e Adleman). A robustez criptográfica do RSA é baseada na dificuldade do problema da *fatoração* de números inteiros muito grandes, resultantes do produto de dois números primos também de grande magnitude. Falamos aqui de números de 2 a 4 mil bits. Até esta data não se conhecem métodos eficientes para resolver essa tarefa usando computadores convencionais. Existem, no entanto, algoritmos que serão capazes de resolver eficientemente esse problema usando computadores quânticos, quando estes se tornarem uma realidade prática.

Outro problema matemático com a mesma característica de vulnerabilidade à criptoanálise quântica é o do *logaritmo discreto*. Trata-se de calcular logaritmos numa estrutura discreta (de grupos cíclicos), problema difícil no universo de grandes números e computadores convencionais. Métodos criptográficos baseados nesse problema ganharam popularidade a partir dos anos 1980, pelos ganhos de eficiência resultantes do uso de chaves menores que as dos métodos baseados em fatoração, possibilitando seu emprego em dispositivos com poucos recursos. O método mais popular dessa classe é o de *curvas elípticas*. Sua implementação é bem mais complexa do que a do RSA, necessitando de dois tipos de aritméticas em estruturas algébricas distintas. Daí, a sua implementação cuidadosa, explorando aspectos matemáticos e de engenharia de algoritmos sobre plataformas específicas, é um problema desafiador e muito interessante.

Motivada pela ameaça quântica, a comunidade de pesquisa criptográfica tem buscado ajuda em outra classe de algoritmos, a dos problemas NP-completos. Esses são problemas historicamente resistentes à resolução eficiente, mas têm a característica peculiar de que, uma vez encontrado um algoritmo eficiente para resolver um deles, então algoritmos eficientes podem ser encontrados para todos eles, mediante um esforço adicional de baixa complexidade. Essa propriedade dá a essa classe um status de alta

dificuldade. Alguns desses problemas, notadamente os oriundos da Teoria dos Reticulados e da Teoria dos Códigos (Corretores de Erros), servem de base a alguns métodos hoje em processo de padronização, após serem aprovados em uma competição pública promovida pelo *National Institute of Standards and Technology dos EUA [NIST]*. A teoria e implementação dessa nova safra de métodos ainda está sob escrutínio intenso da comunidade acadêmica, dada a sua relativa novidade. Em particular, o tamanho das chaves e a obtusidade de alguns métodos são empecilhos à sua adoção imediata. Alguns deles, após aprovação preliminar, foram posteriormente quebrados de forma simples, o que mostra o valor dessa forma de seleção aberta ao público.

Ainda na seara quântica, um método para estabelecimento de chaves secretas proposto em 1984 por Bennett e Brassard, utiliza exclusivamente fenômenos quânticos, sem recorrer a qualquer teoria matemática. Em vez de bits, a informação é codificada e transmitida como partículas elementares (fótons são as mais usadas), de forma que um adversário não consiga "ler" essas partículas sem causar distúrbios nas suas propriedades quânticas. Assim, em vez de esconder (cifrar) um dado em trânsito, o efeito é o de impedir sua leitura não autorizada sem despertar suspeitas.

Para além da criptoanálise

Como vimos, a criptoanálise é realizada, ou pela dedução sistemática de chaves secretas ou privadas, ou pela descoberta de falhas nos pressupostos matemáticos de uma técnica ou na concepção de um protocolo. Há, porém, outras formas de ataque, que visam a implementação de um método numa plataforma computacional específica. Esses são resultantes de falhas na escrita do código (programa) da implementação ou advindas do vazamento de informação sensível por canais inesperados como consumo de energia, tempo de execução e radiação eletromagnética. Tais canais são conhecidos como *canais laterais* e a prevenção de ataques deste tipo é feita pela cuidadosa implementação dos algoritmos, de forma a evitar flutuações nesses vazamentos que possam ser identificados com os bits das chaves ou outras informações sensíveis. Todo projeto atual de algoritmo criptográfico inclui a apresentação de contramedidas por meio de uma implementação imune a tais ataques. Frequentemente, tal implementação incorre em algum tipo de ineficiência quando comparada a uma implementação que vise somente eficiência.

Aplicações avançadas

Até muito recentemente, criptografia era um termo conhecido na comunidade acadêmica e profissional de computação, mas pouco conhecida fora dela. Após o advento das criptomoedas e dos comunicadores instantâneos seguros, como WhatsApp e similares, o prefixo *cripto* pode ser encontrado facilmente em qualquer portal de notícias ou mesa de bar em que se possa pagar a conta usando criptomoedas. De fato, essa *criptomania* se

deve ao desenvolvimento de protocolos mais sofisticados para não só a simulação de moedas e o sigilo ponta-a-ponta dos comunicadores instantâneos, mas também para outras aplicações sofisticadas, como:

1. computação distribuída confiável, usando protocolos conhecidos como *multi-party computation*, ou MPC, que possibilitam a interação confiável de várias partes num mesmo processo, protegendo eventuais informações sensíveis de cada parceiro, como sua identidade, chaves criptográficas, ou dados de qualquer natureza;
2. assinatura automática de contratos, usando protocolos de conhecimento zero (*zero-knowledge* protocols), que possibilitam a verificação de propriedades de um dado sem revelar o seu conteúdo;
3. computação com dados cifrados, usando cifração homomórfica (*homomorphic encryption*), que possibilita a realização de cálculos sobre dados cifrados, resguardando o sigilo do resultado e mesmo a natureza desses cálculos. Essa aplicação é muito útil para dados sensíveis armazenados em nuvens.

Considerações práticas

O emprego de técnicas criptográficas requer cuidados especiais, como já vimos, com a necessidade de prevenção de ataques por canais laterais. É possível escrever uma peça de software criptográfico totalmente aderente do ponto de vista funcional, mas recheada de vulnerabilidades. Geralmente, desenvolvedores de software não têm qualquer treinamento em criptografia, mas são deixados à vontade para desenvolverem código ad hoc ou que usam bibliotecas criptográficas, sem a assistência de alguém com o devido treinamento em criptografia. Assim, é possível que:

1. o uso de bibliotecas seja feito de forma incorreta ou com opções de compilação que introduzam vulnerabilidades como a exposição de canais laterais;
2. sejam usadas versões defasadas de bibliotecas, com vulnerabilidades corrigidas somente em versões posteriores;
3. código ad hoc seja inseguro, com métodos de cifração ingênuos, inventados por iniciativa do desenvolvedor;
4. código seja extremamente ineficiente, introduzindo atrasos insuportáveis para a aplicação a que se destina.

Esses são somente alguns dos percalços, retirados de casos reais, no desenvolvimento de software criptográfico. Por isso, é importante a observância de padrões e melhores práticas da área [NIST2].

Vale notar, finalmente, que uma tendência que cresceu muito nos últimos anos é a transferência de parte da responsabilidade pela segurança de dados para o hardware. É comum, hoje, o emprego de

hardware seguro para armazenamento e computação de dados e trechos sensíveis de aplicações. Tais peças de hardware podem ser dispositivos *stand alone*, ou placas e circuitos integrados, dependendo da criticidade da informação. *Hardware security modules*, por exemplo, são dispositivos *stand alone* dotados de mecanismos de proteção que incluem sensores diversos e provisão para destruição de dados em caso de invasão do dispositivo.

Implicações para o ensino hoje e no futuro

De toda a nossa discussão prévia, fica evidente a necessidade de introdução de disciplinas relacionadas à Criptografia nos cursos de graduação. Também fica claro que não se trata de criar uma só disciplina que abarque toda a gama de material que mal pincelamos acima.

O ideal seria termos, inicialmente, uma disciplina que cubra, de forma introdutória os princípios, técnicas fundamentais, aplicações de suporte e principais aplicações modernas em uso no mundo. Para tal tarefa, não existe um texto em português suficientemente atualizado. Em inglês, talvez o melhor texto hoje seja o de autoria de Stinson e Paterson [SP].

Uma segunda disciplina seria desejável, tendo ou não a primeira como pré-requisito, que cubra com maior detalhe um maior número de algoritmos e protocolos, ressaltando aspectos de complexidade e demonstrações de segurança necessárias em cada caso. Para tal tarefa, um bom texto, mais denso, é o de Katz e Lindell [KL], um bom complemento ao de Stinson.

Com uma ou ambas as disciplinas acima como pré-requisitos, algumas ramificações são possíveis, em oferecimentos conjuntos na pós-graduação. A literatura de apoio será, necessariamente, composta de artigos e outras publicações recentes, além de livros-texto.

1. Uma disciplina teórica para alunos que queiram seguir uma rota de pesquisa, com forte ênfase nos aspectos de complexidade, teórica e prática de algoritmos e protocolos, e suas demonstrações de segurança. Imprescindível aqui é uma boa dose de computação quântica. Um bom texto para essa disciplina é o de autoria de Hoffstein et al. [HPS].
2. Uma disciplina para os que pretendem desenvolver atividades de implementação eficiente de métodos criptográficos, explorando diversas plataformas de mercado, das mais robustas às mais restritas em recursos. Referências adicionais são de autoria de Hankerson et al. [HVM], Koç [Koç], e Menezes et al. [MOV].
3. Uma disciplina voltada a aspectos sociais relacionados ao uso indiscriminado de criptografia, como privacidade, anonimato e eleições eletrônicas.
4. Uma disciplina voltada a gestores de TI, com cobertura mais voltada à gestão de ativos criptográficos e das aplicações que dependem fortemente desses ativos.

Referências

1. [Auma] J.-P. Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption. Primeira Edição (Segunda Edição disponível em outubro de 2024). No Starch Press, 2017.
2. [HPS] J. Hoffstein, J. Pipher, J. H. Silverman. An Introduction to Mathematical Cryptography. Springer, 2014.
3. [HVM] D. Hankerson , S. Vanstone , A. Menezes. Guide to Elliptic Curve Cryptography
4. [KL] J. Katz, Y. Lindell. Introduction to Modern Cryptography, Terceira Edição. CRC Press, 2020.
5. [Koc] Ç. K. Koç, ed. Cryptographic Engineering. Springer 2008.
6. [MOV] A. J. Menezes, P. C. van Oorschot, S.Vanstone. Handbook of Applied Cryptography. CRC Press, 1996. Disponível, reeditado em https://cacr.uwaterloo.ca/hac/
7. [NIST1] Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/post-quantum-cryptography
8. [NIST2] Cryptographic Standards and Guidelines. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
9. [SP] D. R. Stinson, M. Paterson. Cryptography: Theory and Practice, Quarta Edição. CRC Press, 2018.
10. [Wong] D. Wong. Real-world Cryptography. Manning, 2021.

RICARDO DAHAB é professor titular do Instituto de Computação da Universidade Estadual de Campinas, UNICAMP. Tem mestrado pela UNICAMP em Criptografia e doutorado pela Universidade de Waterloo, Canadá, em Combinatória e Otimização. Seus interesses de docência e pesquisa situam-se nas áreas de Algoritmos e Protocolos Criptográficos e Segurança da Informação. Desde 1995 tem publicado trabalhos científicos e orientado teses de doutorado e mestrado nessas áreas, várias das quais receberam prêmios e distinções. Atuou também na área de Teoria dos Grafos. Participou do projeto ICP-EDU, em parceria com a RNP, UFSC, UFMG e Kryptus Tecnologias de Segurança, do qual resultou o primeiro hardware de alta segurança (HSM) totalmente nacional. Junto com as comunidades de criptografia e segurança vem cooperando ativamente na consolidação dessas áreas no Brasil e na América Latina, participando da Comissão Especial de Segurança da SBC, da organização de eventos como o SBSeg, a Escola Avançada de Criptografia da Fapesp, o Latincrypt, a CANS e o PKC. Foi agraciado, em 2011 com o prêmio Zeferino Vaz de Excelência Acadêmica da UNICAMP e, em 2019, com o Prêmio Destaque da Comissão Especial de Segurança da Informação e de Sistemas Computacionais.

ARTIGO

FORMANDO PROFISSIONAIS SOB A PERSPECTIVA DA EVOLUÇÃO NA ADOÇÃO DE SISTEMAS EM NUVEM

POR

Luiz Fernando Rust da Costa Carmo e Ewerton Longoni Madruga

Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)

lfrust@inmetro.gov.br, elmadruga@inmetro.gov.br

Um sistema de software é como uma grande residência: possui diferentes compartimentos, como quartos e salas, construídos com lotes de tijolos de origem distinta. Ou seja, é importante lembrar que um sistema utiliza inúmeros componentes de diferentes fornecedores. E estes componentes de software têm diferentes níveis de maturidade no seu desenvolvimento, o que afeta a possibilidade de introdução de vulnerabilidades ao sistema como um todo. O eixo de Segurança de Sistemas trata dos aspectos dos sistemas compostos por componentes e conexões, e os softwares em uso [SBC 2023].

Os sistemas tradicionais já trazem consigo os seus próprios desafios. Eles executam dentro da empresa, em um computador, conectados à Internet, em uma sala climatizada e com configuração e operação monitoradas localmente. A cibersegurança deste tipo de sistema já vem sendo estudada há décadas e é razoavelmente bem entendida. Seus principais aspectos já são ensinados nos cursos superiores de computação no país, num processo que deve manter-se evolutivo de forma natu-

ral. Entretanto, no momento em que este artigo é escrito, uma explosão de demanda por Inteligência Artificial (IA) Generativa [WIZ 2024] faz com que a computação em nuvem e o crescimento na sua adoção provoque um deslocamento no eixo das discussões a respeito dos aspectos de segurança em sistemas.

Há pouco mais de um ano, a inteligência artificial generativa viu um crescimento explosivo tanto entre os usuários finais quanto nas empresas. Enquanto a IA e a aprendizagem de máquina tradicionais têm sido integradas tanto em empreendimentos científicos quanto comerciais há muitos anos, a IA generativa e os grandes modelos de linguagem (LLMs, na sigla em inglês) em particular tornaram essa tecnologia conhecida por todos. O poder da inteligência artificial generativa é potencialmente transformador. A tendência começou com os lançamentos de serviços de geração de imagens, incluindo *Midjourney e DALL-E 2 (OpenAI)*, em paralelo com modelos como o *Stable Diffusion da Stability.ai* [Roose 2022]. E esta tendência tomou proporções ainda maiores com o lançamento de serviços de geração de texto, e, especialmente, do ChatGPT (também OpenAI), logo a seguir.

Assim, olhando para o longo prazo, o potencial de crescimento da utilização da computação em nuvem dentro das empresas é muito grande [WIZ 2024], especialmente com a chegada das ondas de transformação que tecnologia de IA podem ainda vir a trazer dentro de empresas nos próximos anos. Entretanto, a computação em nuvem não é um assunto que seja refletido na realidade dos cursos de nível superior com a importância que está adquirindo. Gostaríamos de discutir o tema e acrescentar aspectos a serem considerados na hora da montagem do programa de cibersegurança dentro das universidades no país.

Modelos de Serviço

Existem diferentes modelos de serviço em *cloud computing*, que oferecem diferentes níveis de controle e responsabilidade para os usuários: IaaS, PaaS e SaaS. As principais diferenças entre eles são:

1. **Infrastructure as a Service (IaaS):** Nesse modelo, os provedores de serviços em nuvem fornecem infraestrutura básica de TI, como servidores virtuais, gerência de chaves criptográficas, armazenamento e redes. Os usuários têm controle total sobre o sistema operacional, aplicativos e dados, sendo responsáveis por instalar, configurar e gerenciar o software necessário. Exemplos de provedores de IaaS incluem Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).
2. **Platform as a Service (PaaS):** Aqui os provedores de nuvem oferecem plataformas de desenvolvimento e execução de aplicativos, incluindo ferramentas de desenvolvimento, infraestrutura de execução, banco de dados e componentes de middleware. Os usuários desenvolvem

e implantam seus aplicativos na plataforma fornecida, sem se preocupar com a infraestrutura subjacente.

3. **Software as a Service (SaaS):** Nesse modelo, os usuários acessam aplicativos baseados na nuvem através da Internet, em vez de instalá-los localmente em seus dispositivos. Os provedores de serviços em nuvem são responsáveis por toda a infraestrutura, manutenção e atualizações do software. Exemplos de aplicativos SaaS incluem o Zoom, plataforma de videoconferência, e o Microsoft 365, plataforma com editor de texto, planilha e editor de apresentações.

Existem obstáculos em criar um ambiente de ensino de cibersegurança no contexto *cloud computing* em laboratório. Conside-se aqui um modelo de IaaS, por exemplo, que oferece uma conjunto grande de componentes (gerência de chaves, computação virtualizada, banco de dados, repositório de arquivos, orquestração de contêineres, execução de programas sem servidor, etc.) que podem ser interligados de maneiras diversas através de uma interface-console. Construir um protótipo válido na escola ou encontrar uma plataforma de baixo custo que replique em laboratório a experiência de um analista de segurança que audita um ambiente em produção dentro de um provedor de serviços de *cloud computing* não é um processo simples. Um pouco mais adiante, discutimos este problema na seção "Desafios Acadêmicos" e apresentamos possíveis soluções que atendam às instituições de ensino superior no país.

Referência Normativa

Para seguirmos a discussão, é importante contextualizar as normas de mais ampla aplicação que regem qualquer atividade de gestão corporativa com vistas à cibersegurança, utilizando computação em nuvem ou não. Existe uma enorme coleção de normas nesta área, mas, para simplificar a composição de novos planos pedagógicos, é possível estabelecer uma fundamentação regulatória mais básica com três padrões: a) ISO 27001, b) NIST CSF, e c) ISO/IEC 15408. A ISO 27001 [ISO 2022] é um padrão internacional que estabelece os requisitos para um sistema de gestão de segurança da informação (SGSI). Seu principal objetivo é garantir a confidencialidade, integridade e disponibilidade das informações em uma organização, além de minimizar os riscos de segurança da informação.

FIG. 01 | **O CYBERSECURITY FRAMEWORK (CSF), DO NIST**

Já o NIST *Cybersecurity Framework* (CSF) [NIST 2024] é um conjunto de diretrizes, melhores práticas e padrões destinados a ajudar as organizações a melhorarem sua postura de segurança cibernética. Como ilustra a Figura 1, este importante arcabouço concentra-se em cinco áreas principais: identificar, proteger, detectar, responder e recuperar, sendo focado em fornecer orientações práticas e acionáveis para a implementação de medidas de segurança cibernética.

Embora tanto o NIST CSF quanto o ISO 27001 possam ser utilizados em qualquer momento da jornada de segurança de uma organização, cada um tem um estágio de maturidade ideal em que são mais úteis. O NIST CSF é projetado para organizações em estágios iniciais de desenvolvimento de sua cibersegurança. Isso ocorre porque ele serve como um guia para ajudar uma empresa a construir uma estratégia de segurança da informação e estabelecer uma postura de segurança básica. O ISO 27001 é mais adequado para organizações mais maduras e com um risco de segurança aumentado. Ao buscar a certificação ISO 27001, a organização provavelmente já possui um programa geral de cibersegurança em vigor, mas precisa de práticas mais intensivas para fortalecer sua postura e aderir aos padrões do cliente. Possivelmente, porque empresas que compram serviços, para resguardar seu investimento, estabelecem a certificação de um fornecedor como um requisito técnico no processo de compra.

O padrão ISO/IEC 15408 diz respeito ao *Common Criteria for Information Technology Security Evaluation* (Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação) [ISO 2009] é um padrão internacional utilizado para avaliar a segurança e a confiança de produtos e sistemas de tecnologia da informação. Os principais objetivos do *Common Criteria* são estabelecer critérios para avaliação de segurança de produtos e sistemas de TI, fornecer uma estrutura para a avaliação independente de segurança, permitir a comparação entre produtos de segurança, e promover a confiança no uso de produtos de TI.

Durante a pandemia, a distância forçada entre as pessoas trouxe uma explosão do uso de videoconferência para a comunicação em geral,não apenas para reuniões corporativas, mas também para comunicação pessoal, de cunho familiar. O software Zoom tornou-se um grande nome neste setor, tendo investido em computação em nuvem para atender esta demanda explosiva [Bourne 2020].

O serviço da empresa Zoom é um exemplo clássico de um SaaS, que baseia a oferta de serviços na computação em nuvem, e precisa do *Common Criteria* para expandir seu mercado. Numa decisão estratégica para se distanciar dos problemas que teve neste período de crescimento astronômico, e também aproximar-se de clientes corporativos de maior envergadura, a empresa obteve a certificação Common Criteria v3.1 rev 5. [Zoom 2021] para o seu Zoom Client. A familiaridade com este e com os demais padrões discutidos acima é importante e o estudo destes padrões traz um exemplo sobre o que os egressos de um curso de cibersegurança podem encontrar no mercado de trabalho.

Responsabilidade Compartilhada

Os principais provedores de serviços em nuvem (ou, no inglês, *Cloud Service Providers* - CSPs) operam sob um modelo de responsabilidade compartilhada. Isso significa que uma parcela das obrigações de segurança reside com a equipe de segurança da empresa cliente, que contrata o serviço. Transferir operações para uma plataforma de nuvem não significa que uma organização esteja livre de todas as responsabilidades de cibersegurança. O que toca a cada um depende do modelo de serviço empregado.

Por exemplo, no caso do modelo IaaS, os CSPs são responsáveis pela infraestrutura básica da nuvem, incluindo a segurança física das instalações que abrigam os equipamentos. Em outras palavras, os CSPs não são responsáveis pela segurança dos sistemas operacionais ou das pilhas de software necessárias para executar aplicativos ou armazenar dados.

No caso do modelo PaaS, este modelo requer que o provedor assuma maior responsabilidade adicional pelos aplicativos e sistemas operacionais. Não raro, a gerência não técnica de sistemas de computação em nuvem, erroneamente, posiciona-se no sentido de que a segurança da sua aplicação em nuvem é garantida integralmente pelo CSP. Ao contrário, a realidade é que existe este modelo de responsabilidade compartilhada, que significa que o CSP e seus clientes trabalham juntos para garantir a segurança dos dados e das aplicações na nuvem, cada um desempenhando um papel específico na proteção dos recursos.

Catálogos de Vulnerabilidades

Existem diferentes bases que são fundamentais para que a comunidade de profissionais de cibersegurança consiga acompanhar as centenas de vulnerabilidades que surgem diariamente. Quem usa software não deseja estar vulnerável, ou seja, não quer seus dados pessoais ou de clientes roubados por terceiros, por exemplo. Quem fabrica software que é oferecido como produto precisa acompanhar todos os problemas de segurança que surgem ao longo do ciclo de vida do produto. Detalhe – o acompanhamento não é apenas do seu produto, assim também como os componentes de software de terceiros que ele utiliza. Existe, portanto, uma teia de responsabilidades que deve ser bem compreendida para que a qualidade de um produto de software atenda às necessidades mínimas de segurança do cliente.

Por esta razão, existem várias bases de dados que auxiliam os profissionais responsáveis por administrar a segurança tanto de usuários como de produtos de fabricantes. Dois destes catálogos gerenciam não apenas vulnerabilidades de pacotes de software específicos, assim como potenciais classes de vulnerabilidades ('*weaknesses*') de pacotes de software. Uma classe de vulnerabilidades pode ser por exemplo uma que descreva em alto nível o que é um ataque de 'Cross-site Scripting' (XSS). Uma vulnerabilidade desta classe seria listada em outro catálogo com um grau numérico de severidade, e associado a um pacote de software específico.

O catálogo *Common Weakness Enumeration (CWE)*[1] é uma lista de diferentes tipos de falhas de segurança e vulnerabilidades comuns encontradas em software e hardware. Mantido pelo MITRE Corporation, o CWE fornece uma linguagem comum e padronizada para descrever e categorizar falhas de segurança, facilitando a identificação, compreensão e mitigação dessas vulnerabilidades. O CWE é utilizado por organizações de segurança, desenvolvedores de software e profissionais de segurança da informação para melhorar a segurança dos sistemas, ajudando a identificar e corrigir vulnerabilidades conhecidas e a evitar a introdução de outras durante o processo de desenvolvimento de software.

Já o catálogo de *Common Vulnerabilities and Exposures (CVE)*[2] é uma lista pública de informações sobre vulnerabilidades de segurança conhecidas em software e hardware específicos. Mantido pela organização MITRE Corporation, o CVE fornece identificadores únicos (CVE IDs) para cada vulnerabilidade, juntamente com informações detalhadas sobre a vulnerabilidade, sua gravidade e as maneiras de mitigá-la. O objetivo principal do CVE é fornecer uma referência comum para identificar e compartilhar informações sobre vulnerabilidades de segurança, facilitando a colaboração entre os pesquisadores de segurança, fabricantes de produtos e usuários finais para proteger sistemas e dados de contra-ataques maliciosos.

1 https://cwe.mitre.org/

2 https://www.cve.org/

Com muita frequência, surgem vulnerabilidades associadas aos provedores de serviço de nuvem. Como por exemplo, o CVE-2024-28823, que diz respeito a um módulo em *javascript* para acesso a repositórios de arquivos em nuvem através do protocolo HTTPS. A vulnerabilidade é da classe definida por CWE-79, conhecida como '*Cross-Site Scripting (XSS)*'. Este é um dos serviços de nuvem mais básicos e esta vulnerabilidade permite a injeção de código *javascript* não autorizado e potencial vazamento de informação. É desejável que casos como este sejam estudados em sala de aula no contexto de segurança em serviço de nuvem.

Desafio Acadêmico

No currículo de um curso de cibersegurança [SBC 2023], o eixo de formação em segurança de sistemas tem desafios importantes no desenvolvimento de competências quando o contexto é nuvem. Existem aspectos da tecnologia de computação em nuvem em que a reprodução em laboratório é mais simples. Por exemplo, a competência C.2.7 fala da necessidade da utilização de técnicas de resiliência. A replicação de várias instâncias de máquinas virtuais para simular tolerância a falhas de um sistema é algo razoavelmente simples de explicar em sala de aula e montar em laboratório usando Linux, KVM, e QEMU. [FONSECA 2017]

Entretanto, existem também obstáculos. Em primeiro lugar, existe a necessidade de acompanhar a contabilidade de uso dos componentes em nuvem. Alunos devem ser doutrinados a monitorar

muito de perto o custo da atividade sendo realizada. Caso a atividade envolva, por exemplo, o uso de aceleradores de cálculo matemático (GPUs, TPUs, etc.) para treinamento de um modelo em Deep Learning, a conta diária pode ser muito alta. Simular esta contabilização no uso de componentes de serviço em nuvem na escola não é uma tarefa fácil.

Em segundo lugar, os CSPs em geral mantêm disponível uma extensa *Application Programming Interface* (API) para controle de toda sua longa lista de serviços. Autenticação e autorização passam por dar acesso correto aos diversos usuários que controlam o uso da nuvem corporativa. E, ficando apenas neste exemplo, o teste para autorização a esta lista de serviços disponibilizados por CSPs, mesmo considerando os mais básicos, é difícil de ser replicado apenas com Linux, KVM e QEMU.

Os maiores provedores de serviço de nuvem mantêm um programa de certificação de profissionais[3][4]. Na esteira da preparação para esta certificação, estes provedores mantêm também portais educacionais aos quais instituições de ensino no país podem ter acesso sem custo. Esta é uma ótima alternativa que exige apenas o contato da instituição com as academias de cada um dos grandes provedores. É uma solução completa para os dois obstáculos listados acima.

Como alternativa, existem soluções de código aberto que podem ser utilizadas em laboratório. Uma destas alternativas é o OpenStack[5], que é um conjunto de módulos para a criação e gerenciamento de nuvens computacionais públicas e privadas. Ele fornece uma plataforma para a virtualização de recursos de computação, armazenamento e rede, permitindo que os usuários criem e gerenciem nuvens de forma flexível e escalável.

O OpenStack é composto por vários projetos inter-relacionados, cada um sendo associado a uma parte específica da funcionalidade da nuvem, como computação virtual (Nova), armazenamento em bloco (Cinder), armazenamento de objetos (Swift), rede (Neutron) e gerenciamento de identidade (Keystone), entre outros.

Mensagem Final

Conforme explicado no início do artigo, com o surgimento de tecnologias inovadoras como a Inteligência Artificial, existe uma tendência de crescimento na adoção de serviços de *cloud computing* pelas empresas. Daí segue a necessidade de estruturar unidades curriculares que se ocupem em ensinar os diversos aspectos relevantes sobre a segurança de sistemas em contexto de computação em nuvem. Além de padrões internacionais de segurança e bases globais de vulnerabilidades relevantes, discutimos alternativas para que instituições de ensino no país possam superar as dificuldades de trazer uma experiência mais mão na massa em sala de aula ou em laboratórios. Esta experiência nos bancos escolares torna-se crucial

3 https://aws.amazon.com/pt/training/awsacademy/

4 https://learn.microsoft.com/pt-br/training/educator-center/

5 https://www.openstack.org/

na formação de profissionais com perfil tão carente no mercado de trabalho.

Referências

1. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125.
2. Wiz Inc. State of AI in the Cloud, 2024. Obtido em: https://www.wiz.io/blog/key-findings-from-the-state-of-ai-in-the-cloud-report-2024
3. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Padrão número 27001:2022). Obtido em https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en
4. International Organization for Standardization. (2009). Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model (ISO/IEC Padrão número 15408). Obtido em https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en
5. National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. Obtido em https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
6. ROOSE, K. AI-Generated Art Is Already Transforming Creative Work. New York Times, Outubro 2022.
7. BOURNE, J. Zoom makes Amazon Web Services its preferred cloud provider, Dezembro 2020. Obtido em https://www.cloudcomputing-news.net/news/2020/dec/04/zoom-makes-amazon-web-services-its-preferred-cloud-provider
8. ZOOM, Inc. Common Criteria, Dezembro 2021. Obtido em https://www.zoom.com/en/trust/legal-compliance/common-criteria/
9. FONSECA, N. Networking for Big Data: Lab Exercise. UNICAMP, 2017. Obtido em: https://www.ic.unicamp.br/~nfonseca/comsoc-school/2017/lab-exercise.html

EWERTON LONGONI MADRUGA é pesquisador-tecnologista do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO). Tem Bacharelado e Mestrado em Ciências de Computação pela Universidade Federal do Rio Grande do Sul (UFRGS), assim como Doutorado em Engenharia de Computação pela Universidade da California, Santa Cruz. Foi desenvolvedor de sistemas e protocolos de rede na Nokia Networks, em Mountain View, CA, até 2003. Atualmente é pesquisador-tecnologista e coordenador do Curso Técnico em Segurança Cibernética (INMETRO/IFF). Suas áreas de interesse são segurança da informação, sistemas móveis, computação em nuvem e aprendizado de máquina aplicado à técnicas de segurança ofensiva.

LUIZ F RUST C CARMO é formou-se em Engenharia Eletrônica em 1984, obteve o título de M.Sc. em Ciência da Computação em 1988, ambos pela Universidade Federal do Rio de Janeiro (UFRJ), e Ph.D. em Ciência da Computação em 1994, pelo Laboratório de Arquitetura e Análise de Sistemas da Organização Nacional Francesa de Pesquisa Científica (LAAS/CNRS) em Toulouse - França. Desde 2008 é Especialista Sênior do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) e, atualmente, atua como Diretor de Metrologia Científica, Industrial e Tecnologia. É professor ativo nos programas de doutorado em Ciência da Computação na UFRJ (PPGI) e em Metrologia (PPGMT) no Inmetro. Seus interesses de pesquisa incluem segurança da informação, validação de software para sistemas embarcados e transformação digital em metrologia.

ARTIGO

SEGURANÇA NA CONECTIVIDADE: PROTEGENDO REDES E CONEXÕES

POR
Michele Nogueira (UFMG)
michele@dcc.ufmg.br

Vivemos em um mundo hiperconectado em que, através de seus diferentes dispositivos computacionais e da Internet, as pessoas permanecem continuamente conectadas nas ruas, em suas casas, no trabalho e na escola. Isso tem resultado em transformações na sociedade e inovação aceleradas, gerando facilidades e grandes oportunidades para pessoas e instituições [1]. Portanto, a conectividade é a principal sustentação da era digital e desse mundo hiperconectado. Desde a Internet até as redes de acesso existentes em ambientes empresariais, residências, manufaturas, universidades e outros, passando pelos dispositivos da Internet das Coisas (*Internet of Things - IoT*), todo o funcionamento e acesso a serviços diversos depende de uma rede de conexões confiável [1, 2]. Por isso, a segurança na conectividade refere-se à proteção das redes de computadores e dos dados transmitidos por elas contra acessos não autorizados, interceptações e manipulações.

É vital para garantir a segurança das informações em um ambiente digital cada vez mais interconectado. A interconexão entre dispositivos apresenta uma série de desafios, principalmente no que diz respeito à segurança cibernética e, particularmente, relacionados à disponibilidade, confidencialidade e integridade na transmissão dos dados [2]. Assim, este artigo explora de forma abrangente e de fácil leitura os aspectos relacionados à segurança em redes de computadores, suas conexões lógicas e físicas, bem como na interconexão de seus componentes, destacando as melhores práticas, medidas para garantir a confidencialidade dos dados em trânsito, a integridade das mensagens e a disponibilidade da conexão.

As diferentes tecnologias de comunicação, desde Bluetooth, *zigbee*, Wi-Fi até fibra ótica e satélites, interligam nossos dispositivos computacionais cada vez mais diversos, resultando nas redes de computadores. Estas são frequentemente alvos de ataques cibernéticos devido à sua natureza distribuída e à quantidade de dados sensíveis que trafegam por elas. Lembrando que algumas dessas tecnologias possuem limitações em relação à largura de banda, assim como alguns tipos de dispositivos apresentam fortes limitações de recursos computacionais, e, por isto, as redes são facilmente saturadas por ataques como os ataques de negação de serviço (*Distributed Denial of Service - DDoS*) e outros. Para proteger essas redes, é essencial implementar medidas de segurança robustas, incluindo firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS) e sistemas de prevenção de perda de dados (DLP). Além disso, a autenticação forte, por meio de métodos como certificados digitais e autenticação de múltiplos fatores, é crucial para forçar que apenas usuários autorizados tenham acesso às redes de borda e sistemas. A criptografia desempenha um papel fundamental na proteção dos dados em trânsito, impedindo que informações confidenciais sejam interceptadas e até mesmo modificadas por invasores.

As conexões lógicas entre dispositivos em uma rede também requerem atenção especial quando se trata de segurança cibernética. As conexões lógicas, estabelecidas por meio de protocolos de comunicação, são vulneráveis a ataques de *spoofing* e interceptação. Para mitigar esses riscos, é fundamental implementar protocolos seguros, como o SSL/TLS (*Secure Sockets Layer/Transport Layer Security*), e realizar verificações de integridade dos dados transmitidos. Por sua vez, as conexões físicas, incluindo cabos de cobre e cabos de fibra óptica, também são alvos de ataques como sabotagem, interceptação e mesmo roubo desses componentes [3]. Para proteger essas conexões, é importante implementar medidas de segurança física, como o uso de cabos blindados e a restrição do acesso a áreas onde estão localizados os dispositivos de rede.

A interconexão de componentes em uma rede, via *switches*, roteadores e servidores, é crucial para garantir o funcionamento eficiente do sistema [4]. No entanto, essa interconexão representa um ponto fraco em termos de segurança cibernética, principalmente se não forem implementadas as devidas medidas de proteção. Para protegê-la, é essencial

segmentar a rede em zonas de confiança e aplicar políticas de controle de acesso rigorosas. Essas políticas devem ser definidas considerando visões de governança de toda a instituição e não apenas tomando como base uma visão técnica a fim de evitar inconsistências. Além disso, o monitoramento contínuo do tráfego de rede e a implementação de sistemas de detecção de intrusão ajudam a identificar e mitigar ameaças em tempo real.

Principais Técnicas de Segurança de Conectividade

Conforme mencionado, existem algumas formas principais para assegurar as redes de comunicação e seus componentes. Detalhamos um pouco mais as principais técnicas a seguir.

Firewall: um dispositivo de segurança de rede que monitora o tráfego de entrada e saída da rede e decide se permite ou bloqueia tráfego específico com base em um conjunto definido de regras de segurança. As regras definidas em um firewall pelo administrador da rede/sistema devem estar em consonância com as políticas gerais da instituição, incluindo uma visão de governança da mesma. Existem hoje firewalls que trabalham na camada de rede e outros que trabalham na camada de aplicação, seguindo a terminologia da pilha de protocolos TCP/IP.

Sistema de Detecção de Intrusões (IDS) e Sistema de Prevenção de Intrusões (IPS): sistemas que verificam o tráfego da rede para identificar ataques via análise de anomalias ou com base em assinaturas de ataques e então bloquear ativamente os mesmos. Os IDSs e IPSs fazem isso correlacionando enormes quantidades de dados e o que é considerada uma inteligência global sobre ameaças para não apenas bloquear atividades maliciosas, mas também rastrear a progressão de arquivos suspeitos e malware em toda a rede para evitar a propagação de surtos e reinfecções.

Segurança da carga de trabalho: protege as cargas de trabalho (dados) que se movem entre diferentes ambientes de nuvem e ambientes híbridos. Essas cargas de trabalho distribuídas possuem superfícies de ataque maiores, que devem ser protegidas sem afetar a agilidade dos negócios e operações.

Segmentação de rede: esta é uma forma de dividir a rede de uma organização em diferentes sub-redes. Esta técnica, que também auxilia na organização da rede, permite controlar melhor o fluxo de entrada e saída de dados das sub-redes e implementar firewalls específicos por sub-rede. Essa técnica permite a criação de zonas protegidas, como sub-redes apenas para servidores de grande importância que serão controlados por regras mais rigorosas de acesso. A segmentação de rede usando a tecnologia definida por software coloca o tráfego de rede em diferentes classificações e facilita a aplicação de políticas de segurança. Idealmente, as classificações são baseadas na identidade do endpoint e não apenas em endereços IP. Pode-se atribuir direitos de acesso com base na função, localização e muito mais, para que o nível certo de acesso seja concedido às pessoas certas e os dispositivos

suspeitos sejam contidos e corrigidos.

Rede privada virtual (Virtual Private Network - VPN): uma rede virtual que criptografa a conexão de um terminal a uma rede, geralmente pela Internet. Normalmente, uma VPN de acesso remoto usa protocolos como IPsec ou Secure Sockets Layer para autenticar a comunicação entre o dispositivo e a rede. Essa técnica cria um túnel virtual entre dois endpoints.

Antimalwares: "Malware", abreviação de "software malicioso", inclui vírus, worms, cavalos de Tróia, ransomware e spyware. Em algumas situações, o malware infecta uma rede, mas permanece inativo por dias ou até semanas. Os melhores programas anti malware não apenas verificam malware na entrada, mas também rastreiam arquivos continuamente para encontrar anomalias, remover malware e corrigir danos.

Inteligência artificial aplicada à classificação de comportamento: para detectar um comportamento anormal da rede, muitas vezes é necessário conhecer o que seria considerado o comportamento padrão. Diante de um volume cada vez maior de dados e tráfego de rede, a aplicação de técnicas de inteligência artificial e, particularmente, de aprendizado de máquina, auxilia e torna mais eficiente a classificação de tráfego de rede, inclusive a classificação de tráfego com comportamento anormal. As ferramentas de análise comportamental discernem automaticamente atividades que se desviam da norma. Esse tipo de técnica ajuda e economiza tempo de equipes técnicas de segurança nas organizações que identificam melhor os indicadores de comprometimento que representam um problema potencial e remediam as ameaças rapidamente.

Prevenção de perda de dados: As organizações devem certificar-se de que os seus funcionários não enviam informações sensíveis para fora da rede. As tecnologias de prevenção contra perda de dados, ou DLP, visam impedir que as pessoas carreguem, encaminhem ou até mesmo imprimam informações críticas de maneira insegura.

Melhores Práticas em Segurança de Conectividade

Além das medidas específicas mencionadas acima, existem várias melhores práticas que podem ajudar a fortalecer a segurança da conectividade em uma rede:

1. Atualizações regulares de software: manter todos os dispositivos e sistemas de rede atualizados com as últimas correções de segurança é essencial para evitar vulnerabilidades conhecidas;
2. Políticas de senha fortes: exigir o uso de senhas fortes e alterá-las regularmente pode ajudar a evitar ataques de força bruta e comprometimento de contas de usuário. Essas políticas devem ser definidas seguindo as diretrizes de segurança da instituição;
3. Monitoramento de atividades suspeitas: implementar sistemas de monitoramento de segurança que

alertem os administradores sobre atividades suspeitas pode ajudar a identificar e responder rapidamente a possíveis violações de segurança;

4. Treinamento de conscientização em segurança: educar os usuários sobre as melhores práticas de segurança, como reconhecer e-mails de phishing e evitar o compartilhamento de informações confidenciais, pode ajudar a reduzir o risco de ataques cibernéticos;

5. Backup regular de dados: realizar backups regulares dos dados críticos da rede é essencial para garantir a recuperação rápida em caso de falha de segurança ou desastre.

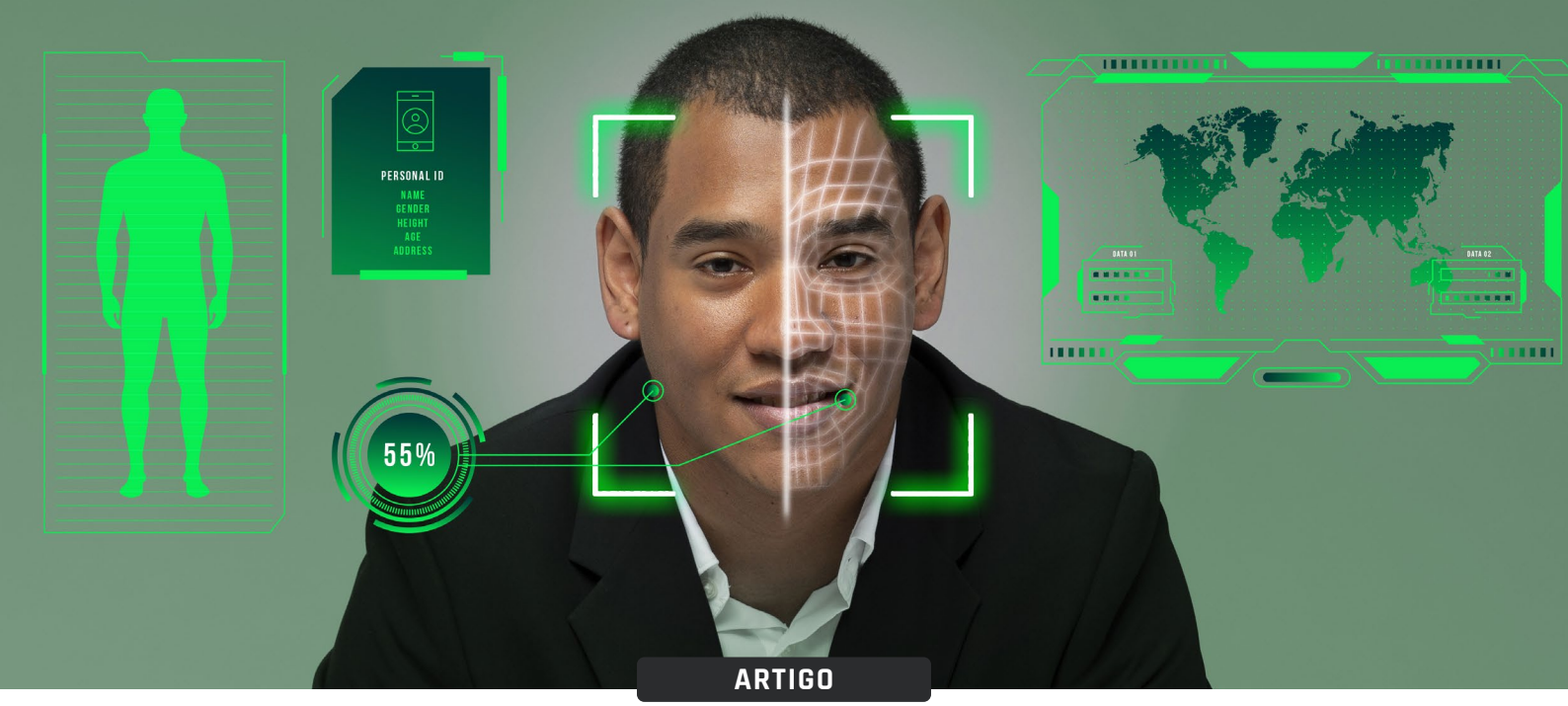
Considerações Finais

A segurança na conectividade é um aspecto fundamental da infraestrutura de rede moderna. Proteger as redes de computadores, conexões lógicas e físicas, bem como a interconexão de componentes, é essencial para garantir a integridade e confidencialidade dos dados. Ao implementar medidas de segurança robustas e seguir as melhores práticas recomendadas, as organizações mitigam os riscos de ataques cibernéticos e mantém suas redes seguras e protegidas. É importante ter sempre uma visão de futuro e integrar no dia a dia conhecimentos avançados e técnicas inovadoras como aquelas baseadas em Inteligência Artificial a fim de antecipar possíveis ameaças na rede e permitir a proteção mais eficiente das redes e dos sistemas.

Referências

1. Michele Nogueira. Segurança e privacidade dos dados no mundo hiperconectado. Computação Brasil - Revista da Sociedade Brasileira de Computação, no. 45, pg. 36-39, Julho 2021.
2. DE NEIRA, ANDERSON BERGAMINI ; KANTARCI, BURAK ; Nogueira, Michele. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks, v. 1, p. 109553, 2023.
3. Conexis Brasil Digital. 2,89 milhões de metros de cabos de telecom foram roubados ou furtados no primeiro semestre de 2023. Último acesso: 28 de abril de 2024.
4. REDES DE COMPUTADORES E A INTERNET: Uma abordagem top-down. 8ª Edição. James F. Kurose e Keith W. Ross. ISBN: 9788582605585
5. Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy. A survey on data leakage prevention systems. Journal of Network and Computer Applications. Vol. 62, 2016, Pages 137-152. ISSN 1084-8045.

MICHELE NOGUEIRA, D.Sc. é Cientista da Computação atuando na área de redes de computadores e segurança de redes. Possui doutorado em Ciência da Computação pela Sorbonne Université - UPMC/LIP6, França (2009) e realizou Pós-doutorado na Universidade Carnegie Mellon (CMU), EUA. É professora associada do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), membro sênior da Association for Computing Machinery (ACM) e do Institute of Electrical and Electronics Engineers (IEEE). Foi coordenadora da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (SBC) e foi a primeira mulher a coordenar o Comitê Técnico da Internet da IEEE Communications Society (EUA). É líder do Centro de Ciência de Segurança Computacional e coordena o projeto temático MCTIC/ FAPESP MENTORED, no qual um dos objetivos é criar um ambiente experimental acadêmico para Cibersegurança em parceria com a Rede Nacional de Ensino e Pesquisa (RNP).



ARTIGO

A SEGURANÇA DE SOFTWARE NECESSITA DE ATUALIZAÇÃO QUANDO CONFRONTADA COM A REALIDADE DA APRENDIZAGEM AUTOMÁTICA DISTRIBUÍDA?

POR

Nuno Neves
Universidade de Lisboa
nuno@di.fc.ul.pt

O Aprendizado de Máquina (Machine Learning, ML) está a ter um impacto profundo na sociedade, transformando vários aspectos das nossas vidas. Ao analisar grandes conjuntos de dados (*datasets*), os algoritmos de ML podem fornecer recomendações personalizadas, melhorar diagnósticos médicos, otimizar processos empresariais e aprimorar experiências dos utilizadores. No entanto, a adoção generalizada do aprendizado de máquina também levanta preocupações éticas e sociais, incluindo questões relacionadas com a segurança e a privacidade.

A ML distribuída emergiu como um desenvolvimento relativamente recente, mas promissor, com o potencial de revolucionar várias áreas aplicacionais, embora acompanhada de novos desafios na cibersegurança. Torna-se assim necessário abordar esses desafios de uma forma eficaz, para garantir o desenvolvimento e implementação responsável das tecnologias de ML distribuída, maximizando os seus benefícios e mitigando os riscos potenciais para os indivíduos e a sociedade. Este aspecto é particularmente importante no ensino superior, onde os currículos devem adaptar-se às mudanças tecnológicas. É essencial incorporar as atualizações que garantam que os estudantes estão preparados para se tornarem profissionais competentes e responsáveis neste cenário em rápida evolução.

Vamos usar a Aprendizagem Federada (Federated Learning, FL) para identificar

e ilustrar benefícios e riscos específicos. A FL é um paradigma de aprendizagem distribuída que facilita o treino de modelos em vários dispositivos sem a necessidade de trocar os dados [McMahan17]. Esta abordagem inovadora trata de preocupações com a privacidade, como as delineadas no GDPR [GDPR16] e CCPA [Bukaty19], pois garante que os registros armazenados permanecem nos dispositivos respectivos, enquanto permite o treino colaborativo de um modelo global. Além disso, a FL melhora a generalização do modelo aproveitando do recolhimento descentralizado de dados, o que muitas vezes resulta em um conjunto de amostras mais diversificado. Essa diversidade contribui para uma melhor cobertura do espaço de entrada, aprimorando, em última instância, a capacidade do modelo de generalizar quando implantado em ambientes de produção.

Logo, a FL encontrou aplicação em um amplo espectro de tarefas. Exemplos como a condução autônoma e o prognóstico de doenças ilustram o seu papel crucial, ainda que numerosas outras aplicações menos críticas também explorem os seus benefícios. As plataformas como o Google GBoard para previsão e sugestão da próxima palavra e a Siri para o reconhecimento automático da fala são exemplos muito difundidos. Considerando em maior detalhe a área da saúde, as vantagens da FL tornam-se evidentes, especialmente ao enfrentar o desafio de diagnosticar doenças raras. Tipicamente, os hospitais têm poucos pacientes para cada doença rara, e os seus registros devem ser mantidos privados. Treinar um modelo com apenas esses registros levaria a que muitos diagnósticos fossem errados, uma vez que a precisão do modelo seria baixa. A FL aborda essa limitação ao permitir a colaboração de vários hospitais, cada um com alguns registros, mas que na globalidade já teriam uma dimensão apreciável, facilitando assim o desenvolvimento de modelos mais robustos.

Em mais detalhe, a FL opera da seguinte maneira: inicialmente, um modelo global é criado por um servidor central que é então distribuído por um subconjunto dos dispositivos, normalmente referidos como clientes ou participantes, onde ocorre o treino local. Durante esta fase, os parâmetros do modelo são atualizados com base no conjunto de dados disponíveis em cada dispositivo. Uma vez concluído o treino local, cada dispositivo transmite de volta para o servidor central as atualizações que ocorreram nos parâmetros (ou gradientes). Essas atualizações são agregadas no servidor para formar uma nova versão do modelo global. O processo é repetido por várias rodadas até que o modelo global atinja o desempenho desejado. Ao adotar esta abordagem descentralizada, a FL facilita o treino colaborativo de modelos enquanto protege a privacidade dos dados. Os registros armazenados localmente permanecem seguros, pois nunca são partilhados externamente aos dispositivos.

Contudo, a natureza distribuída da FL cria um ambiente ideal para entidades maliciosas (adversários) poderem manipular o comportamento do modelo global final [Fang20, Tolpegin20, Zhang22] ou tentar inferir informações sensíveis sobre

os dados de treino e/ou modelo [Yue23]. Como existe potencialmente o envolvimento de muitos dispositivos (dependendo da situação, entre algumas dezenas e as centenas de milhares [Kairouz21]), assegurar que todos exibem consistentemente um comportamento correto é uma tarefa extremamente difícil. Ademais, a detecção de uma conduta maliciosa apresenta desafios significativos, pois é inerentemente complexo distinguir entre as atualizações maliciosas e as válidas, uma vez que existe sempre alguma variabilidade decorrente da diversidade dos registros armazenados localmente. É essencial relembrar que os dados guardados nos dispositivos são não-i.i.d. (independentes e identicamente distribuídos), algo que é desejável e esperado, como mencionado anteriormente. Por estas razões, é vital compreender em maior detalhe, como é que este tipo de aplicações podem ser atacadas e como podem ser protegidas.

Vetores de Ameaça

De um ponto de vista genérico, a aprendizagem distribuída (e, em particular, a FL) está suscetível aos mesmos vetores de ameaça que nos são familiares, como os ataques à cadeia de fornecimento (*supply chain*) e os ataques on-line. No entanto, compreender efetivamente como essas ameaças se manifestam nos obriga à aquisição de conhecimentos especializados.

Por exemplo, as vulnerabilidades da cadeia de fornecimento aparecem na rede formada pelas entidades envolvidas no desenvolvimento, distribuição e manutenção do software. Essas ameaças podem surgir em várias etapas no desenvolvimento do software, incluindo a aquisição de componentes ou bibliotecas de terceiros, a integração de serviços ou dependências externas e a disseminação de atualizações de software. Exemplos comuns de ataque incluem, a introdução de código malicioso nas bibliotecas para que mais tarde este seja executado em conjunto com o resto do software, o comprometimento dos canais de distribuição das aplicações levando à disseminação de produtos adulterados ou falsificados, e a exploração de vulnerabilidades em componentes desenvolvidos por terceiros.

Todas estas ameaças são extensíveis ao software que utiliza ML distribuída. No entanto, surgem também várias ameaças especializadas que podem representar riscos consideráveis para a segurança. Alguns ataques eficazes incluem:

1. **Ataques de Envenenamento de Dados (Data Poisoning Attacks):** os adversários podem manipular os dados de treino para minar o desempenho dos modelos de ML. Uma vez que os conjuntos de dados demoram muito tempo a criar e exigem uma quantidade significativa de esforço, as organizações tendem a utilizar o que está disponível publicamente ou a adquiri-los de terceiros (pelo menos nas primeiras etapas do desenvolvimento do modelo). Além disso, esses conjuntos de dados frequentemente contêm um grande número de amostras,

tornando inviável a validação manual (por exemplo, verificar que as etiquetas corretas foram atribuídas às imagens). Logo, através da injeção de amostras cuidadosamente elaboradas nos dados de treino, os atacantes podem influenciar o comportamento final do modelo e comprometer a sua precisão ou robustez.

2. **Ataques de Envenenamento do Modelo (Model Poisoning Attacks):** na FL, enquanto o modelo é treinado, clientes controlados pelo adversário podem alterar maliciosamente as atualizações que enviam para o servidor central. Estas atualizações maliciosas podem ser criadas, por exemplo, através da manipulação do procedimento de treino local, ou modificando os hiperparâmetros, ou o critério que está a ser otimizado (loss function). Por fim, estas atualizações, quando agregadas, visam introduzir vulnerabilidades ou comportamentos maliciosos no modelo global. Logo, ao incorporar o modelo resultante numa aplicação, potencialmente pode-se causar comportamentos inesperados em condições específicas.
3. **Ataques de Inferência do Modelo (Model Inference Attacks):** se os atacantes tiverem acesso ao modelo final, podem tentar inferir informações confidenciais sobre os registros que foram utilizados durante o treino. O adversário usa as respostas produzidas pelo modelo alvo, como as suas predições sobre exemplos escolhidos, para fazer inferências probabilísticas sobre os dados de treino. Existem diversas variantes deste ataque, como aquelas que visam determinar se uma determinada amostra foi usada no treino, inferir atributos específicos como, por exemplo, informações demográficas, ou reconstruir exemplos particulares. Estes ataques comprometem a privacidade, especialmente em contextos em que são utilizados dados sensíveis, como nas atividades na área da saúde.
4. **Ataques de Reutilização do Modelo (Model Reuse Attacks):** o adversário tenta replicar um modelo alvo embora não tenha acesso aos seus parâmetros ou aos dados que foram usados no treino. Neste tipo de ataque, o adversário geralmente interage com o modelo alvo ao submeter amostras selecionadas de entrada e observar as correspondentes previsões de saída. Ao questionar estrategicamente o modelo alvo e ao analisar as suas respostas, o atacante irá construir um modelo substituto, que irá imitar o comportamento do modelo original de uma maneira muito precisa. Novamente, o objetivo é quebrar a confidencialidade, mas neste caso, do modelo propriamente dito.

Na FL, as ameaças on-line podem ser realizadas durante o treino por qualquer cliente que decida agir maliciosamente. Os ataques acima podem ser executados

com diferentes níveis de sucesso e dificuldade, uma vez que o atacante controla apenas um número limitado dos dispositivos envolvidos. Compreender as capacidades e os efeitos destas ameaças em cenários práticos é um desafio importante por si só, cuja resposta ainda não é clara, pois novas estratégias de ataque e de mitigação continuam a ser desenvolvidas a um ritmo elevado pelos pesquisadores.

Potenciais Defesas

Estas ameaças representam riscos significativos para a integridade, confidencialidade e disponibilidade dos sistemas, obrigando à implementação de mecanismos adequados de segurança, e requerendo um comportamento confiável de todas as entidades envolvidas no processo de desenvolvimento de software. Tratar destas ameaças requer a aplicação de medidas robustas, incluindo práticas seguras de manipulação de dados, revisão minuciosa do código, avaliação de vulnerabilidades, gestão de riscos na cadeia de fornecimento e monitoramento dos sistemas de ML.

No entanto, para tratar dos riscos próprios das aplicações distribuídas de ML, torna-se imperativo elaborar estratégias de defesa bem-adaptadas à ameaça específica e ao ambiente onde o software irá operar. Por exemplo, considerando a ameaça de envenenamento de dados, várias estratégias de mitigação podem ser exploradas:

1. **Filtragem e Pré-processamento de Dados:** baseia-se na utilização de técnicas de pré-processamento de dados para identificar e filtrar registros potencialmente maliciosos, antes de os incorporar no processo de treino. Contudo, é importante considerar que embora os clientes benignos possam aplicar este tipo de abordagem, ela é insuficiente num cenário de FL, pois os clientes maliciosos podem sempre optar por usar dados corrompidos.
2. **Métodos de Agregação Robustos:** o servidor utiliza algoritmos de agregação que são resilientes à influência de dados corrompidos, como a agregação de média aparada (trimmed mean aggregation). Por vezes, este tipo de abordagem pode levar a uma redução da precisão do modelo global, uma vez que os dados são diversos, introduzindo um compromisso de difícil gestão – um conflito entre a segurança e a utilidade do modelo.
3. **Privacidade Diferencial (Differential Privacy)**: a introdução de perturbações (ou ruído) nas atualizações do modelo pode garantir que as contribuições individuais não afetem significativamente o modelo resultante, reduzindo assim a eficácia dos ataques. Novamente, à medida que a quantidade de ruído aumenta, é alcançada uma melhor proteção, mas com o custo de uma redução na precisão.

4. **Deteção de Anomalias**: a utilização de métodos de detecção de anomalias no servidor serve para identificar desvios nas atualizações dos clientes, podendo reconhecer a presença de atividade maliciosa.

Normalmente, as organizações conseguem mitigar os riscos e proteger a integridade e confidencialidade dos seus ativos se utilizarem uma combinação de estratégias de defesa e adotarem as melhores práticas para o treino seguro de modelos. Todavia, esta é uma área ainda com muitas incertezas, existindo uma investigação importante no desenvolvimento de novas técnicas e metodologias para defender o software de ML contra as ameaças emergentes.

Curriculum de Segurança de Software

As competências incluídas no currículo de Segurança de Software [SBC23] mantêm-se pertinentes quando aplicadas à construção de aplicações distribuídas de ML. No entanto, estas devem ser evoluídas e adaptadas a este domínio emergente, caso contrário, a sua eficácia na proteção da informação e dos sistemas pode diminuir. Por exemplo, será que é possível delinear corretamente os requisitos de segurança de uma aplicação de ML sem o conhecimento dos ataques de envenenamento de dados? Será que os estudantes conseguem escolher mecanismos apropriados para garantir a confidencialidade se não compreenderem os ataques de reutilização de modelo? Podem os estudantes testar eficazmente um software de ML sem reconhecerem o potencial dum ataque de envenenamento do modelo? Parece-nos que a resposta "não" é a mais apropriada a todas estas questões. Por conseguinte, é imperativo integrar no currículo o conhecimento específico às ameaças na ML e as respectivas estratégias de mitigação, assegurando que os alunos estão equipados para enfrentar os desafios singulares colocados por este tipo de software.

Ademais, em cursos de engenharia e outros cursos com uma elevada formação prática, é fundamental proporcionar aos estudantes oportunidades para experimentar e avaliar os efeitos dos ataques em contextos diversos. O sucesso de um ataque muitas vezes depende das capacidades do adversário, e a restrição das mesmas leva a diferentes graus de eficácia. A implementação de medidas de segurança pode (ou não) mitigar significativamente o impacto dessas ameaças, limitando assim o seu potencial. Ao envolver os alunos em exercícios práticos que simulam cenários do mundo real e que encorajem a implementação de contramedidas, eles são levados a uma melhor compreensão dos princípios de segurança e preparados para enfrentar os respectivos desafios de forma eficaz.

Felizmente, no âmbito das aplicações de FL, surgiram algumas ferramentas para facilitar a experimentação e teste de mecanismos de segurança. Exemplos incluem o FedML [Han23] e o FADO [Rodrigues23]. O principal objetivo destas ferramentas é fornecer uma plataforma que simplifique a implementação, treino e avaliação de modelos usando FL.

Simultaneamente, elas fornecem implementações pré-construídas das classes de ataque essenciais e defesas inovadoras, permitindo que os estudantes simulem várias ameaças e avaliem os riscos mais relevantes, ganhando entendimento sobre os benefícios e limitações dos métodos de proteção existentes. Essas ferramentas também facilitam a implementação de novas estratégias de ataque e defesa, possibilitando comparações justas em condições padronizadas. No final, estas poderão contribuir para uma melhor compreensão das vulnerabilidades e medidas de segurança em FL, ajudando a orientar esforços futuros para melhorar a segurança.

Referências

1. [Bukaty19] Bukaty, P.. The California Consumer Privacy Act (CCPA): An implementation guide. IT Governance Publishing, 2019
2. [Fang20] Fang, M., Cao, X., Jia, J., Gong, N.. Local model poisoning attacks to Byzantine-robust federated learning. USENIX Conference on Security Symposium, 2020
3. [GDPR16] European Parliament and Council of the European Union, General Data Protection Regulation, 2016
4. [Han23] Han, S., et al. FedMLSecurity: A Benchmark for Attacks and Defenses in Federated Learning and Federated LLMs, arXiv:2306.04959, 2023
5. [Kairouz21] Kairouz, P., et al., Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1-2):1–210, 2021
6. [McMahan17] McMahan, H., Moore, E., Ramage, D., Hampson, S., Arcas, B.. Communication-efficient learning of deep networks from decentralized data. International Conference on Artificial Intelligence and Statistics, 2017
7. [Rodrigues23] Rodrigues, F., Simões, R., Neves, N., FADO: A Federated Learning Attack and Defense Orchestrator, Workshop on Dependable and Secure Machine Learning (DSML), June 2023.
8. [SBC23] Sociedade Brasileira de Computação, Referenciais de Formação para o Curso de Bacharelado em CiberSegurança, 2023
9. [Tolpegin20] Tolpegin, V., Truex, S., Gursoy, M., Liu, L.. Data poisoning attacks against federated learning systems. European Symposium on Research In Computer Security, 2020
10. [Yue23] Yue, K., et al., Gradient Obfuscation Gives a False Sense of Security in Federated Learning, USENIX Security Symposium, 2023
11. [Zhang22] Zhang, Z., et al., Neurotoxin: Durable backdoors in federated learning. International Conference on Machine Learning, 2022

NUNO NEVES é Professor Catedrático no Departamento de Informática da Faculdade de Ciências da Universidade de Lisboa (Portugal). Ele lidera a linha de investigação de Sistemas Descentralizados Seguros e Confiáveis na unidade de investigação LASIGE. Suas principais áreas de interesse são o desenho de soluções que promovam a melhoria da segurança de software e dos sistemas distribuídos. Foi coordenador do Mestrado em Segurança Informática, e ao longo dos últimos dez anos tem sido responsável pela disciplina de Segurança de Software. Tem participado em diversas atividades na comunidade dos sistemas confiáveis, tendo presidido recentemente ao IEEE Computer Society Technical Committee on Dependable Computing and Fault Tolerance (2021-2023).

POSCOMP 2024

EXAME NACIONAL PARA INGRESSO NA PÓS-GRADUAÇÃO EM COMPUTAÇÃO

Concursos fundatec 50 ISO 9001

SBC

Prova Online!

Inscreva-se no POSCOMP 2024!

www.sbc.org.br/poscomp

Inscrições: 12/04 a 23/04/2024

Prova: 04/05/2024

Acesse o Edital do POSCOMP 2024 em www.sbc.org.br/poscomp

ARTIGO

OS DESAFIOS DA COMPONENTIZAÇÃO PARA A SEGURANÇA E A FORMAÇÃO DE EQUIPES

POR
Roberto Gallo
gallo@kryptus.com

A segurança de um sistema sempre depende da segurança de seus componentes. Esta afirmação, apesar de aparentemente simples e respaldada pelo senso comum, esconde um universo de fatores que desafiam mesmo as mais competentes equipes no projeto, desenvolvimento, deployment e manutenção de sistemas computacionais compostos em os manter seguros durante todo o seu ciclo de vida.

Um exame da literatura, dos repositórios de vulnerabilidades conhecidas (vide os CVE mantidos pelo MITRE) e mesmo da mídia sobre o tópico nos permite identificar casos significativos nos quais algum aspecto da componentização de sistemas deu causa a problemas de segurança que possivelmente poderiam ser evitados com uma maior difusão dos conhecimentos em segurança para as equipes de projetos de sistemas computacionais. Alguns exemplos marcantes incluem:

1. os ataques de cadeia logística sobre o Orion da SolarWinds[1] e sobre o XZ outbreak (CVE-2024-3094) onde estes componentes utilizados por outras soluções foram subvertidos, comprometendo os sistemas que os utilizam;
2. os ataques de canais colaterais Downfall sobre CPU Intel (CVE-2023-12301), Inception sobre CPU AMD (CVE-2023-12302) e mais recentemente o ataque GoFetch sober CPU Apple Mx (2024) que permitiram o vazamento de informações (chaves criptográficas) entre processos (componentes) de um sistema;
3. os casos de arquitetura inadequada em conjunto com má configuração de buckets S3 da Amazon que deram origem a célebres vazamentos de dados como o de 1TB da Attunity em 2019 e de 100 milhões de clientes da Capital One em 2019.

Durante este artigo, exploraremos as comunalidades de diversos casos de falhas de segurança, aparentemente bastante distintas, mas que possuem como causa raiz, e, portanto, respostas, na organização e na ação coordenada dos diversos times responsáveis pelo desenvolvimento, aquisição, integração e testes de sistemas e de seus componentes associados.

1 https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

Alguns problemas da componentização

A modularização de sistema na forma de componentes possui inúmeros benefícios amplamente conhecidos e difundidos tanto na academia como na indústria, em particular a facilitação da manutenção e dos testes, a reusabilidade, redução de custos e de riscos e a escalabilidade do sistema e do processo de desenvolvimento [1].

Estes benefícios, no entanto, não escapam dos fundamentos teóricos intrínsecos da computação, nem de fenômenos concretos comuns que são fontes de ameaças, e os quais, surpreendentemente, não estão incorporados no *mindset* de muitos profissionais egressos do ensino superior em Computação. A seguir, de forma sumária por conta do limite de espaço desta publicação, elenco alguns dos principais:

1. O **Teorema de Rice**, fundamental da computação, diz que qualquer propriedade não-trivial dos programas é indecidível. Isso significa que não há um algoritmo geral que possa decidir para qualquer programa e qualquer entrada possível para ele, se ele possui uma determinada propriedade comportamental que, por exemplo, não permita a execução de alguma operação insegura.

   Na prática, isso significa que testes de segurança de programas têm assertividade limitada, baseados em casos e necessariamente apoiado por métodos heurísticos.

   Além disso, apesar de clássico e

amplamente conhecido, ainda sim muitos desenvolvedores mantêm certa ilusão de que algumas tecnologias são "balas de prata", a exemplo de plataformas de virtualização.

2. **Compor políticas de segurança é muito difícil**: a composição de políticas de segurança individuais de componentes em uma política resultante para um sistema é um problema NP ou até exponencial, mesmo utilizando-se modelos formais com restrições, a exemplo das Redes de Petri estendidas [2].

   O resultado é que mesmo que exista uma descrição fiável, formal do que se esperar sobre a segurança de um componente (uma raridade), não é trivial compor tal descrição em uma política de segurança para o sistema resultante.

   Talvez pela dificuldade, talvez pelo aspecto tipicamente qualitativo dos requisitos de segurança, observa-se que na média poucos profissionais entrando no mercado possuem formação no assunto.

   Também é sintomático que a maior parte das licenças de software expressem que "este software não vem com garantia nenhuma, nem a garantia de servir para um fim específico";

3. **Modelagens otimistas ou rasas**: frequentemente, os pesquisadores e os praticantes em computação não consideram em seus modelos (teóricos e/ou mentais) que algoritmos e a suas realizações na forma de programas não são objetos concretos, mas apenas instruções para um ou mais elementos processantes (CPUs, MCUs, GPUs, NPUs, FPGAs), organizados em um ou mais equipamentos, executarem.

   Essa redução de modelagem rotineiramente implica em assunções otimistas e irreais sobre a isolação entre os componentes de software e sobre dados sensíveis. Por exemplo, a arguição de que um sistema implementa "proteções em camada" quando os seus componentes executam todos em uma mesma máquina, sob um mesmo usuário, é geralmente falsa pois possui diversos modos comuns de falha (i.e., item que, se atacado, viola a segurança de mais de um componente, como o processador, o disco, e o kernel).

   Outro erro que frequentemente se mostra fatal é considerar máquinas virtuais (ou *containers*) como realmente isoladas, mesmo com inúmeros casos de "escape" das principais tecnologias nos últimos anos.

4. **Excessos nas abstrações e dependências de software**: a excessiva abstração dos recursos computacionais em APIs e frameworks e o vertiginoso aumento do número de dependências de software simultaneamente facilitam a inserção proposital de vulnerabilidades e também dificultam, ou mesmo impedem, que as equipes res-

ponsáveis pela implementação, manutenção e segurança de corretamente mantenham uma modelagem atualizada de ameaças e de arquitetura de sistema.

Pouco se tem noção do problema, mas dados do Apache Maven [3] indicam que a aplicação média em Java em 2022 dependia de aproximadamente 40 (!) bibliotecas de terceiros. Neste contexto, uma chance de apenas 1,7% de contaminação por ataque *supply chain* individual de componente leva a uma chance composta de comprometimento da aplicação de 50%.

Por outro lado, sabe-se bem da disciplina de Engenharia de Software que a corrosão de arquitetura [4] é um elemento que dificulta a identificação e correção de problemas de segurança, tornando o ciclo de mitigações lento.

5. **Muitos desenvolvedores sobrestimam a dificuldade de um ataque**: nestes últimos 25 anos pude observar um padrão – a maioria dos desenvolvedores, mesmo aqueles formados em nossas melhores escolas, nunca viu um ataque real, prático, sendo executado sobre um sistema conhecido ou desenvolvido por eles. Como resultado, muitos deles subestimam, quando não simplesmente ignoram, ameaças típicas.

   Por outro lado, ao trabalhar em diversos casos de clientes em minha trajetória profissional junto de uma equipe competente de pesquisadores em segurança, pude observar que em torno de 9 de cada 10 casos pudemos "vencer" e tomar o controle de sistemas, às vezes atacando um único módulo, mas muitas vezes abusando da arquitetura – este tipo de experiência muitas vezes não é oferecida nos currículos básicos de formação de profissionais de Computação.

   Esta dicotomia, da falta de repertório, tem o frequente efeito que pode ser descrito como "gente nova comete erros clássicos".

Melhores práticas para a segurança de sistemas compostos

As melhores práticas de segurança para sistemas compostos e seus componentes varia a depender de seus objetivos de segurança e de asseguramento, já que diversas metodologias e escolhas de engenharia possuem impacto em custos, trabalho adicional, escolhas tecnológicas e prazos de execução. Ainda não se pretende ser exaustivo nas práticas, mas apenas listar algumas que aparentemente recebem muito pouca atenção nos currículos de graduação.

Antes de avançar, faz-se necessário o estabelecimento de alguns termos usados nesta seção. Um **objetivo de segurança**, também chamado de **reivindicação** de segurança, do inglês "claim" é uma descrição daquilo que uma peça de software, subsistema ou o próprio sistema diz que entrega. Por exemplo: "Claim 1: a mensagem tem confidencialidade garantida

com nível de segurança de 2256 contra adversários não-quânticos". Já o **asseguramento** ("assurance") se refere ao nível de certeza que um dado "claim" é verdadeiro. Por exemplo, o Claim 1 é verdadeiro com "alto nível de probabilidade" ou "com prova formal".

A experiência prática mostra que conceber, implementar e manter componentes e sistemas com nível alto de segurança tende a ser relativamente menos trabalhoso do que obter alto nível de asseguramento, principalmente pelos efeitos do Teorema de Rice e da Composição de Políticas de Segurança. Em geral, o alto nível de esforço necessário para se obter alto nível de asseguramento é incompatível com muitos cenários de uso, chegando a ser 3.83 maior [5] do que para asseguramentos mais relaxados, a exemplo dos níveis EAL 1 versus EAL 7 no padrão ISO/IEC 15408 – "Common Criteria".

Em suma, é fundamental harmonizar a criticidade do caso de uso com os objetivos de segurança e os níveis de asseguramento sob a perspectiva das capacitações das equipes envolvidas, bem como dos recursos disponíveis. Em termos de práticas, observamos como mais efetivas:

1. **Baseline de vocabulário e metodologias:** todos os integrantes das equipes devem ser treinados para utilizar uma nomenclatura comum para se expressar em termos de objetivos de segurança, ameaças, vulnerabilidades, verificações de segurança, resposta a incidentes, etc., utilizando para isso algum framework documentado de gestão de ciclo de vida seguro de sistemas, a exemplo do Microsoft SDL ou do modelo SAMM;
2. **O arquiteto de solução deve ser o dono da segurança em projetos pequenos e médios:** em projetos de pequena até média escala, é importante que o arquiteto da solução, ou papel similar, entenda *todos os módulos e os componentes* de sistema, tanto em termos de código fonte, como em termos de arquitetura e também seja versado nos principais tipos de ataques. Esta é uma posição bastante exigente, mas que reduz em muito a necessidade de formalização do processo de desenvolvimento e manutenção de software. Em geral, a formação deste talento envolve trilhas de formação em ciclo de vida seguro (p.e. MS-SDL, SAMM), tecnologias específicas usadas na aplicação, e segurança ofensiva (p.e. CEH, CompTIA PenTest+, ECSA/LPT);
3. **Projetos críticos de qualquer tamanho requerem formalismo**: é fundamental o emprego de uma metodologia de asseguramento, a exemplo da NATO AEP-67 ENGINEERING FOR SYSTEM ASSURANCE NATO IN PROGRAMMES, que apresenta uma forma de documentar e demonstrar as reivindicações de segurança e os respectivos níveis de asseguramento durante o ciclo de vida da solução, levando-se em conta todos os seus componentes. Pelo seu poder de coordenação e nível de esforço ajustável, a NATO

AEP-67 tem sido empregada com sucesso em diversos projetos com sucesso, bem como serviu de base para treinamento de equipes [6], assunto que é tratado mais adiante;

4. **Separar na origem qual o software descartável daquele de produção**: é preciso evitar utilizar na produção a mentalidade de software descartável, típico das etapas de prototipação, onde o uso de versões "*nightly build*" de componentes é comumente feito pelas equipes de desenvolvedores entusiastas e que buscam sempre as "últimas features". O congelamento dos componentes em versões "Long Term Support - LTS" tem papel fundamental no provimento de sistemas seguros não só porque garantem a manutenibilidade de longo prazo do sistema composto, mas fundamentalmente porque "congelam" a superfície de ataques e reduzem a inserção de defeitos de segurança ao longo do tempo, permitindo que a equipe possua um melhor modelo formal e/ou mental daquilo que quer proteger.

Casos de asseguramento como ferramenta de formação de equipes

Casos de asseguramento na forma da NATO AEP-67 organizam reivindicações de segurança de forma hierárquica, conforme exemplo da figura 1. Cada "claim" pode ser suportado por uma ou mais reivindicações intermediárias ("sub-claims"), recursivamente.

No exemplo oferecido, o "claim A" requer simultaneamente que os sub-claim 1 e 2 (e possivelmente outros) sejam verdadeiros para que ele seja verdadeiro. Em um certo momento um sub-claim deve ser evidenciado ou assumido como verdadeiro, com um certo nível de certeza. No caso do sub-claim 1, ele é mostrado verdadeiro através de argumentação e de critério de avaliação pré-definido.

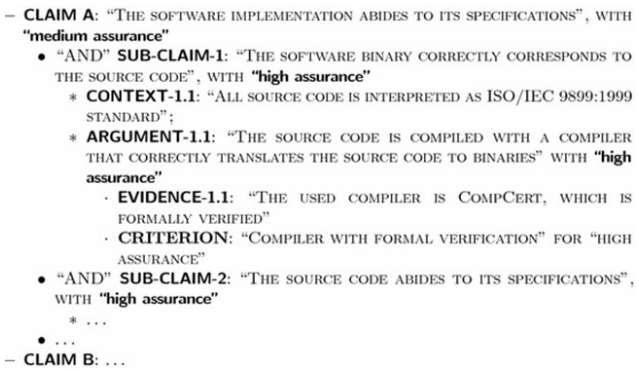


FIG. 01 | **EXCERTO DE UM CASO DE ASSEGURAMENTO, FONTE [6].**

Como o leitor atento pode imaginar, os casos de asseguramento podem se tornar bastante detalhados já que garantir que determinada asserção é verdadeira pode requer diversas condições intermediárias, afetando muitos componentes de sistemas. E mais, os casos de asseguramento são flexíveis o suficiente para incorporar as diferentes fases do ciclo de vida de um componente ou sistema.

Pois bem, justamente esta capacidade (ou necessidade) de expressão e detalhamento na composição dos casos de asseguramento é que tem se mostrado instrumental no treinamento e no aperfeiçoamento de equipes que lidam com o projeto, desenvolvimento e manuten-

ção de sistemas, conforme reportamos no em [6]. Naquele projeto, estudantes de pós-graduação e graduação da Unicamp foram organizados em times que tinham por objetivo implementar um serviço de mensageria seguro e assegurado por grupo, documentar as suas garantias de segurança e, posteriormente, atacar o sistema da outra equipe. Os times foram assim conduzidos por todo o ciclo de vida de suas soluções, provendo insights poderosos sob a visão holística necessária na área de segurança da informação.

No experimento educacional, os casos de asseguramento se mostram fundamentais pelo menos em três aspectos educacionais: (i) obrigaram cada um dos estudantes a desafiar as suas assunções sobre a segurança dos componentes do sistema, (ii) demonstraram para a equipe a necessidade de se definir e documentar políticas/reivindicações de seguranças simples e precisas para os componentes dos sistemas, e (iii) serviram como eixo de comunicação objetivo entre os membros das equipes, otimizando esforços e limitando lacunas.

Longe de ser apenas um ganho teórico e um exercício acadêmico, depois do experimento reportado em [6], pude ver em primeira mão como os casos de asseguramento foram fundamentais para aperfeiçoamento contínuo, "*on-the-job training*" de profissionais. Mais do que isso, tais casos têm servido aos *stakeholders* dos sistemas desenvolvidos já que passam a ter uma descrição precisa daquilo que podem esperar sobre os seus sistemas.

Conclusão

A concepção, implementação, obtenção e manutenção de sistemas compostos seguros é um desafio feroz e requer acima de tudo consciência situacional das equipes envolvidas. Isto é, em que pese os benefícios de negócio da modularização de software, esta mesma organização em componentização abstrai diversos dos caminhos práticos que os adversários utilizam para realizar ataques de sucesso.

Para minimizar o número de vulnerabilidades é necessário que as equipes de desenvolvimento, operação e segurança possuam a mesma modelagem de ameaças, vocabulário e práticas de desenvolvimento, bem como visão holística sobre os sistemas e seus componentes. Para este fim, metodologias e frameworks como o Microsoft SDL, SAMM e NATO AEP-67 têm se demonstrado efetivas.

Além disso, as equipes dedicadas à concepção e desenvolvimento devem ter contato reiterado com as equipes de segurança de forma a se manterem educadas nas técnicas de ataques e, sobretudo, no frequente baixo esforço necessário para um ataque de sucesso.

Na visão deste autor, nada impede que todos estes conhecimentos e práticas sejam incorporados nos currículos de graduação e pós-graduação em Computação.

Referências

1. Len Bass, Paul Clements e Rick Kazman, "Software Architecture in Practice", 4ª Edição, agosto de 2021.
2. Yen, Hsu-Chun. "On the Regularity of Petri Net Languages." Proceeding of 13th IEEE Annual International Phoenix Conference on Computers and Communications (1994): 329.
3. A. M. Mir, M. Keshani and S. Proksch, "On the Effect of Transitivity and Granularity on Vulnerability Propagation in the Maven Ecosystem," 2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Taipa, Macao, 2023, pp. 201-211, doi: 10.1109/SANER56733.2023.00028.
4. M. Ullah Khan, M. Munib, U. Manzoor and S. Nefti, "Analyzing risks at architectural level," International Conference on Information Society (i-Society 2011), London, UK, 2011, pp. 231-236, doi: 10.1109/i-Society18435.2011.5978442.
5. Kou, K., Jeong, J., & Lee, G. (2008). Definition of Evaluation Assurance Levels and Estimation of Evaluation Efforts for Operational System Based ISO/IEC 19791. 2008 International Conference on Security Technology, 176-183. https://doi.org/10.1109/SECTECH.2008.41
6. Gallo, R., Dahab, R. (2015). Assurance Cases as a Didactic Tool for Information Security. In: Bishop, M., Miloslavskaya, N., Theocharidou, M. (eds) Information Security Education Across the Curriculum. WISE 2015. IFIP Advances in Information and Communication Technology, vol 453. Springer, Cham. https://doi.org/10.1007/978-3-319-18500-2_2

ROBERTO GALLO é veterano em defesa e segurança cibernética para aplicações de Estado, telecomunicações, militares, (contra-)inteligência e corporativas. Atuação nos âmbitos acadêmico, profissional e institucional. Possui Doutorado e Mestrado em Ciência da Computação com foco em segurança cibernética pela UNICAMP. Possui graduação em engenharia de computação pela mesma universidade.

ARTIGO

CIBERSEGURANÇA, COMPLIANCE DIGITAL E CUSTO REPUTACIONAL

POR

Flúvio Cardinelle Oliveira Garcia
fluvio.fcog@pf.gov.br | fluvio.garcia@pucpr.br

Num mundo global e hiperconectado onde se estima que os custos decorrentes de atividades espúrias on-line serão de US$ 10,5 trilhões anualmente[1] em 2025 e que o Brasil figura como líder do *ranking* de ataques DDoS[2] na América Latina pelo 10º ano consecutivo, segundo no top 5 mundiais,[3] além de ser considerado o

1 MORGAN, Steve. Cybercrime to cost the world $10,5 trillion annually by 2025. Cybercrime Magazine, nov. 13, 2020. Disponível em: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Acesso em: 15 abr. 2024.

2 Um ataque DDoS (Distributed Denial of Service) é uma tentativa maliciosa de tornar um serviço on-line indisponível, sobrecarregando-o com um grande volume de tráfego de internet. Nesse tipo de ataque, os computadores de diversos dispositivos comprometidos, conhecidos como bots ou "zumbis", são coordenados por um atacante para enviar tráfego para o alvo simultaneamente. Isso sobrecarrega os recursos do sistema, como largura de banda, capacidade de processamento ou memória, impedindo que os usuários legítimos acessem o serviço. Os ataques DDoS podem causar interrupções graves em serviços on-line, como sites, servidores de jogos, serviços em nuvem e aplicativos web. Eles são frequentemente usados por motivos diversos, incluindo extorsão, protestos políticos, sabotagem ou simplesmente para causar interrupções e danos.

3 MARIN, Jorge. Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda. TECMUNDO, out. 2023. Disponível em: https://www.tecmundo.com.br/seguranca/272995-brasil-lider-ranking-ataques-ddos-america-latina-10-vez-entenda.htm. Acesso em: 15 abr. 2024.

segundo maior alvo de ciberataques do planeta,[4] a iniciativa dos Referenciais de Formação em Cibersegurança não é apenas inovadora e bem-vinda, mas necessária.

Dentre os eixos de formação considerados como referenciais para o curso de Cibersegurança, destaca-se o de Segurança Organizacional, o qual, conforme diretrizes da Sociedade Brasileira de Computação, "envolve a proteção da organização contra ameaças e gestão de risco para apoiar os objetivos da organização" e estabelece como competência a ser atingida "elaborar estratégias de governança de acordo com **regulamentações**, boas práticas e propósito do negócio"[5] (grifei).

Ao esquadrinhar as competências derivadas do eixo em questão, depara-se com conteúdos específicos que objetivam o conhecimento e a implementação de identificação de riscos de segurança, avaliação, análise e controle de riscos, governança e políticas de segurança, governança de privacidade, planejamento estratégico de cibersegurança, plano de resposta a incidentes, **leis, ética e conformidade de segurança,** dentre outros tantos.

Os grifos previamente feitos chamam a atenção para elementos que precisam nortear, rigorosamente, o planejamento, a implementação e a execução de toda e qualquer atividade a ser devolvida por um profissional de cibersegurança: o respeito às normas jurídicas (princípios e regras) vigentes no país.

É nesse contexto que o *compliance* digital tem lugar. Numa tradução literal, a palavra *compliance* advém do verbo to *comply*, do inglês cumprir, e significa estar em conformidade.[6] Trata-se de um conceito relacional, cujo escopo somente é conhecido em face do objeto com o qual se relaciona, afinal de contas, quem está em conformidade o está em relação a algo.[7] Sendo assim, o estado de conformidade a que se refere o *compliance* digital diz respeito ao cumprimento de leis, princípios, procedimentos, regras, regulamentos internos e externos, contratos e quaisquer outras espécies normativas, formais ou não, nacionais e internacionais, que permeiam e disciplinam as condutas que se desenvolvem no mundo digital.[8]

Faleiros Júnior,[9] acertadamente, afirma que o estudo do *compliance* está vinculado, obrigatoriamente, com os assuntos

4 R7 TECNOLOGIA E CIÊNCIA. Brasil é o 2º maior alvo mundial de ciberataques, revela estudo. out. 2021, atualizado em abr. 2024. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022/. Acesso em: 15 abr. 2024.

5 SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125. Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/book/125. Acesso em: 15 abr. 2024.

6 SAAVEDRA, Giovani Agostini; CRESPO, Liana I. A. Cunha. Compliance: origem e aspectos práticos. In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp. 30-31.

7 No Brasil, o compliance tornou-se mais conhecido após a Lei nº 12.846, de 1º de agosto de 2013, também chamada de Lei Anticorrupção. Precipuamente, a ideia foi evitar condutas corruptivas e fraudulentas nas empresas. Depois, os programas de compliance foram estendidos para outras frentes.

8 Ibidem, pp. 30-31 e 37.

9 FALEIROS JÚNIOR, José Luiz de Moura. Notas introdutórias ao compliance digital. In: CAMARGO et al (coords.). Direito digital: novas teses jurídicas. vol. 2. 2ª ed. Rio de Janeiro: Lumen Juris, 2019, pp. 116-118.

de governança corporativa, gestão de risco, ética e moral, representado pela sigla GRC:

> O "G" representa Governança e relaciona-se a controle, supervisão e gestão de uma companhia, envolvendo análise, organizações, metas, processos e objetivos. O "R" trata dos riscos existentes, inerentes ao negócio e outros que possam ocorrer por fatores internos ou externos, envolvendo um trabalho preventivo de mapeamento para que condutas indesejadas não sejam praticadas. O "C" cuida do Compliance, que se liga [a] questões de diversas matérias e não só financeiras, jurídicas ou contáveis.

A importância do aspecto preventivo do *compliance* digital é potencializada num ambiente globalizado e competitivo onde segurança, transparência, qualidade e integridade são exigidos a todo tempo e compõem o denominado custo reputacional da empresa.[10]

O paralelismo existente entre os pilares de um programa efetivo de *compliance* e aqueles utilizados em sistemas de gerenciamento de risco na segurança da informação é evidente. Ambos pressupõem, em síntese: apoio da liderança, código de ética, políticas e procedimentos bem definidos, educação, comunicação e treinamento constantes, monitoramento e auditoria, análise e aplicação de medidas de correção, mapeamento de risco e, se cabível, *due diligence* de terceiros.[11]

O processo de concretização de programa de *compliance* digital é contínuo, precisa se adaptar e responder aos riscos decorrentes de fatores internos e externos da empresa. Não se trata apenas de respeito às leis, regras, regulamentos, normas e procedimentos. Mais do que isso, busca implantar uma verdadeira cultura de prevenção de ações antiéticas, amorais e ilegais a fim de resguardar e, preferencialmente, incrementar de modo positivo o custo reputacional da organização.

O alcance e a relevância do *compliance* digital têm se ampliado significativamente, sobretudo a partir de 2014, com a promulgação da Lei nº 12.965, de 23 de abril de 2014, mais conhecida como Marco Civil da Internet (MCI).[12] Considerada como uma espécie de Constituição da Internet,[13] o referido texto normativo

10 Custo reputacional é o prejuízo financeiro ou impacto negativo que uma empresa sofre devido a danos em sua reputação. Esses danos podem ser causados por uma série de fatores, como escândalos, má conduta corporativa, produtos defeituosos, práticas comerciais antiéticas, entre outros. O custo reputacional pode se manifestar de várias formas, incluindo perda de clientes, queda nas vendas, desvalorização da marca, litígios, multas e até mesmo penalidades regulatórias. Manter uma boa reputação é crucial para a sustentabilidade e sucesso a longo prazo de uma empresa.

11 SAAVEDRA, Giovani Agostini; CRESPO, Liana I. A. Cunha. Compliance: origem e aspectos práticos. In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp. 37-41.

12 Por óbvio, antes de 2014 já existiam leis e regulamentações às quais os profissionais das mais diversas áreas de Tecnologias da Informação e Comunicação (TICs) estavam (e estão) sujeitos, como a Constituição Federal de 1988, o Código Penal de 1940 e as leis especiais sobre direitos autorais (Lei nº 9.610/1998) e de propriedade industrial (Lei nº 9.279/1996), o Código Civil de 2002, o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei do E-Commerce (Decreto nº 7.962/2013), as normas ISO/IEC, dentre outras tantas. Contudo, foi a partir da regulamentação da internet no Brasil, por meio da Lei nº 12.965/2014 e do Decreto nº 8.771/2016, e da proteção legal e específica de dados pessoais, pela Lei nº 13.709/2018, que o compliance digital ganhou maior vulto no país.

13 GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini. Metodologia jurídica político-constitucional e o marco civil da internet: contribuição ao direito digital. In: MASSO, Fabiano Del; ABRUSIO, Juliano; FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet: Lei 12.965/2014. São Paulo: RT, 2014, p. 23. Não obstante reconhecerem que o MCI é chamado de Constituição da Internet, os autores salientam que, como legislação federal, deve ser utilizado e interpretado em conformidade com a Constituição Federal de 1988 (p. 26).

veio a estabelecer princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil, determinando as diretrizes de atuação da União, dos Estados, do Distrito Federal e dos Municípios quanto à matéria (art. 1º, MCI).

O MCI entra em vigor quase 20 anos após a internet estar em uso no país. Sua mensagem principal: deixar claro que a rede mundial de computadores não pode ser considerada uma "terra sem lei". A premissa maior, que fica clara quando da leitura da lei, é que a utilização da internet deve ser feita de forma ética, respeitando-se a *novatio legis* que dispõe, expressamente, acerca de direitos e garantias dos usuários da rede, obrigações impostas aos provedores de conexão e de aplicações e sanções administrativas que poderão ser infligidas a todos aqueles que ofenderem as regulamentações ora positivadas.

Fundamentado no respeito à liberdade de expressão, no reconhecimento da escala mundial da rede, nos direitos humanos, na pluralidade e diversidade, na abertura e na colaboração, nas livres iniciativa e concorrência, na defesa do consumidor e na finalidade social da rede (art. 2º, MCI), o Marco Civil da Internet parece estar sedimentado em três pilares: a neutralidade da rede, a privacidade dos usuários e a liberdade de expressão.[14]

Dentre os direitos e garantias assegurados aos usuários encontram-se a inviolabilidade da intimidade e da vida privada, bem como do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas; a não suspensão da conexão à rede, salvo por falta de pagamento do serviço; a manutenção da qualidade contratada da conexão; a publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; a acessibilidade; a observância às normas de proteção e defesa do consumidor; o direito à privacidade, à liberdade de expressão e à proteção de seus dados pessoais (art. 7º, MCI).

Mais do que resguardar as prerrogativas legais dos usuários de internet, há outras obrigações que precisam ser cumpridas pelos provedores de conexão e de aplicativos, como, por exemplo: tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação (neutralidade, art. 9º, MCI); fornecer às autoridades administrativas competentes o acesso aos dados cadastrais dos usuários (nome, prenome, estado civil, profissão, filiação, e endereço), independentemente de ordem judicial (art. 10, §3º, MCI c/c art. 11, Decreto nº 8.771/2016[15]); e guardar, pelo tempo determinado na lei, os registros de conexão e de acesso a aplicações, preservando seu sigilo e somente fornecendo-os às autoridades competentes mediante ordem judicial (arts. 10, 13 e 15, MCI).

14 Ibidem, p. 24.

15 O Decreto nº 8.771, de 11 de maio de 2016, tem por objetivo regulamentar a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Consoante preconiza o artigo 17 do Decreto nº 8.771/2016, cabe à Agência Nacional de Telecomunicações (Anatel) a regulação, a fiscalização, a apuração de ofensas aos ditames do MCI e a aplicação das sanções administrativas. O descumprimento às normas sujeita o infrator, sem prejuízo das demais sanções cíveis (indenizações e reparações de danos, morais e/ou patrimoniais) e penais (penas privativas de liberdade, restritivas de direito e/ou multas), às sanções administrativas previstas no artigo 12 do MCI, quais sejam: advertência, multa simples de até 10% do faturamento do grupo econômico no Brasil no seu último exercício; multa diária limitada ao mesmo patamar da multa simples; e suspensão temporária ou proibição de exercício de atividades. É importante ressaltar que a conformidade com o Marco Civil da Internet é obrigatória mesmo para entidades jurídicas sediadas no exterior, desde que o serviço seja disponibilizado ao público brasileiro ou que pelo menos uma empresa do mesmo conglomerado possua uma sede no Brasil (art. 11, §3º, MCI).

A rigorosa observância aos ditames do Marco Civil da Internet é fundamental para assegurar a proteção dos direitos dos usuários on-line, promover a transparência e a equidade na rede. Obedecer a essa lei é crucial não apenas para garantir a segurança e a privacidade dos usuários, mas também para promover um ambiente digital mais ético e confiável, com chances mais efetivas de se combater ataques cibernéticos e, assim, aperfeiçoar a cibersegurança na rede mundial de computadores.

Não se trata apenas de conformidade legal, mas de medida essencial para proteger a reputação e a confiança do público na empresa, posto que, como se sabe, incidentes de segurança cibernética, como vazamento de dados ou violações de privacidade, podem acarretar sérios reflexos negativos para a imagem da organização. Sendo assim, o profissional de cibersegurança precisa estar atento para evitar ofensas ao MCI e adotar medidas preventivas concretas para garantir uma presença on-line sólida e confiável da empresa nos mais diversos ambientes digitais em que atua, preservando sua reputação, credibilidade e integridade no mercado.

Na mesma esteira normativa, a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), é reconhecida como um marco jurídico importantíssimo na consolidação do direito à proteção de dados pessoais no Brasil, hoje estampado em cláusula pétrea na Constituição Federal de 1988 (CF/88) como direito fundamental,[16] incluída pela Emenda Constitucional nº 115, de 2022.

Inspirada na *General Data Protection Regulation* (GDPR), publicada em 25 de maio de 2018, com força de lei, no âmbito da União Europeia, a LGPD brasileira sistematiza e estabelece, em seus 65 artigos, direitos para os titulares de dados, obrigações para os agentes de tratamento (controladores e operadores) e procedimentos documentais relativos à privacidade e à proteção de dados, digitais ou não,

16 CF/88, art. 5º, LXXIX: "é assegurado, nos termos da lei [LGPD], o direito à proteção dos dados pessoais, inclusive nos meios digitais".

como, por exemplo, a confecção de ROPA (*Records Of Processing Activities*), DPIA (*Data Protection Impact Assessment*), PIA (*Privacy Impact Assessment*) e LIA (*Legitimate Interest Assessment*), conforme se depreende da leitura dos artigos 5º, XVII, 10, §3º, 18, 30, 32, 37 e 38, da lei.

Os fundamentos que disciplinam a proteção de dados pessoais adotados pela LGPD assemelham-se àqueles já consagrados pelo MCI,[17] com especial distinção à autodeterminação informativa, vale dizer, ao poder e à capacidade de o indivíduo decidir se seus dados - digitais e/ou físicos - poderão ser tratados[18], de que forma e com qual finalidade. Como regra, basta que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional, para que haja a plena incidência dos rigores da LGPD (art. 3º, LGPD).[19]

Se a privacidade é um direito consagrado na CF/88 (art. 5º, X)[20], no MCI (arts. 3º, II, e 8º, 11, caput e §3º)[21] e na LGPD (arts. 1º, 2º, II e 17),[22] a proteção de dados é incontestavelmente um dos meios para se efetivar o referido direito, assegurando

17 LGPD, art. 2º. "A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

18 A LGPD, em seu art. 5º, X, define tratamento como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

19 Por força do art. 4º da LGPD, não se aplica a lei ao tratamento de dados pessoais: "I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

20 CF/88, art. 5º, X. "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

21 MCI, art. 3º, II. "A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade;"; art. 8º. "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet"; art. 11, caput, §3º. "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros" e "Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações".

22 LGPD, art. 1º. "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"; art. 2º, II. "A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;"; e art. 17. "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei".

ao titular, pessoa natural a quem se referem os dados pessoais que serão objeto de tratamento (art. 5º, V, LGPD), o amplo rol de prerrogativas listadas nos artigos de 18 a 22 do normativo. Dentre essas, destacam-se: ser informado sobre incidentes envolvendo seus dados; receber explicação e esclarecimentos sobre algoritmos e modelos que fazem uso de seus dados; acessar seus dados e obter cópia; solicitar a correção, alteração, anonimização, bloqueio, exclusão e/ou eliminação de dados; confirmar a existência de tratamento; revogar consentimento previamente concedido; e de pleitear portabilidade informacional.

Aos agentes de tratamento de dados, classificados como controladores e operadores,[23] a LGPD determina observar, dentre outras obrigações, as de resguardar os direitos dos titulares de dados; adotar medidas técnicas, administrativas e de gestão para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que impliquem em tratamento inadequado ou ilegal (art. 46); indicar o controlador um encarregado para tratamento de dados (art. 41); obedecer aos princípios da finalidade, adequação, necessidade, livre acesso, preservação da qualidade dos dados, transparência, segurança (*privacy by default e privacy by design*), prevenção e não discriminação, responsabilização e prestação de contas (art. 6º);[24] e comunicar, com a devida urgência, à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares envolvidos a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48).

Além disso, incumbe-lhes tratar dados pessoais somente se presente ao menos uma das hipóteses legais autorizativas, a saber, o consentimento, o cumprimento de obrigação legal, a execução de políticas públicas, estudos por órgãos de pesquisa, execução de contrato, exercício regular de direito, proteção da vida, tutela da saúde, proteção do crédito e legítimo interesse (arts. 7º ao 14); garantir a segurança

23 Conforme art. 5º, incisos IX, VI e VII, o controlador e o operador são considerados agentes de tratamento de dados. O primeiro definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; e o segundo, "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

24 LGPD, art. 6. "I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

da informação (disponibilidade, integridade e confidencialidade) em relação aos dados pessoais (art. 47); elaboração de ROPA, DPIA, PIA e/ou LIA, nas hipóteses em que a lei exigir (artigos 5º, XVII, 10, §3º, 18, 30, 32, 37 e 38).[25]

Tal qual ocorre com os violadores do MCI, aqueles que transgredirem os preceitos da LGPD estarão sujeitos a diversas sanções administrativas que podem ser aplicadas pela ANPD, criada por força do artigo 55-A da LGPD, com autonomia técnica e decisória para, entremeio a outras relevantes atividades (art. 55-J, LGPD), fiscalizar e sancionar condutas, comissivas e omissivas, que atentem contra as normas de proteção de dados instituídas pela lei.

Dentre as sanções administrativas possíveis de serem aplicadas pela ANPD, sem prejuízos de outras punições administrativas, civis e/ou penais previstas em outras legislações (p.ex., MCI), estão: advertência; multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio e/ou eliminação dos dados pessoais; suspensão parcial do funcionamento do banco de dados e/ou do exercício da atividade de tratamento dos dados pessoais a que se refere a infração; e a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52, LGPD). O artigo 42 da LGPD é cristalino ao prever que os agentes de tratamento de dados (controladores e operadores) serão obrigados a reparar eventuais danos patrimoniais, morais, individuais ou coletivos, decorrentes de violação à legislação de proteção de dados pessoais, em razão de seu exercício de atividade de tratamento de dados.

Sob a perspectiva do *compliance* digital, importa salientar que a boa-fé e a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas são parâmetros legais levados em consideração quando da aplicação de sanções pela ANPD, podendo resultar em um abrandamento significativo da penalidade (art. 52, §1º, II, VII a X, LGPD).

Eis aí, estreme de dúvidas, reflexos positivos e benefícios concretos reconhecidos pela legislação diante da implementação de políticas internas, controle, capacitação, treinamento e demais ações, protocolos e procedimentos de natureza preventiva visando à identificação precoce de irregularidades, à conformidade organizacional com os normativos vigentes e à minimização de responsabilidades.

Resta evidente a relação existente entre a LGPD e as atividades desenvolvi-

25 Para mais informações sobre os documentos citados (ROPA, DPIA, PIA e LIA), sugere-se a leitura do texto Risk assessments e relatório de impacto: ferramentas para avaliação de riscos em programas de compliance digital e de proteção de dados, de autoria de Marcelo Xavier de Freitas Crespo (In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp.157-182.

das pelos profissionais de cibersegurança, sobretudo no que se refere à implementação de medidas adequadas para proteção de dados pessoais contra acessos não autorizados, vazamentos e outras ameaças cibernéticas.

A segurança da informação (conjunto de práticas, tecnologias e procedimentos projetados para proteger sistemas de informação contra ataques cibernéticos), a identificação e a gestão de riscos (avaliação de vulnerabilidades, ameaças e impactos potenciais sobre dados pessoais e sistemas de informação), a resposta a incidentes (implementação de planos de resposta e ações para mitigar danos e proteger os direitos e liberdades dos titulares dos dados) e a cultura de segurança (conscientização e educação sobre os riscos de segurança envolvendo todos os colaboradores e fornecedores da empresa) são pautas comuns e cruciais tanto à cibersegurança quanto à proteção e à privacidade de dados.

A desconformidade organizacional quanto às disposições da LGPD representa não apenas um risco financeiro direto, mas também pode ter um impacto duradouro e prejudicial em sua reputação, sobretudo diante da possibilidade de publicização da infração como sanção administrativa (art. 52, IV, LGPD). O custo reputacional da organização pode ser gravemente atingido pela perda de confiança dos clientes diante de eventual violação da privacidade de seus dados pessoais; pelos danos à imagem e à credibilidade da empresa, notadamente em tempos digitais onde as notícias se espalham rapidamente; pelo ajuizamento de ações judiciais reparatórias e indenizatórias diante de prejuízos causados aos titulares; e pelo impacto negativo nos relacionamentos comerciais (fornecedores, parceiros e outras partes interessadas).

A implementação de um efetivo *compliance* digital requer uma abordagem abrangente, não apenas para o atendimento de leis e regulamentos, mas também para estabelecer uma imagem ética e íntegra perante o mercado. Uma reputação positiva é essencial para se destacar no mercado competitivo atual, especialmente em ambientes digitais, onde as informações circulam com velocidade e uma má conduta pode resultar em danos irreparáveis à imagem e à credibilidade da empresa.

Para alcançar uma cultura de integridade, é necessário o comprometimento de toda a organização, desde a alta diretoria até os colaboradores e parceiros comerciais. Isso inclui o estabelecimento de políticas claras, treinamento constante e efetivo, e a criação de canais de comunicação abertos para denúncias, sugestões e *feedback*.

A mudança cultural é essencial e deve ser apoiada por iniciativas como treinamento, conscientização e orientação. Além disso, avaliações de risco regulares são indispensáveis para identificar vulnerabilidades e implementar medidas preventivas e corretivas.

O programa de *compliance*, por sua vez, deve ser visto como um processo contínuo e adaptativo, fundamental para garantir a integridade e o sucesso da empresa no ambiente digital e além dele.

E nesse contexto, a atuação proativa do profissional de cibersegurança se mostra fundamental.

Há muito mais a se dizer acerca de outras regulamentações, algumas em vigor, outras em discussão no Congresso Nacional, que envolvem assuntos tecnológicos de interesse da cibersegurança, como é o caso da Inteligência Artificial e da Internet das Coisas. Contudo, a importância dos temas impõe certo aprofundamento, o qual deixaremos para outra oportunidade.

Referências

1. BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. Proteção de Dados e Privacidade: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.
2. CAMARGO et al (coords.). Direito digital: novas teses jurídicas. vol. 2. 2ª ed. Rio de Janeiro: Lumen Juris, 2019.
3. CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3).
4. MARIN, Jorge. Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda. TECMUNDO, out. 2023. Disponível em: https://www.tecmundo.com.br/seguranca/272995-brasil-lider-ranking-ataques-ddos-america-latina-10-vez-entenda.htm. Acesso em: 15 abr. 2024.
5. MASSO, Fabiano Del; ABRUSIO, Juliano; FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet: Lei 12.965/2014. São Paulo: RT, 2014.
6. MORGAN, Steve. Cybercrime to cost the world $10,5 trillion annually by 2025. Cybercrime Magazine, nov. 13, 2020. Disponível em: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Acesso em: 15 abr. 2024.
7. PIRONTI, Rodrigo. Lei Geral de Proteção de Dados: estudos sobre um novo cenário de governança corporativa. Belo Horizonte: Fórum, 2020.
8. PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ. CiberSegurança: bacharelado. Disponível em: https://www.pucpr.br/cursos-graduacao/ciberseguranca/. Acesso em: 15 abr. 2024.
9. R7 TECNOLOGIA E CIÊNCIA. Brasil é o 2º maior alvo mundial de ciberataques, revela estudo. out. 2021, atualizado em abr. 2024. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022/. Acesso em: 15 abr. 2024.
10. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/book/125. Acesso em: 15 abr. 2024.

FLÚVIO CARDINELLE OLIVEIRA GARCIA é Graduado em Ciências da Computação pela Universidade Católica de Brasília. Graduado em Direito pelo Centro Universitário de Brasília. Pós-graduado em Direito Eletrônico e Tecnologia da Informação pelo Centro Universitário da Grande Dourados. Mestre em Direito Processual Penal pela Pontifícia Universidade Católica de São Paulo. Doutor em Direito Penal Econômico pela Pontifícia Universidade Católica do Paraná. Pós-doutorado pela PUCPR. Delegado de Polícia Federal atualmente lotado na Superintendência da Polícia Federal no Paraná, sediada em Curitiba/PR. Desde 2002 tem atuado e se especializado na investigação de crimes de alta tecnologia praticados pela rede mundial de computadores.

ARTIGO

A IMPORTÂNCIA DOS FATORES HUMANOS PARA A CIBERSEGURANÇA

POR

Cristine Hoepers (CERT.br)

cristine@cert.br

O eixo Fatores Humanos do documento com os referenciais de formação para o curso de Bacharelado em Cibersegurança define que um profissional que vá atuar nessa área deve ter a competência de "*estabelecer um plano de mitigação de ataques de engenharia social e conscientização de usuário visando a proteção de dados pessoais e organizacionais*".

Para realmente entendermos a importância desse eixo e como podemos abordar essa missão de proteger o ser humano (que em nossa profissão chamamos casualmente de "usuário") e seus dados, convido o leitor a embarcar comigo em uma reflexão sobre como nossa evolução nos moldou, como esse conhecimento é essencial para construirmos qualquer plano de conscientização, qual o nosso papel como profissionais de computação, quais os desafios para um futuro com IA ubíqua e como devemos tratar **o ser humano como o elo principal da cadeia**, e não o elo mais fraco.

Do Fogo ao Smartphone

Uma das coisas mais fascinantes na história da humanidade é nossa habilidade de modificar nosso ambiente, principalmente através do domínio da energia e do desenvolvimento de novas tecnologias. Quase todos os saltos civilizatórios estiveram associados a uma quebra de paradigma na forma de produzir e utilizar energia que, por sua vez, leva à possibilidade de novas tecnologias, levando a avanços na produção, utiliza-

ção e armazenamento de energia, o que viabiliza novas tecnologias. Desde que os hominídeos dominaram o fogo, estamos nesse ciclo virtuoso de evolução [1].

Infelizmente, sempre que esses avanços ocorrem, não há como escolher somente os benefícios de uma tecnologia, pois ela também pode ser utilizada para fins negativos. Com a revolução da informação não foi diferente, pois temos um conjunto de tecnologias, baseadas em software, que foram desenvolvidas por seres humanos para o uso por seres humanos, não sendo possível prever os tipos de uso que a tecnologia terá.

Estamos em um momento desta evolução em que boa parte da humanidade anda diariamente com um computador conectado à Internet no bolso. Este computador, que chamamos de smartphone, nos permite facilidades que há menos de 20 anos eram inimagináveis: ter documentos pessoais à mão; ter uma biblioteca inteira num aplicativo; fazer uma chamada de vídeo com a família; ter um mapa com GPS e não se perder, mesmo numa cidade estranha; reservar hotéis e passagens; pagar contas; fazer compras on-line; acessar o banco; entre muitas outras possibilidades, incluindo atividades relacionadas ao trabalho. E todos esses serviços dependem, também, do acesso à Internet e da disponibilidade e confiabilidade dos sistemas em nuvem, que também são extremamente visados por atacantes, pois ali estão concentrados os dados de praticamente todos os cidadãos e empresas.

Ou seja, não é à toa que os atacantes também direcionam seus ataques a conseguir acesso aos serviços de nuvem e aos dispositivos de usuários finais, estes últimos visados inclusive para furto, considerando que são hoje a nossa carteira.

Fomos da Caverna ao Espaço, mas Ainda Somos Praticamente os Mesmos

Embora a tecnologia tenha evoluído exponencialmente nos últimos séculos, a cognição, os instintos e o raciocínio do ser humano ainda são muito similares aos do período Paleolítico. Nós achamos que as pessoas tomam decisões por motivos racionais (lobo frontal), mas a verdade é que na maior parte de nossa evolução, nós dependemos majoritariamente do nosso instinto de fuga e luta (sistema límbico). Com isso, nossas decisões são muito mais emocionais do que racionais. Mesmo sem saber, os atacantes exploram exatamente o fato de que nossas emoções falam mais alto que nossa razão [1, 2].

Em geral, quando uma pessoa "cai" em um golpe nos perguntamos como a pessoa não percebeu, pois era "lógico" que era um golpe, bastava refletir e analisar. E o uso dessas palavras já nos dá uma dica que a pessoa não raciocinou, ou seja, seu cérebro não ativou as áreas mais recentes de raciocínio lógico, mas sim houve ativação direta das áreas de reação emocional do sistema límbico, o que foi cunhado como sequestro límbico (do Inglês "*amigdala hijacking*" [3]).

Os ataques de engenharia social sempre existiram, e exploram exatamente essa característica do nosso cérebro, ao ludibriar a pessoa com o uso de ardis

combinados com uma reação emocional forte. No passado, quase todos os golpistas precisavam também ser bons atores, pois eles precisavam ficar cara a cara com as vítimas para convencê-las a comprar um bilhete premiado da loteria ou uma casa pré-moldada, mas que nunca seriam entregues.

Infelizmente, os sistemas informatizados tornaram mais fácil a vida dos golpistas, pois agora é necessário apenas ter uma história comovente ou amedrontadora, e combiná-la com a tecnologia, seja enviando mensagens, criando sites ou aplicativos falsos.

A Importância do Letramento Digital

Por trabalhar com segurança há mais de 25 anos, com bastante frequência me perguntam "Qual sistema é o mais seguro?". Minha resposta invariavelmente é "o sistema que você conhece, sabe como usar, mantém atualizado e com mecanismos de segurança".

Dito isso, conhecer e saber usar um sistema requer o que hoje se convencionou chamar de letramento digital. Infelizmente, o baixo letramento digital da população brasileira é uma realidade que torna mais difícil o uso seguro da tecnologia. Os dados da TIC Domicílios mostram claramente que, apesar de 84% da população declarar que usa a Internet regularmente, menos da metade possui habilidades básicas como copiar e colar textos ou ativar configurações de segurança e privacidade [4].

Os fatores humanos devem, ou ao menos deveriam, estar sempre em mente nas fases de projeto e desenvolvimento de qualquer tecnologia, pois ela será utilizada por pessoas que não são especialistas e precisaria ser dotada de boa usabilidade e acessibilidade. Porém, a realidade atual está longe de ser ideal, pois infelizmente a maior parte dos sistemas é complexa para a maior parte das pessoas, o que se reflete nesse baixo índice de habilidades por parte dos cidadãos.

O Marco Civil da Internet diz em seu artigo 26 que "*O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico*."[5] Porém, sabemos que o cidadão em geral chega ao mercado de trabalho com conhecimentos muito rudimentares de uso de tecnologia e quase nulos de uso seguro. As organizações, de forma geral, contratam os funcionários assumindo que entendem a tecnologia, mas vemos pela TIC Domicílios que o cenário está bem longe disso.

O Cenário Perfeito para a Engenharia Social

Dicas básicas de segurança que são parte de qualquer material de conscientização, como "acesse somente sites com https", "verifique se o endereço é o do site que você quer acessar" ou "use somente aplicativos oficiais", requerem conhecimentos sobre o sistema operacional e sua interface, o navegador, domínios na Inter-

net, o ecossistema de desenvolvimento de aplicativos, entre outros. Por consequência, vemos no dia a dia, que muitas campanhas de conscientização falham, pois as pessoas não têm os conhecimentos básicos de informática para entender o que está sendo ensinado.

O uso acelerado e ubíquo da tecnologia sem um letramento adequado leva ao cenário atual, em que os atacantes têm uma grande vantagem, pois eles podem criar esquemas elaborados de fraude, que se valem da dificuldade das pessoas de entender as interfaces e as mensagens que lhe são apresentadas. Some-se a isso técnicas como imprimir senso de urgência ou instigar medo, que levam a reações emocionais e não racionais, e temos o cenário perfeito para a engenharia social moderna.

Como ter Efetividade em uma Campanha de Conscientização

Para quem trabalha com segurança é chave entender não só as vulnerabilidades técnicas do mundo em que vivemos, mas também os fatores humanos que estão envolvidos, pois estes são parte do projeto e do desenvolvimento dos sistemas, da compreensão e uso da tecnologia e da motivação dos atacantes. E esses mesmos fatores humanos são os que nos fazem agir sem pensar em momentos de estresse, vulnerabilidade que é explorada em ataques de Engenharia Social.

Soma-se a isso o fato que as campanhas em geral focam em "o que" fazer, e não em "por que" fazer. Esse é um ponto que precisa ser repensado, pois somos movidos não por razão, mas sim por emoção e confiança [2]. Explicar "porque" uma medida é necessária e como pode ajudar a pessoa é tão importante quanto explicar como implementar uma medida. A pessoa precisa ver a necessidade e entender que ela será beneficiada tanto quanto a organização. Se não houver o entendimento do porquê uma medida é importante, ela será burlada no momento em que o usuário sentir que precisa mais agilidade no trabalho e que a medida está "atrasando" sua rotina.

Também **é importante focar no Princípio de Pareto**. Pergunte-se: "Quais são os 20% das medidas que podem reduzir 80% dos riscos?" Se uma pessoa for confrontada com uma lista enorme de medidas que "precisa" implantar e ficar com a sensação de que "ou implementa tudo ou não está protegido" a reação natural é pensar "então nem vale a pena fazer nada". N**ão podemos, como profissionais, anestesiar os usuários, nem educar pelo medo.** Precisamos ter uma postura positiva, constante e confiável, que leve as pessoas a querer nos procurar, apontar problemas e alertar o mais cedo possível de que algo pode estar errado.

Precisamos ter os usuários como nossos aliados, como parceiros que vão identificar quando as ferramentas falharem – e as ferramentas falham mais frequentemente do que gostaríamos de admitir. Precisamos mudar nossa mentalidade e entender que o usuário é o elo mais importante da cadeia, não o mais fraco. Os sistemas são feitos para que ele possa cumprir uma missão, uma tarefa. **As medidas de segurança não podem**

impedir o trabalho, senão serão burladas. E o usuário que entende o porquê segurança é importante e que se sente à vontade para procurar a equipe técnica quando encontra problemas é capaz de detectar incidentes enquanto ainda é possível mitigá-los e evitar os efeitos mais danosos.

Também é necessário ter cuidado com a linguagem, que precisa ser simples, e com o projeto e diagramação do material. Infelizmente, com o ambiente atual de excesso de informação em redes sociais, com mensagens curtas, a maior parte das pessoas não lerá textos grandes nem procurará por mais informações. Temos que fazer o projeto de folhetos, sites e aplicativos pensando que precisamos colocar a informação diagramada de forma a atrair o olhar, com imagens que complementem e chamem a atenção. As pessoas não lerão o material do início ao fim, elas passarão os olhos, e precisamos formatar a mensagem para esse novo leitor [6].

O que nos Aguarda no Futuro?

Algoritmos de inteligência artificial (IA) existem há décadas, mas um dos limitantes do avanço no uso era o fato de que não havia poder computacional para treinar os algoritmos e utilizá-los em tempo hábil para a maior parte das tarefas. Com a evolução da tecnologia esse cenário mudou e vivemos um momento em que os usos estão se tornando crescentes, para o bem e para o mal. É difícil dizer o que vai acontecer, mas dadas as capacidades e usos atuais, já temos alguns problemas à nossa porta.

Os profissionais que atuarão com segurança e conscientização terão pela frente o desafio de **ensinar mais que dicas de segurança,** precisarão **desenvolver o pensamento crítico dos usuários**. Será necessário pensar em como proteger dados sensíveis de vazamentos via ferramentas de IA em nuvem, sejam elas chats, ferramentas de auxílio para programação (os "co-pilots") ou quaisquer outras que surgirem.

O pensamento crítico será chave para diferenciar fatos de *deep fakes*, pois os criminosos poderão usar IA para automatizar várias partes do processo de Engenharia Social, reduzindo a interatividade necessária hoje e aumentando a credibilidade das mensagens. Além disso, tanto vídeo quanto áudio serão mais facilmente manipulados, requerendo perspicácia e pensamento crítico dos usuários para detectar fraudes.

Será necessário educar os usuários para esse cenário e esclarecer que os criminosos usarão os dados que eles mesmos colocam em redes sociais, pessoais ou de trabalho para treinar a IA, que poderá facilmente inferir relações de trabalho e de parentesco, e criar golpes personalizados sem interação dos fraudadores.

E será necessário que os profissionais aprendam a usar a IA a seu favor, seja incrementando ferramentas de detecção ou automatizando tarefas como buscas por vulnerabilidades e análise de segurança código, por exemplo.

Mas, mais que tudo, **é necessário que profissionais de cibersegurança incluam em sua formação a compreensão daquilo**

que nos faz humanos, tanto pontos fortes quanto pontos fracos, e adequem sua mensagem ao público ao invés de esperar que ele tente se adequar aos nossos jargões e nossa forma de lidar com a tecnologia. Recomendo a todos a leitura não só das referências deste artigo, mas também de outros materiais que tragam insights sobre como pensamos e porque agimos de determinadas maneiras. Seremos profissionais melhores se entendermos melhor nossos usuários, os seres humanos.

A tecnologia é feita de humanos para humanos - precisamos sempre nos lembrar disso!

Referências

1. VINCE, G. Transcendence: How Humans Evolved through Fire, Language, Beauty, and Time. New York: Basic Books, 2020. ISBN: 9780465094912.
2. SINEK, S. Start with Why: How Great Leaders Inspire Everyone to Take Action. London: Portfolio/Penguin, 2009. ISBN: 9781101149034.
3. ROWLES, R. Amygdala Hijacking and Social Engineering. Social-Engineer, LLC, 2023. Disponível em: https://www.social-engineer.org/social-engineering/amygdala-hijacking-and-social-engineering/. Acesso em: 23 mar. 2024.
4. CETIC.BR/NIC.BR. TIC Domicílios 2023 – Indivíduos. Disponível em: https://cetic.br/pt/tics/domicilios/2023/individuos/. Acesso em: 23 mar. 2024.
5. LEI Nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 mar. 2024.
6. STIMAC, Stephanie. Design for Developers. New York: Manning, 2023. ISBN: 9781617299476.

CRISTINE HOEPERS é Gerente do CERT.br/NIC.br, é formada em Ciências da Computação pela UFSC e Doutora em Computação Aplicada pelo INPE. É, também instrutora autorizada do Software Engineering Institute, da Carnegie Mellon University, e ministra os cursos do CERT®/CC no Brasil. Em 2020 recebeu do M3AAWG, maior organização mundial de combate a abusos on-line, o prêmio anual Mary Litynski por seu trabalho para aumentar a resiliência da Internet. Atua nas áreas de Gestão de Incidentes, Privacidade, Implantação de CSIRTs, Honeypots e Combate a Fraudes na Internet.

ARTIGO

CIBERSEGURANÇA, SOCIEDADE E FUTURO

POR
Patricia Peck Garrido Pinheiro
patriciapeck@peckadv.com.br

Desde 1990, com a aceleração da digitalização da sociedade, em que bens corpóreos foram sendo substituídos por bens digitais, e o modelo de riqueza passou a estar mais centrado nos dados, houve uma maior necessidade de se investir em cibersegurança. Afinal, assim como as instituições passaram a ter uma maior necessidade de gestão de ativos intangíveis, também aumentou a preocupação com as ameaças e ataques a este patrimônio incorpóreo. Por esta razão, a demanda por soluções de cibersegurança e de equipes especializadas trouxe para pauta prioritária de Conselhos de Empresas o indicador de conformidade em segurança cibernética, que passou a estar mais presente também nos relatórios anuais das companhias (*anual reports*).

Contudo, devido à dinâmica da própria tecnologia e seus impactos sobre cultura e comportamento, se por um lado há um grande mercado em expansão, que carece de mais profissionais qualificados, por outro lado, os criminosos cibernéticos também evoluíram e sofisticaram a técnica, exigindo um ritmo de atualização constante.

Hoje, a Internet tem um alcance muito amplo, se fazendo presente em todas as camadas sociais e setores econômicos. Tendo sido tratada como direito essencial

na legislação do Marco Civil da Internet em 2014, ela se mostrou ainda mais relevante recentemente para o enfrentamento de pandemias. Mas, apesar de toda adesão à transformação digital, ainda há desafios em três níveis a serem tratados pela cibersegurança: 1) no nível técnico; 2) no nível da governança; 3) no nível das pessoas.

Além da necessidade de adoção de ferramentas protetivas, passou a ser um requisito essencial ter regras claras para legitimidade e viabilidade legal da proteção de patrimônio e reputação, que saltou do monitoramento padrão para uso de recursos com maior capacidade de detenção e resposta em qualquer lugar e a qualquer momento.

Ou seja, onde houver maior aplicação de protocolos de segurança, sempre há que se adequar ao uso transparente, com avisos de ciência prévios, respeitando questões relacionadas à privacidade e proteção de dados pessoais. Este equilíbrio tem envolvido equipes multidisciplinares, que também atuam sob o prisma de gestão de riscos e realização de campanhas educativas.

A relação de tempo real com o uso dos recursos e das informações e a ocorrência de incidentes, que podem ocasionar uma grande exposição, passaram a exigir uma cibersegurança mais holística e preventiva, além da necessidade de resposta rápida, neutralização de eventos e reação imediata para contenção de ataques, que podem vir de qualquer lugar, por acesso interno ou externo, ultrapassando barreiras territoriais.

No contexto da economia global digital, a segurança pressupõe estado de alerta permanente e treinamento, que deve alcançar das equipes especializadas até o usuário comum.

A chegada da inteligência artificial novamente provocou um certo desequilíbrio no ambiente de cibersegurança, na medida em que os infratores passaram a usar recursos como *deep fake* para burlar os sistemas de autenticação. Uma das premissas mais importantes no âmbito da segurança cibernética é a validação e checagem de identidades confiáveis. Qualquer vulnerabilidade neste mecanismo coloca em risco toda a proteção.

Portanto, o debate dos padrões mínimos de cibersegurança, que passaram a ser tratados por regulamentações mais recentes, como a Lei de Proteção de Dados Pessoais (LGPD), até exigências específicas e setorizadas, como ocorre no setor Financeiro, de Energia, de Saúde, tudo isso, passou a provocar o nascimento de um ecossistema da cibersegurança, culminando na recente criação da Comissão Nacional de Cibersegurança (CNCiber).

Como evitar situações como ataque de *data poisoning* (envenenamento de dados), que podem provocar grandes estragos? Passamos a conviver com todo tipo de golpe, que vai do uso de vírus ao *ransomware*, chegando até o uso de IAs maliciosas.

Todos esses assuntos são necessários na abordagem educativa da cibersegurança, pois não há como estabelecer uma estrutura forte e abrangente

de segurança cibernética sem entender os dilemas técnicos, sociais e culturais envolvidos. Isto porque precisamos alinhar a necessidade de medidas de segurança robustas para as pessoas e organizações com a salvaguarda dos direitos fundamentais e respeito aos princípios nacionais e internacionais. Além dos custos relacionados, a conformidade desempenha um papel crucial no gerenciamento de segurança, para garantia de controles de segurança apropriados, o que só é possível quando alinhado com a legislação pertinente e regulamentação setorial aplicável.

No contexto da cibersegurança, enquanto matéria que vive em contínua atuação e readequação, alinhada com o processamento massivo de dados, faz-se essencial promover uma cultura de cibersegurança mais responsiva e proativa, em vez de meramente reativa, absorvendo princípios como o *ethics by design*[1] *e o privacy by design*[2].

Outro desafio é responder ao crime cibernético com maior efetividade, conseguindo "desarmar" e "desfazer" as quadrilhas que inclusive compartilham na deep web suas abordagens, ferramentas, metodologias e ainda comercializam os resultados do crime. Novamente, somente trazendo uma ação em rede, com integração de inteligência e contrainteligência, será possível ganhar esta verdadeira guerra contra o crime organizado digital.

Devido à natureza transfronteiriça do ciberespaço, a cibersegurança de fato se tornou uma pauta internacional e multiterritorial. A colaboração entre todos os atores envolvidos passou a ser crucial para garantir maior proteção dos ativos e segurança dos indivíduos.

No Brasil, como já mencionado, neste sentido, avançamos tanto com a Convenção de Budapeste, como com a criação do Comitê Nacional de Cibersegurança (CNCiber), parte da Política Nacional de Cibersegurança (PNCiber), que tem o objetivo de contribuir para a orientação da atividade de cibersegurança no país, envolvendo diretrizes, ações, incremento da matéria de segurança e métodos de governança.

Mas, ainda é preciso melhorar muito a capacidade de identificação de autoria inequívoca no ambiente digital, com compromisso ação coordenada e célere daqueles que são responsáveis pelas por-

1 EUROPEAN COMMISSION. The aim of Ethics by Design is to incorporate ethical principles into the development process allowing that ethical issues are addressed as early as possible and followed up closely during research activities. It explicitly identifies concrete tasks which can be taken and can be applied to any development methodology (e.g. AGILE, V-Method or CRISP-DM). However, the advised approach should be tailored to the type of research being proposed keeping also in mind that ethics risks can be different during the research phase and the deployment or implementation phase. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, 25 November 2021. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Acesso em 10.Abr.2024. Tradução livre: Comissão Europeia. Ética por Design e Ética de Uso Abordagens para Inteligência Artificial. O objetivo do Ethics by Design é incorporar princípios éticos no processo de desenvolvimento, permitindo que as questões éticas sejam abordadas o mais cedo possível e acompanhadas de perto durante as atividades de pesquisa. Identifica explicitamente tarefas concretas que podem ser tomadas e aplicadas a qualquer metodologia de desenvolvimento (por exemplo, AGILE, V-Method ou CRISP-DM). No entanto, a abordagem recomendada deve ser adaptada ao tipo de pesquisa que está sendo proposta, tendo também em mente que os riscos éticos podem ser diferentes durante a fase de pesquisa e a fase de implantação ou implementação.

2 PINHEIRO, Patricia Peck. Privacy by design é um conceito criado pela canadense Ann Cavoukian, que estabelece que é necessário adotar medidas preventivas desde a concepção de cada projeto, para evitar que resultados indesejáveis ocorram. Disponível em: https://www.linkedin.com/pulse/patr%C3%AD-

tas de entrada, seja da Internet ou das aplicações. Isso sim irá permitir pegar literalmente o "bandido com a mão na máquina", além da necessidade de políticas públicas para se evitar reincidência. Além disso, um dos principais pontos que também merecem atenção e aperfeiçoamento está relacionado com a questão "quem vigia o vigia", ou seja, como tomar cuidado com aqueles que têm maior acesso e conhecimento e evitar desvios éticos desta função tão relevante.

Novamente, toda esta realidade demonstra a necessidade de um aprofundamento no ensino da segurança cibernética que prepare cuidadosamente as pessoas, tanto para a ação quanto para a reação, com foco de estudo em pormenores técnicos, instruções práticas, abordagens das escolas de pensamento, dilemas éticos, influência de questões climáticas, riscos e mitigação, para que possamos enfrentar as certezas e incertezas do futuro da sociedade digital e robótica e torná-la mais segura para todos.

cia=-peck-news-patricia-peck-pinheiro-phd1-f?trk-public_post. Acesso em 10.Abr.2024.

Referências:

1. EUROPEAN COMMISSION. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, 25 November 2021. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Acesso em 10.Abr.2024.
2. GOODMAN, Marc. Future Crimes. Ed. HSM. 2014. Pg 19, pg 253.
3. PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva. 7ª. edição. 2021.
4. PINHEIRO, Patricia Peck. Segurança Digital. Ed. GEN. 2020.
5. PINHEIRO, Patricia Peck. Patricia Peck News. Disponível em: https://www.linkedin.com/pulse/patr%C3%ADcia-peck-news-patricia-peck-pinheiro-phd-1f?trk=public_post. Acesso em 10.Abr. 2024.

PATRICIA PECK GARRIDO PINHEIRO é CEO e sócia-fundadora do escritório Peck Advogados. Advogada especialista em Direito Digital, Propriedade Intelectual, Proteção de Dados e Cibersegurança. Graduada e Doutorada pela Universidade de São Paulo, PhD em Direito Internacional com tese defendida sobre Propriedade Intelectual da Inteligência Artificial. Nomeada como Membro Titular para o Comitê Nacional de Cibersegurança (CNCiber). Conselheira titular nomeada para o Conselho Nacional de Proteção de Dados (CNPD). Autora/coautora de 46 livros de Direito Digital. Presidente do Instituto Peck de Cidadania Digital. Programadora desde os 13 anos. Certificada em Privacy e Data Protection EXIN.

Organização: UnB, UFRGS Universidade Federal do Rio Grande do Sul

Realização: SBC Sociedade Brasileira de Computação

Patrocinadores: calriz, aws, CNPq, cgi.br, fapdf, CAPES

Apoio: GigaCandanga, RNP

Agência oficial: Grupo RS

Associe-se à SBC ou renove sua associação!

Faça parte da **maior** Comunidade de Computação da América Latina que trabalha a mais de 45 anos em prol do **desenvolvimento tecnológico e científico da Computação** no Brasil.

Acesse os links abaixo e confira todos os nossos benefícios para associados!

- Desconto em inscrições de eventos realizados anualmente pela SBC
- Acesso à rede sem fio Eduroam
- Acesso às listas de discussão mantidas pela SBC

Confira os Benefícios de Associação à SBC em www.sbc.org.br/beneficios

Associe-se ou Renove sua Associação
www.centraldesistemas.sbc.org.br/mom

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO
SBC@SBC.ORG.BR
FONE: +55 51 3308-6835

facebook.com/sbcbrasil instagram.com/sbcoficial (51) 99252-6018

Sociedade Brasileira
de Computação

sbc.org.br