Capítulo

VV

Bacharelado em CiberSegurança

Altair Olivo Santin, Aldri Luiz dos Santos e Marcos Antonio Simplicio Junior

Resumo

Este documento apresenta o Referencial de Formação na área de Computação para o curso de bacharelado em CiberSegurança (RF-CS-21). Ele foi construído a partir da noção de competência do CC2020 da Association for Computing Machinery (ACM). As 12 competências específicas que o CC2020 relaciona para o Bacharel em CiberSegurança foram sumarizadas em oito eixos de formação. Cada eixo de formação relaciona os conhecimentos que são importantes no desenvolvimento das competências dos egressos do curso. Também é abordado um eixo com competências de fundamentos da Computação. Este Referencial visa auxiliar no desenvolvimento de matrizes curriculares em Instituições de Ensino Superior no Brasil e na escrita do Projeto Pedagógico do Curso.

VV.1. Apresentação

A Sociedade Brasileira de Computação (SBC), por meio de sua Diretoria de Educação e da aprovação da Diretoria e Conselho da SBC designou pela portaria de no. 020 de 23 de julho de 2021, a comissão para elaborar o Referencial de Formação para o Curso de Bacharelado em CiberSegurança (RF-CS-21). A comissão foi composta pelos professores: Altair Olivo Santin, da Escola Politécnica da Pontifícia Universidade Católica do Paraná (PUCPR); Aldri Luiz dos Santos, do Departamento de Ciência da Computação do ICEx - Instituto de Ciências Exatas da Universidade Federal de Minas Gerais (UFMG); e Marcos Antonio Simplicio Junior, do Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo (USP).

O trabalho da comissão teve início em 01 de maio de 2021 e foi orientado pelas seguintes diretrizes:

1. Alinhamento com as Diretrizes Curriculares Nacionais (DCN) da Computação;
2. Alinhamento com os Referenciais de Formação (RFs) para os Cursos de Graduação em Computação da SBC.

Este documento está baseado no relatório do grupo de trabalho CSEC2017 (cybered.hosting.acm.org/wp/) da ACM, que coloca CiberSegurança como uma nova área da computação no Guia de Referência Curricular de CiberSegurança (GRCC). Os outros cinco cursos da Computação são: Engenharia da Computação, Ciência da Computação, Sistemas de Informação, Tecnologia da Informação e Engenharia de Software. Essas áreas já se encontram regulamentadas pela resolução CNE/CES 5/2016 do MEC, resultado da ação de grupos de trabalho da diretoria de educação da SBC na construção dos RFs, cuja última atualização foi em 2017 (www.sbc.org.br/documentos-da-sbc/summary/131-curriculos-de-referencia/1165-referenciais-de-formacao-para-cursos-de-graduacao-em-computacao-outubro-2017). Essas áreas da Computação servem como fundamentação para o novo curso de CiberSegurança. O resultado desse trabalho, iniciado em 2015, encontra-se relatado no documento "***Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity***" do grupo de trabalho CSEC2017, datado de 31 de dezembro de 2017 e

atualizado sob demanda no domínio cybered.acm.org. A metodologia adotada é baseada em competências, segundo a taxonomia de Bloom revisada (Ferraz e Belhot, 2010; Scallon, 2015).

Este documento está organizado em oito seções. Na Seção II.2 é apresentado um breve histórico do curso de CiberSegurança. A Seção II.3 caracteriza os benefícios dos cursos de Bacharelado em CiberSegurança para a sociedade. A Seção II.4 descreve aspectos relacionados à formação profissional de CiberSegurança. A Seção II.5 apresenta o perfil do egresso, indicando as competências dos egressos dos cursos de Computação em geral, e dos egressos dos cursos de CiberSegurança em específico. A Seção II.6 apresenta os eixos de formação, competências e conhecimentos que compõem o RF-CS-21. A Seção II.7 apresenta as atividades complementares à formação do bacharel em CiberSegurança. Por fim, a Seção II.8 encerra o documento com agradecimentos, e é seguida das referências bibliográficas utilizadas.

VV.2. Breve histórico do curso

Ao longo da última década, a comunidade de segurança tem se reunido no Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), evento anual promovido pela Comissão Especial de Segurança da Informação e de Sistemas Computacionais (CESeg) da SBC. As discussões promovidas nesse fórum têm por objetivo consolidar as áreas que exigem CiberSegurança, demonstrando a multidisciplinaridade 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 tem como consequência subtrair recursos humanos da própria área de Tecnologia da Informação (TI). Além da área de TI, por si só, já ser carente de pessoal, essa estratégia não proporciona a formação ampla, consolidada e multidisciplinar necessária para profissionais de CiberSegurança.

Em 2015, a CESeg esteve presente no evento *International Security Education Workshop* no *Georgia Institute of Technology*, organizado pela Intel. Em 2016, também esteve presente no *International Security Education Workshop*, um evento conjunto com o *Colloquium for Information Systems Security Education*, no qual aconteceu a reunião do *ACM Joint Task Force on Cybersecurity Education* (AJTFCE), organizado pela Intel. O AJTFCE foi um movimento internacional conjunto envolvendo as seguintes entidades: *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). O objetivo do AJTFCE foi criar o Guia de Referência Curricular de CiberSegurança (GRCC).

De maneira geral, o GRCC define o conceito de CiberSegurança como 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. É um curso de natureza interdisciplinar, incluindo aspectos da lei, política, fatores humanos, ética e gestão de risco, com o objetivo de considerar contextos adversariais. Esse conceito explicita as diferenças em relação ao conceito de segurança da informação (SI) e CiberSegurança. Essencialmente, a SI 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.

Em fevereiro de 2018, a CESeg entrou em contato com a Diretoria de Educação da SBC para iniciar o processo de criação de um referencial para o curso de Bacharelado em CiberSegurança (BCS).

Em 2019, a CESeg esteve presente em audiência pública na Comissão de Defesa do Consumidor, na Câmara dos Deputados, designada pela SBC para levar o posicionamento da comunidade de pesquisadores da área de CiberSegurança acerca da Lei Geral de Proteção de Dados (LGPD). Na ocasião, também foi apresentada a iniciativa de criação do BCS, e reivindicada uma cadeira no conselho da Agência Nacional de Proteção de Dados (ANPD).

Em 2019, a CESeg participou ativamente do Workshop de Educação em Computação (WEI), durante o qual foi conduzido um painel com a presença dos convidados Prof. Dr. Claudio R. Brito, Jr Past President of IEEE Education Society, e da Profa. Dra. Melany Ciampi, do Intersociety Cooperation Committee da IEEE

Education Society.

Em 2020, a CESeg participou novamente do WEI, apresentando uma visão dos eixos de formação do BCS. No mesmo ano, na reunião plenária da CESeg foi aprovada a criação de uma comissão de educação da CESeg.

Em 2021, a comissão de educação da CESeg iniciou os seus trabalhos. Em uma reunião com a diretoria de educação da SBC, foram requisitados os eixos de formação do BCS e as modificações necessárias para inserir a CiberSegurança nas DCNs da Computação. Os resultados desse trabalho foram apresentados no Curso de Qualidade no Ensino da Computação do CSBC (CQ 2021). No mesmo ano, também foram feitas duas apresentações deste material junto à comunidade da CESeg, no Fórum de Segurança Corporativa (FSC) e no Workshop de Regulação, Avaliação da Conformidade, Certificação e Educação em Cibersegurança (WRAC+).

Em julho de 2021, sob coordenação da diretoria de educação da SBC, a comissão de educação da CESeg deu início à escrita do Referencial de Formação do BCS.

VV.3. Os benefícios do curso para a Sociedade

A educação na área de CiberSegurança tem crescido consideravelmente nas últimas décadas. No entanto, a sua necessidade como uma área autônoma é frequentemente desconsiderada ou negligenciada como um fator crítico de sucesso, ao desenvolver um quadro de profissionais necessários na sociedade para proteger seus ativos. Recentemente, entidades internacionais relevantes na área de CiberSegurança 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).

Há consenso que enfrentar os desafios de ensino em CiberSegurança deve ser uma prioridade para a segurança nacional e todos os setores da sociedade. Portanto, há a necessidade de estruturação da área, tanto na atualidade quanto pensando nas necessidades do futuro.

Em contraposição a essa necessidade, os egressos dos cursos de graduação em Computação, na maioria das vezes, não possuem uma formação específica e consolidada na área de CiberSegurança que lhes permita desempenhar as funções demandadas pelo mercado. Isso vale para iniciativas que abordam o tema de CiberSegurança de forma parcial, como costumeiramente ocorre em certificações oferecidas no mercado, ou de propostas que inserem esse importante tema já no ensino médio. Assim, embora esses cursos ajudem a expandir a força de trabalho de CiberSegurança, o que ainda se observa é que a disponibilidade de vagas em CiberSegurança permanece maior do que o número de profissionais qualificados para preenchê-las, indicando um cenário de demanda reprimida. Segundo o *International Information System Security Certification Consortium* (ISC2), em 2021, há carência de 441 mil profissionais na área de CiberSegurança no Brasil (www.isc2.org/Research/Workforce-Study, pag. 26).

A área de CiberSegurança tem a necessidade de profissionais com formação integral, mais ampla e profunda no tema. Em particular, a formação na área deve contemplar os eixos de dados, software, componentes, conexões, sistemas, pessoas, organizações e sociedade, todos elementos essenciais que compõem o ecossistema computacional moderno.

É, portanto, imprescindível formar profissionais capazes de atuar neste complexo espectro de conhecimentos, assumindo diferentes papéis e fornecendo garantias de segurança do ponto de vista estratégico. Adicionalmente, além de ser uma área básica da computação, CiberSegurança é um curso interdisciplinar que inclui aspectos legais, políticos, fatores humanos, éticos e de gestão de riscos.

VV.4. Aspectos relacionados com a formação de um profissional de CiberSegurança

O bacharel em CiberSegurança deve ter uma formação sólida e ampla, contemplando competências gerais e específicas do RF-CS-21, além de outros aspectos relacionados com a sua formação profissional. Esses aspectos têm como objetivo garantir uma formação que permita ao egresso refletir sobre o mundo, entender e resolver problemas computacionais aplicados em diversas áreas, e agir de forma consciente, ética, empreendedora e inovadora, contribuindo para a evolução e melhoria da sociedade.

Para atingir esses objetivos, durante o curso de CiberSegurança é importante que o estudante adquira conhecimentos, desenvolva ações e desempenhe papéis complementares à sua formação. Para desenvolver esta formação complementares há várias opções, como:

- Atuar com profissionais de diferentes áreas do conhecimento para identificar oportunidades do mercado e atender as necessidades da sociedade, demonstrando capacidade de trabalhar em equipe.
- Praticar a interdisciplinaridade para que possa atuar em diferentes domínios, considerando as diversas especificidades de sistemas computacionais modernos.
- Realizar ações empreendedoras na busca de soluções mais eficazes, incluindo novas tecnologias, produtos e serviços.
- Aprender de forma contínua e autônoma sobre métodos, instrumentos, tecnologias de infraestrutura e domínios de aplicação da computação, além de se adequar rapidamente às mudanças tecnológicas e aos novos ambientes de trabalho.
- Exercitar a inovação em computação, por meio de conhecimentos científicos e tecnológicos que vão além dos necessários para suas aplicações tradicionais.
- Participar de intercâmbios e internacionalização da ciência e tecnologia.
- Envolver-se em pesquisa científica.
- Interagir com empresas em estágio, laboratórios-empresa e empresas júnior.

VV.5. Perfil do egresso

A seguir, são apresentados o Perfil Geral dos Egressos na Área de Computação e o Perfil Específico para o Bacharel em CiberSegurança.

Perfil Geral dos Egressos dos Cursos de Bacharelado e de Licenciatura na Área de Computação

O texto a seguir foi extraído integralmente das DCN16 (MEC, 2016)

"*Os cursos de bacharelado e de licenciatura da área de Computação devem assegurar a formação de profissionais dotados:*

1. *do conhecimento das questões sociais, profissionais, legais, éticas, políticas e humanísticas;*
2. *da compreensão do impacto da computação e suas tecnologias na sociedade no que concerne ao atendimento e à antecipação estratégica das necessidades da sociedade;*
3. *da visão crítica e criativa na identificação e resolução de problemas contribuindo para o desenvolvimento de sua área;*
4. *da capacidade de atuar de forma empreendedora, abrangente e cooperativa no atendimento às demandas sociais da região onde atua, do Brasil e do mundo;*
5. *da capacidade de utilizar racionalmente os recursos disponíveis de forma transdisciplinar;*
6. *da compreensão das necessidades da contínua atualização e aprimoramento de suas competências e habilidades;*
7. *da capacidade de reconhecer a importância do pensamento computacional na vida cotidiana, como também sua aplicação em outros domínios e ser capaz de aplicá-lo em circunstâncias apropriadas; e*
8. *da capacidade de atuar em um mundo globalizado do trabalho.*"

Perfil Específico de Egressos dos Cursos de Bacharelado em CiberSegurança

É importante frisar que as competências do profissional egresso do curso de CiberSegurança deverão ser abrangentes e consistentes de modo a contemplar:

1. Formação baseada nas áreas fundamentais da computação (ex., Ciência da Computação etc.);
2. Conceitos transversais que sejam amplamente aplicáveis ao espectro de especializações da CiberSegurança (ex., CiberSegurança herdada de uma perspectiva adversarial – "pensar como o atacante");
3. Competências e habilidades essenciais de CiberSegurança, tendo como embasamento os eixos de

formação especificados neste documento;
4. As demandas do mercado de trabalho e da sociedade;
5. A conduta ética e responsabilidades profissionais.

VV.6. Eixos de formação, competências e conteúdos

O RF-CS-21 está alinhado com a proposta da *Association for Computing Machinery* (ACM), *IEEE Computer Society* (IEEE-CS), da *Association for Information Systems Special Interest Group on Information Security and Privacy* (AIS SIGSEC), e da *International Federation for Information Processing Technical Committee on Information Security Education* (IFIP WG 11.8).

O RF-CS-21 está estruturado de acordo com a estrutura conceitual apresentada no Capítulo I dos RFs dos cursos de graduação em computação (SBC 2017). Doze competências e habilidades, gerais e específicas, são propostas para os egressos dos Cursos de Bacharelado em CiberSegurança:

i. Gerenciar tecnologias e sistemas computacionais de CiberSegurança, considerando boas práticas de segurança e privacidade.
ii. Incorporar requisitos de CiberSegurança na modelagem e implementação de soluções em vários domínios de aplicação.
iii. Incorporar requisitos de escalabilidade, usabilidade e interoperabilidade na construção de soluções seguras.
iv. Avaliar a experiência do usuário na interação com ferramentas e políticas de segurança, visando a melhoria da usabilidade no atendimento aos requisitos de CiberSegurança.
v. Aplicar técnicas e ferramentas na proteção de dados armazenados, em trânsito ou em processamento.
vi. Incorporar propriedades de segurança da informação e de sistemas de modo confiável durante todo o ciclo de vida do software (criação, implantação, uso e retirada de operação).
vii. Promover a integração segura dos componentes de sistemas, considerando: projeto, aquisição, teste, análises e manutenção destes componentes.
viii. Proteger a conexão física e lógica usada na interação entre componentes de sistemas.
ix. Compreender a segurança de sistemas de maneira abrangente considerando aspectos essenciais como políticas de segurança, controle de acesso, autenticação, monitoramento, testes, documentação e recuperação.
x. Atuar na proteção de dados pessoais, privacidade e conscientização de segurança no contexto organizacional e na vida pessoal.
xi. Atuar no planejamento estratégico, gestão de riscos, governança e políticas das corporações em consonância com a ética, leis, normas e padrões e boas práticas de segurança.
xii. Compreender os impactos de CiberSegurança na sociedade global, considerando ameaças, leis, ética e políticas na proteção de segurança corporativa, segredos de estado e da privacidade dos indivíduos.

Para promover a proficiência na área, os cursos de CiberSegurança requerem conteúdos que incluem conhecimento teórico essencial para desenvolver competências técnicas que apoiam a aplicação deste conhecimento, que para os egressos dos Cursos de Bacharelado em CiberSegurança, foram agrupados em **oito eixos de formação**.

Cada eixo de formação corresponde a uma macro competência e relaciona um grupo de **competências derivadas** (competências e habilidades oriundas), as quais, se desenvolvidas em conjunto, levarão o estudante a atingir a competência do eixo. Em conjunto, os eixos possibilitam ao egresso do Bacharelado em CiberSegurança atuar profissionalmente de maneira interdisciplinar em várias áreas de aplicação da computação. Os eixos de formação traduzem o entendimento de que tal formação deve levar em conta: a capacidade de atuar em todas as fases que envolvem CiberSegurança em soluções diversas, desde a concepção de sistemas computacionais seguros até a efetiva implementação de soluções adequadas; a capacidade de se atualizar, buscar novos conhecimentos, e promover inovações tecnológicas; e, a capacidade de se engajar em estudos avançados visando o desenvolvimento da ciência e da tecnologia. Em resumo, os eixos de formação são os seguintes:

1. Segurança de Dados
2. Segurança de Sistemas
3. Segurança de Conexão
4. Segurança de Software
5. Segurança de Componentes
6. Segurança Organizacional
7. Fatores Humanos em Segurança
8. Segurança e Sociedade

Um eixo de formação tem a seguinte estrutura:

- **Código**: algarismo indo-arábico que identifica o eixo de formação.
- **Título**: rótulo que identifica o eixo de formação.
- **Descrição**: texto sumário que contextualiza a competência associada ao eixo de formação.
- **Competência de eixo**: descrição da competência associada ao eixo de formação.
- **Competências derivadas**: lista de competências, oriundas das 12 competências e habilidades, gerais e específicas, definidas pelas DCN16 (MEC, 2016), necessárias para construir a competência de eixo. Cada competência derivada é constituída dos seguintes subcampos:
  - **Código**: é formado pela junção da letra C (inicial da palavra "competência"), do código do eixo (1 a 8) e de um número indo-arábico que ordena sequencialmente a competência derivada no contexto do eixo de formação.
  - **Classificação**: um dos seis níveis do processo cognitivo da Taxonomia de Bloom Revisada (Ferraz e Belhot, 2010).
  - **Conteúdo**: lista de conhecimentos que devem ser trabalhados para desenvolver a competência derivada.

Uma competência das DCN16 pode estar presente em mais de um eixo, sendo que o conteúdo é específico para cada relacionamento entre eixo de formação e competência das DCN16. Assim, uma competência DCN pode requerer diferentes conhecimentos, dependendo do eixo. Da mesma forma, um conhecimento pode estar presente em mais de um eixo. E, ainda, um conhecimento pode estar presente em mais de uma competência das DCN16 de certo eixo.

Um curso pode usar uma estratégia para implementar sua matriz curricular tal que cada disciplina seja desenhada para desenvolver no estudante uma ou mais competências das DCN16, no contexto de um ou mais eixos de formação. Assim, cada disciplina deverá abordar (integral ou parcialmente) os conhecimentos recomendados para as respectivas competências das DCN16, de acordo com eixos de formação em questão.

A seguir, cada eixo de formação é detalhado em termos de suas competências derivadas e conhecimentos associados.

0. EIXO DE FORMAÇÃO: FUNDAMENTOS DE COMPUTAÇÃO

O eixo de formação em Fundamentos de Computação concentra-se em fornecer embasamento computacional essencial aos profissionais da área de CiberSegurança. Tem como conhecimentos básicos: conceitos de soluções algorítmicas; limites da computação; ambiente de programação; dimensões quantitativas de problemas computacionais; aspectos fundamentais da área de Ciência da Computação; resolução de problemas usando ambientes de programação, tanto no desenvolvimento de sistemas como na gestão de infraestrutura; e realização de trabalho cooperativo.

COMPETÊNCIA: *Aplicar algoritmos, programação e aspectos fundamentais da área de Ciência da Computação.*

Competências derivadas	Classificação	Conteúdos
C.0.1. Identificar problemas que tenham solução algorítmica (CG-I)	**Aplicar**	Algoritmos
		Metodologia Científica
		Lógica Matemática
		Matemática Discreta
C.0.2. Conhecer os limites da computação (CG-II)	**Aplicar**	Complexidade de Algoritmos
		Teoria da Computação
C.0.3. Resolver problemas usando ambientes de programação (CG-III)	**Criar**	Algoritmos
		Técnicas de Programação
		Estrutura de Dados
		Lógica Matemática
C.0.4. Compreender e explicar as dimensões quantitativas de um problema (CG-IV)	**Aplicar**	Complexidade de Algoritmos
		Matemática Discreta
		Probabilidade e Estatística
		Álgebra Linear
C.0.5. Empregar temas e princípios recorrentes, como abstração, complexidade, princípio de localidade de referência (caching), compartilhamento de recursos, segurança, concorrência, evolução de sistemas, entre outros, e reconhecer que esses temas e princípios são fundamentais à área de ciência da computação (CE-X)	**Aplicar**	Complexidade de Algoritmos
		Teoria da Computação
		Inteligência Artificial e Computacional
		Sistemas Distribuídos
		Redes de Computadores
		Processamento Paralelo
		Segurança de Sistemas Computacionais

		Arquitetura e Organização de Computadores
		Banco de Dados
		Sistemas Operacionais
		Sistemas Concorrentes
C.0.6. Resolver problemas usando ambientes de programação no desenvolvimento de sistemas (CG-III)	**Criar**	Algoritmos
		Programação Orientada a Objetos
		Programação Funcional
		Banco de Dados
		Interação Humano-Computador
		Programação Imperativa
		Sistemas Concorrentes
		Processamento Paralelo
		Processamento Distribuído
		Sistemas de Tempo Real
C.0.7. Resolver problemas usando ambientes de programação na gestão de infraestrutura (CG-III)	**Aplicar**	Programação Imperativa
		Programação Orientada a Objetos
		Programação em Linguagem Script
		Programação em Linguagem de Montagem
C.0.8. Ser capaz de realizar trabalho cooperativo e entender os benefícios que este pode produzir (CG-XII)	**Aplicar**	Aplicável a todos os conteúdos, utilizando práticas pedagógicas colaborativas

1. EIXO DE FORMAÇÃO: SEGURANÇA DE DADOS
O eixo de Segurança de Dados concentra-se na proteção de dados armazenados, no seu processamento e em trânsito. Este eixo requer aplicação de modelos matemáticos e algoritmos para sua implementação completa. Tem como conhecimentos essenciais: conceitos básicos de criptografia; autenticação e integridade de dados;

comunicação fim-a-fim; forense digital; e segurança de armazenamento da informação.

COMPETÊNCIA: *Aplicar técnicas de criptografia para garantir as propriedades de segurança e proteção de dados armazenados ou em processamento.*

Competências derivadas	Classificação	Conteúdos
C.1.1. Empregar conceitos e técnicas de criptografia	**Aplicar**	Fundamentos de Segurança e Criptografia
		Técnicas Avançadas de Criptografia
		Princípios Matemáticos de Criptografia
		Algoritmos de Cifração Simétricos (Chave Secreta)
		Algoritmos de Cifração Assimétricos (Chave Pública)
C.1.2. Usar técnicas de integridade, autenticidade e irretratabilidade de dados	**Aplicar**	Mecanismos Criptográficos de Integridade
		Mecanismos Criptográficos de Autenticidade
		Assinaturas Digitais
		Certificação Digital
C.1.3. Distinguir as técnicas de criptoanálise	**Conhecer**	Ataques Clássicos por Criptoanálise
		Ataques por Canais Laterais
		Ataques contra Algoritmos de Chave Secreta
		Ataques contra Algoritmos de Chave Pública
C.1.4. Desenvolver técnicas de autenticação	**Aplicar**	Métodos de Criptográficos de Autenticação
		Técnicas de Ataque a Autenticação
		Armazenamento

		Criptográfico de Dados
C.1.5. Operar criptossistemas e protocolos de comunicação segura	**Aplicar**	Gestão de Chaves
		Protocolos de Segurança nas Camadas de Transporte e Aplicação
		Protocolos de Segurança na Camada de Rede
		Protocolos da Camada de Enlace
C.1.6. Usar **técnicas** de proteção de dados armazenados	**Aplicar**	Criptografia de Disco
		Exclusão Segura de Dados
		Mascaramento Seguro de Dados
		Criptografia de Banco de Dados
C.1.7. Empregar técnicas de proteção de dados em processamento	**Aplicar**	Técnicas de Processamento de Dados Cifrados
		Mecanismos de Processamento Seguro usando Hardware

270

2. EIXO DE FORMAÇÃO: SEGURANÇA DE SISTEMAS

O eixo de Segurança de Sistemas trata dos aspectos dos sistemas compostos por componentes e conexões, e os softwares em uso. A segurança de sistemas deve ser entendida como a integração completa de subsistemas, componentes e conexões de maneira holística. Tem como conhecimentos essenciais política de segurança; autenticação; controle de acesso; monitoração; recuperação; forense digital; teste e documentação.

COMPETÊNCIA*:* *Conceber a solução de segurança considerando todos os componentes do sistema de modo integrado.*

Competências derivadas	Classificação	Conteúdos
C.2.1. Planejar o Sistema de segurança	**Criar**	Fundamentos de Engenharia de Sistemas de Segurança
		Modelos de Ameaças
		Análise de Requisitos de Segurança

		Boas Práticas de Engenharia de Sistemas de Segurança
C.2.2. Empregar autenticação em sistemas computacional	**Aplicar**	Gestão de Identidades e Acesso (IAM)
		Métodos de Autenticação
		Arcabouços de Autenticação
C.2.3. Desenvolver os modelos de controle de acesso e autorização	**Aplicar**	Controle de Acesso Físico
		Modelos de Controle de Acesso e Autorização
		Segurança de Confiança Zero
C.2.4. Construir defesa contra intrusões	**Aplicar**	Segurança Ofensiva e Defensiva
		Detecção de Intrusão
		Auditoria de Segurança
		Software Malicioso
C.2.5. Praticar a forense digital	**Aplicar**	Processo de Investigação
		Aquisição e Preservação da Evidência
		Análise da Evidência
		Resultados da Análise Forense
		Estados de Casos de Segurança de Sistemas
C.2.6. Usar técnicas de resiliência	**Aplicar**	Mecanismos de Disponibilidade de Segurança de Sistemas
		Mecanismos de Confiabilidade de Segurança de Sistemas

		Mecanismos de Manutenibilidade de Segurança de Sistemas
C.2.7. Operacionalizar a descontinuidade (descomissionamento) do sistema	**Aplicar**	Mecanismos de Desativação do Sistema de Segurança
		Mecanismos de Destruição Segura e Descarte de Dados
C.2.8. Preparar teste do sistema	**Aplicar**	Validação de Requisitos do Sistema de Segurança
		Validação da Composição dos Componentes da Segurança do Sistema
		Teste Unitário e da Segurança do Sistema
C.2.9. Definir o papel da segurança em arquiteturas comuns de sistemas	**Compreender**	Computação em Nuvem
		Sistemas de Controle Industrial
		Internet das Coisas
		Sistemas Embutidos (embarcado)
		Sistemas Móveis
		Sistemas Baseados em Tecnologia Imersivas
		Sistemas Autônomos
		Sistemas Colaborativo Descentralizado
		Sistemas de Propósito Geral
C.2.10. Operar mecanismos relacionados à privacidade	**Aplicar**	Abordagens de Proteção de Privacidade e suas Limitações (ex., Anonimização e Pseudônimos)

		Tecnologia de Privacidade (ex., Tor e Cifração de Dados)
		Métricas de Avaliação de Privacidade em Conjuntos de Dados
		Violações de Privacidade

3. EIXO DE FORMAÇÃO: SEGURANÇA DE CONEXÃO

O eixo de Segurança de Conexão concentra-se em aspectos de rede e comunicação das ligações lógicas e físicas entre os componentes. Questões de segurança na interligação de componentes dentro de sistemas maiores podem ser abordadas por meio de exemplos, abstraindo-se a essência e introduzindo o vocabulário adequado. Tem como conhecimentos essenciais sistemas, arquiteturas, modelos e padrões; interfaces de componentes físicos, interfaces de componentes de software; ataques as conexões e meios de transmissão.

COMPETÊNCIA: *Aplicar os mecanismos de segurança nos vários níveis de abstrações da comunicação.*

Competências derivadas	Classificação	Conteúdos
C.3.1. Empregar ferramentas e técnicas de segurança nas interfaces de conexão físicas e de acesso ao meio	**Aplicar**	Segurança para Acesso ao Meio Físico nas Redes Sem-fio (ex., wiretapping, black/worm/gray hole, jamming, frequency-hopping)
		Segurança na Camada de Enlace
C.3.2. Organizar a segurança nas camadas de redes	**Aplicar**	Hardening de Rede
		Sistema de Detecção/Prevenção de Intrusão
		Firewall e Redes Virtuais Privadas
		Honeypots and Honeynets
		Monitoramento e Análise de Tráfego de Redes
		Controle de Acesso à Rede (NAC)
		Perímetro de Rede

		Desenvolvimento e Imposição de Políticas de Segurança
		Segurança no Procedimento Operacional de Redes
		Protocolos de Segurança em Redes (ex., IPSec)
C.3.3. Empregar técnicas de segurança em aplicações e middleware	**Aplicar**	Defesa em Profundidade
		Minimização da Superfície e Vetores de Exposição
		Protocolos de Middleware (interface), Transporte, Aplicação
		Técnicas Inteligentes de Detecção de Ameaças

4. EIXO DE FORMAÇÃO: SEGURANÇA DE SOFTWARE

O eixo de Segurança de Software aborda o desenvolvimento e uso de software que preserva confiavelmente as propriedades de segurança da informação e sistemas que a protege. A segurança do software depende da aderência dos requisitos às necessidades do software e da qualidade do desenvolvimento, implementação, testes, manutenção e documentação. Tem como conhecimentos essenciais os princípios fundamentais de projeto incluindo o privilégio mínimo, especificação aberta, separação de responsabilidade, validação de entradas; requisitos de segurança e seus papéis no projeto; aspectos de implementação; análise estática e dinâmica de código em testes de software; gerenciamento de configuração e correção de software; ética, especialmente no desenvolvimento, testes e divulgação de vulnerabilidade.

COMPETÊNCIA: *Empregar técnicas seguras no ciclo de desenvolvimento de software.*

Competências derivadas	Classificação	Conteúdos
C.4.1. Usar técnicas e princípios fundamentais de software seguro	**Aplicar**	Princípio do Mínimo Privilégio
		Princípio de Falhas-Seguras (fail-safe) por Padrão
		Princípio da Mediação Completa (evitando contorno de controle)
		Princípio de Separação de Deveres
		Princípios da Confiança

		Mínima e Confiança Zero
		Princípio da Simplicidade do Software
		Vantagens e Desvantagens de Segurança em Projeto Aberto
		Desenvolvimento em Camadas, Modular e Componentizado
		Segurança por Projeto
C.4.2. Praticar princípios fundamentais de projeto de segurança de software	**Aplicar**	Levantamento e Especificação de Requisitos de Segurança
		Integração de Segurança no Ciclo de Desenvolvimento de Software
		Linguagem de Programação Projetadas para Segurança
C.4.3. Empregar boas práticas de desenvolvimento seguro	**Aplicar**	Validação de Entradas e Verificação do que Representam
		Uso Correto de APIs
		Uso Correto de Mecanismos de Segurança
		Garantia de Estados Consistentes dos Softwares
		Manipulação Correta de Erros e Exceções
		Programação Defensiva
		Encasulamento Adequado de Estruturas e Módulos
		Considerar os Riscos Externos ao Software em Tempo de Execução
C.4.4. Desenvolver análise e testes de segurança	**Aplicar**	Análise Estática e Dinâmica da Segurança do Código

		Teste Unitário de Segurança
		Teste de Integração de Segurança
		Teste de Segurança de Software
C.4.5. Empregar conceitos de segurança na implantação, manutenção e documentação de software	**Aplicar**	Configuração de Segurança
		Atualização e Ciclo de Vida de Vulnerabilidades
		Análise de Compatibilidade do Ambiente e Requisitos de Segurança do Software
		Impactos de Segurança na Descontinuidade (descomissionamento) de software
		DevSecOps
		Documentação de Segurança

273

5. EIXO DE FORMAÇÃO: SEGURANÇA DE COMPONENTES		
O eixo de Segurança de Componentes aborda o projeto, aquisição, teste, análise e manutenção de componentes integrados em um sistema maior. Preocupa-se com a interdependência de segurança dos componentes, no seu projeto, fabricação, aquisição, teste e análise. Tem como conhecimentos essenciais identificação e tratamento de vulnerabilidades; questões de ciclo de vida; princípios de projeto seguro; segurança na gestão da cadeia de suprimento e engenharia reversa. **COMPETÊNCIA:** *Distinguir os aspectos essenciais de segurança no contexto de hardware e software, seus benefícios e limitações.*		
Competências derivadas	**Classificação**	**Conteúdos**
C.5.1. Interpretar aspectos de segurança de componentes no contexto de hardware	**Compreender**	Componentes de Hardware para Segurança (ex., PUF, SmartCard, HSM, TPM, token)
		Ambientes de Execução Confiável (TEE)
		Ataques a Componentes de Hardware para Segurança

C.5.2. Distinguir aspectos de segurança de componentes no contexto de software	**Compreender**	Aplicar Técnicas de Ofuscação
		Gestão de Segredos
		Riscos da Cadeia de Suprimentos
		Engenharia Reversa de Projeto
		Engenharia Reversa de Software

274

6. EIXO DE FORMAÇÃO: SEGURANÇA ORGANIZACIONAL

O eixo de Segurança Organizacional envolve a proteção da organização contra ameaças e gestão de risco para apoiar os objetivos da organização. O profissional de segurança deve compreender a governança em uso e sua conformidade com os propósitos do negócio. Tem como conhecimentos essenciais: gestão de risco; governança e políticas de segurança; leis, ética e conformidade; e estratégia e planejamento de CiberSegurança.

COMPETÊNCIA: *Elaborar estratégias de governança de acordo com regulamentações, boas práticas e o propósito do negócio.*

Competências derivadas	Classificação	Conteúdos
C.6.1. Desenvolver estratégias de gestão de riscos de segurança em sistemas computacionais	**Aplicar**	Identificação de Riscos de Segurança
		Avaliação e Análise de Riscos
		Ameaças internas
		Medição de Riscos, Modelos e Métodos de Avaliação
		Controle de Riscos
C.6.2. Organizar governança e políticas de segurança em sistemas computacionais	**Aplicar**	Governança de Segurança
		Políticas de Segurança
		Implicações do Contexto Organizacional em CiberSegurança
		Governança de Privacidade

		Leis, Ética e Conformidade de Segurança
C.6.3. Empregar ferramentas de gestão analítica de dados de segurança	**Aplicar**	Métricas Analíticas de Segurança
		Inteligência de Segurança
C.6.4. Organizar o planejamento de ciberSegurança	**Criar**	Planejamento Estratégico de CiberSegurança
		Gestão Operacional e Tática do Plano de CiberSegurança
C.6.5. Propor estratégias de gestão de incidentes	**Criar**	Criação e Aplicação de Plano de Resposta a Incidentes
		Criação e Aplicação do Plano de Recuperação de Desastres
		Criação e Aplicação de Plano de Continuidade do Negócio
C.6.6. Desenvolver programas de gestão de ciberSegurança	**Aplicar**	Aplicação de Técnicas e Ferramentas de Gestão de Recursos de Segurança (e.g. inventário de segurança)
		Aplicação de Métricas de Segurança na Tomada de Decisão, Planejamento e Análise de Sistemas

275

7. EIXO DE FORMAÇÃO: FATORES HUMANOS EM SEGURANÇA

O eixo de Fatores Humanos em Segurança contempla proteção de dados no contexto da vida pessoal e sua interação com as organizações. Os indivíduos têm responsabilidade sobre a confidencialidade, integridade, autenticidade, irretratabilidade e disponibilidade de seus sistemas computacionais pessoais e organizacionais, quando pertinente ao contexto. Tem como conhecimentos essenciais gestão de identidade; engenharia social; compreensão e conscientização; postura social guiada a privacidade e segurança; e segurança e privacidade de dados pessoais.

COMPETÊNCIA: *Estabelecer um plano de mitigação de ataques de engenharia social e conscientização de usuário visando a proteção de dados pessoais e organizacionais.*

Competências derivadas	Classificação	Conteúdos
C.7.1. Desenvolver estratégias de ataque e mitigação de engenharia social	**Aplicar**	Tipos de Engenharia Social
		Ataques de Engenharia Social e Comportamento do Usuário
		Detecção e Mitigação de Ataques de Engenharia Social
C.7.2. Construir abordagens de conhecimento e conscientização de segurança	**Aplicar**	Percepção de Risco de Segurança
		Educação do Usuário para CiberSegurança
		Conscientização sobre Vulnerabilidade e Ameaças de CiberSegurança
		Cuidados Individuais com CiberSegurança
C.7.3. Elaborar abordagens de usabilidade de segurança e privacidade	**Criar**	Usabilidade e Experiência do Usuário
		Fatores Humanos de Segurança
		Políticas de Conhecimento e Conscientização de Segurança

276

8. EIXO DE FORMAÇÃO: SEGURANÇA E SOCIEDADE

O eixo de Segurança e Sociedade aborda cibercrimes, privacidade e aspectos legais, éticos e políticos. Também, discute as relações estabelecidas entre estes aspectos, como eles impactam a sociedade como um todo, e sua relevância para a segurança de ativos e segredos em ambientes governamentais e corporativos. Tem como conhecimentos essenciais crimes, leis, ética, política e privacidade no ciberespaço.

COMPETÊNCIA: *Distinguir os aspectos essenciais de segurança e privacidade na conjuntura global.*

Competências derivadas	Classificação	Conteúdos
C.8.1. Descrever o universo dos cibercrimes	**Compreender**	Comportamentos de

		Cibercriminosos
		Terrorismo no Ciberespaço
		Investigação de Cibercriminosos
		Economia do Cibercrime
C.8.2. Entender o universo de leis anti-cibercrimes	**Compreender**	LGPD e GDPR
		Fundamentos Constitucionais das Leis no Ciberespaço
		Propriedade Intelectual de CiberSegurança
		Convenções e Acordos multinacionais para Cibercrime (ex., *Budapest Convention on cybercrime and the G-7 Cybersecurity Accord on financial institutions*)
C.8.3. Relacionar a ética e a ciberSegurança	**Compreender**	Ética Profissional e Código de Conduta
		Ética e Leis
		Éticas e Conflitos
		Ética na Tecnologia
		Hacking Ético
C.8.4. Definir políticas de ciberSegurança	**Compreender**	Ciberguerras
		Políticas Públicas Nacionais e Internacionais para CiberSegurança
		Implicações Econômicas da CiberSegurança
C.8.5. Descrever aspectos gerais de privacidade	**Compreender**	Fundamentos de Privacidade, Uso Apropriado e Compartilhamento

		Impactos das Políticas de Privacidade do Estado nas Empresas Internacionais
		Privacidade e Sociedade
		Privacidade *vs.* Usabilidade e Auditabilidade de Sistemas

VV.7. Atividades complementares

De acordo com as DCN16 (MEC, 2016), as Atividades Complementares são componentes curriculares que devem incorporar-se ao perfil do egresso. Elas deverão possibilitar o desenvolvimento de habilidades interpessoais (*soft skills*), conhecimentos, competências e o saber ser do estudante, inclusive as adquiridas fora do ambiente acadêmico, que serão reconhecidas mediante processo de validação internos.

As Atividades Complementares podem incluir atividades desenvolvidas na própria Instituição ou em outras instituições, em variados ambientes sociais, técnico-científicos ou profissionais de formação profissional, incluindo:

- Experiências de trabalho;
- Estágios não obrigatórios;
- Extensão universitária
- Iniciação científica;
- Participação em eventos técnico-científicos;
- Publicações científicas;
- Programas de monitoria e tutoria;
- Disciplinas de outras áreas;
- Representação discente em comissões e comitês;
- Participação em empresas juniores e startups;
- Incubadoras de empresas;
- Atividades de empreendedorismo e inovação.

VV.8. Agradecimentos

Agradecemos o apoio da CESeg, diretoria de educação e diretoria da SBC e de nossas IES de filiação PUCPR, UFMG e USP por nos apoiar nesta atividade e fazer com que este documento e iniciativa se tornassem uma realidade.

Referências

[Scallon, 2015] Scallon, Gerard. Avaliação da Aprendizagem numa abordagem por competências, Tradução Juliana Vermelho Martins - Curitiba: PUCPRess, 2015. ISBN: 978-8568324059

[Ferraz, 2010] FERRAZ, Ana Paula do Carmo Marcheti and BELHOT, Renato Vairo. Taxonomia de Bloom: revisão teórica e apresentação das adequações do instrumento para definição de objetivos instrucionais. Gest. Prod. [online]. 2010, vol.17, n.2, pp.421-431. ISSN 0104-530X. doi: 10.1590/S0104-530X2010000200015. Acesso em: 24 maio de 2022.

[MEC, 2016] Diretrizes Curriculares Nacionais para os Cursos de Graduação em Computação (DCN16). Disponível em: http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=52101-rces005-16-pdf&category_slug=novembro-2016-pdf&Itemid=30192. Resolução CNE/CES nº 5, de 16 de novembro de 2016. Acesso em: 24 maio de 2022.

[SBC 2017] Zorzo, A. F.; Nunes, D.; Matos, E.; Steinmacher, I.; Leite, J.; Araujo, R. M.; Correia, R.; Martins, S. “Referenciais de Formação para os Cursos de Graduação em Computação”. Sociedade Brasileira de Computação (SBC). 153p, 2017. ISBN 978-85-7669-424-3